Introduction to Number Theory Lecture Notes

Adam Boocher (2014-5), edited by Andrew Ranicki (2015-6)

December 4, 2015

1 Introduction (21.9.2015)

These notes will cover all material presented during class. These lectures have been compiled from a variety of sources, mainly from the recommended books:

- Elementary Number Theory, by Kenneth H. Rosen, 6th Edition, 2011, Pearson. Library: QA241Ros
- A friendly introduction to number theory by J. H. Silverman, Prentice Hall, 2013.Library: QA241Sil

These books are both excellent sources of examples, additional practice problems and I find them to be eminently readable. They are on reserve in the Murray Library.

1.1 A Preview: Pythagorean Triples

(Pink type = either internal or external webreference).
The classical theorem of Pythagoras[1] states that if a, b, c are the side lengths of a right triangle, (c being the hypotenuse) then

$$a^2 + b^2 \ = \ c^2 .$$

In this lecture we shall answer the following

Question 1.1. *What are the natural number solutions (a, b, c) to the equation $a^2 + b^2 \ = \ c^2$? Such a solution is called a Pythagorean triple.*

Example 1.2. *Some easy-to-remember Pythagorean triples are e.g.* $(3, 4, 5), (5, 12, 13), (8, 15, 17)$.

A first question we might ask if there are infinitely many such triples. However, we see that as soon as we have a single solution, we have found infinitely many:

[1] Extract from the Danny Kaye film Merry Andrew (1958)

Remark 1.3. *If (a, b, c) is a Pythagorean triple, and d is any positive integer then so is (da, db, dc).*

Proof. We just check that

$$(da)^2 + (db)^2 \;=\; d^2(a^2 + b^2) \;=\; d^2(c^2) \;=\; (dc)^2.$$

□

Given this fact, we define a **primitive Pythagorean triple (PPT)** to be a Pythagorean triple such that a, b, c have no common factor. This means that there is no number d that divides all of a, b, c. We can now rephrase Question 1.1 as: What is the set of PPTs?

As a first step, let's consider the possible parities of the numbers (the parity of a number refers to whether the number is even or odd). It's straightforward to check that the square of an even number is even, and the square of an odd number is odd. With that in mind, the only possible solutions to $a^2 + b^2 \;=\; c^2$ must be of the form

$$\begin{aligned} \text{odd} + \text{odd} &\;=\; \text{even} \\ \text{odd} + \text{even} &\;=\; \text{odd} \\ \text{even} + \text{even} &\;=\; \text{even} \end{aligned}$$

We can rule out the last possibility since that would imply that a, b, c are divisible by 2. We can also rule out the first possibility: Suppose that

$$a \;=\; 2x + 1, \quad b \;=\; 2y + 1, \quad c \;=\; 2z.$$

Then after simplifying we see that

$$4x^2 + 4x + 4y^2 + 4y + 2 \;=\; 4z^2.$$

But this is impossible, since the right hand side is divisible by 4 but the left hand side is not!

Hence we can reformulate Question 1.1 as

Question 1.4. *Find all natural number solutions to $a^2 + b^2 \;=\; c^2$ with a odd, b even, and a, b, c have no common factors.*

Remark 1.5. *Notice that requiring that a, b, c have no common factor is the same as requiring that no two of them share a common factor. Indeed, if p was a common prime factor, then if p divides, say c and b, then it divides $c^2 - b^2$ and hence it divides a^2. But now by prime factorisation, this means it divides a.*

Let's get to work! We can note that

$$a^2 \;=\; c^2 - b^2 \;=\; (c - b)(c + b)$$

In other words, the product of $(c - b)$ and $(c + b)$ is a perfect square. We shall now show that $c - b$ and $c + b$ are relatively prime. Indeed, suppose that they both shared a common prime factor d, then certainly d should divide their sum and difference. Thus d divides

$$(c - b) + (c + b) \;=\; 2c, \quad \text{and} \quad (c + b) - (c - b) \;=\; 2b.$$

But now b and c have no common factor, so it must be that d divides 2. But d cannot be 2 since $c+b$ is odd! But now as $c-b, c+b$ have no factors in common (i.e. they are **relatively prime**) we see that the only way that their product can be a square is if both factors are squares: the proof relies on unique factorization of integers [2]. Here is the proof: for distinct odd primes $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_\ell$ and positive integers $e_1, e_2, \ldots, e_k, f_1, f_2, \ldots, f_\ell \geqslant 1$

$$c-b \;=\; p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \;,\; c+b \;=\; q_1^{f_1} q_2^{f_2} \ldots q_\ell^{f_\ell}$$

we have that

$$a^2 \;=\; (c-b)(c+b) \;=\; p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} q_1^{f_1} q_2^{f_2} \ldots q_\ell^{f_\ell}$$

so that each of $e_1, e_2, \ldots, e_k, f_1, f_2, \ldots, f_\ell$ is even, and $c-b$, $c+b$ are both squares. Thus

$$c+b \;=\; s^2 \;,\; c-b \;=\; t^2,$$

where $s > t \geqslant 1$ are odd integers with no common factors. Then

$$a \;=\; \sqrt{(c-b)(c+b)} \;=\; \sqrt{s^2 t^2} \;=\; st \;.$$

We can now solve for b and c to obtain our first

Theorem 1.6. *Every PPT (a,b,c) with a odd satisfies*

$$a \;=\; st \;,\; b \;=\; \frac{s^2-t^2}{2} \;,\; c \;=\; \frac{s^2+t^2}{2},$$

where $s > t \geqslant 1$ are chosen to be odd integers with no common factors.

You should notice that we have only completed "half" of this proof. To complete it, we should show that for every such choice of s, t we actually obtain a PPT, which is immediate from the algebraic identity

$$xy \;=\; (\frac{x+y}{2})^2 - (\frac{x-y}{2})^2$$

with $x = s^2$, $y = t^2$.

This theorem is quite striking at first glance, but it still leaves a bit to be desired as to "why" PPTs should have such a special form. Also, we seemed to have gotten lucky with our even/odd analysis in the proof. Indeed, for many problems in number theory, things won't work out this nicely! However, there is a nice method which extends a bit more generally, which we present here.

1.2 A Geometric Derivation

Notice that if (a,b,c) is a PPT then $(a/c, b/c)$ is a point with rational coordinates on the unit circle $x^2+y^2 \;=\; 1$. As students in the North, we naturally notice that $N \;=\; (0,1)$ is a point on the circle. Never matter that one of the coordinates is zero, we can worry about that later. The key insight is to now notice that if (x,y) is another point on the circle with

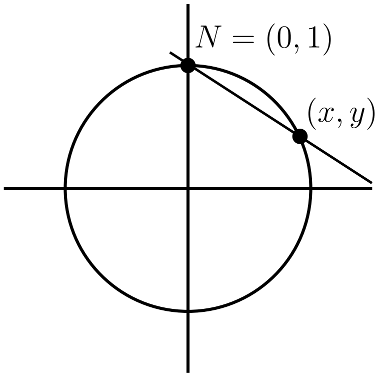

Figure 1: Geometric Method of Finding Pythagorean Triples

rational coordinates then the slope of the line between these two points will have rational slope. The converse is also true, which we prove now:

Suppose that $P = (x, y)$ is a point on the unit circle such that the line between N and P has a rational slope m. Then $m = (y-1)/x$ or equivalently $y = mx + 1$. Since P lies on the unit circle, we can conclude that

$$x^2 + (mx+1)^2 = 1$$

$$(1+m^2)x^2 + 2mx + 1 = 1$$

$$x((1+m^2)x + 2m) = 0$$

This equation describes the set of points that lie on the intersection of the circle and the line. The solution $x = 0$ is the point N, and the solution $x = (-2m)/(1+m^2)$ describes the point P. Using $y = mx + 1$ we have proven

Theorem 1.7. *Every point on the circle $x^2 + y^2 = 1$ with rational coordinates is of the form*

$$(x,y) = \left(\frac{-2m}{1+m^2}, \frac{1-m^2}{1+m^2}\right)$$

where m is a rational number. (Except for the point $(0,-1)$ which is the limiting value as $m \to \infty$.)

If we write $m = u/v$ and clear denominators, then we see that this formula becomes:

$$(x,y) = \left(\frac{-2uv}{u^2+v^2}, \frac{v^2-u^2}{v^2+u^2}\right)$$

which if we plug into the equation for the unit circle and simplify we get

$$x^2 + y^2 = 1$$

[2] to be covered in the next lecture

$$
\begin{aligned}
(-2uv)^2 + (v^2 - u^2)^2 &= (v^2 + u^2)^2 \\
(uv)^2 + \left(\frac{v^2 - u^2}{2}\right)^2 &= \left(\frac{v^2 + u^2}{2}\right)^2 .
\end{aligned}
$$

Comparing with 1.6 we see that we've found exactly the same points! You may have seen these formulae in trigonometry: for any angle θ

$$(\sin 2\theta, \cos 2\theta) = (\frac{2\tan\theta}{1+\tan^2\theta}, \frac{1-\tan^2\theta}{1+\tan^2\theta})$$

with $m = -\tan\theta = \tan(\pi - \theta)$ here.

There are lots of other questions we might want to answer. For example, if c is given, do there exist a and b so that $a^2 + b^2 = c$? If so, how many such a and b are there? For example

$$33^2 + 56^2 = 65^2 \text{ and } 16^2 + 63^2 = 65^2.$$

It turns out that the a highbrow way to view this question (and others) involves passing to the so-called ring of Gaussian integers - which involves imaginary numbers. We shall return to this topic at the end of the course once we have a larger toolkit.

Main Points from Lecture 1:

- Know how to find infinitely many PPTs
- Be able to use the geometric method of using lines with rational slope to find rational points. Memory of this method is important. Memory of the actual formulas is not.
- Have familiarity with basic divisibility arguments.

2 The Primes (24.9.2015)

Notation: $\mathbb{Z}$ = ring of integers $\{0, \pm1, \pm2, \dots\}$;
$\mathbb{N}$ = set of positive integers $\{1, 2, 3, \dots\}$;
$\mathbb{Q}$ = field of rational numbers $\{n/m : m \in \mathbb{N}, n \in \mathbb{Z}\}$;
$\mathbb{R}$ = field of real numbers.

2.1 Prime Numbers

A positive integer $p > 1$ is called **prime** if $p \neq mn$ for all $m, n \in \mathbb{N}$ with $m > 1$ and $n > 1$. Otherwise (i.e., if $c > 1$ can be written as $c = mn$ for some $m, n \in \mathbb{N}$ with $m > 1$ and $n > 1$) then c is called **composite**.

Theorem 2.1 (Fundamental Theorem of Arithmetic)**.** *Every $n \in \mathbb{N}$ has a unique representation as a product of primes:*

$$n = p_1^{e_1} \cdots p_k^{e_k}, \qquad \textit{where } k \geqslant 0 \textit{ and each } e_j \in \mathbb{N}.$$

[Convention: empty products (here, for $n = 1$, are $= 1$, and empty sums are $= 0$.]

This theorem was proved in Year 1 (in Proofs and Problem-solving). See Martin Liebeck: A concise introduction to Pure Mathematics, Chapman and Hall 2000. A visualisation of this theorem can be seen at http://www.datapointed.net/visualizations/math/factorization/animated-diagrams/

Remark 2.2. *We've known some version or other of the FTA for most of our lives, and as such it probably seems like a rather obvious, and daresay, even boring fact. However, it's really quite a striking feature of the natural numbers. Later in the course we will encounter other number systems (i.e. rings) in which unique factorization into primes does not hold. For an excursion in this direction, take a look at Silverman's discussion on the $\mathbb{E}-$world, in which he talks about the set of even numbers.*

Proposition 2.3. *Suppose $p, n, m \in \mathbb{N}$ with p prime and p dividing nm (i.e., $pr = nm$ for some $r \in \mathbb{N}$). Then either $p \mid n$ ("p divides n") or $p \mid m$ (or possibly both).*

Proof. By Theorem 2.1 every integer $r \in \mathbb{N}$ has a unique expression as product

$$r \ = \ p^e r_0$$

with $e \geqslant 0$ and r_0 a product of primes $\neq p$. Think of the exponent e as the analogue of the logarithm of r which only takes note of the powers of p in r, noting that

1. $p \mid r$ if and only if $e \geqslant 1$, just like $x \geqslant 1$ if and only if $\log x \geqslant 0$,
2. for the product $r'' = rr'$ of $r, r' \in \mathbb{N}$ with $r = p^e r_0$, $r' = p^{e'} r'_0$

   $$r'' \ = \ p^{e''} r''_0 \ = \ p^{e+e'}(r_0 r'_0)$$

   so that $e'' = e + e'$ just like $\log xx' = \log x + \log x'$.

Do this kind of factorization for r, n, m

$$r \ = \ p^e r_0 \ , \ n \ = \ p^f n_0 \ , \ m \ = \ p^g m_0 \ .$$

From $pr = nm$ we have

$$p^{e+1} r_0 \ = \ p^{f+g} n_0 m_0 \ ,$$

and

$$e + 1 \ = \ f + g \in \mathbb{N}$$

At least one of f, g must be $\geqslant 1$, so that either $p \mid n$ or $p \mid m$. □

This result is false for composite numbers, as e.g., $6 = 2 \cdot 3$, and so $6 \mid 2 \cdot 3$, but $6 \nmid 2$ and $6 \nmid 3$. More generally, if $c = nm$ with $n > 1$, $m > 1$ (so c composite) then $c \mid nm$ but $c \nmid n$ and $c \nmid m$. In general, if you see a non-example like this, remember it! This is the best way to remember the hypotheses of theorems.

Example 2.4. *If p is a prime number and p divides $2n$ then either p divides 2 or p divides n. We used this fact in the first lecture when we were discussing Pythagorean triples.*

Theorem 2.5. *If n is composite then it must be divisible by some prime $\leqslant \sqrt{n}$.*

Proof. If all prime factors of n are $> \sqrt{n}$ then clearly all factors of n are $> \sqrt{n}$. Thus since n is composite, we have some factorisation $n = ab > \sqrt{n}\sqrt{n} = n$, a contradiction. □

This gives us a reasonable algorithm to enumerate, the first few primes. Suppose we wanted to enumerate all primes less than 100. We could write the first 100 numbers down, and then cross off all multiples of 2, 3, 5, and 7. By the previous theorem, any numbers remaining must be prime, since $\sqrt{100} = 10$. This is called the Sieve of Eratosthenes. For an animation and more information click: http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes

2.2 Distribution of the primes

A whole course could be devoted to the distribution of the prime numbers. Basically the main motivating question asks: How are the primes interspersed among the natural numbers? As a first step, we know from Euclid that there are infinitely many primes:

Theorem 2.6. *(Euclid) There are infinitely many prime numbers.*

Proof. Suppose that there were only finitely many primes $p_1, \ldots, p_k$. Then consider the integer $N = p_1 \cdots p_k + 1$. This number is not divisible by any of the p_i (it has remainder 1 upon division). However, by Theorem 2.1 it must be divisible by some prime p. Since this p is none of our p_i we have a contradiction. We must not have written down all the primes. □

The same proof shows that there are infinitely many odd primes. In other words, there are infinitely many prime numbers of the form $2k + 1$. On the first homework assignment you will prove that there are infinitely many prime numbers of the form $4k + 3$. In fact, these are the special cases $(a, b) = (2, 1)$ and $(4, 3)$ of a much stronger statement:

Theorem 2.7 (Dirichlet's Theorem)**.** *If a and b are positive integers not divisible by the same prime then there are infinitely many primes of the form $ak + b$.*

The proof of this theorem is difficult, and is beyond the scope of this course. It is just the tip of the iceberg concerning questions about the distribution of the primes. My favourite theorem of this type, for which we **do** have an elementary proof is the following. It provides yet another proof that there are infinitely many primes.

Theorem 2.8. *The sum of the reciprocals of the primes diverges*

$$\sum_{p \text{ prime}} \frac{1}{p} \to \infty.$$

We will need the following tools for the proof:

0. The Fundamental Theorem of Arithmetic.
1. $1/(1-x) = 1 + x + x^2 + \cdots + x^n + \cdots$.
2. $\log(1-x) = -x - x^2/2 - x^3/3 - \cdots - x^n/n - \cdots$.
3. The harmonic series $1 + 1/2 + 1/3 + 1/4 + \cdots$ diverges.

(Tools 1-3 were introduced in Calculus, (recall that the series $\sum 1/n^s$ converges if and only if $s > 1$.)

Proof. Let n be a natural number. We define the following product:

$$\lambda(n) = \prod_{p \leqslant n} \left(\frac{1}{1 - \frac{1}{p}} \right)$$

Our first goal is to prove that $\lambda(n)$ diverges. To see this, note that we can rewrite each of the factors as an infinite sum using Tool 1.

$$\lambda(n) = \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right)\cdots$$

When we expand this product, we will obtain all fractions of the form

$$\frac{1}{2^{a_1} 3^{a_2} \cdots p_k^{a_k}}$$

where all prime factors $\leqslant n$ appear. By the fundamental theorem of arithmetic, we'll get all the numbers $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$ (and many many more). Therefore

$$\lambda(n) > 1 + 1/2 + 1/3 + \ldots + 1/n.$$

Hence as $n \to \infty$, $\lambda(n) \to \infty$ by Tool 3. In particular this means that $\log \lambda(n) \to \infty$ as $n \to \infty$.

Our second (and final goal) is to relate $\lambda(n)$ with the series $\sum 1/p$. To do this, we take logs. By basic properties of logs of products and reciprocals, we obtain:[3]

$$\log(\lambda(n)) = \sum_{p \leqslant n} - \log(1 - 1/p).$$

[3] If you're reading these notes, now is a good time to grab a pen and paper and track the following derivations carefully. The concepts aren't difficult, but unfortunately the notation can make this seem a bit intimidating.

Using Tool 2, we obtain:

$$\begin{aligned}-\log(1-1/p) &= \frac{1}{p}+\frac{1}{2p^2}+\frac{1}{3p^3}+\frac{1}{4p^4}+\cdots \\ &< \frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\cdots \\ &= \frac{1}{p}(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}+\cdots) \\ &= \frac{1}{p}\cdot\frac{1}{1-1/p}=\frac{1}{p}\cdot\frac{p}{p-1} \\ &\leqslant \frac{2}{p}.\end{aligned}$$

But then this means that

$$\log\lambda(n) < \sum_{p\leqslant n}\frac{2}{p}.$$

Since the left hand side diverges, we have that $\sum_{p\leqslant n}\frac{2}{p}$ diverges. Division by two yields the result. □

This Theorem is somewhat surprising, since for instance the sum $1+1/4+1/9+1/16+\cdots$ converges, yet $\sum 1/p$ diverges. Hence it might be appropriate to say that "There are more prime numbers than square numbers." However this sentence is pure nonsense without a proper definition. Along a different track, one way of measuring how many prime numbers there are is to consider the fraction of natural numbers that the primes comprise.

Consider the function

$$\pi(n) = \#\{primes\ p \leqslant n\}.$$

E.g. $\pi(5)=3$, $\pi(100)=25$, and $\pi(5000)=669$. In 1850 Chebyshev proved that there exist real numbers C_1, C_2 with $0<C_1<1<C_2$ such that

$$C_1(n/\log n) < \pi(n) < C_2(n/\log n)$$

In particular, in the limit we have

$$\lim\frac{\pi(n)}{n} = 0\ .$$

In other words, the primes have density 0 in the natural numbers. For an awesome elementary proof of this fact, check out http://www.math.udel.edu/~idmercer/primes-density.pdf.

It is interesting to ask how quickly this ratio $\pi(n)/n$ approaches zero.

Theorem 2.9. *When n is large, the number of primes less than x is approximately equal to $x/\ln x$. In other words*

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln(x)} = 1.$$

This theorem was conjectured by many in the late 18th century, and was first noticed by observing tables of prime numbers made by hand. It was first proved independently by Hadamard and de la Valée-Poussin in 1896. Their proofs use complex analysis. An elementary proof was discovered by Paul Erdös and Atle Selberg in 1949. Proofs from the Book is a great book, containing many beautiful and elegant proofs of theorems, which is available for download from within the EASE network. For an excellent story, check out Don Zagier's The First 50 Million Prime Numbers, or watch the video of Barry Mazur talking about the Riemann Hypothesis `http://fora.tv/2014/04/25/Riemann_Hypothesis_The_Million_Dollar_Challenge`. We don't have time in this course to go much more into the theory of the distribution of the primes, but there are many accessible introductions to this area.

Finally, it wouldn't be a lecture about the distribution of the primes if we didn't include at least two open conjectures.

The Twin Prime Conjecture is that there are infinitely many primes p such that $p+2$ is also prime. In 2013 Yitang Zhang proved that there exists an integer $N < 7,000,000$ such that there is an infinite number of primes p such that $p+N$ is also prime - a rather romantic story! The current record for the lower bound is that there exists an integer $N \leqslant 246$ such that there is an infinite number of primes p such that $p+N$ is also prime: there is up to date information on the website
http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes.

Conjecture 2.10. *(Twin Prime Conjecture) There are infinitely many prime numbers p such that $p+2$ is also prime. These are called twin primes.*

Conjecture 2.11. *(Goldbach Conjecture) Every even integer larger than 2 can be written as a sum of two primes.*

There is even a novel about the Goldbach Conjecture. Extra credit (and fame and fortune) goes to anyone who can solve it!

Main Points from Lecture 2:

- Statement of the Fundamental Theorem of Arithmetic and fluency in using uniqueness to prove statements such as Prop 2.3.
- Proof of the infinitude of primes and its variants.
- The statement that $\sum 1/p$ diverges.

3 The greatest common divisor, the lowest common multiple and the Euclidean Algorithm (28.9.2015)

The **greatest common divisor** (gcd) of $n, m \in \mathbb{N}$ is, as the name suggests, the largest integer that divides both of them. Such an integer always exists, as $1 \mid n$ and $1 \mid m$ (so common divisors exist) and clearly no common divisor can exceed $\min(n, m)$ (so we are taking the maximum over a nonempty finite set. To recap: $1 \leqslant \gcd(n, m) \leqslant \min(n, m)$.

In some texts the gcd is called the hcf ("highest common factor"). We will often denote the gcd of a and b simply by (a, b). In particular, if $(a, b) = 1$ then we say that a and b are relatively prime.

The **least common multiple** (lcm) of $n, m \in \mathbb{N}$ is the smallest integer that both n and m divide. Again, such an integer exists, as n and m both divide nm. So clearly

$$\max(n, m) \leqslant \operatorname{lcm}(n, m) \leqslant nm.$$

Example 3.1. *One way of computing the* gcd *is to factorize. For example* $24 = 2^3 \cdot 3$ *and* $84 = 2^2 \cdot 3 \cdot 7$. *Hence the greatest common factor is* $2^2 \cdot 3 = 12$.

As we'll see shortly, there is a method for computing the gcd *that doesn't involve factoring. This is a good thing as factoring is quite slow.*

Proposition 3.2. *Given* $m, \in \mathbb{N}$ *let* $p_1, \dots, p_k$ *be the primes dividing* m *or* n *(i.e.,* mn*), and write*

$$m = \prod_{i=1}^{k} p_i^{e_i}, \qquad n = \prod_{i=1}^{k} p_i^{f_i},$$

where $e_i \geqslant 0$*,* $f_i \geqslant 0$*. Then*

(i) $\gcd(m, n) = \prod_{i=1}^{k} p_i^{\min(e_i, f_i)}$*;*

(ii) $\operatorname{lcm}(m, n) = \prod_{i=1}^{k} p_i^{\max(e_i, f_i)}$*;*

(iii) $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$*;*

(iv)

$$\gcd\left(\frac{n}{\gcd(n, m)}, \frac{\operatorname{lcm}(n, m)}{n}\right) = 1.$$

Proof. (i) Suppose that $d \mid m$. Then $dd' = m$ say. so any prime dividing d will divide $dd' = m$. Hence d is of the form

$$d = \prod_{i=1}^{k} p_i^{e_i'}, \qquad \text{where } e_i' \geqslant 0.$$

Since $d \mid m$, clearly $e_i' \leqslant e_i$.

If also $d \mid n$, then $e_i' \leqslant f_i$. so $e_i' \leqslant \min(e_i, f_i)$. But $\prod_{i=1}^{k} p_i^{\min(e_i, f_i)}$ divides both m and n, so it is their gcd.

(ii) Similarly if $m \mid \ell$ and $\ell = \prod_{i=1}^{k} p_i^{f_i'} \cdot \ell'$ say, where ℓ' is a product of primes different from $p_1, \dots, p_k$, then also $m \mid \prod_{i=1}^{k} p_i^{f_i'}$, so we can take $\ell' = 1$ (i.e., ignore it!). Hence

$$\prod_{i=1}^{k} p_i^{e_i} \mid \prod_{i=1}^{k} p_i^{f_i'},$$

so that $e_i \leqslant f_i'$. Similarly $n \mid \ell$ gives $f_i \leqslant f_i'$. Hence $f_i' \geqslant \max(e_i, f_i)$. But clearly m and n both divide $\prod_{i=1}^k p_i^{\max(e_i,f_i)}$, so this must equal $\operatorname{lcm}(m, n)$.

(iii) If e and f are any two real numbers then

$$\min(e, f) + \max(e, f) = e + f,$$

since one of $\min(e, f)$ and $\max(e, f)$ is e and the other is f. Hence

$$\gcd(m, n) \cdot \operatorname{lcm}(m, n) = \prod_{i=1}^{k} p_i^{\min(e_i,f_i)+\max(e_i,f_i)} = \prod_{i=1}^{k} p_i^{e_i+f_i} = mn.$$

(iv) We have using (iii) that

$$\gcd\left(\frac{n}{\gcd(n, m)}, \frac{\operatorname{lcm}(n, m)}{n}\right) = \gcd\left(\frac{n}{\gcd(n, m)}, \frac{m}{\gcd(n, m)}\right) = \frac{\gcd(n, m)}{\gcd(n, m)} = 1.$$

□

Proposition 3.3. *Suppose that* $(a, b) = d$. *Then* $(a/d, b/d) = 1$.

Proof. Suppose that $c = (a/d, b/d)$ is the gcd. Then $a/d = c \cdot k$ and $b/d = c \cdot l$. Clearing fractions we see that $a = ckd$ $b = cld$. But then cd is a common factor of a and b. Since d was the $gcd(a, b)$ we must have that $cd = d$ and hence $c = 1$. □

Proposition 3.4. *If* a, b, c *are integers then* $(a + cb, b) = (a, b)$.

Proof. Let $d = (a + cb, b)$ and $e = (a, b)$. Since e divides a and b it surely divides $a + cb$ and b, so $e \mid d$. Conversely, since $d \mid b$, it follows that if $d \mid a + cb$ then $d \mid (a + cb) - cb$ and hence $d \mid a$. Thus d divides a and b whence $d \mid e$. Since d and e divide one another, they must be equal. □

Question 3.5. *If* a *and* b *are integers, then what is the set of values that* $ax + by$ *can take on as* x, y *range through all integers? We call such numbers* **linear combinations of** a **and** b**.**

This question is related to the postage stamp question which asks if you have postage stamps of values a and b, what are the possible values of total postage that you can make. Note in this case, we are only allowed to nonnegative combinations of a and b, whereas in the Question we allow all integers.

Example 3.6. *What integers are of the form* $8x + 12y$*?*

First notice that any integer of this form is definitely a multiple of 4*, as it is the* gcd *of* 8 *and* 12*. Further, notice that if we could somehow write* $4 = 8x_0 + 12y_0$ *then we would be able to write* **any** *multiple of* 4 *as*

$$4k = 8(kx_0) + 12(ky_0).$$

In this case, it's easy to see that we can indeed write $4 = 8(-1) + 12(1)$*. Thus our answer is that*

$$\{8x + 12y,\ |x, y \in \mathbb{Z}\} = \{4k \mid k \in \mathbb{Z}\} = 4\mathbb{Z}.$$

In general the following is true:

Theorem 3.7. *The set of linear combinations of two numbers a and b is equal to the set of multiples of (a, b)*

$$\{ax + by, \ |x, y \in \mathbb{Z}\} = \{(a, b)k \mid k \in \mathbb{Z}\} = (a, b)\mathbb{Z}.$$

Proof. As in the example, it is clear that any combination must be a multiple of (a, b) since this divides bother ax and by. What remains to be shown is that (a, b) can indeed be written as a linear combination of a and b. To see this, we argue by contradiction. Suppose that d is the smallest positive integer that is a linear combination of a and b.[4] Say that $d = am + bn$. Now by the division algorithm, we have that

$$a = dq + r, \ 0 \leqslant r < d.$$

Now $r = a - dq = a - (am + bn)q = (1 - m)a + nqb$ is yet another linear combination of a and b. But by assumption, d was the smallest positive such number. Hence $r = 0$, and $a = qd$. Thus $d \mid a$. Similarly $d \mid b$. Hence d is a common divisor of a and b and now the first sentence of this proof shows that $d = (a, b)$. □

Corollary 3.8. *If $(a, b) = 1$ then there exists $m, n \in \mathbb{Z}$ with $am + bn = 1$.*

Theorem 3.7 says something quite useful: That the smallest positive integer which can be written as a linear combination of a and b is (a, b). In the next section, we exploit this to create an algorithm to compute (a, b).

3.1 Finding the gcd without factoring - The Euclidean Algorithm

Given $a, b \in \mathbb{N}$ with $a \geqslant b$ (say). Our goal is to compute $g = (a, b)$.

The **Division Algorithm** is key ingredient: we can first divide b into a to get

$$a \ = \ bq + r \qquad (q \in \mathbb{N}, 0 \leqslant r < b) \ ,$$

with q the **quotient** and r the **remainder**. Notice that

$$(a, b) \ = \ (b, a - bq) \ = \ (b, r)$$

where the first equality comes from $(a, b) = (b, a)$ and Proposition 3.4.

We can continue with a, b replaced by $a_1 = b$, $b_1 = r$. Apply the division algorithm again: $b = q_1 r + r_1$ say. Then also $g = \gcd(b, r) = \gcd(a_1, b_1)$ with $a_1 > b_1$. Continue in this way to obtain a sequence of successively smaller remainders

$$r_0 \ = \ r > r_1 > \cdots > r_k > r_{k+1} \ = 0 \ .$$

The last non-zero remainder is $g = \gcd(r_k, 0) = r_k$. Note that $k \leqslant b$, so there are at most b iterations.

More formally, the Euclidean Algorithm for finding the greatest common divisor $g = (a, b)$ of $a \geqslant b \geqslant 1$ generates a sequence of ordered pairs $a_n \geqslant b_n \geqslant 1$ for $n = 0, 1, \ldots, k$ and $r_n > r_{n+1}$ by the computer 'pseudo-code' :

[4] Why does such a number exist?

1. START $a_0 := a$, $b_0 := b$

2. APPLY DIVISION $a_n := q_n b_n + r_n$

3. $a_{n+1} := b_n$, $b_{n+1} := r_n$

4. REPEAT DIVISION

5. STOP WHEN $r_{k+1} = 0$

6. PRINTOUT "$(a, b) = r_k$"

Example 3.9. *Use the Euclidean Algorithm to compute* $(87, 51)$*:*

$$\begin{array}{rclrcl}
a_0 & = & b_0q_0 + r_0 & 87 & = & 51 \cdot 1 + 36 \\
a_1 & = & b_1q_1 + r_1 & 51 & = & 36 \cdot 1 + 15 \\
a_2 & = & b_2q_2 + r_2 & 36 & = & 15 \cdot 2 + 6 \\
a_3 & = & b_3q_3 + r_3 & 15 & = & 6 \cdot 2 + 3 \\
a_4 & = & b_4q_4 + r_4 & 6 & = & 3 \cdot 2 + 0\ .
\end{array}$$

Thus $(87, 51) = 3$*, the last nonzero remainder. If we want to write* 3 *as a linear combination of* 51 *and* 87 *we can just step backwards through this:*

$$\begin{aligned}
3 &= 15 - 6(2) \\
&= 15 - (36 - 15 \cdot 2) \cdot 2 = 15(5) - 36(2) \\
&= (51 - 36)(5) - 36(2) = 51(5) - 36(7) \\
&= 51(5) - (87 - 51)(7) = 51(12) - 87(7).
\end{aligned}$$

Main Points from Lecture 3:

- How to compute the gcd of two numbers from a factorization or from the Euclidean Algorithm

- The gcd of a, b is an integer combination of a and b.

- All integer combinations of a, b are multiples of the gcd.

4 Linear Diophantine Equations (1.10.2015)

In this lecture we will learn how to solve equations of the form $ax + by = c$ where a, b, c are integers, and we seek integer solutions $(x, y) \in \mathbb{Z}^2$ [5]. The complete algorithmic method for finding all the integer solutions of $ax + by = c$ will require the 'Extended Euclidean Algorithm' for finding one solution (x, y) of $ax + by = \text{g.c.d.}(a, b)$, in a subsequent lecture. But today we shall concentrate on two questions:

[5] Do not confuse the ordered pair $(x, y) \in \mathbb{Z}^2$ with the integer $(x, y) = \text{g.c.d.}(x, y) \in \mathbb{Z}$

1. When does $ax + by = c$ have integer solutions (x, y)?

2. If there exists a solution at all, how many solutions are there altogether?

In subsequent lectures we shall also study the same questions $\bmod n$, for a given integer $n \geqslant 2$.

Note that describing the set of real solutions $(x, y) \in \mathbb{R}^2$ of $ax + by = c$ is easy: if $(a, b) \neq (0, 0)$ there is a line of solutions, given by $y = (c-ax)/b$ if $b \neq 0$, and by $x = (c-by)/a$ if $a \neq 0$. If $(a, b) = (0, 0)$ there is a solution if and only if $c = 0$, in which case every $(x, y) \in \mathbb{R}^2$ is a solution.

However it's not so clear what to do for integer solutions $(x, y) \in \mathbb{Z}^2$ of $ax + by = c$ with $(a, b, c) \in \mathbb{Z}^3$. We'll see that the answer comes quickly with the help of the Euclidean Algorithm.

Let's work out a few examples to see the salient points:

$$12x + 18y = 10$$

As in our work with linear combinations, we see that the left hand side is always divisible by $(12, 18) = 6$. But the right hand side is not. Therefore this equation has no solution. Hence we have

$$\boxed{\text{If } ax + by = c \text{ has an integer solution then } c \text{ must be an integer multiple of g.c.d.}(a, b).}$$

This is a direct consequence of Theorem 3.7 from the last lecture: the set of linear combinations of two numbers a and b is equal to the set of multiples of g.c.d.(a, b)

$$\{ax + by \mid x, y \in \mathbb{Z}\} \ = \ \{\text{g.c.d}(a, b)k \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}\ .$$

With that in mind let's try an example that has a chance of having solutions:

$$12x + 18y = 42.$$

We can divide through by $(12, 18) = 6$ to obtain $2x+3y = 7$, and now we can spot a solution in our heads: $2(2) + 3(1) = 7$. It is instructive to find another solution in a more systematic way: Notice that the Euclidean Algorithm produces a solution $2(-1) + 3(1) = 1$. We can multiply everything by 7 to obtain $2(-7) + 3(7) = 7$. What is the relationship between our two solutions $(x, y) = (2, 1)$ and $(x, y) = (-7, 7)$? The answer is the following Theorem

Theorem 4.1. *The equation $ax + by = c$ has an integer solution if and only if c is divisible by $d =$ g.c.d.(a, b). If this is the case, then there are infinitely many solutions. If (x_0, y_0) is one particular solution, then all solutions are of the form*

$$x = x_0 - (b/d)n, \quad y = y_0 + (a/d)n$$

where n is an integer.

Proof. By the discussion preceding this theorem, it is clear that a solution exists only if $d \mid c$. In this case a solution always exists as the Euclidean Algorithm will always yield a solution to $d = as + bt$. Multiplying both sides by c/d will yield a solution. To see that there are infinitely many solutions, let's check that the ordered pair

$$(x_0 - (b/d)n, y_0 + (a/d)n)$$

is indeed a solution:

$$a(x_0 - (b/d)n) + b(y_0 + (a/d)n) = (ax_0 + by_0) - (ab/d)n + (ba/d)n = (c) + 0 = c.$$

Now suppose that (x_1, y_1) is an arbitrary solution. This means that $ax_1 + by_1 = c$. Notice

$$a(x_0 - x_1) + b(y_0 - y_1) = c - c = 0.$$

This means that $a(x_0 - x_1) = -b(y_0 - y_1)$. Let us now divide through by d to obtain

$$\frac{a}{d}(x_0 - x_1) = -\frac{b}{d}(y_0 - y_1).$$

Now since a/d and b/d are relatively prime, we see that $a/d \mid (y_0 - y_1)$ hence $y_0 - y_1 = (a/d)n$. Substituting and canceling, we obtain:

$$\frac{a}{d}(x_0 - x_1) = -\frac{b}{d}\frac{a}{d}n$$

$$(x_0 - x_1) = -\frac{b}{d}n.$$

In summary we have shown that

$$x_1 \quad = \quad x_0 + \frac{b}{d}n \text{ and } y_1 \quad = \quad y_0 - \frac{a}{d}n \ .$$

The signs are different from the ones in the statement of the theorem, but since n is allowed to be positive or negative, this is the same solution set as we required. □

The format for the solutions of an inhomogeneous linear Diophantine equation

$$\boxed{\text{General solution} = \text{homogeneous solution} + \text{particular solution}}$$

may be familiar to you from the solutions of an inhomogeneous linear differential equation.

Many times we will be interested in knowing the natural number solutions to an equation. In this case it is possible that there may be no solutions, or only finitely many.[6]

[6] Can you think of an equation with no natural number solutions?

Example 4.2. *A farmer wishes to buy* 100 *animals and spend exactly* \$100*. Cows are* \$10*, sheep are* \$3 *and pigs are* \$0.50*. Is this possible?*

Solution: The system of equations is

$$c + s + p = 100, \quad 10c + 3s + 0.50p = 100.$$

Substituting $p = 100 - c - s$ *we obtain*

$$10c + 3s + 0.50(100 - c - s) = 100$$

$$20c + 6s + 100 - c - s = 200$$

$$19c + 5s = 100.$$

As $(19, 5) = 1$ *this equation will have infinitely many integer solutions. We can find one by the Euclidean Algorithm.*

Scratchwork:

$$19 = 5(3) + 4, \quad 5 = 4 + 1$$

$$1 = 5 - 4 = 5 - (19 - 5(3)) = 19(-1) + 5(4)$$

$$100 = 19(-100) + 5(400).$$

Hence $c = -100, s = 400$ *is one integer solution. By the Theorem, all solutions are of the form*

$$c = -100 - 5n, \quad s = 400 + 19n.$$

Since we are looking for positive integer solutions, we see that $-100 - 5n > 0$ *and* $400 + 19n > 0$*. This yields* $-20 > n$ *and* $-21 \leqslant n$*, hence* $n = -21$ *gives the unique solution in positive integers. This yields*

$$c = 5, \quad s = 1, \quad p = 94.$$

4.1 Multivariate linear equations over $\mathbb{Z}$

Given integers $a_1, a_2, \ldots, a_n, b$, how do we find all $(x_1, \ldots, x_n)$:

$$a_1 x_1 + \cdots + a_n x_n = b? \tag{1}$$

Important easy cases

1. $g = \gcd(a_1, \ldots, a_n) \nmid b$. Then the LHS of (1) is divisible by g, but the RHS is not, so (1) has no solution in integers.

2. $a_1 = 1$. Then $x_2, x_3, \ldots, x_n$ can be chosen to be **any** integers, with (1) then determining x_1. Clearly this gives **all** solutions of (1) in this case.

Example for 1. The equation $6x_1 + 8x_2 = 11$ has no integer solution, as the LHS is even while the RHS is odd.

Example for 2. The general integer solution of $x_1 + 7x_2 + 9x_3 = 3$ is $(x_1, x_2, x_3) = (3 - 7x_2 - 9x_3, x_2, x_3)$ for x_2, x_3 arbitrary in $\mathbb{Z}$.

General strategy for solving (1): Make linear changes of variables to successively reduce the minimum modulus of coefficients of (1). Keep doing this until either

- get case where $\gcd(a_1, a_2, \ldots, a_n) \nmid b$, so no solution, as in 1. above;
- get a coefficient $= 1$, and so can solve as in 2. above.

This is best illustrated by an example.

Example. Solve $3x + 4y + 5z + 6w = 7$ for integers x, y, z, w.

Solution. Write equation as $3(x + y) + y + 5z + 6w = 7$, and put $u = x + y$. So $3u + y + 5z + 6w = 7$, and $x = u - y$.
Now choose u, z, w arbitrarily in $\mathbb{Z}$. Then $y = 7 - 3u - 5z - 6w$ and $x = u - y = -7 + 4u + 5z + 6w$. Thus the general solution is $(x, y, z, w) = (-7 + 4u + 5z + 6w, 7 - 3u - 5z - 6w, z, w)$.

Solution algorithm for solving (1) in integers:

- Pick the a_i of smallest modulus. If $|a_i| = 1$, can solve (1) as in 2. above.
- Otherwise, when smallest modulus of a_i is $\geqslant 2$: For convenience assume $a_1 > 0$ and it is the a_i of smallest modulus. If all the a_i divisible by a_1 and $a_1 \nmid b$, then no solution by 1. above. If all the a_i divisible by a_1 and $a_1 \mid b$, then simply divide the equation by a_1. Now the new a_1 is $= 1$, so can solve it by 2. above.

  Otherwise,, choose an a_1 **not** divisible by a_1 – assume it is a_2. Write $a_2 = qa_1 + a_2'$, where $0 < a_2' < a_1$, and put $u = x_1 + qx_2$. Then (1) becomes

$$a_1x_1 + (qa_1 + a_2')x_2 + a_3x_3 \cdots + a_nx_n = b,$$

  or

$$a_1u_1 + a_2'x_2 + a_3x_3 \cdots + a_nx_n = b. \tag{2}$$

  This new equation (2) has smallest coefficient $a_2' < a_1$. So we can repeat the process. Keep repeating until we get either 1. (so no solution) or 2. (so can write down solution). In the latter case we use the linear equations generated (e.g., $u_1 = x_1 + qx_2$) to get expressions for the original variables.

4.2 Review of Congruences

We now briefly review properties of congruences. A solid mastery of the basics will be necessary for the course. At the end of this section will be many problems designed to give you practice working with congruences. Please let me know if you have any questions either before or after class (or in an email). The material in this section is found in Rosen 4.1 (Introduction to Congruences)

The congruence $a \equiv b \bmod n$ means that the difference $(a - b)$ is divisible by n. In other words, a is equal to a multiple of n plus b. In other words, $a = nq + b$.

Example 4.3.

$$15 \equiv 1 \bmod 7$$
$$-3 \equiv 14 \bmod 17$$
$$10 \equiv 0 \bmod 5$$

I find it helpful to thing of negative numbers as being "less than a multiple of n". For example $30 \equiv -4 \bmod 17$ because "30 is 4 less than a multiple of 17."

There are multiple ways to represent numbers using congruences, and we call each set of equivalences a **congruence class**. For example

$$\cdots - 4 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \cdots \bmod 5$$

Is the congruence class of the 1 mod 5.

Definition 4.4. *A complete system of residues mod n is a set of integers such that every integer is congruent mod n to exactly one integer in the set. A least positive reside for an integer a is the smallest positive integer b such that* $a \equiv b \bmod n$.

Example 4.5. *Modulo* 5*, a complete system of residues if* $\{0, 1, 2, 3, 4\}$. *Another is* $\{-2, -1, 0, 1, 2\}$. *Yet another is* $\{0, 1, 2, 3, 19\}$.

Arithmetic with congruences behaves extremely well, as we summarize here:

Theorem 4.6. *If a, b, c, d and n are integers with $n > 0$ and $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then*

$$a + c \equiv b + d \bmod n.$$
$$a - c \equiv b - d \bmod n.$$
$$ac \equiv bd \bmod n.$$

The proofs of these exercises follow from the definition of modular arithmetic. The third property is a special case of Problem 2c on the first Homework. We present the proof here.

Proof. If $a \equiv b \bmod n$ then $a = kn + b$ for some integer k. Similarly, $c = \ell n + d$. Thus

$$ac = (kn + b)(\ell n + d) = k\ell n^2 + b\ell n + dkn + db$$

and therefore $ac - bd = n(k\ell n + b\ell + dk)$ is a multiple of n. Hence $ac \equiv bd \bmod n$. □

Example 4.7. *Compute:* $93 \cdot 17$ *mod* 6. *Since* $93 \equiv 3 \bmod 6$ *and* $17 \equiv -1 \bmod 6$ *we conclude that* $93 \cdot 17 = -3 \bmod 6$.

Finally, we discuss exponents and their role in modular arithmetic. It is not true that we can reduce the exponents mod n in computations:

$$2^{10} \equiv 1024 \equiv 4 \bmod 5$$

$$2^0 \equiv 1 \bmod 5.$$

However, two algorithms exist which can help us readily compute high powers of numbers mod n.

In general, the method that works best is successive squaring. Simply compute successive squares, reducing mod n when necessary. Then use these numbers to compute the desired power. This is best illustrated by an example.

Example 4.8. *Compute the least positive residue mod* 7 *of* 2^{37}. *We compute powers,* $2^2 \equiv 4$
$2^4 \equiv 4^2 \equiv 2$
$2^8 \equiv 2^2 \equiv 4$
$2^{16} \equiv 4^2 \equiv 2$
$2^{32} \equiv 2^2 \equiv 4$
Thus $2^{37} = 2^{32} \cdot 2^4 \cdot 2^1 = 4 \cdot 2 \cdot 2 \equiv 2 \bmod 7$.

4.3 Lots of Practice Problems with Congruences

(The Starred Problems will appear on the next Homework to be Handed-In)

1. Show that the following congruences hold:

$$13 \equiv 1 \bmod 2, \quad 111 \equiv -9 \bmod 40, \quad 69 \equiv 62 \bmod 7.$$

2. Show that if a is an odd integer then $a^2 \equiv 1 \bmod 8$. (Try to find two proofs, one using modular arithmetic and one that doesn't)

3. Find the least positive residue of $1! + 2! + 3! + \cdots 100!$ mod 7

4. Show by mathematical induction that if n is a positive integer then $4^n \equiv 1+3n \bmod 9$.

5. Find the least positive residue mod 47 of 2^{200}.

6. $\star$ Show that for every integer n there are infinitely many Fibonacci numbers f_k such that m divides f_k. (Hint: Show that the sequence of least positive residues mod n of the fibonacci numbers is a repeating sequence.)

7. $\star$ If a, b, c, m are integers such that $m > 0$, $d = (c, m)$ and $ac \equiv bc \bmod m$ then $a = b \bmod m/d$.

Main Points from Lecture 4:

- How to solve systems of linear diophantine equations using the Euclidean Algorithm
- Basic properties of congruences

5 The Extended Euclidean Algorithm and Linear Modular Congruences (5.10.2015)

5.1 The Extended Euclidean Algorithm

So far we have only used the Euclidean Algorithm in the classical way: Given a and b, use the algorithm to find their gcd. We can then back-substitute to find a solution to the equation $ax + by = \gcd(a, b)$. We now present a way that does this all at once called the Extended Euclidean Algorithm.

The basic idea is simple: Given $a > b \geqslant 1$ our goal is to not only find $z = \gcd(a, b)$ but also an integer solution $(x, y) \in \mathbb{Z}^2$ the equation $ax + by = z$. This is done by extending the steps in the Euclidean Algorithm from the sequence of reminders in successive divisions

$$r_0 > r_1 > \cdots > r_k = \gcd(a, b) > r_{k+1} = 0$$

to a sequence of integer vectors $v_{-2}, v_{-1}, \ldots, v_k \in \mathbb{Z}^3$

$$\begin{aligned}
v_{-2} &= (x_{-2}, y_{-2}, r_{-2}) = (1, 0, a) , \\
v_{-1} &= (x_{-1}, y_{-1}, r_{-1}) = (0, 1, b) , \\
v_0 &= (x_0, y_0, r_0) , \\
&\vdots \\
v_k &= (x_k, y_k, r_k) \in \mathbb{Z}^3
\end{aligned}$$

such that

$$ax_n + by_n = r_n \text{ for } n = -2, -1, 0, 1, \ldots, k .$$

Then $(x, y) = (x_k, y_k) \in \mathbb{Z}^2$ is such that

$$ax + by = r_k = z = \gcd(a, b)$$

as required.

Proposition 5.1. *(Extended Euclidean Algorithm) Given $a, b \in \mathbb{N}$ and $z = \gcd(a, b)$, there exist integers $(x, y) \in \mathbb{Z}^2$ such that:*

$$ax + by = z \qquad \textit{Bézout's Identity} .$$

Proof. As usual, it may be assumed that $a > b \geqslant 1$. For any vectors $v = (x, y, r)$, $v' = (x', y', r') \in \mathbb{Z}^3$ such that

$$ax + by \ = \ r \text{ and } ax' + by' \ = \ r' \in \mathbb{Z}$$

(i.e. on the integer plane $ax + by - z = 0$ in $\mathbb{Z}^3 \subset \mathbb{R}^3$ normal to $(a, b, -1) \in \mathbb{Z}^3$) and any integers $c, c' \in \mathbb{Z}$ the integer linear combination

$$v'' \ = \ cv + c'v' \ = \ (cx + c'x', cy + c'y', cr + c'r') \ = \ (x'', y'', r'') \in \mathbb{Z}^3$$

is also on the integer plane, with

$$\begin{aligned} ax'' + by'' \ &= \ a(cx + c'x') + b(cy + c'y') \\ &= \ c(ax + by) + c'(ax' + by') \\ &= \ cr + c'r' \ = \ r'' \in \mathbb{Z} \ . \end{aligned}$$

This is called the **Principle of Linear Superposition**. The formula for constructing the sequence of vectors $v_0, \dots, v_k \in \mathbb{Z}^3$ involves the integer linear combinations used to obtain r_{n+1} from r_n and r_{n-1}. By construction, the r_n's are the successive remainders in the divisions

$$a_n \ = \ q_n b_n + r_n \ (n = 0, 1, \dots, k + 1)$$

with the sequence $(a_n, b_n) \in \mathbb{N}^2$ of pairs such that $a_n > b_n \geqslant 0$ given by the Euclidean Algorithm

$$\begin{array}{lcll} (a_0, b_0) & = & (a, b) \ , & r_0 \ = \ a_0 - q_0 b_0 \\ (a_1, b_1) & = & (b_0, r_0) \ , & r_1 \ = \ a_1 - q_1 b_1 \\ & \vdots & & \quad \vdots \\ (a_{k+1}, b_{k+1}) & = & (b_k, r_k) \ , & r_{k+1} \ = \ 0 \text{ (terminate)} \end{array}$$

such that

$$a_n \ = \ q_n b_n + r_n \text{ for } n = 0, 1, \dots, k, k + 1$$

with $z = \gcd(a, b) = r_k$. The remainder r_{n+1} is obtained from r_n and r_{n-1} by a particular linear integer combination

$$r_{n+1} \ = \ a_{n+1} - q_{n+1} b_{n+1} \ = \ r_{n-1} - q_{n+1} r_n \ .$$

Use the same linear integer combination to define

$$v_{n+1} \ = \ v_{n-1} - q_{n+1} v_n \in \mathbb{Z}^3$$

which coordinate-wise is

$$x_{n+1} \ = \ x_{n-1} - q_{n+1} x_n \ , \ y_{n+1} \ = \ y_{n-1} - q_{n+1} y_n \ , \ r_{n+1} \ = \ r_{n-1} - q_{n+1} r_n \in \mathbb{Z} \ .$$

You do not have to memorize these formulae in order to implement the Extended Euclidean Algorithm, assuming that you can implement the Euclidean Algorithm itself. You only need to know the initial values

$$v_{-2} \;=\; (1,0,a)\ ,\ v_{-1} \;=\; (0,1,b) \in \mathbb{Z}^3$$

and the idea that the integer linear combinations of the Euclidean Algorithm in the third coordinate govern the iteration of $v_0, v_1, v_2, \ldots, v_k \in \mathbb{Z}^3$ in the Extended Euclidean Algorithm. □

We illustrate with an example: $\gcd(91,77)$.

Notice that the following equations hold obviously.

$$\begin{aligned} E(-2):\ 91(1)+77(0) = 91, &\quad v_{-2} = (1,0,91) \\ E(-1):\ 91(0)+77(1) = 77, &\quad v_{-1} = (0,1,77) \end{aligned}$$

We have written the coefficients to the right. Now notice what happens when we subtract the second equation from the first $E(0) = E(-2) - E(-1)$.

$$E(0):\ 91(1) - 77(1) = 14, \quad v_0 = v_{-2} - v_{-1} = (1,-1,14)$$

Now we can set $E(1) = E(-1) - 5 \cdot E(0)$:

$$E(1):\ 91(-5) + 77(6) = 7, \quad v_1 = (-5,6,7)$$

As $14 = 2.7$ we are done:

$$-5.91 + 6.77 \;=\; \gcd(91,77) \;=\; 7\ .$$

If you look at the numbers on the right side of the equation, they are simply the remainders that come up in the Euclidean Algorithm. Hence 7 is the last nonzero remainder so it is the gcd. Hence we have found $91(-5) + 77(6) = 7$. This algorithm can be done rapidly if we ignore writing the equations and just work with the vectors.

Example 5.2. *Compute* $\gcd(561,306)$ *using the Extended Euclidean Algorithm: We begin with the vectors* $v_{-2} = (1,0,561)$ *and* $v_{-1} = (0,1,306)$ *and just subtract one from the other successively:*

$$\begin{aligned} v_{-2} &= (1,0,561) \\ v_{-1} &= (0,1,306) \\ v_0 &= (1,-1,255), \quad (v_0 = v_{-2} - v_{-1}) \\ v_1 &= (-1,2,51), \quad (v_1 = v_{-1} - v_0) \\ v_2 &= (6,-11,0), \quad (v_2 = v_0 - 5v_1). \end{aligned}$$

Thus the gcd is 51 and $561(-1) + 2(306) = 51$.

5.2 Linear modular congruences

We now solve congruences of the form

$$ax \equiv c \bmod n.$$

Recall that from the definition this means that $ax - c = ny$ for some integer y. Rewriting we can think of this as a linear diophantine equation

$$ax - ny = c.$$

(Notice the roles of the letters is slightly different here than it was before.) Hence for a solution to exist, if $d = (a, n)$, it must be the case that $d \mid c$. Further, if one solution (x_0, y_0) exists then there are infinitely many solutions, given by Theorem 4.1:

$$x = x_0 + (n/d)t, \quad y = y_0 + (a/d)t.$$

Since we are solving a congruence, however, it makes sense to talk about the congruence classes which are solutions. In other words, we want to know how many incongruent solutions there are to the equation mod n.

Theorem 5.3. *If $d = (a, n)$ divides c then the congruence $ax \equiv c \bmod n$ has exactly d incongruent solutions mod n.*

Proof. Let x_0 be a solution to the congruence. By the discussion above, we know that all solutions are of the form $x_0 + (n/d)t$ where $t \in \mathbb{Z}$. We now see how many of these are incongruent mod n. Suppose that we have

$$x_1 = x_0 + (n/d)t_1, \quad x_2 = x_0 + (n/d)t_2.$$

Then $x_1 - x_2 = (n/d)(t_1 - t_2)$. Hence x_1 and x_2 are congruent mod n if and only if $(n/d)(t_1 - t_2)$ is a multiple of n. This occurs exactly when there exists an integer ℓ such that $(n/d)(t_1 - t_2) = \ell n$. Simplifying we see $(t_1 - t_2) = \ell d$, which is equivalent to

$$t_1 \equiv t_2 \bmod d.$$

Summing up, the solutions x that are inequivalent mod n are exactly the ones that have corresponding values of t that are inequivalent mod d. There are d such classes for t, which proves the theorem. □

Note the special case when $d = (a, n) = 1$.

Corollary 5.4. *If $(a, n) = 1$ then the congruence $ax = c \bmod n$ has a unique solution.*

An Algorithm: To solve a congruence of the form $ax \equiv c \bmod n$ we can proceed algorithmically:

First we check the necessary condition that $d = (a, n)$ divides c.

If so, then we expect there to be d distinct solutions mod n. To find one of these, write

$$d = ax_0 + ny_0$$

Then going mod n, we see that x_0 is a solution to the congruence.

The set of all solutions is then

$$\{x_0, x_0 + (n/d), x_0 + 2(n/d), \dots, x_0 + (d-1)(n/d)\} \;=\; \{x_0 + t(n/d) \,|\, 0 \leqslant t \leqslant d-1\} \,.$$

Example 5.5. *To find all solutions to* $9x \equiv 12 \bmod 15$*, we first check that* $d = (9, 15) = 3$ *indeed divides 12. By the Theorem there will be* 3 *inequivalent solutions. By the Euclidean Algorithm, we see that*

$$d = 15(-1) + (2)(9).$$

Hence $9(2) \equiv 3 \bmod 15$ *and thus* $9(8) \equiv 12 \bmod 15$*. Thus* $x = 8$ *is a solution. All solutions will therefore be of the form* $8+(15/3)t = 8+5t$ *for* $t = 0, 1, 2$*. Hence the congruence classes of the solutions are* $3, 8, 13$*.*

Main Points from Lecture 5:

- Using the Extended Euclidean Algorithm to write $\gcd(a, b)$ as an integer combination of a and b.
- The number of solutions to the congruence $ax \equiv c \bmod n$ is $d = (a, n)$.
- All solutions are of the form $x_0 + t(n/d)$ for $t = 0, 1, \dots, d-1$.

6 Modular Inverses and the Chinese Remainder Theorem (8.10.2015)

A solution $x_0 \bmod n$ to the congruence $ax_0 \equiv 1 \bmod n$ is called an **inverse** of a mod n, written

$$x_0 \equiv a^{-1} \bmod n \,.$$

By Corollary 5.4, this solution is unique. Inverses are incredibly useful, because if you have one, then it allows you to easily solve all other congruences, by ‘reverse engineering’: the equation $ax \equiv b \bmod n$ is solved by $x \equiv a^{-1}b \bmod n$, that is $x \equiv x_0 b \bmod n$. But beware: this only works if $a^{-1} \bmod n$ is actually defined, i.e. if $\gcd(a, n) = 1$.

Example 6.1. *Find all solutions to* $7x \equiv 1 \bmod 31$*. We use the Extended Euclidean Algorithm to determine that*

$$(31)(-2) + 7(9) = 1$$

so that $9 = 7^{-1} \bmod 31$*, and* $x \equiv 9 \bmod 31$*.*

An important special case is when $n = p$ is a prime number. In this case, every nonzero number a has a unique inverse. For example, we list the inverses mod 11 in the following table

a	1	10	2	3	5	7
a^{-1}	1	10	6	4	9	8

Notice in this table we have chosen the representatives $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ to represent the nonzero congruence classes mod p. However, if we chose $\{-1, -2, -3, -4, -5, 1, 2, 3, 4, 5\}$, the table would be:

a	1	-1	2	3	5	-4
a^{-1}	1	-1	-5	4	-2	-3

Theorem 6.2. *A number a is equal to its own inverse mod p if and only if $a \equiv \pm 1 \bmod p$.*

Proof. Since $1^2 = (-1)^2 = 1$, we see that ± 1 are their own inverses. To see that there are no others, notice that $a^2 \equiv 1 \bmod p$ means that $a^2 - 1$ is a multiple of p. But then p must divide $(a+1)(a-1)$ meaning that p must divide either $a + 1$ or $a - 1$. Hence $a \equiv \pm 1 \bmod p$. □

Theorem 6.3. *[Chinese Remainder Theorem] Given $m_1, \ldots, m_k \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1 \quad (i \neq j)$ ("pairwise coprime"), and $a_1, \ldots, a_k \in \mathbb{Z}$, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

has a solution $x \in \mathbb{Z}$.

Proof. In fact x can be constructed explicitly. For $i = 1, \ldots, k$ define m_i^* to be the inverse modm_i of $m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$, so that

$$m_1 \ldots m_{i-1} m_i^* m_{i+1} \ldots m_k \equiv 1 \bmod m_i.$$

Then $x = \sum_{i=1}^k a_i m_1 \ldots m_{i-1} m_i^* m_{i+1} \ldots m_k \equiv a_i \bmod m_i$ for $i = 1, \ldots, k$, because every term except the ith is divisible by m_i. □

Remark 6.4. *Notice that if $n \in \mathbb{N}$ with $n = \prod_{i=1}^k p_i^{e_i}$ where p_i are distinct primes. Then $x \equiv a \bmod n$ is the unique solution to the system of congruences*

$$x \equiv a \bmod p_i^{e_i}, \quad i = 1, \ldots, k.$$

Indeed, $(x - a)$ is divisible by n if and only if it is divisible by $p_i^{e_i}$ for all i.

Then, if x_0 is one solution to this set of congruences, it's easy to see (how?) that the general solution is $x = x_0 + \ell m_1 \cdots m_k$ for any integer ℓ. In particular, there is always a choice of ℓ giving a unique solution x in the range $0 \leqslant x < m_1 \cdots m_k$ of the set of congruences.

6.1 Examples and Exercises

Example 6.5. *This example comes from the ancient Chinese puzzle (third century C.E.) in* **Master Sun's Mathematical Manual**. *Find a number that leaves a remainder 1 when divided by 3, a remainder of 2 when divided by 5 and a remainder of 3 when divided by 7.*

This system of equations is

$$x \equiv 1 \bmod 3$$
$$x \equiv 2 \bmod 5$$
$$x \equiv 3 \bmod 7.$$

We have $k = 3$ *equations, so following the solution in the theorem, we form all products of* $k - 1 = 2$ *moduli and compute inverses.*

$$(m_1) \equiv (5 \cdot 7)^{-1} \bmod 3$$
$$(m_2) \equiv (3 \cdot 7)^{-1} \bmod 5$$
$$(m_3) \equiv (3 \cdot 5)^{-1} \bmod 7$$

We can check that these numbers are $(m_1', m_2', m_3') = (2, 1, 1)$. *Hence*

$$x = (1) \cdot 2 \cdot 5 \cdot 7 + (2) \cdot 3 \cdot 1 \cdot 7 + (3) \cdot 3 \cdot 5 \cdot 1 = 70 + 42 + 45 = 157.$$

Is a solution. Furthermore, since $2 \cdot 5 \cdot 7 = 105$ *all solutions are of the form* $157 + 105n$. *In particular, the smallest positive solution is* $x = 52$.

There is also an iterative way to find a solution

Example 6.6.

$$x \equiv 1 \bmod 5$$
$$x \equiv 2 \bmod 6$$
$$x \equiv 3 \bmod 7.$$

The first equation says $x = 5t + 1$, *and hence the second says* $5t + 1 \equiv 2 \bmod 6$. *This is the same as*

$$5t \equiv 1 \bmod 6$$

we can multiply both sides by 5 *(the inverse of* 5*) to obtain*

$$t \equiv 5 \bmod 6\ .$$

Hence $t = 6s + 5$, *so that* $x = 30s + 26$. *Finally we substitute in to obtain*

$$30s + 26 \equiv 3 \bmod 7$$

$$2s \equiv 5 \bmod 7$$

$$s \equiv 6 \bmod 7.$$

Thus $s = 6$, *and* $x = 30(6) + 26 = 206$.

This second method allows an algorithm for solving systems of congruences even in the case when the m_i are not relatively prime (when a solution exists. See Exercises 15-20 in Rosen 4.3) For this course it is important to know the statement and proof of the Chinese Remainder Theorem. For solving practical problems, either method is acceptable.

Remark 6.7. *Notice that we can in fact solve any system of congruences of the form $ax = b \bmod m$ using the methods above, provided that a has an inverse mod m. The first step is just to multiply both sides of the congruence by a^{-1}.*

6.2 Exercises

1. Find all the solutions of

   - $$\begin{aligned} x &\equiv 4 \bmod 11 \\ x &\equiv 3 \bmod 17 \end{aligned}$$

   - $$\begin{aligned} x &\equiv 0 \bmod 2 \\ x &\equiv 0 \bmod 3 \\ x &\equiv 1 \bmod 5 \\ x &\equiv 6 \bmod 7. \end{aligned}$$

2. Show that if $(a, b) = 1$ and c is an integer, then there exists an integer n such that $(an + b, c) = 1$.

3. Solve the system:

   $$\begin{aligned} x &\equiv 4 \bmod 6 \\ x &\equiv 13 \bmod 15 \end{aligned}$$

   Note that the moduli are NOT relatively prime.

Main Points from Lecture 6:

- The inverse of a exists mod n if and only if $(a, n) = 1$.
- If $ax + ny = 1$ then x is the inverse of a mod n.
- Method and proof of the Chinese Remainder Theorem

7 Solving Polynomial Equations and Hensel's Lemma (12.10.2015)

Let's begin with a one sentence summary of what the Chinese Remainder Theorem says from last time:

> Knowing a number x mod N is equivalent to knowing x mod each of the prime powers $p_j^{e_j}$ in $N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

For example, knowing that $x \equiv 27 \bmod 30$ is the same as knowing

$$x \equiv 1 \bmod 2, \quad x \equiv 0 \bmod 3, \quad x \equiv 2 \bmod 5.$$

Example 7.1. *How many solutions $x \bmod pq$ does the equation $x^2 \equiv 1 \bmod pq$ have, where p and q are distinct odd primes?*

Solution: By the CRT we know that this is equivalent to finding solutions of the form $x^2 \equiv 1 \bmod p$ and $x^2 \equiv 1 \bmod q$. These each have exactly two solutions: $+1, -1$. (We are excluding the case $p = 2$ because in this case $1 = -1$). Hence in total there are four possible systems of congruences, so in total there are 4 solutions.

For example the square roots of 1 mod 77 are equal to $\{1, 34, 43, 76\}$

More generally, we can show that if $N = p_1 \cdots p_k$ is a product of distinct odd primes then $x^2 \equiv 1 \bmod N$ has 2^k distinct solutions mod N. We say that 1 has 2^k square roots.

This motivates a question: If we know $x \bmod p$, what can we say about $x \bmod p^2$?

Example 7.2. *Solve the polynomial congruence $2x^3 + 7x - 4 \equiv 0 \bmod 200$.*

Solution: Notice that $200 = 2^3 \cdot 5^2 = 8 \cdot 25$ This problem is equivalent to solving the system of equations

$$2x^3 + 7x - 4 \equiv 0 \bmod 8$$

$$2x^3 + 7x - 4 \equiv 0 \bmod 25.$$

We can check that $x \equiv 4 \bmod 8$ (just by trial and error) and later today we'll show that $x \equiv 16 \bmod 25$. These two linear equations combine by the CRT to show that the solution is $x \equiv 116 \mod 200$.

The CRT provides a very effective way of chopping up a problem into smaller pieces by turning the problem "Solve $f(x) \equiv 0 \mod n$" into a system of problems "Solve $f(x) \equiv 0 \bmod p_i^{e_i}$" if $n = \prod p_i^{e_i}$. In this section we will develop a method for solving polynomial equations of the form $f(x) = 0 \bmod p^e$.

Continuing the example, notice that to solve the equation $2x^3 + 7x - 4 \bmod 5$ we only need to test $0, 1, 2, 3, 4$. This is reasonably quick. And we see that all solutions satisfy $x \equiv 1 \bmod 5$. However, we'd like to avoid check all the numbers $0, \dots, 24$ to solve this equation mod 25. Notice that any solution x to

$$2x^3 + 7x - 4 \equiv 0 \bmod 25$$

is also a solution mod 5. Hence $x \equiv 1 \bmod 5$. Hence $x = 5t + 1$. Substituting we see that

$$2(5t+1)^3 + 7(5t+1) - 4 \equiv 0 \bmod 25$$

$$2(\cancel{(5t)^3} + \cancel{3 \cdot (5t)^2} + 3 \cdot 5t + 1) + 35t + 7 - 4 \equiv 0 \bmod 25.$$

$$2(3 \cdot 5t + 1) + 35t + 7 - 4 \equiv 0 \bmod 25.$$

$$65t + 5 \equiv 0 \bmod 25.$$

$$15t + 5 \equiv 0 \bmod 25.$$

(Notice that everything on the left was divisible by 5). We can eliminate a factor of 5 by Exercise 4.3.7. Hence

$$3t + 1 \equiv 0 \bmod 5.$$

which has $t \equiv 3 \bmod 5$ is its unique solution. Hence $x \equiv 16 \bmod 25$ is the unique solution to our original equation. We say that $x \equiv 16 \bmod 25$ is a "lift" of the solution $x \equiv 5 \bmod 5$.

Hensel's Lemma is a number theory version of Newton's calculus method of approximating a solution of a differential equation $f(x) = 0$ by using Taylor's theorem. If x_0 is an approximate solution with $f'(x_0) \neq 0$ then the graph $y = f(x)$ can be replaced near $(x_0, f(x_0))$ by the tangent line

$$y \; = \; f(x_0) + (x - x_0)f'(x_0) \; .$$

The tangent line intersects the x-axis $y = 0$ at

$$x_1 \; = \; x_0 - \frac{f(x_0)}{f'(x_0)}$$

which with luck is either a solution or at least a better approximate solution, meaning that either $f(x_1) = 0$ or $|f(x_1)| < |f(x_0)|$ with $f'(x_1) \neq 0$. Now proceed in this way, defining a sequence of ever better (hopefully!) approximations

$$x_{n+1} \; = \; x_n - \frac{f(x_n)}{f'(x_n)} \; (n = 0, 1, 2 \ldots) \qquad (*)$$

with the limit

$$x_\infty \; = \; \lim_n x_n$$

defined, and such that $f(x_\infty) = 0$. The number theory version is for a polynomial function

$$f(x) \; = \; \sum_{i=0}^{j} a_i x^i \; (a_i \in \mathbb{Z})$$

in which one seeks integer solutions $x \in \mathbb{Z}$ of $f(x) = 0 \in \mathbb{Z}$. The derivative is then again a polynomial function with integer coefficients

$$f'(x) \; = \; \sum_{i=1}^{n} i a_i x^{i-1} \; .$$

However, in number theory the passage from one approximation to another is rather more complicated than $(*)$, and proceeds mod prime powers p^k for each prime p separately, and $k = 1, 2, \ldots$. In the first instance, we only consider one prime p, and how to lift[7] a solution $r \bmod p^{k-1}$ to a solution $s \bmod p^k$, if possible.

Theorem 7.3. (Hensel's Lemma) *Suppose that $f(x)$ is a polynomial with integer coefficients and k is an integer with $k \geqslant 2$. Suppose further that $r \in \mathbb{Z}$ is a solution of the congruence $f(r) \equiv 0 \bmod p^{k-1}$. Then there are three possibilities for the number of solutions $s \bmod p^k$ of $f(s) \equiv 0 \bmod p^k$ which are lifts of $r \bmod p^{k-1}$. There are 1, p or 0 solutions, according to:*

1. *if $f'(r) \not\equiv 0 \bmod p$ there is a unique solution $s \bmod p^k$ of $f(s) \equiv 0 \bmod p^k$ lifting $r \bmod p^{k-1}$. There is a unique integer t $(0 \leqslant t \leqslant p-1)$ such that*

   $$t \equiv -f'(r)^*(f(r)/p^{k-1}) \bmod p$$

   where $f'(r)^*$ is the inverse of $f'(r)$ mod p. The unique solution is the mod p^k reduction $s = r + tp^{k-1} \in \mathbb{Z}$;

2. *if $f'(r) \equiv 0 \bmod p$ and $f(r) \equiv 0 \bmod p^k$, there are p solutions $s \bmod p^k$ of $f(s) \equiv 0 \bmod p^k$ lifting $r \bmod p^{k-1}$. The p solutions are the p lifts $s = r + tp^{k-1} \bmod p^k$ $(0 \leqslant t \leqslant p-1)$ of $r \bmod p^{k-1}$;*

3. *if $f'(r) \equiv 0 \bmod p$ and $f(r) \not\equiv 0 \bmod p^k$, then there are no solutions, i.e. there is no $s \in \mathbb{Z}$ such that $f(s) \equiv 0 \bmod p^k$ and $s \bmod p^k$ is a lift of $r \bmod p^{k-1}$.*

Example 7.4.

1. *Let $p = 2$, $f(x) = x + 1$, so that $r = 1 \in \mathbb{Z}$ is a solution of $f(r) \equiv 0 \bmod 2$, with $f(r) = 2 \in \mathbb{Z}$, $f'(r) = 1 \not\equiv 0 \bmod 2$. Then $t = 1$ is the unique integer with $0 \leqslant t < 2$ such that*

   $$t \equiv -f'(1)^*(f(1)/2) \bmod 2$$

   and $s = 1 + 2 = 3 \bmod 4$ is the unique solution of $f(s) \equiv 0 \bmod 4$ lifting $1 \bmod 2$.

2. *Let $p = 2$, $f(x) = x^2 - 1$, so that $r = 1 \in \mathbb{Z}$ is a solution of $f(r) \equiv 0 \bmod 2$, with $f(r) = 0 \in \mathbb{Z}$, $f(r) \equiv 0 \bmod 4$, $f'(r) \equiv 0 \bmod 2$. Then for any integer $t \in \mathbb{Z}$ $s = 2t + 1 \in \mathbb{Z}$ is such that $f(s) \equiv 0 \bmod 4$ and $s \bmod 4$ is a lift of $1 \bmod 2$. There are two solutions $s \bmod 4$ of $f(s) \equiv 0 \bmod 4$ lifting $r \equiv 1 \bmod 2$, namely $s \equiv 1 \bmod 4$ and $s \equiv 3 \bmod 4$.*

3. *Let $p = 2$, $f(x) = x^2 + 1$, so that $r = 1 \in \mathbb{Z}$ is a solution of $f(r) \equiv 0 \bmod 2$, with $f(r) = 2 \in \mathbb{Z}$, $f(r) \not\equiv 0 \bmod 4$, $f'(r) \equiv 0 \bmod 2$. There is no solution $s \in \mathbb{Z}$ of $f(s) \equiv 0 \bmod 4$, let alone one which lifts $1 \bmod 2$.*

The Wikipedia article on Hensel's Lemma is recommended as background reading.

[7] By definition, $s \bmod p^k$ is a **lift** of $r \bmod p^{k-1}$ if r is the reduction of s. Every $r \bmod p^{k-1}$ has p lifts $s = s_0 + tp^{k-1} \bmod p^k$ $(0 \leqslant t \leqslant p-1)$, with $s_0 \bmod p^k$ any one lift.

7.1 A fireside Chat With Hensel's Lemma

It's fair to say that the statement of Hensel's Lemma is a bit intimidating - but that doesn't mean that the concept is difficult. Hopefully the following chat between Hensel's Lemma and some guy named Earle will help with the concept.

Earle: So what's the deal with you, anyway?

HL: Well, I provide a method of telling how many solutions you have mod p^2 given solutions mod p.

Earle: Is that it?

HL: Well, I can inductively be used to find solutions mod p^3, p^4, and on and on. In an advanced course, you might wonder if there's a limit term at p^∞, and the answer is YES, and that concerns the p-adics and ...

Earle: Whoa, let's worry about that in the advanced course. So tell me, in layman's terms what your lemma does.

HL: Well suppose you've got a polynomial, and all you know is the following table of numbers

x	0	1	2	3	4
$f(x)$	10	1	6	-7	25

Then what are the solutions to $f(x) \equiv 0 \bmod 5$?

Earle: Well you just have to check the equivalence classes, so it looks like $x \equiv 0$ and $x \equiv 4$ are the only solutions.

HL: Good. Now what can you say about the solutions to $f(x) \equiv 0 \bmod 25$?

Earle: Well I don't know. I mean I know that x has to be 0 or 4 mod 5. So that means x has to be either $0, 5, 10, 15, 20$ or $4, 9, 14, 19, 24$.

HL: Do you know anything else?

Earle: Well from the given information I guess I know that $f(4) = 25$ so $f(4) \equiv 0 \bmod 25$. So that's one solution. And I know that $f(0) = 10$ so 0 is NOT a solution mod 25.

HL: Good. That's really all you can say. But now what if I told you that $f'(0) = 2$?

Earle: Oh, then the theorem says that $f(x) \equiv 0 \bmod 25$ should have a unique solution... or something, right? But I don't remember the formula, there's a t and a $r + tp^{k-1}$ blech.

HL: Mostly right. It says that there is a unique solution with x congruent to 0 mod 5. So only one of the numbers $0, 5, 10, 15, 20$ is going to be a solution. And check out Corollary 8.3 for a more convenient way to work. This wasn't written on the board during class, but it's very helpful. It says that a solution mod 25 will just be given by

$$r_2 = r - f'(r)^* f(r)$$

In other words, take the root from the previous step and then subtract off a correction term.

Earle: This is like Newton's method, isn't it?

HL: It is indeed! So

$$r_2 = 0 - ((2)^*)(10)$$

Earle: Wait a second, when you take the inverse of 2, is that mod 5 or mod 25?

HL: Well it turns out that it won't matter, but in the statement of the lemma, this inverse business is ALWAYS just mod p. So yea, you just want the inverse mod 5.

Earle: Ok, so $r_2 = 0 - (3)(10) = -30$ which is -5 mod 25 which is 20 mod 25. Pretty cool. I don't even have to check those other candidates among $0, 5, 10, 15, 20$. I know that 20 has got to be the solution.

HL: Ok, now what if I told you that $f'(4) = 0$.

Earle: Oh that'd be a sad day.

HL: Not so much. My Theorem says that if $f'(4)$ is zero - then either ALL of the lifts of 4 are solutions, or NONE of the lifts are solutions.

Earle: Oh, so I could just check one to see whether or not it was a solution.

HL: Yea, and you may as well just check 4 itself.

Earle: Ok $f(4) = 25 \equiv 0$ mod 25 so that means we have one solution, so they must all be solutions! So all of $4, 9, 14, 19, 24$ are solutions.

HL: Yep. And summing up, that means that 20 and $4, 9, 14, 19, 24$ are the solutions mod 25.

Earle: That was pretty easy. Can we do another step?

HL: Sure. To lift that 0 mod 5 solution we can just do another round of that formula:

$$r_3 = r_2 - f'(r)^*(f(r_2))$$

where r was the original solution mod 5.

Earle: Wait wait, this is the part that really confuses me. First of all didn't you mean to put an r_2 into that $f'(r)^*$ term?

HL: Well I could have, but it won't make a difference. Remember, r_2 and r are the same mod 5. So that means that $f'(r)$ and $f'(r_2)$ are the same mod 5. And since we take our inverses mod 5, this is all that matters.

Earle: Oh ok. Ohhh so that inverse term... it's gonna be 3 again, cause at every step I'm just applying $f'(0)^*$? So

$$r_3 = 20 - 3f(20)$$

HL: Looks good to me.

This concludes our fireside chat with Hensel's Lemma. I hope this has been helpful.

Main Points from Lecture 7:

- How to apply the Chinese Remainder Theorem to solving equations mod N via factorization.
- The statement and application of Hensel's Lemma.

8 The Proof of Hensel's Lemma and Example (15.10.2015)

To prove Hensel's Lemma we will need the following Integrality Lemma on the Taylor series of a polynomial with integer coefficients. Notice that this Taylor series is finite since the derivatives of a polynomial are eventually all zero. Indeed, if $f(x)$ is a polynomial of degree n then the $(n+1)$-st derivative $f^{(n+1)}(x)$ is always zero. Furthermore, the converse is true: if a differentiable function $f : \mathbb{R} \to \mathbb{R}$ is such that $f^{(n+1)}(x) = 0$ for all $x \in \mathbb{R}$ then f is a degree n polynomial with real coefficients. This being a course on number theory we are only concerned with functions $f : \mathbb{Z} \to \mathbb{Z}$, and polynomials with integer coefficients.

Lemma 8.1. *(Integrality Lemma) If $f(x)$ is a polynomial of degree n with integer coefficients then*

$$f(a+b) \;=\; f(a) + f'(a)b + \frac{f''(a)}{2!}b^2 + \cdots + \frac{f^{(n)}(a)}{n!}b^n$$

where the coefficients $f(a), f'(a), \dfrac{f''(a)}{2!}, \dots, \dfrac{f^{(n)}(a)}{n!}$ *are polynomials in* a *with integer coefficients.*

Proof. All but the integrality of the coefficients follows from the Taylor expansion about the point $x = a$. To see that the coefficients are integers consider first the special case of a degree m 'monomial' $f(x) = x^m$, when

$$\frac{f^{(k)}(a)}{k!} = \begin{cases} \dfrac{m(m-1)\dots(m-k+1)}{k!}x^{m-k} = \dbinom{m}{k}x^{m-k} & \text{if } 0 \leqslant k \leqslant m \\ 0 & \text{if } k > m \ . \end{cases}$$

For the general case of a degree n polynomial

$$f(x) = \sum_{m=0}^{n} c_m x^m \ (c_m \in \mathbb{Z})$$

we have

$$\frac{f^{(k)}(a)}{k!} = \sum_{m=0}^{n} c_m \binom{m}{k} x^{m-k} \ (\text{with } x^{m-k} = 0 \text{ if } k > m) \ .$$

□

Example 8.2. *For a cubic polynomial with integer coefficients*

$$f(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 \ (c_0, c_1, c_2, c_3 \in \mathbb{Z})$$

and any $a, b \in \mathbb{Z}$

$$\begin{aligned} f(a+b) &= c_0 + c_1(a+b) + c_2(a+b)^2 + c_3(a+b)^3 \\ &= (c_0 + c_1 a + c_2 a^2 + c_3 a^3) + (c_1 + 2c_2 a + 3c_3 a^2)b + (c_2 + 3c_3 a)b^2 + c_3 b^3 \\ &= f(a) + f'(a)b + \frac{f''(a)}{2!}b^2 + \frac{f'''(a)}{3!}b^3 \end{aligned}$$

with

$$f(a) = c_0 + c_1 a + c_2 a^2 + c_3 a^3 \ , \ f'(a) = c_1 + 2c_2 a + 3c_3 a^2 \ ,$$
$$\frac{f''(a)}{2!} = c_2 + 3c_3 a \ , \ \frac{f'''(a)}{3!} = c_3$$

polynomials in a *with integer coefficients.*

Proof of Hensel's Lemma. Recall that we are assuming that r is a solution of $f(r) \equiv 0 \bmod p^{k-1}$. We seek solutions mod p^k that are congruent to r mod p^{k-1}. In other words, we are looking for solutions mod p^k of the form $s = r + tp^{k-1}$. We will seek precise conditions for t. Notice that the Integrality Lemma 8.1 says

$$f(r + tp^{k-1}) = f(r) + f'(r)tp^{k-1} + \frac{f''(r)}{2!}t^2 p^{2k-2} + \cdots$$

with integer coefficients $\dfrac{f^{(k)}(r)}{k!}$. Notice that all terms but the first two are zero mod p^k (since $k \geqslant 2$). Hence

$$f(r + tp^{k-1}) \equiv f(r) + f'(r)tp^{k-1} \bmod p^k.$$

Since we are assuming $r + tp^{k-1}$ is a solution mod p^k the left hand side is zero and we can conclude that

$$f'(r)tp^{k-1} \equiv -f(r) \bmod p^k.$$

But we are assuming that $f(r) \equiv 0 \bmod p^{k-1}$ so dividing the equation

$$f'(r)tp^{k-1} \;=\; -f(r) + np^k \in \mathbb{Z} \text{ (for some } n \in \mathbb{Z})$$

by p^{k-1} we see that

$$f'(r)t \equiv -f(r)/p^{k-1} \bmod p\ .$$

Now we just examine cases. If $f'(r)$ is nonzero mod p then this equation must have a unique solution for t

$$t \equiv -f'(r)^* f(r)/p^{k-1} \bmod p$$

where the * denotes inverse mod p. This establishes part 1. of Hensel's Lemma.

So suppose that $f'(r) \equiv 0 \bmod p$. Then the equation is of the form

$$0t \equiv -f(r)/p^{k-1} \bmod p.$$

If the right hand side is nonzero, this has no solutions. If the right hand side is zero, then any value of t gives a solution, proving 2. And if the right hand side is non-zero, then no value of t gives a solution, proving 3. □

One Corollary of Hensel's Lemma provides a particularly easy method for computing "lifts" of solutions mod p.

Corollary 8.3. *Suppose that r is a solution to $f(r) \equiv 0 \bmod p$ where p is prime. If $f'(r) \neq 0 \bmod p$ then there is a unique solution r_k mod p^k for each $k = 2, 3, \ldots$ such that*

$$r_k = r_{k-1} - f(r_{k-1})f'(r)^*.$$

where $f'(r)^*$ is the inverse of $f'(r)$ mod p.

Proof. We see from the hypotheses of Hensel's lemma that we are in Case 1. Hence r lifts to a unique solution r_2 mod p^2 with $r_2 = r + tp$ with $t = -f'(r)^*(f(r)/p)$ mod p. Hence

$$r_2 \;=\; r - f'(r)^*(f(r)) \bmod p^2\ .$$

It follows from $f(r) \equiv 0 \bmod p$ that $r_2 \equiv r \bmod p$, and hence that

$$f'(r_2) \equiv f'(r) \not\equiv 0 \bmod p\ .$$

Using Hensel's Lemma again, we see that the unique solution mod p^3 is then

$$r_3 \equiv r_2 - f(r_2)f'(r)^* \bmod p^3\ .$$

Continuing this way we see that we can obtain solutions mod p^k for all k. □

Example 8.4. *Find the solutions of*

$$x^3 + x^2 + 29 \equiv 0 \bmod 25.$$

Solution: Let $f(x) = x^3 + x^2 + 29$*. Then the solutions mod* 5 *are* $x \equiv 3 \bmod 5$*. Since* $f'(x) = 3x^2 + 2x$*, we have* $f'(3) \equiv 3 \neq 0$ *mod* p*. Also* $f(3) = 15$ *Hence the unique solution mod* 25 *is*

$$r_2 \equiv 3 - 15(3)^{-1} \equiv 3 - 15(2) \equiv -27 \equiv 23$$

is the unique solution mod 25*.*

I have posted in the "Background material" directory of LEARN a scan of Section 4.4 of Rosen's **Elementary Number Theory and Its Applications** which has a few more examples worked out in detail.

8.1 Exercises

1. Find all solutions to $x^2 + 4x + 2 = 0 \bmod 7^3$.
2. Find all solutions to $x^2 + x + 34 = 0 \bmod 81$.
3. How many incongruent solutions are there to $x^5 + x - 6 \equiv 0 \bmod 144$?

Main Points from Lecture 8:

- The method and proof of Hensel's Lemma.

9 The finite field $\mathbb{F}_p$ (19.10.2015)

For the next two weeks we will be studying in detail the integers mod p, where p is prime. The set of congruence classes mod p forms a field, which we now review:

9.1 Fields

A **field** F is a set supplied with two binary operations '+' and '×' (i.e., maps from $F \times F$ to F), and containing special elements 0 and 1 such that

- F is an abelian group under + (meaning that $a + b = b + a \in F$ for all $a, b \in F$), with 0 as its identity element, and $-a$ as the (additive) inverse of $a \in F$;
- $F^\times = F \setminus \{0\}$ is an abelian group under $\times$, with 1 as the identity element, and a^{-1} the (multiplicative) inverse of $a \in F^\times$;

- The Distributive Law holds: for all $a, b, c \in F$ we have
$$a \times (b + c) = a \times b + a \times c.$$
This describes how + and × interact in F.

As a consequence of these rules, we can show (won't prove)

Proposition 9.1. *For $a, b \in F$ we have*

- $a \times 0 = 0$*;*
- $a \times (-b) = -(a \times b)$*;*
- *Cancellation Law: if $a \times b = 0$ then $a = 0$ or $b = 0$ (or both).*

Examples of fields are: the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, and the finite fields $\mathbb{F}_p$ for p prime – see below.

9.1.1 Construction of $\mathbb{F}_p$

Start with the integers $\mathbb{Z}$ and a prime p, and define an equivalence relation on $\mathbb{Z}$ by saying that two integers a and b are equivalent if $a \equiv b \bmod p$. This defines an equivalence relation on $\mathbb{Z}$. The elements of $\mathbb{F}_p$ are the equivalence classes under this relation. Taking equivalence class representatives to be $0, 1, 2, 3, \ldots, p-1$, we can effectively regard $\mathbb{F}_p$ as the set $\{0, 1, 2, 3, \ldots, p-1\}$. Addition, negation, multiplication and reciprocals are performed mod p, so that the result can always be chosen to be in $\{0, 1, 2, 3, \ldots, p-1\}$.

For example, in $\mathbb{F}_7$, $3 + 4 = 0$ as in $\mathbb{Z}$ we have $3 + 4 = 7 \equiv 0 \bmod 7$. Hence also $-3 = 4$ and $-4 = 3$ in $\mathbb{F}_7$. Further, because $3 \times 5 = 15 \equiv 1 \bmod 7$, we have $3^{-1} = 5$ and $5^{-1} = 3$ in $\mathbb{F}_7$.

9.2 Solving equations in $\mathbb{F}_p$

For any field F let $F[x]$ be the set of polynomials $f(x) = \sum\limits_{i=0}^{m} a_i x^i$ in x with coefficients $a_i \in F$, for variable $m \geqslant 0$. The set $F[x]$ has both addition and multiplication

$$\begin{aligned}
+ \ :\ F[x] \times F[x] \to F[x] \ ;\ (f(x), g(x)) &= (\sum_{i=0}^{m} a_i x^i, \sum_{j=0}^{n} a_j x^j) \\
\mapsto f(x) + g(x) = (f+g)(x) &= \sum_{k=0}^{\max(m,n)} (a_k + b_k) x^k \ , \\
.\ :\ F[x] \times F[x] \to F[x] \ ;\ (f(x), g(x)) &= (\sum_{i=0}^{m} a_i x^i, \sum_{j=0}^{n} a_j x^j) \\
\mapsto f(x)g(x) = (fg)(x) &= \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} \ .
\end{aligned}$$

but not division. ($F[x]$ is a 'ring' which is not a field). The **degree** of a polynomial $f(x) = \sum_{i=0}^{m} a_i x^i$ is

$$\text{degree}(f(x)) \;=\; \text{the largest } i \leqslant m \text{ such that } a_i \neq 0 \in F \ .$$

Note that

$$\begin{aligned} \text{degree}(f(x)+g(x)) &\leqslant \max(\text{degree}(f(x)), \text{degree}(g(x))) \ , \\ \text{degree}(f(x)g(x)) &= \text{degree}(f(x)) + \text{degree}(g(x)) \ . \end{aligned}$$

We now restrict our congruences to a prime modulus p, and consider the solutions of equations $f(x) = 0$ for $f(x) \in \mathbb{F}_p[x]$ and $x \in \mathbb{F}_p$. This is equivalent, for $f(x) \in \mathbb{Z}[x]$, of solving $f(x) \equiv 0 \bmod p$ for $x \in \{0, 1, 2, \ldots, p-1\}$.

Theorem 9.2. *A nonzero polynomial $f \in \mathbb{F}_p[x]$ of degree n has at most n roots x in $\mathbb{F}_p$.*

Proof. Use induction: for $n = 1$, $f(x) = ax + b$ say, with $a \neq 0$, whence $f(x) = 0$ has a solution $x = -a^{-1}b$ in $\mathbb{F}_p$.

Now assume $n \geqslant 1$ and that the result holds for n. Take $f(x) \in \mathbb{F}_p[x]$ of degree $n+1$. If $f = 0$ has no roots $x \in \mathbb{F}_p$ the result is certainly true. Otherwise, suppose $f(b) = 0$ for some $b \in \mathbb{F}_p$. Now divide $x - b$ into $f(x)$, (i.e., one step of the Euclidean algorithm for polynomials) to get $f(x) = (x-b)f_1(x) + r$ say, where f_1 is of degree n, and $r \in \mathbb{F}_p$. Putting $x = b$ shows that $r = 0$. Hence $f(x) = (x-b)f_1(x)$, where f_1 has, by the induction hypothesis, at most n roots $x \in \mathbb{F}_p$. So f has at most $n+1$ roots $x \in \mathbb{F}_p$, namely b and those of $f_1 = 0$. Hence the result is true for $n+1$ and so, by induction, true for all $n \geqslant 1$. □

Note that the proof, and hence the result, holds equally well when $\mathbb{F}_p$ is replaced by **any** field F.

Question. Where in the above proof was the fact that we were working over a field used? There were two places. Once in the base case when $n = 1$ and then once again when we concluded that if $(x-b)f_1(x) = 0$ then either one of the factors must equal zero.

Remark 9.3. *Note that this theorem is not true if we work mod a composite number. For instance, the polynomial $x^2 - 1$ has 4 roots mod 15. It's instructive to really think the above proof through using this polynomial to see where it breaks down. Notice also that*

$$x^2 - 1 = (x-1)(x+1) = (x-4)(x+4)$$

has two different factorizations!

9.3 Some Special Congruences - Wilson's Theorem and Fermat's Theorem

We now prove some special congruences that will be useful for the rest of the course.

Theorem 9.4 (Wilson's Theorem). *If p is prime then $(p-1)! \equiv -1 \bmod p$.*

Proof. Recall that by Theorem 6.2 the only numbers that are their own inverse mod p are 1 and $p-1$. Hence if we rearrange the terms

$$(p-1)! = 1 \cdot 2 \cdots (p-1) = 1 \cdot (p-1) \cdot (2 \cdot 2^{-1}) \cdots (a \cdot a^{-1})$$

where on the right we have paired each number a with its inverse. It's clear that this product is equal to $(p-1) \cdot (1 \cdots 1) \equiv -1 \bmod p$. □

Theorem 9.5. *[Fermat's Little Theorem] If p is a prime then for all integers a, $a^p \equiv a \bmod p$. If further, $a \not\equiv 0 \bmod p$ then $a^{p-1} \equiv 1 \bmod p$.*

Proof. Notice that the second statement follows from the first by multiplying both sides by a^{-1} (which exists if and only if $a \not\equiv 0 \bmod p$.) To prove the first statement we argue by induction. Clearly the statement if true if $a = 0$. Now notice that by the binomial theorem

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

Recall that $\binom{p}{k}$ is divisible by p for $1 \leqslant k \leqslant p-1$ (Why?). Hence

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

Now by induction we have

$$(a+1)^p \equiv a + 1.$$

This proves the result for all positive integers, and since this is a statement about congruences, this takes care of all the equivalence classes (including the class of negative ones). □

In class, we used Fermat's Theorem to provide another proof of Wilson's Theorem. See if you can fill in the details! The rough outline is that Fermat's Theorem says that each nonzero element of $\mathbb{F}_p$ is a solution to the equation $x^{p-1} - 1 = 0$. Now use the fact that you've found $p-1$ roots of this equation, and a little factorization to finish the job!

Main Points from Lecture 9:

- Definition and basic properties of a field
- Definition of $\mathbb{F}_p$
- The number of roots in $\mathbb{F}_p$ of a polynomial of degree n is at most n
- Statement and two proofs of Wilson's Theorem
- Statement (and your favorite proof) of Fermat's Little Theorem

10 Primitive Roots and the Structure of $\mathbb{F}_p$ (22.10.2015)

10.1 A Warmup for Things to Come:

We start today with defining the**Euler φ-function**: this is is the number of positive integers not exceeding n that are coprime to n

$$\varphi(n) \;=\; \text{the number of } a \text{ such that } 1 \leqslant a \leqslant n \text{ and greatest common divisor } (a, n) = 1\ .$$

Example 10.1. *The values of $\varphi(n)$ of the numbers n with $1 \leqslant n \leqslant 12$.*

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

We will study this function in more detail next week, but for today we note one beautiful property of φ:

Theorem 10.2. *If $n \in \mathbb{N}$ then*

$$\sum_{d|n} \varphi(d) = n.$$

Proof. This proof is pretty intuitive. We want to show that a sum of a bunch of numbers is equal to n. A good way to show something like this is to establish a bijection between the numbers $\{1, \ldots, n\}$ and the things you are trying to count. For us, we are going to do the following: To each integer $1 \leqslant a \leqslant n$, compute (a, n). This is certainly some number d that divides n. Now the following equation is obvious:

$$\sum_{d|n} \#\{a \mid (a, n) = d\} \;=\; n$$

Indeed, every number from 1 to n appears in exactly one of the sets. On the other hand, it's easy to see that

$$\#\{a \mid (a, n) = d\} \;=\; \varphi(n/d)$$

since if $(a, n) = d$ then $(a/d, n/d) = 1$. (Conversely, if $(b, n/d) = 1$ then $(bd, n) = d$.) Therefore:

$$n \;=\; \sum_{d|n} \varphi(n/d).$$

Now whether we sum $\varphi(d)$ or $\varphi(n/d)$ we should get the same thing. □

This is one of those proofs for which working through it with an example in mind is very helpful.

Example 10.3. *In this table for each divisor $d|12$ the second row groups together all the numbers $1 \leqslant a \leqslant 12$ with greatest common divisor d:*

d	1	2	3	4	6	12
a	$1,5,7,11$	$2,10$	$3,9$	$4,8$	6	12
$12/d$	12	6	4	3	2	1
$\varphi(12/d)$	4	2	2	2	1	1

Each $a = 1, 2, \ldots, 12$ appears exactly once in the second row, verifying that

$$\sum_{d|12} \#\{a \mid (a,12) = d\} \ = \ 12 \ .$$

The numbers in the fourth row are the number of elements in the corresponding entry of the second row, verifying that

$$\#\{a \mid (a,12) = d\} \ = \ \#\{a/d \mid (a/d, 12/d) = 1\} \ = \ \varphi(12/d) \ ,$$

and hence that

$$\sum_{d|12} \varphi(12/d) \ = \ 12 \ .$$

10.2 $\mathbb{F}_p$ and its groups under + and ×

We are now going to explore the structure of the field $\mathbb{F}_p$, using the rudiments of group theory. Only cyclic groups are actually required.

Recall:

Definition 10.4. *A* **group** *G is a set with a product operation*

$$G \times G \to G \ ; \ (g,h) \mapsto gh$$

and an identity element $1 \in G$ such that

- *the product is associative $(gh)i = g(hi) \in G$ for all $g, h, i \in G$,*
- *$g1 = 1g = g \in G$ for each $g \in G$,*
- *for each $g \in G$ there exists an inverse $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1 \in G$.*

Definition 10.5. *A group G is* **abelian** *if $gh = gh \in G$ for all $g, h \in G$.*

In fact, we shall only need to consider abelian groups in this course.

Definition 10.6. *Let G be a group. We say that an element $g \in G$* **generates** *G if the set of powers of g and g^{-1} is equal to all of G. If such a g exists, we say that G is* **cyclic** *and we write $G = \langle g \rangle$.*

Note that a cyclic group G is necessarily abelian, since for any $m, n \in \mathbb{Z}$

$$g^m g^n = g^{m+n} = g^n g^m \in G .$$

Definition 10.7. *If $g \in G$, we say that the* **order** *of g is the smallest positive integer n such that $g^n = 1$, or infinity if $g^n \neq 1$ for all $n \geqslant 1$.*

Example 10.8. (i) *The integers $\mathbb{Z}$ with respect to addition are an infinite cyclic group, with identity $0 \in \mathbb{Z}$. The generator $1 \in \mathbb{Z}$ has infinite order.*
(ii) *For any $n \geqslant 1$ the integers mod n with respect to addition are a finite cyclic group $\mathbb{Z}_n$, with identity $0 \in \mathbb{Z}_n$. The generator $1 \in \mathbb{Z}_n$ has order n.*

There is a close connection between the order of a group element and the greatest common divisor in number theory:

Proposition 10.9. *For any group G, if $g \in G$ has order n than $g^k \in G$ has order $n/(n,k)$*

Proof. The first value of $j = 1, 2, 3, \ldots$ such that $(g^k)^j = 1 \in G$ is also the first value of j such that $n \mid kj$, and this is $j = n/(n,k)$. □

A finite group G is cyclic if and only if there is an element $g \in G$ with order equal to the number of elements in G.

Notice that by definition, in a field F there are two groups: the additive group $(F, +)$, with 0 as the identity element, and the multiplicative group $(F^\times, \times)$, with $F^\times = F\backslash\{0\}$ and 1 as the identity element.

For the finite field $\mathbb{F}_p$ the additive group $(\mathbb{F}_p, +)$ is fairly simple to describe. It is a cyclic group of order p, with every non-zero element a generator. The multiplicative group $(\mathbb{F}_p^\times, \times)$ is also cyclic (as proved in the next section), but of order $p-1$, and only some non-identity elements are generators. **Note the essential difference between the orders of elements in the additive and multiplicative groups**. In the workshop you will work out several examples to determine the number of elements of each possible order in $(\mathbb{F}_p, +)$ and $(\mathbb{F}_p^\times, \times)$. Here are some examples.

Some orders of elements in $(\mathbb{F}_7, +)$ and $(\mathbb{F}_7^\times, \times)$

n	0	1	2	3	4	5	6
order under +	1	7	7	7	7	7	7

,

n	1	2	3	4	5	6
order under ×	1	3	6	3	6	2

Some orders of elements in $(\mathbb{F}_{11}, +)$ and $(\mathbb{F}_{11}^\times, \times)$

n	0	1	2	3	4	5	6	7	8	9	10
order under +	1	11	11	11	11	11	11	11	11	11	11

n	1	2	3	4	5	6	7	8	9	10
order under ×	1	10	5	5	5	10	10	10	5	2

Some orders of elements in $(\mathbb{F}_{13}, +)$ and $(\mathbb{F}_{13}^{\times}, \times)$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
order under +	1	13	13	13	13	13	13	13	13	13	13	13	13

n	1	2	3	4	5	6	7	8	9	10	11	12
order under ×	1	12	3	6	4	12	12	4	3	6	12	2

Hopefully the pattern in the table for the operation + is clear. As an exercise, prove that if p is prime, then the order (under plus) of an element $1 \leqslant a \leqslant p-1$ is precisely equal to p. However, under × the situation is clearly a bit more subtle. In these examples, it's true that there is an element of order $p-1$ in each case.

10.3 $\mathbb{F}_p^{\times}$ is cyclic!

As before, we denote the group of nonzero elements of $\mathbb{F}_p$ by $\mathbb{F}_p^{\times}$. We now state the rather surprising fact:

Theorem 10.10. *$\mathbb{F}_p^{\times}$ is a finite cyclic group of order $p-1$.*

Definition 10.11. *We call an element $x \in \mathbb{F}_p^{\times}$ a* **primitive root** *if x is a generator for $\mathbb{F}_p^{\times}$. In other words, if $x, x^2, x^3, \ldots, x^{p-1}$ are all distinct numbers mod p. We may also say that x is a primitive root mod p.*

It is easy to see that an element x is primitive if and only if its order is equal to $p-1$.

For example, if $p = 7$ then we could try a few numbers:

$$\langle 1 \rangle = \{1, 1^2, 1^3, \ldots, \} = \{1\}$$

$$\langle 2 \rangle = \{2, 2^2, 2^3\} = \{1, 2, 4\}$$

$$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{1, 2, 3, 4, 5, 6\}$$

So 3 is a generator for the multiplicative group $\mathbb{F}_p^{\times}$ when $p = 7$. However, the numbers 1 and 2 failed to generate everything.

As the example above indicates, 3 is a primitive root mod 7. As another example, if $p = 23$ then 5 is the smallest positive integer which is a primitive root. As we'll see, the theory of these roots can be quite mysterious. The following lemma will be useful:

Lemma 10.12. *Let G be a group and $g \in G$. If for integers m, n, we have $g^m = 1$ and $g^n = 1$ then $g^{\gcd(m,n)} = 1$.*

Proof. Note that since g^{-1} exists, it makes sense to talk about both positive at negative powers of g. Thus since $\gcd(m,n)$ can be written as $mx + ny = \gcd(m,n)$, we see that

$$a^{\gcd(m,n)} = (a^m)^x \cdot (a^n)^y = 1.$$

□

Lemma 10.13. *Let G be a finite group, of cardinality N. For every $g \in G$ the order of g divides N.*

Proof. $g^N = 1$ by an application of the Lagrange theorem that the cardinality of a subgroup of G (in this case the cyclic subgroup generated by g) divides the cardinality of G. Let m denote the order of g, so that $g^m = 1$. Suppose that m does not divide N. Then $\gcd(m, N) < m$. But then by Lemma 10.12 $g^{\gcd(m,N)} = 1$. This is a contradiction since we assumed that m was the smallest positive integer k such that $g^k = 1$. □

Let $N(d)$ denote the number of elements of order d in $\mathbb{F}_p^\times$. Since $|\mathbb{F}_p^\times| = \varphi(p) = p-1$, by Lemma 10.13 $N(d) = 0$ unless $d \mid p-1$. Let's go back to the table above with $p = 13$. For each $d \mid p-1 = 12$ we see that we have

$$N(12) = 4,\ N(6) = 2,\ N(4) = 2,\ N(3) = 2,\ N(2) = 1,\ N(1) = 1\ .$$

These values are exactly the same as the values of the Euler φ function!

Theorem 10.14. *For any prime p and $d \in \mathbb{N}$*

$$N(d) = \begin{cases} \varphi(d) & \textit{if } d \mid p-1 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We assume $d \mid p-1$, and proceed in two steps. First we will show that $N(d) \leqslant \varphi(d)$.

Let's do it! If $N(d) = 0$ there is nothing to prove, since $\varphi(d) \geqslant 0$. If $N(d) > 0$ there is some element $a \in \mathbb{F}_p^\times$ of order d. In other words, the elements

$$\{a, a^2, a^3, \ldots, a^d = 1\}$$

are all distinct in $\mathbb{F}_p^\times$. The equation $x^d = 1 \in \mathbb{F}_p^\times$ thus has exactly d roots, namely $a, a^2, \ldots, a^d$. (Recall from Theorem 9.2 that a degree d polynomial can have at most d roots). By Proposition 10.9 a^k has order $d/(k,d)$, so that a^k has order d if and only if $(k,d) = 1$.

Thus we have shown that the elements of order d in $\mathbb{F}_p^\times$ are precisely those elements a^k with $(k,d) = 1$. In other words, there are $\varphi(d)$ of them. (Remark: We have shown that if $N(d) > 0$ then $N(d) = \varphi(d)$. This is nice, but unfortunately doesn't help with the proof since we use different means from here onwards).

We are now ready for the second step. Showing that $N(d) = \varphi(d)$. We will use the fact that $N(d) \leqslant \varphi(d)$. Notice that every element in $\mathbb{F}_p^\times$ has some order. And there are $p-1$ elements. And the order of elements must divide $p-1$. Thus

$$p - 1 = \sum_{d \mid p-1} N(d)$$

And by Step 1, we have

$$p - 1 \leqslant \sum_{d \mid p-1} \varphi(d)$$

But now by Theorem 10.2, we know that the right hand side is $p-1$. But this must mean that the inequality $\leqslant$ is actually an equality. So this means that $N(d) = \varphi(d)$ for all $d \mid p-1$. □

Proof of Theorem 10.10. Since p is prime $N(p-1) = \varphi(p-1) > 0$, so that there exists a primitive root $x \in \mathbb{F}_p^\times$, i.e. an element of order $p-1$. Thus $\mathbb{F}_p^\times$ is cyclic, with generator x. □

The special case $d = p-1$ of Theorem 10.14 gives that $\mathbb{F}_p^\times$ has exactly $N(p-1) = \varphi(p-1)$ primitive roots. Here are some examples:

- $\mathbb{F}_7$ has $\varphi(6) = 2$ primitive roots, namely 3,5.
- $\mathbb{F}_{11}$ has $\varphi(10) = 4$ primitive roots, namely 2,6,7,8.
- $\mathbb{F}_{13}$ has $\varphi(12) = 4$ primitive roots, namely 2,6,7,11

10.4 Taking nth roots in $\mathbb{F}_p^\times$

Take an odd prime p and g a fixed primitive root $\bmod p$. Then for any $B \in \mathbb{F}_p^\times$ we define the **index** (old-fashioned word) or **discrete logarithm** (current jargon) of B, written $\operatorname{ind} B$ or $\log_p B$, as the integer $b \in \{0, 1, \ldots, p-2\}$ such that $B = g^b$ in $\mathbb{F}_p$. Clearly the function $\log_p$ depends not only on p but also on the choice of the primitive root g.

Proposition 10.15. *Given $n \in \mathbb{N}$ and $B \in \mathbb{F}_p^\times$, the equation $X^n = B$ in $\mathbb{F}_p^\times$ has a solution $X \in \mathbb{F}_p^\times$ iff $\gcd(n, p-1) \mid \log_p B$.*

When $\gcd(n, p-1) \mid \log_p B$ then the number of distinct solutions X of $X^n = B$ in $\mathbb{F}_p^\times$ is $\gcd(n, p-1)$.

Proof. Write $B = g^b$, $X = g^x$, so that $g^{nx} = g^b$, giving $nx \equiv b \bmod p-1$. Hence the number of solutions is $\gcd(n, p-1)$. □

For large primes p, the problem of finding the discrete logarithm $\log_p B$ of B appears to be an intractable problem, called the **Discrete Logarithm Problem**. Many techniques in Cryptography depend on this hypothesis. See e.g.,

http://en.wikipedia.org/wiki/Discrete_logarithm

Main Points from Lecture 10:

- Definition and properties of $\varphi(n)$
- The multiplicative group of $\mathbb{F}_p$ is cyclic.
- Definition of primitive roots

11 Multiplicative Functions (26.10.2015)

Euler's φ function is very useful, as we have seen. A large part of the reason why is because it is a multiplicative function. Before going on for a more detailed study of primitive roots, we study multiplicative functions in general.

11.1 Arithmetic functions - more about φ

Arithmetic functions are functions $f : \mathbb{N} \to \mathbb{N}$ or $\mathbb{Z}$ or maybe $\mathbb{C}$, usually having some arithmetic significance. An important subclass of such functions are the multiplicative functions: such an f is **multiplicative** if

$$f(nn') = f(n)f(n')$$

for all $n, n' \in \mathbb{N}$ with n and n' coprime ($\gcd(n, n') = 1$). By convention, $f(1) = 1$.

Proposition 11.1. *If f is multiplicative and $n_1, \dots, n_k$ are pairwise coprime ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) then*

$$f(n_1 n_2 \dots n_k) = f(n_1)f(n_2)\dots f(n_k).$$

This is readily proved by induction.

Corollary 11.2. *If n factorises into distinct prime powers as $n = p_1^{e_1} \dots p_k^{e_k}$ then*

$$f(n) = f(p_1^{e_1}) \dots f(p_k^{e_k}).$$

So multiplicative functions are completely determined by their values on prime powers. Some examples of multiplicative functions are

- The identity function: $f(n) = n$;
- The constant function $f(n) = 1$;
- The '1-detecting' function $\Delta(n)$, equal to 1 at $n = 1$ and 0 elsewhere – obviously multiplicative;
- $\tau(n) = \sum_{d|n} 1$, the number of divisors of n;
- $\sigma(n) = \sum_{d|n} d$, the sum of the divisors of n.

Proposition 11.3. *The functions $\tau(n)$ and $\sigma(n)$ are both multiplicative.*

Example 11.4. *Let's check that $\sigma(36) = \sigma(9 \cdot 4) = \sigma(9)\sigma(4)$. The divisors of 36 are*

$$1, 2, 3, 4, 6, 9, 12, 18, 36$$

their sum is 91. On the other hand the divisors of 9 and 4 are respectively

$$1, 3, 9, \text{ and } 1, 2, 4$$

Hence $\sigma(9) = 13$ and $\sigma(4) = 7$. Luckily $13 \cdot 7 = 91$.

A curious thing happened on the way to this result. Notice that 36 had nine divisors and that 9 and 4 each had three apiece. If we were gamblers, we might wager that this is no coincidence. We might wager that any divisor of 36 is a product of a divisor of 9 and a divisor of 4, and that this could be done in a unique way. Stop here and think through why this should be true.

Lemma 11.5. *If a and b are relatively prime then any factor of ab can be written as a product of a factor of a times a factor of b in a unique way. Hence the number of divisors of ab is equal to the number of divisors of a times the number of divisors of b. In terms of the function τ we have proven that $\tau(n)$ is a multiplicative function.*

Notice that the Lemma is not true is if a and b fail to be relatively prime. For instance if $a = 4, b = 12$ then the factor $d = 4$ of 48 can be written in many ways as a product of factors of a and b: $4 = 4 \cdot 1 = 2 \cdot 2 = 1 \cdot 4$. The point is that if a and b are relatively prime, there's only one way to do this!

The proof of this lemma is pretty straightforward and is left as an exercise - think about the prime factors that divide a and b and those that divide ab.

To show that σ is multiplicative, we will prove a stronger result that puts σ and τ in a broader context. This is the operation "hat".

Definition 11.6. *Given an arithmetic function f, define its 'sum over divisors' function*

$$\widehat{f}(n) \; = \; \sum_{d|n} f(d) \; .$$

This is sometimes also called the **summatory function** *of f.*

Notice that if f is a function, then $\widehat{f}$ is another function, and one that depends on f.

For example $\widehat{f}(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$, which clearly depends on f.

For instance if $f(n) = n$ then

$$\widehat{f}(n) = \sum_{d|n} f(d) = \sum_{d|n} d = \text{ the sum of all divisors of } n = \sigma(n).$$

We could write this as $\widehat{f} = \sigma$. Or since $f(n) = n$, we could write $\widehat{n} = \sigma$. During class, someone asked why we didn't write $\widehat{d} = \sigma$. This is a good question, and one to think about. The answer is just that the functions $f(d) = d$ and the function $f(n) = n$ are the same function. In some circles they have even a third name - the identity function. It's good to be able to keep these things straight.

For further practice, check that $\widehat{1} = \tau$. Remember, the function $f(n) = 1$ is NOT the identity function, it's the constant function that sends everything to 1.

The following proposition shows the **important** fact that if f is a multiplicative function, then so is $\widehat{f}$.

Proposition 11.7. *Let $F(n) = \widehat{f}(n)$. If f is multiplicative, then F is also multiplicative.*

Proof. The relationship between F and f is that $F(n)$ adds up the values of $f(d)$ on all divisors d of n. Now suppose that $n = ab$ with a and b coprime. We want to show that $F(ab) = F(a)F(b)$, given that $f(ab) = f(a)f(b)$. Notice:

$$F(ab) = \sum_{d|ab} f(d)$$

$$F(a)F(b) = (\sum_{d|a} f(d))(\sum_{e|b} f(e)) \tag{3}$$

We want to show these two are equal. But by the Lemma, we know that every divisor d of ab can be written uniquely as a product of divisors of a and b. Hence

$$F(ab) = \sum_{\substack{d|a \\ e|b}} f(de) = \sum_{\substack{d|a \\ e|b}} f(d)f(e) \tag{4}$$

where the last equality holds since f is multiplicative. Now it is clear that this is equal to $F(a)F(b)$ because each term of the right hand side of (4) is equal to a term of (3) and vice versa. □

Hence we have shown that $\widehat{f}$ is multiplicative whenever f is. Thus we know that σ and τ are multiplicative since they are the hats of the (obviously) multiplicative functions $f(n) = n$ and $f(n) = 1$.

Remark 11.8. *It's fun sometimes to see what properties multiplicative functions have to have by default. For instance, notice that from the definition we see that $f(1) = f(1{\cdot}1) = f(1)f(1)$. So $(f(1))^2 = f(1)$. This only has two possible solutions in $\mathbb{Z}$ so $f(1)$ is either 1 or 0. If $f(1) = 0$ then we can prove that $f(n) = f(n \cdot 1) = f(n)f(1) = 0$ for all n. So in other words, we have shown that if f is not the zero function, then $f(1) = 1$.*

To close our tour of multiplicative functions, let's study our friend φ, defined by

$$\varphi(n) \;=\; \text{the number of } a \text{ such that } 1 \leqslant a \leqslant n \text{ and greatest common divisor } (a, n) = 1 \;.$$

As a warmup, let's compute!

Proposition 11.9. *If p is prime and k is a positive integer then $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. In particular $\varphi(p) = p - 1$.*

Proof. There are p^k numbers between 1 and p^k. Of these, the ones that are relatively prime to p^k are the ones who are NOT divisible by p. There are p^{k-1} multiples of p in this range, hence

$$\varphi(p^k) \;=\; \#\{1, 2, \ldots, p^k\} - \#\{p, 2p, 3p, \ldots, p^k\} \;=\; p^k - p^{k-1} \;.$$

□

Theorem 11.10. *Euler's φ function is multiplicative.*

Notice that this theorem shows that if $n = p_1^{e_1} \cdots p_n^{e_n}$ then $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_n^{e_k})$. Each factor is easy to compute by the Proposition above. In fact, since $\varphi(p^e) = p^e(1 - \frac{1}{p})$ we see that

$$\varphi(n) = p_1^{e_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

which proves:

Corollary 11.11. *If n is an integer, then*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Remark 11.12. *Notice that this is a quite a nice formula, but in practice it's probably easiest to just remember the formula $\varphi(p^k) = p^k - p^{k-1}$ and use this to compute φ.*

Example 11.13.

$$\varphi(300) = \varphi(3)\varphi(4)\varphi(25) = (3-1)(4-2)(25-5) = 2 \cdot 2 \cdot 20.$$

Proof of Theorem. Take n and n' coprime, and let

$$\{i : 1 \leqslant i \leqslant n, \gcd(i,n) = 1\} = \{a_1 < a_2 < \cdots < a_{\varphi(n)}\},$$

the **reduced residue classes** mod$n$. Similarly, let

$$\{j : 1 \leqslant j \leqslant n', \gcd(j,n') = 1\} = \{a'_1 < a'_2 < \cdots < a'_{\varphi(n')}\}.$$

The idea is now that numbers that are relatively prime to nn' are gotten by combining pairs of (a_i, a'_j) using the Chinese Remainder Theorem in a unique way. Hence the number of relatively prime integers to nn' is equal to the product of $\varphi(n)\varphi(n')$.

If $x \in \{1, 2, \ldots, nn'\}$ and $\gcd(x, nn') = 1$ then certainly $\gcd(x,n) = \gcd(x,n') = 1$, so that

$$x \equiv a_i \bmod n \qquad x \equiv a'_j \bmod n' \tag{5}$$

for some pair a_i, a'_j. Conversely, given such a pair a_i, a'_j we can solve (5) using the CRT to get a solution $x \in \{1, 2, \ldots, nn'\}$ with $\gcd(x, nn') = 1$. Thus we have a bijection between such x and such pairs a_i, a'_j. Hence

$$\#\{\text{such } x\} = \varphi(nn') = \#\{a_i, a'_j\} = \varphi(n)\varphi(n').$$

□

12 The multiplicative group of units $\bmod\ n$, Euler's Theorem and more about Primitive Roots (29.10.2015)

We begin with a definition:

Definition 12.1. *A number $1 \leqslant a \leqslant n$ which has an inverse x modulo n*

$$ax \equiv 1 (\operatorname{mod} n)$$

is called a ***unit modulo*** *n.*

Proposition 12.2. (i) *a is a unit* $\bmod n$ *if and only if a, n are coprime.*
(ii) *The set of units mod n forms a finite abelian group, the* **group of units** $\bmod n$ $\mathbb{Z}/n\mathbb{Z}^\times$ *under multiplication* $\bmod n$.[8] *The group $\mathbb{Z}/n\mathbb{Z}^\times$ is of order $\varphi(n)$.*

Proof. (i) a is coprime to n if and only if there exist $x, y \in \mathbb{Z}$ such that

$$ax + ny \;=\; 1 \in \mathbb{Z}\ .$$

Then x mod n is the inverse of a mod n.
(ii) We have to show that the operation of multiplication is well-defined on the set of units. I.e. that the product of two units is a unit.[9] This follows since the inverse of ab is the product of the inverses of a and b. By the definition of the Euler φ-function, there are precisely $\varphi(n)$ residues $a(\bmod n)$ coprime to n. We also should show that every element has an inverse (by definition), that 1 is in this set (obvious) and that the multiplication is associative (again obvious). In short there wasn't much to see in this proof. Better ask for our money back. □

For some integers n the group $\mathbb{Z}/n\mathbb{Z}^\times$ is cyclic, while for other n the group it is not cyclic (although always a product of cyclic groups).

Here is the definition of a primitive root (10.11) again.

Definition 12.3. *We say that a is a* **primitive root modulo** *n if $(a, n) = 1$ and the following $\varphi(n)$ numbers*

$$\{a, a^2, a^3, \ldots, a^{\varphi(n)}\}$$

are distinct modulo n, i.e. if $\mathbb{Z}/n\mathbb{Z}^\times$ is cyclic, with generator a. In other words, a has (maximal) order equal to $\varphi(n)$. In this case we say that n has a primitive root.

Like so much else in number theory, primitive roots were first studied by Gauss, in the early 19th century. The Wikipedia article on primitive roots
https://en.wikipedia.org/wiki/Primitive_root_modulo_n
and the multiplicative group of units
https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n
are very informative!

Example 12.4. (i) *For a prime p the group of units $\mathbb{Z}/p\mathbb{Z}^\times = \mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ is a cyclic group of order $\varphi(p) = p - 1$ by Theorem 10.10, with $\varphi(p-1)$ generators (= primitive roots).*
(ii) *Consider $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, the integers modulo 4. The units are the numbers relatively prime to 4, which are*

$$\mathbb{Z}/4\mathbb{Z}^\times = \{1, 3\}$$

[8] There are many notations for this group. Some people write $\mathbb{Z}/n\mathbb{Z}^\times$. Others use $U(\mathbb{Z}_n)$ or $U(\mathbb{Z}/n\mathbb{Z})$. What's important is to remember that this group is not all of the numbers from 1 to n, but only those numbers that are coprime to n.

[9] Some of you might call this "showing that the set is closed under multiplication"

This is a cyclic group of order two, and the element 3 *indeed has order* $\varphi(4) = 2$*, so 3 is a primitive root for* 4.
(iii) *Consider* $\mathbb{Z}/8\mathbb{Z} = \{0,1,2,3,4,5,6,7\}$*, the integers modulo 8, with units*

$$\mathbb{Z}/8\mathbb{Z}^{\times} = \{1,3,5,7\}$$

a group of order $\varphi(8) = 4$. *However, the 3 non-identity elements* $3,5,7$ *all have order* 2*, forming the* **Klein 4-group** V*, the non-cyclic finite group of order 4:*
https://en.wikipedia.org/wiki/Klein_four-group.
Thus there are no primitive roots for 8. But you can hear the Klein group sing:
https://www.youtube.com/watch?v=BipvGD-LCjU.

Given an integer $n \geqslant 1$ and a residue $a(\bmod n)$ it is easy to check if a is a unit $\bmod n$: just apply the Euclidean algorithm to calculate the greatest common divisor (a,n) and see if it is 1. (For a prime power $n = p^k$ there is an even easier procedure: just check if the reduction $a(\bmod p)$ is non-zero.) It is also easy to check if n has primitive roots - see Theorem 12.8 below. But there is no general formula for deciding which units $a \in \mathbb{Z}/n\mathbb{Z}^{\times}$ are primitive roots of n: you just have to calculate the order of $a \in \mathbb{Z}/n\mathbb{Z}^{\times}$, i.e. work out the first integer $m = 1,2,\dots$ such that $a^m \equiv 1(\bmod n)$, and see if it is $m = \varphi(n)$. Of course, some ways of doing this are more efficient than others. For low values of n there is nothing for it but to work out $a, a^2, \dots, a^m \equiv 1 \bmod n$ and see if $m = \varphi(n)$ - even in the prime power case $n = p^k$.

Here is a table of results for $n \leqslant 12$:

n	$\varphi(n)$	$\mathbb{Z}/n\mathbb{Z}^{\times}$	primitive roots
2	1	$\{1\}$	$\{1\}$
3	2	$\{1,2\}$	$\{2\}$
4	2	$\{1,3\}$	$\{3\}$
5	4	$\{1,2,3,4\}$	$\{2,3\}$
6	2	$\{1,5\}$	$\{5\}$
7	6	$\{1,2,3,4,5,6\}$	$\{3,5\}$
8	4	$\{1,3,5,7\}$	NONE
9	6	$\{1,2,4,5,7,8\}$	$\{2,5\}$
10	4	$\{1,3,7,9\}$	$\{3,7\}$
11	10	$\{1,2,3,4,5,6,7,8,9,10\}$	$\{2,6,7,8\}$
12	4	$\{1,5,7,11\}$	NONE

Theorem 12.5. *If* $n = m_1 m_2 \dots m_k$ *is an expression of* n *as a product of powers of distinct primes* $m_i = p_i^{e_i}$ $(1 \leqslant i \leqslant k)$ *then the group of units* $\bmod n$ *is the product*

$$\mathbb{Z}/n\mathbb{Z}^{\times} \ = \ \mathbb{Z}/m_1\mathbb{Z}^{\times} \times \mathbb{Z}/m_2\mathbb{Z}^{\times} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}^{\times} \ .$$

Proof. As in the proof of the Chinese Remainder Theorem 6.3 we have that $(m_i, m_j) = 1$ for $i \neq j$, and define m_i^* to be the inverse $\bmod m_i$ of $m_1 \dots m_{i-1} m_{i+1} \dots m_k$, so that

$$m_1 \dots m_{i-1} m_i^* m_{i+1} \dots m_k \equiv 1 \bmod m_i.$$

Then $a \in \mathbb{Z}/n\mathbb{Z}$ is a unit mod n if and only if each $a \in \mathbb{Z}/m_i\mathbb{Z}$ is a unit mod m_i, and the function

$$\mathbb{Z}/n\mathbb{Z}^\times \to \mathbb{Z}/m_1\mathbb{Z}^\times \times \mathbb{Z}/m_2\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}^\times \ ;$$
$$a \bmod n \mapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k)$$

is an isomorphism of groups (= bijection which preserves the group multiplication) with inverse

$$\mathbb{Z}/m_1\mathbb{Z}^\times \times \mathbb{Z}/m_2\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times \ ;$$
$$(a_1, a_2, \ldots, a_k) \mapsto \sum_{i=1}^{k} a_i m_1 m_2 \ldots m_{i-1} m_i^* m_{i+1} \ldots m_k \ .$$

□

Recalling that if you have a finite group G of order $|G|$ then every element g in the group satisfies $g^{|G|} = e$ where e is the identity, we obtain

Theorem 12.6 (Euler's Theorem). *If n is a positive integer then $a^{\varphi(n)} \equiv 1 \bmod n$ for every a with $(a, n) = 1$.*

Proof. If $(a, n) = 1$ then a is a unit modulo n. Hence it is in the group G of units modulo n. But this means that it satisfies $a^{|G|} = 1$ in this group. Since $|G| = \varphi(n)$ we are done. □

Remark 12.7. *Euler's Theorem is a generalization of Fermat's Little Theorem, since $\varphi(p) = p - 1$.*

An Application: We can use Euler's Theorem to find inverses: Indeed, we know that $a \cdot a^{\varphi(n)-1} = 1 \bmod n$ so that $a^{\varphi(n)-1}$ is the inverse of a modulo n. For instance if $ax \equiv b \bmod n$ has a solution that it must be

$$x = a^{\varphi(n)-1} b \bmod n.$$

You might wonder: Modulo p there was always a primitive root - i.e. an element of order $p - 1$ (the biggest possible order). Must there always be an element of order $\varphi(n)$ modulo n? The answer to this question is NO, but in some cases the answer is YES.

The following theorem states exactly which integers n have primitive roots.

Theorem 12.8. *A positive integer n has a primitive root if and only if n is one of the following numbers*

$$2, \ 4, \ p^k, \ 2 \cdot p^k$$

where p is an odd prime and k is a positive integer.

Proof. Section 9.3 of Rosen, posted on LEARN. □

We have seen already that 4 has a primitive root, and have also shown that p has a primitive root for all p. What remains is to show that that in the remaining cases p^k $(k \geqslant 1)$ and $2p^k$ there is indeed a primitive root, and that also all other numbers lack a primitive root. The statement of this theorem is important to know, though. As is the following:

Theorem 12.9. *If n has a primitive root then it has $\varphi(\varphi(n))$ primitive roots.*

Proof. The double φ is NOT a typo, and although this looks a bit intimidating, the proof is actually really calming. Indeed, it's just three baby steps:

First, the group of units modulo n is a group G with $|G| = \varphi(n)$.

Second, if n has a primitive root, then this means that G is cyclic.

Third, if G is a cyclic group of order m then G has $\varphi(m)$ many generators. (Proved in Lemma 12.10 below).

The result now follows. □

Lemma 12.10. *If G is a cyclic group of order m then G has $\varphi(m)$ many generators.*

We won't present the proof in class, but because it was on the homework, I'm including a different solution here:

Proof. This was essentially one of your homework problems, but here's the idea. If G is cyclic, then that means that $G = \langle g \rangle$ is generated by some element g. Hence every element of the group is a power of g:

$$G = \{g, g^2, \ldots, g^m\}$$

Now we just have to figure out how many elements have order m. Well g^k has order m if and only if m is the smallest positive integer such that $(g^k)^m = 1$. (The word "smallest" is the important word here, we already know that $(g^k)^m = 1$, since EVERY element in a group satisfying $x^m = 1$.)

Now suppose that n is the smallest power such that $(g^k)^n = 1$. Then $(g^k)^n = g^{kn}$ and $g^{kn} = 1$ if and only if $kn \equiv 0 \bmod m$. Hence we have that kn is a multiple of m, and n is the smallest positive integer n with this property. Now if $(k, m) = d$ then

$$(x^k)^{m/d} = (x^m)^{k/d} = (x^m)^{\text{an integer}} = 1$$

so certainly $n < m/d$. Hence if $n = m$ then $d = 1$ and m and k are relatively prime. Conversely, it's easy to check that if k and m are relatively prime that kn is a multiple of m if and only if n is a multiple of m. □

This proof had a lot of steps, and the technicalities obscure the fact that this result is simple, nice, and really intuitive. If this proof doesn't feel like a part of your repertoire, then try a few examples:

(If G is cyclic of order 20, then $G = \{g, g^2, \ldots, g^{20}\}$. Work out the order of the elements g^10, g^2, g^3, g^5, g^7 and look for patterns. Try to write your own proof of the above, etc.)

Main Points from Lecture 12:

- Definition and basic properties of the group $\mathbb{Z}/n\mathbb{Z}^\times$ of units mod n
- Euler's Theorem
- Primitive roots mod n

13 Mersenne primes and perfect numbers (2.11.2015)

For any number p define the **Mersenne number**

$$M_p = 2^p - 1 .$$

If M_p is prime then p is prime (this was Problem 6 on Homework 1), and M_p is called a **Mersenne prime**. Note that there are primes p which are not Mersenne, e.g. $p = 11$. Mersenne primes are called after the 17th century French mathematician and theologian Marin Mersenne. The Wikipedia pages https://en.wikipedia.org/wiki/Marin_Mersenne, https://en.wikipedia.org/wiki/Mersenne_prime are very informative!

A positive integer n is called **perfect** if it is the sum of its proper (i.e., excluding n itself) divisors. There is a surprising connection between perfect even numbers and the Mersenne primes $M_p = 2^p - 1$. The Euclid-Euler theorem proved below gives the equivalence of the following conditions for an even number n:

- n is perfect,
- $n = M_p(M_p + 1)/2$ for a Mersenne prime p,
- $8n + 1$ is a square and $M_p = (\sqrt{8n+1} - 1)/2$ is a Mersenne prime.

The first four Mersenne primes

$$M_2 = 3 , \ M_3 = 7 , \ M_5 = 31 , \ M_7 = 127$$

and the first four perfect numbers have been known since ancient times:

$$\begin{aligned}
6 &= M_2(M_2+1)/2 = 1+2+3 , \\
28 &= M_3(M_3+1)/2 = 1+2+4+7+14 , \\
496 &= M_5(M_5+1)/2 = 1+2+4+8+16+31+62+124+248 , \\
8128 &= M_7(M_7+1)/2 = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064 .
\end{aligned}$$

Recall the multiplicative function

$$\sigma(n) = \sum_{d|n} d .$$

A number n is perfect if and only if $\sigma(n) = 2n$.

Theorem 13.1. (Euclid and Euler) *An even number n is perfect if and only if it is of the form $n = 2^{p-1}(2^p - 1) = M_p(M_p + 1)/2$ for some Mersenne prime $M_p = 2^p - 1$.*

Proof. We first prove that if M_p is a Mersenne prime then $n = 2^{p-1}(2^p - 1)$ (with $2^p - 1$ is prime) is perfect. Since σ is multiplicative, we have that

$$\sigma(n) \ = \ \sigma(2^{p-1})\sigma(2^p - 1)$$

with

$$\begin{aligned} \sigma(2^{p-1}) \ &= \ 1 + 2 + 2^{+} \cdots + 2^{p-1} \ = \ 2^p - 1 \ , \\ \sigma(q) \ &= \ q + 1 \text{ for } q \text{ prime.} \end{aligned}$$

Thus

$$\sigma(n) \ = \ (2^p - 1)(2^p) \ = \ 2n \ .$$

This was Euclid's bit.

Conversely, suppose that n is an even perfect number. Then we can write $n = 2^k \cdot t$ where t is an odd number. Then perfection implies that

$$2^{k+1}t = 2n = \sigma(n) = (2^{k+1} - 1)\sigma(t) \tag{6}$$

This implies that 2^{k+1} divides $\sigma(t)$ (since the other factor on the right is odd). Thus we can write $\sigma(t) = 2^{k+1}s$. Our goal is to show that $k + 1 = p$ is prime and $s = 1$. Now canceling we see that

$$t = (2^{k+1} - 1)s$$

If $s > 1$ then t clearly has $1, s, t$ as factors. Thus

$$\sigma(t) \geqslant 1 + t + s = 1 + (2^{k+1}s - s) + s = 1 + (2^{k+1}s)$$

but this is a contradiction, because we assume that $\sigma(t) = 2^{k+1}s$.

Hence $s = 1$ and we have that $\sigma(t) = 2^{k+1}$, and Equation (6) says that

$$t = (2^{k+1} - 1).$$

This information about t and $\sigma(t)$ implies that t must in fact be prime, as required : $t = M_p$ is a Mersenne prime. This was Euler's bit. □

Later, when we discuss primality testing we will see that there is a relatively efficient algorithm to check whether a number of the form $M_p = 2^p - 1$ is prime. (The Lucas-Lehmer test) A good source of information on Mersenne numbers is
http://primes.utm.edu/mersenne/index.html

It is an unsolved problem as to whether there are any odd perfect numbers. See e.g., http://en.wikipedia.org/wiki/Perfect_number for lots on this problem.

GIMPS, the Great Internet Mersenne Prime Search
https://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search,
http://www.mersenne.org/primes/?press=M57885161
is a collective effort to hunt down Mersenne primes. Here is a listing of the 48 known (as of September 2015) primes p such that $M_p = 2^p - 1$ is a Mersenne prime
2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689,

9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657
https://oeis.org/A000043.
The largest known Mersenne prime is in fact the largest known prime

$$M_{32582657} = 2^{32582657} - 1$$

with 9,808,358 digits. It is tantalizingly close to claiming the \$100,000 award offered by an anonymous donor for finding a 10 million digit prime number. Incidentally, the Online Encyclopedia of Integer Sequences
https://oeis.org
is a marvellous compendium of integer sequences of all kinds!

Main Points from Lecture 13:

- Definition of Mersenne prime M_p
- Definition of perfect number
- The Euclid-Euler Theorem

14 The Möbius function $\mu(n)$, Möbius inversion and the convolution $f * g$ (5.11.2015)

Recall from Chapter 11 that an arithmetic function $f : \mathbb{N} \to \mathbb{N}$ (or to $\mathbb{Z}$ or to $\mathbb{C}$) is **multiplicative** if

$$f(mn) = f(m)f(n) \text{ for } \textbf{coprime} \text{ integers } m, n \geqslant 1$$

and $f(1) = 1$. Recall also the **summatory function** of f

$$\widehat{f}(n) = \sum_{d|n} f(d) .$$

In Proposition 11.7 it was proved that if $f(n)$ is multiplicative, then so is $\widehat{f}(n)$. The classic formula of Möbius Inversion recovers the function $f(n)$ from the function $\widehat{f}(n)$ (without assuming multiplicativity) using the Möbius function $\mu(n)$. The main results of this Chapter is that $f(n)$ is multiplicative if and only if $\widehat{f}(n)$ is multiplicative. (One way round was already proved in Chapter 11). The relationship between $f(n)$ and $\widehat{f}(n)$ is seen to be a special case of the convolution $(f * g)(n)$ of arithmetic functions $f(n)$, $g(n)$. The convolution will give a systematic construction of multiplicative functions.

14.1 The Möbius function $\mu(n)$

Let's start with a few examples - following the notation of Rosen, we will let $F(n) = \widehat{f}(n)$.

$$\begin{aligned} F(1) &= f(1) \\ F(2) &= f(1) + f(2) \\ F(3) &= f(1) + f(3) \\ F(4) &= f(1) + f(2) + f(4) \\ F(5) &= f(1) + f(5) \\ F(6) &= f(1) + f(2) + f(3) + f(6) \end{aligned}$$

If we solve these equations for $f(n)$ in terms of $F(n)$ we see

$$\begin{aligned} f(1) &= F(1) \\ f(2) &= F(2) - F(1) \\ f(3) &= F(3) - F(1) \\ f(4) &= F(4) - F(2) \\ f(5) &= F(5) - F(1) \\ f(6) &= F(6) - F(2) - F(3) + F(1). \end{aligned}$$

Experimentally it seems that

$$f(n) = \sum_{d|n} \mu_{n,d} F(d)$$

where $\mu_{n,d}$ seems to be either $0, 1$ or -1. We will prove that there exists a multiplicative function $\mu(n)$ such that

$$f(n) = \sum_{d|n} \mu(n/d) F(d) .$$

This allows us to invert the process of passing to a summatory function $f \mapsto \widehat{f}$.

Definition 14.1. *The* **Möbius function** $\mu(n)$ *is defined as*

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 \mid n \text{ for some prime } p; \\ (-1)^k & \text{if } n = p_1 p_2 \ldots p_k \text{ for distinct primes } p_i. \end{cases}$$

In particular, $\mu(1) = 1$ and $\mu(p) = -1$ for a prime p. It is immediate from the definition that μ is multiplicative.

Proposition 14.2. *The summatory function of μ is the 1-detecting function $\Delta(n)$*

$$\widehat{\mu}(n) = \Delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 . \end{cases}$$

Proof. We need to check that $\sum_{k|n} \mu(k) = \Delta(n)$. Recall that $\Delta(n)$ is one if $n = 1$ and zero otherwise. Since μ is multiplicative, it suffices to compute $\sum_{k|n} \mu(k)$ when $n = p^e$ is a power of a prime. If $e > 0$ then

$$\sum_{k|p^e} \mu(k) = \mu(1) + \mu(p) + \cdots \mu(p^e) = 1 - 1 = 0.$$

If $e = 0$ then of course $\widehat{\mu}(1) = \mu(1) = 1$. Hence $\widehat{\mu}(n) = 0$ unless $n = 1$, and we are done. □

Integers with $\mu(n) = \pm 1$ are called **squarefree**.

The Möbius function arises in many kinds of **inversion** formulae. The fundamental one is the following.

Proposition 14.3. (**Möbius inversion**) *Let $f(n)$ be an arithmetic function, and let*

$$F(n) \;=\; \widehat{f}(n) \;=\; \sum_{d|n} f(d) \quad (n \in \mathbb{N}) \;.$$

Then for all $n \in \mathbb{N}$ we can recover $f(n)$ from $F(n)$ by

$$f(n) \;=\; \sum_{d|n} \mu(n/d) F(d) \;.$$

Proof. We will simplify

$$\sum_{d|n} \mu(n/d) F(d) \;=\; \sum_{d|n} \mu(n/d) \sum_{k|d} f(k) \quad (n \in \mathbb{N})$$

by interchanging the order of summation to make $\sum_{k|n}$ the outer sum. First note that we can swap d and n/d in the sum:

$$\begin{aligned} \sum_{d|n} \mu(n/d) \sum_{k|d} f(k) &= \sum_{e|n} (\mu(e) \sum_{k|(n/e)} f(k)) \\ &= \sum_{e|n} (\sum_{k|(n/e)} \mu(e) \cdot f(k)) \;. \end{aligned}$$

Notice that the pairs of integers (e, k) such that $e \mid n$ and $k \mid n/e$ is the same as the set of pairs is the same as those with $k \mid n$ and $e \mid (n/k)$. So

$$\begin{aligned} \sum_{e|n} (\sum_{k|(n/e)} \mu(e) \cdot f(k)) &= \sum_{k|n} (\sum_{e|(n/k)} \mu(e) f(k)) \\ &= \sum_{k|n} f(k) \left(\sum_{e|(n/k)} \mu(e) \right) \;. \end{aligned}$$

The inner bracket is $\widehat{\mu}(n/k)$ which is nonzero if and only if $n = k$. In this case, $\widehat{\mu}(1) = 1$. Hence we have that the sum above reduces to

$$\sum_{k|n} f(k) \left(\sum_{e|(n/k)} \mu(e) \right) = f(n) \cdot 1 = f(n).$$

□

14.2 Some Examples of Using Möbius Inversion

There are two main uses of Möbius Inversion. The first is that we can just apply the formula to immediately obtain identities which might be difficult to obtain directly.

Example 14.4. *By definition,*

$$\sigma(n) \ = \ \widehat{n} \ = \ \sum_{d|n} d \ .$$

Möbius inversion gives that

$$n \ = \ \sum_{d|n} \mu(n/d)\sigma(d) \ .$$

Example 14.5. *By definition*

$$\tau(n) \ = \ \widehat{1}(n) \ = \ \sum_{d|n} 1 \ .$$

Möbius inversion gives that

$$1 \ = \ \sum_{d|n} \mu(n/d)\tau(d) \ .$$

Proposition 14.6. (i) *The summatory function of the Euler φ-function*

$$\varphi(n) \ = \sum_{1 \leqslant a \leqslant n, (a,n)=1} 1$$

is

$$\widehat{\varphi}(n) \ = \ \sum_{d|n} \varphi(d) \ = \ n \ .$$

(ii) *Möbius inversion expresses $\varphi(n)$ as*

$$\varphi(n) \ = \ \sum_{d|n} \mu(n/d)d$$

Proof. (i) Every integer m with $1 \leqslant m \leqslant n$ has a greatest common divisor (m,n). For each divisor $d \mid n$ there are exactly $\varphi(n/d)$ integers m with $1 \leqslant m \leqslant n$ and $(m,n) = d$, namely $a_1 d, a_2 d, \dots, a_{\varphi(n/d)} d$ with $a_1, a_2, \dots, a_{\varphi(n/d)}$ the integers a with $1 \leqslant a \leqslant n/d$ coprime to n/d. The summatory function is

$$\begin{aligned}
\widehat{\varphi}(n) \ &= \ \sum_{d|n} \varphi(d) \\
&= \ \sum_{d|n} \varphi(n/d) \text{ (since } d \mid n \text{ if and only if } n/d \mid n) \\
&= \ \sum_{d|n} \sum_{1 \leqslant a \leqslant n/d, (a,n/d)=1} 1 \\
&= \ n \ .
\end{aligned}$$

(ii) Immediate from (i). □

Numerical example $\varphi(12) = 4$ because there are exactly 4 numbers $1 \leqslant a \leqslant 12$ coprime to 12, namely $a = 1, 5, 7, 11$. On the other hand, there are 6 divisors: 1,2,3,4,6,12, so

$$\begin{aligned}\varphi(12) &= \sum_{d|12} \mu(12/d)d \\ &= \mu(12/1)1 + \mu(12/2)2 + \mu(12/3)3 + \mu(12/4)4 + \mu(12/6)6 + \mu(12/12)12 \\ &= 0 + 2 + 0 - 4 - 6 + 12 \ = \ 4 \ .\end{aligned}$$

The second main use of Möbius inversion is the following converse of Proposition 11.7:

Proposition 14.7. *If an arithmetic function $f(n)$ is such that $F(n) = \widehat{f}(n)$ is multiplicative, then $f(n)$ is multiplicative.*

Proof. Suppose that m_1, m_2 are coprime integers $\geqslant 1$. If d is a divisor of m_1m_2 then $d = d_1d_2$ where $d_1 \mid m_1$, $d_2 \mid m_2$ with d_1, d_2 coprime. Using the Möbius inversion formula and the fact that μ and F are multiplicative we see that

$$\begin{aligned}f(m_1m_2) &= \sum_{d|m_1m_2} \mu(d)F(m_1m_2/d) \\ &= \sum_{d_1|m_1, d_2|m_2} \mu(d_1d_2)F(m_1/d_1)F(m_2/d_2) \\ &= \left(\sum_{d_1|m_1} \mu(d_1)F(m_1/d_1)\right)\left(\sum_{d_2|m_2} \mu(d_2)F(m_2/d_2)\right) \\ &= f(m_1)f(m_2) \ .\end{aligned}$$

□

Conclusion: $f(n)$ if and only if $\widehat{f}(n)$ is multiplicative.

Remark 14.8. *This gives another proof that φ is multiplicative, say from the fact that $\widehat{\varphi} = n$ (Proposition 14.6 (i)) is multiplicative.*

14.3 Convolution

It is not accident that an arithmetic function $f(n)$ is multiplicative if and only if the summatory function $\widehat{f}(n)$ is multiplicative!

Definition 14.9. *The* **convolution** *of arithmetic functions $f(n)$, $g(n)$ is the arithmetic function*

$$(f * g)(n) \ = \ \sum_{d|n} f(d)g(n/d) \ .$$

(This is the number theory analogue of the convolution of continuous functions $f(x)$, $g(x)$, defined by $(f * g)(x) = \int\limits_{-\infty}^{\infty} f(y)g(x-y)dy$, which plays such an important role in functional analysis, e.g. Fourier analysis.)

Example 14.10. *We have already had several examples of convolutions:*
(i) *By Example 14.4* $\sigma = n * 1$, $\mu * \sigma = n$.
(ii) *By Example 14.5* $\tau = 1 * 1$, $\mu * \tau = 1$.
(iii) *By Proposition 14.6* $n = \varphi * 1$, $\mu * n = \varphi$.
Can you spot a common feature of (i), (ii) *and* (iii)*? Yes, if* $g = f * 1$ *then* $\mu * g = f$, *and in fact* $g = \widehat{f}$.

Basic properties: the convolution is commutative and associative; for any arithmetic functions $f(n)$, $g(n)$, $h(n)$

$$f * g \ = \ g * f \ , \ (f * g) * h \ = \ f * (g * h) \ .$$

(Why?) We have met the unit before:

Example 14.11. *Convolution with the 1-detecting* Δ*-function* $\Delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$ *does not change anything:*

$$f * \Delta \ = f \ .$$

Proposition 14.12. *If* $f(n)$ *and* $g(n)$ *are multiplicative functions then so is their convolution* $(f * g)(n)$.

Proof. As in the proof of Proposition 14.7 we have that for coprime integers $m_1, m_2 \geqslant 1$

$$\begin{aligned}(f * g)(m_1 m_2) \ &= \ \sum_{d_1 | m_1, d_2 | m_2} f(d_1 d_2) g(m_1 m_2 / d_1 d_2) \\ &= \ \Bigg(\sum_{d_1 | m_1} f(d_1) g(m_1/d_1) \Bigg) \Bigg(\sum_{d_2 | m_2} f(d_2) g(m_2/d_2) \Bigg) \\ &= \ (f * g)(m_1)(f * g)(m_2) \ .\end{aligned}$$

□

Remark 14.13. (i) *The summatory function of an arithmetic function* $f(n)$ *is the convolution with the constant function* $1(n) = 1$

$$\widehat{f} \ = \ f * 1 \ .$$

Since 1 is multiplicative Proposition 14.12 recovers Proposition 11.7, that if f *is multiplicative then so is* $\widehat{f}$.
(ii) *By Proposition 14.2 the convolution of the constant function* 1 *and the Möbius function* $\mu(n)$ *is the 1-detecting function*

$$1 * \mu \ = \ \Delta \ .$$

(iii) *From* (i) *and* (ii) *and the associativity of the convolution we have a new proof of the Möbius inversion Proposition 14.3, that we can recover any arithmetic function* $f(n)$ *from its summatory function* $\widehat{f}(n)$ *as the convolution with the Möbius function* $\mu(n)$

$$f \ = \ f * \Delta \ = \ f * (1 * \mu) \ = \ (f * 1) * \mu \ = \ \widehat{f} * \mu \ .$$

Since μ is multiplicative Proposition 14.12 recovers Proposition 14.7, that if $\widehat{f}$ is multiplicative then so is f.

The Wikipedia pages
https://en.m.wikipedia.org/wiki/Multiplicative_function
https://en.m.wikipedia.org/wiki/Möbius_inversion_formula
are useful introductions.

The book Number Theory in Science and Communication With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity by Manfred Schröder is a wonderful account of the applications of number theory to the real world!

Main Points from Lecture 14:

- Definition of Möbius function $\mu(n)$
- Möbius inversion
- Convolution

15 Quadratic Residues (9.11.2015)

15.1 Quadratic residues and nonresidues

Given a quadratic equation with real (or rather complex) coefficients

$$x^2 + ax + b \;=\; 0$$

it is possible to "complete the square"

$$(x + a/2)^2 \;=\; a^2/4 - b$$

and solve by taking square roots of the discriminant

$$x + a/2 \;=\; \pm\sqrt{a^2/4 - b}\ .$$

What about quadratic equations modulo n, of the form

$$x^2 + ax + b \equiv 0 (\operatorname{mod} n)$$

for $a, b(\operatorname{mod} n)$? If $n = 2m - 1$ is an odd integer, then $2m \equiv 1(\operatorname{mod} n)$ and

$$(x + am)^2 \;=\; a^2m^2 - b \bmod n\ .$$

To proceed further need to know if the discriminant $r = a^2m^2 - b$ is a square $\operatorname{mod} n$. If $n = 2m - 1$ is an odd prime this can be decided as follows.

Let then p be an odd prime, and $r \in \mathbb{F}_p^\times$. If the equation $x^2 = r$ has a solution $x \in \mathbb{F}_p^\times$ then r is called a **quadratic residue** $\operatorname{mod} p$. If there is no such solution x, then r is called a **quadratic nonresidue** $\operatorname{mod} p$.

Proposition 15.1. *Take p an odd prime, and g a primitive root* $\bmod p$. *Then the quadratic residues* $\bmod p$ *are the even powers of g, while the quadratic nonresidues* $\bmod p$ *are the odd powers of g. (So there are $\frac{p-1}{2}$ of each.)*

Proof. Suppose $r \in \mathbb{F}_p^\times$, with $r = g^k$ say. If k is even then $r = (g^{k/2})^2$, so that r is a quadratic residue $\bmod p$. Conversely, if $x = g^\ell$, $x^2 = r$, then $g^{2\ell-k} = 1$, so that $2\ell - k$ is a multiple of $p-1$, which is even. So k is even. □

15.2 The Legendre symbol

Let p be an odd prime, and $r \in \mathbb{F}_p^\times$. Then the **Legendre symbol** is defined as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 \text{ if } r \text{ is a quadratic residue mod } p; \\ -1 \text{ if } r \text{ is a quadratic nonresidue mod } p. \end{cases}$$

Note that, on putting $r = g^k$ for a primitive root g we see that

$$\left(\frac{g^k}{p}\right) = (-1)^k = \begin{cases} 1 \text{ if } k \text{ is even;} \\ -1 \text{ if } k \text{ is odd.} \end{cases}$$

Next, recall Fermat's Theorem: that $r^{p-1} = 1$ for all $r \in \mathbb{F}_p^\times$. This is simply a consequence of $\mathbb{F}_p^\times$ being a group of size (order) $p-1$. (We know that $g^{\#G} = 1$ for each g in a finite group G.)

Proposition 15.2 (Euler's Criterion)**.** *For p an odd prime and $r \in \mathbb{F}_p^\times$ we have in $\mathbb{F}_p^\times$ that*

$$\left(\frac{r}{p}\right) = r^{\dfrac{(p-1)}{2}} \in \{+1, -1\} \ . \tag{7}$$

Proof. If $r = g^k$ then for k even

$$r^{\frac{p-1}{2}} = g^{k\frac{p-1}{2}} = (g^{p-1})^{k/2} = 1^{k/2} = 1,$$

while if k is odd, $k\frac{p-1}{2}$ is not a multiple of $p-1$, so $r^{\frac{p-1}{2}} \neq 1$. However, $r^{p-1} = 1$ by Fermat, so $r^{\frac{p-1}{2}} = \pm 1$ and hence $r^{\frac{p-1}{2}} = -1$. So, by Proposition 15.1, we have (7), as required. □

Theorem 15.3. *In particular ($r = -1$), for p an odd prime, we have*

$$\left(\frac{-1}{p}\right) = (-1)^{\dfrac{p-1}{2}} = \begin{cases} 1, & \textit{if } p \equiv 1 \bmod 4 \\ -1, & \textit{if } p \equiv -1 \bmod 4. \end{cases}$$

Lemma 15.4. *Let p be an odd prime, and a, b be integers not divisible by p. We have*

1. *$a \equiv b \bmod p$ implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*;*

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*;*

3. $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. Let g be a primitive root mod$p$. Then $\left(\frac{g^k}{p}\right) = (-1)^k$, from which the results follow easily. □

Example 15.5. *Determine whether or not* 90 *is a square mod* 11*.*

Solution: We are asked to compute $\left(\frac{90}{11}\right)$ *By the Lemma above we see that*

$$\left(\frac{90}{11}\right) = \left(\frac{9}{11}\right)\left(\frac{10}{11}\right) = 1 \cdot \left(\frac{-1}{11}\right).$$

(Since 9 *is clearly a square). Now by the Theorem, we know that* -1 *is a quadratic residue if and only if* p *is congruent to* 1 *mod* 4*. Since* $11 \equiv 3 \bmod 4$ *we see that* -1 *is not a quadratic residue. Thus*

$$\left(\frac{90}{11}\right) = -1$$

and 90 *is not a quadratic residue.*

To some extent, Euler's criterion allows us to determine whether or not a is a quadratic residue. However, since it involves taking a large power, it is not clear how effective this is. At the same time, the Lemma above shows that to compute Legendre symbol $\left(\frac{a}{p}\right)$, it suffices to consider only the prime factors q of a and compute $\left(\frac{q}{p}\right)$. Since we can reduce mod p, we can assume that $q < p$. From this perspective, it is natural to ask whether or not there is some relationship between $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$. The answer is a resounding Yes and is one of the most celebrated results of number theory. In the next section we present this theorem of Quadratic Reciprocity and a sketch of the proof.

Main Points from Lecture 15:

- Quadratic residues
- The Legendre symbol
- Euler's criterion

16 Quadratic Reciprocity (12.11.2015)

16.1 Introduction

Recall that the Legendre symbol $\left(\dfrac{a}{p}\right)$ is defined for an odd prime p and integer a coprime to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue } \bmod p; \\ -1 \text{ otherwise;} \end{cases}$$

The Law of Quadratic Reciprocity (stated below) decides if the equation $x^2 \equiv a(\bmod p)$ has a solution $x(\bmod p)$ by allowing the calculation of $\left(\dfrac{a}{p}\right)$. But to actually find a solution still need to choose a primitive root $g \in \mathbb{F}_p^\times$, and write $a \equiv g^k (\bmod p)$. Then $\left(\dfrac{a}{p}\right) = (-1)^k$, and there is a solution if and only if k is even, in which case $x \equiv g^{k/2}(\bmod p)$ is a solution. For $n, a \in \mathbb{N}$ the Law of Quadratic Reciprocity can be used to study the prime factors $p \mid n^2 - a$.

Recall too that for a, b coprime to p

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(easily proved by writing a, b as powers of a primitive root), and that, by Euler's Criterion(Proposition 15.2),

$$\left(\frac{-1}{p}\right) = (-1)^{\dfrac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4 \\ -1, & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

Theorem 16.1 (Law of Quadratic Reciprocity (Legendre, Gauss))**.** *For distinct odd primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\dfrac{p-1}{2}.\dfrac{q-1}{2}}.$$

(Thus $\left(\dfrac{p}{q}\right) = \left(\dfrac{q}{p}\right)$ unless p and q are both $\equiv -1 \bmod 4$, in which case $\left(\dfrac{p}{q}\right) = -\left(\dfrac{q}{p}\right)$.)

There are now 246 recorded proofs of this (not all different), including six by Gauss – see http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

We'll give one of Gauss's proofs, using

Lemma 16.2 (Gauss's Lemma)**.** *For an odd prime p, put $p' = \frac{p-1}{2}$, and let a be an integer coprime to p. Consider the sequence*

$$a, 2a, 3a, ..., p'a,$$

reduced $\bmod p$ *to lie in* $(-\frac{p}{2}, \frac{p}{2})$. *Then* $\left(\dfrac{a}{p}\right) = (-1)^\nu$, *where ν is the number of negative numbers in this sequence.*

Proof. Now all of $a, 2a, 3a, ..., p'a$ are $\equiv$ mod$p$ to one of $\pm 1, \pm 2, \ldots, \pm p'$. Further,

- no two are equal, as $ia \equiv ja \bmod p \Rightarrow i \equiv j \bmod p$;
- none is minus another, as $ia \equiv -ja \bmod p \Rightarrow i + j \equiv 0 \bmod p$.

So they must be $\pm 1, \pm 2, \ldots, \pm p'$, with each of $1, 2, \ldots, p'$ occurring with a **definite sign**. Hence

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot p'a \equiv (\pm 1) \cdot (\pm 2) \cdot \ldots \cdot (\pm p') \bmod p,$$

giving

$$a^{p'}(p')! \equiv (-1)^{\nu}(p')! \bmod p,$$

and so, as $(p')!$ is coprime to p, that

$$a^{p'} \equiv (-1)^{\nu} \bmod p.$$

Finally, using Euler's criterion (Prop. 15.2), we have

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^{\nu} \bmod p.$$

Hence $\left(\frac{a}{p}\right) = (-1)^{\nu}$. □

We can use Gauss's Lemma to evaluate $\left(\frac{2}{p}\right)$.

Proposition 16.3. *For p an odd prime we have* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(This is equal to 1 when $p \equiv \pm 1 \bmod 8$, and to -1 when $p \equiv \pm 3 \bmod 8$.)

Proof. There are four similar cases, depending on $p \bmod 8$. We give the details for $p \equiv 3 \bmod 8$, $p = 8\ell + 3$ say. Then $p' = 4\ell + 1$, and, taking $a = 2$ in Gauss's Lemma, we see that for the sequence

$$2, 4, 6, \ldots, 4\ell, 4\ell + 2, \ldots, 8\ell + 2$$

that this becomes

$$2, 4, 6, \ldots, 4\ell, -(4\ell + 1), -(4\ell - 1), \ldots, -3, -1$$

when reduced mod$p$ into the range $(-\frac{p}{2}, \frac{p}{2})$. This clearly has 2ℓ positive members, and hence $\nu = p' - 2\ell = 2\ell + 1$ negative members. Hence $\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1$. □

Doing the other three cases would be a good exercise!

We now use Gauss's Lemma with $a = q$ to prove the Law of Quadratic Reciprocity.

Proof of Theorem 16.1. Take distinct odd primes p and q. For $k = 1, 2, \ldots, p'$ write (one step of the Euclidean algorithm)

$$kq = q_k p + r_k \tag{8}$$

say, where $1 \leqslant r_k \leqslant p-1$ and

$$q_k = \left\lfloor \frac{kq}{p} \right\rfloor . \tag{9}$$

(The quotient in the division algorithm is here expressed in terms of the floor function

$$\lfloor x \;\rfloor \;:\; \mathbb{R} \to \mathbb{Z} \;;\; x \mapsto \lfloor x \rfloor = \text{largest integer} \leqslant x \;.$$

For any integers $A, B \geqslant 1$, $A = QB + R$ with $Q = \lfloor A/B \rfloor$.) Now, working in $\mathbb{F}_p$ we have

$$\{q, 2q, \ldots, p'q\} = \{r_1, r_2, \ldots, r_{p'}\} = \{a_1, a_2, \ldots, a_t\} \cup \{-b_1, -b_2, \ldots, -b_\nu\},$$

as in Gauss's Lemma. So the a_i's are in $(0, \frac{p}{2})$ and the $-b_i$'s are in $(-\frac{p}{2}, 0)$. (In fact $t = p' - \nu$, but not needed.) Now put

$$a = \sum_{i=1}^{t} a_i, \qquad\qquad b = \sum_{i=1}^{\nu} b_i.$$

So, by the definition of the a_i's and $-b_i$'s we have

$$\sum_{k=1}^{p'} r_k = a - b + \nu p. \tag{10}$$

Now, in the proof of Gauss's Lemma we saw that

$$\{a_1, a_2, \ldots, a_t\} \cup \{b_1, b_2, \ldots, b_\nu\} = \{1, 2, \ldots, p'\},$$

so that

$$\frac{p^2-1}{8} = 1 + 2 + \cdots + p' = a + b. \tag{11}$$

and

$$\begin{aligned}
\frac{p^2-1}{8} q &= \sum_{k=1}^{p'} kq \\
&= p \sum_{k=1}^{p'} q_k + \sum_{k=1}^{p'} r_k && \text{(using (8))} \\
&= p \sum_{k=1}^{p'} q_k + a - b + \nu p, && \text{(using (10).)}
\end{aligned} \tag{12}$$

Next, on subtracting (12) from (11) we get

$$\frac{p^2-1}{8}(q-1) = p\sum_{k=1}^{p'} q_k - 2b + \nu p.$$

Reducing this mod 2 we have $0 \equiv \sum_{k=1}^{p'} q_k - \nu \bmod 2$, or $\nu \equiv \sum_{k=1}^{p'} q_k \bmod 2$. Thus Gauss's Lemma gives

$$\left(\frac{q}{p}\right) = (-1)^\nu = (-1)^{\sum_{k=1}^{p'} q_k} = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor},$$

using (9).

Now, reversing the rôles of p and q we immediately get

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor},$$

where of course $q' = (q-1)/2$, and we've replaced the dummy variable k by ℓ. So

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left\{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor\right\}},$$

which equals $(-1)^{p'q'}$, by the following proposition. □

Proposition 16.4. *Let p and q be two coprime odd positive integers. Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Proof. Consider the rectangle with corners $(0,0)$, $(p/2,0)$, $(0,q/2)$ and $(p/2,q/2)$. (Suggest you draw it, along with its diagonal from $(0,0)$ to $(p/2,q/2)$, and the horizontal axis the k-axis, the vertical axis the ℓ-axis. The diagonal is then the line with equation $\ell = kq/p$.) We count the number of integer lattice points (k,ℓ) strictly inside this rectangle in two different ways. First we note that these points form a rectangle with corners

$$(1,1), \left(\frac{p-1}{2}, 1\right), \left(1, \frac{q-1}{2}\right), \left(\frac{p-1}{2}, \frac{q-1}{2}\right),$$

so that there are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ of them in all.

On the other hand, we count separately those below, above and on the diagonal. **Below** the diagonal we have, for $k = 1, \ldots \frac{p-1}{2}$ that $\left\lfloor \frac{kq}{p} \right\rfloor$ is the number of points (k,ℓ) with $1 \leqslant \ell \leqslant \frac{kq}{p}$, i.e., below the diagonal, in the kth column. So the total is $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.

To count the number of lattice points above the diagonal, we flip the diagram over, reversing the rôles of p and q, and of k and ℓ. Then we get that the number of points **above** the diagonal is $\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor$. It remains to check that there are no lattice points actually **on** the diagonal. For if the integer lattice point (k,ℓ) were on the diagonal $\ell = kq/p$ we would have $\ell p = kq$ so that, as p and q are coprime, $p \mid k$. But $k < p$, so this is impossible. □

16.2 Proofs of Infinitude of Primes

Euclid's proof of the infinitude of primes was remarkable for its simplicity. To review, he argued that if there are only finitely many primes $p_1, \ldots, p_k$ then the number $p_1 \cdots p_k + 1$ is not divisible by any prime, an absurdity. Thus there must be infinitely many.

You can actually get pretty far by just modifying this proof a little bit. For instance, consider the following

Claim 16.5. *If n is congruent to 3 mod 4 then it has a prime factor congruent to 3 mod 4.*

The proof is simple: n is odd, so its factors are all odd. Such factors are either 1 or 3 mod 4. If they were all 1, then n itself would be 1 mod 4, which is isn't. So n has to have a factor congruent to 3 mod 4.

This claim gives us an easy proof of the following

Theorem 16.6. *There are infinitely many primes of the form $4k + 3$.*

Proof. Suppose there were only finitely many such primes, call them $p_1, \ldots, p_k$. Then consider the number

$$N = 4p_1 \cdots p_k - 1.$$

Then N is clearly congruent to 3 mod 4, and thus has a prime factor that is 3 mod 4 by the claim. However, at the same time, N is not divisible by any of the p_i. Hence they cannot have been a full list of primes that were 3 mod 4. □

We might hope that we could continue in this fashion to do other cases, but we soon run into difficulties. For instance if we tried to prove that there are infinitely many primes congruent to 1 mod 4 then this approach would not work. The problem is that the Claim above is not true if we replace 3 with 1. Indeed, the issue is that pairs of factors that are congruent to 3 mod 4 multiply to give 1 mod 4. For instance $3 \cdot 7 = 21$.

Using the Law of Quadratic Reciprocity, we can improve this somewhat.

Theorem 16.7. *There are infinitely many primes of the form $4k + 1$.*

Proof. Suppose there were only finitely many such primes, call them $p_1, \ldots, p_k$. Then consider the number

$$N = 4(p_1 \cdots p_k)^2 + 1.$$

Then N is clearly congruent to 1 mod 4. Now let q be a prime factor of N. Then mod q we see that

$$0 \equiv 4(p_1 \cdots p_k)^2 + 1$$

and thus

$$-1 \equiv (2p_1 \cdots p_k)^2$$

so -1 is a square mod q. But by QR, we know that -1 is a square if and only if q is congruent to 1 mod 4. Hence all prime factors of N are congruent to 1 mod 4. However, at the same time, N is not divisible by any of the p_i. Hence they cannot have been a full list of primes that were 1 mod 4. □

Problem 2 on Workshop 5 deals with showing there are infinitely many primes congruent to 7 mod 8. For that problem you want to consider a number of the form $(4p_1 \cdots p_k)^2 - 2$. You can also use this approach to show that there are infinitely many primes of the form $8k+3$ and $8k+5$, where you would use numbers of the form $(p_1 \cdots p_k)^2+2$ and $(p_1 \cdots p_k)^2+4$ respectively.

Main Points from Lecture 16:

- The Law of Quadratic Reciprocity
- Gauss's Lemma
- Infinities of primes satisfying certain properties

17 Some Diophantine Equations (16.11.2015)

17.1 Fermat's method of descent

Equations to be solved in integer variables are called **Diophantine** equations, in honour of Diophantus of Alexandria, who in the 3rd century AD is first recorded as working on them.

Around 1640, Fermat developed a method for showing that certain Diophantine equations had no (integer) solutions. In essence, the method is as follows: assume that the equation **does** have a solution. Pick the 'smallest' (suitably defined) one. Use the assumed solution to construct a smaller solution, contradicting the fact that the one you started with was the smallest. This contradiction proves that there is in fact no solution. The technique is called **Fermat's method of descent.** It is, in fact, a form of strong induction. (Why?)

We illustrate the method with three examples.

17.2 A 2-variable quadratic equation with no nonzero integer solution

Proposition 17.1. *The equation $x^2 = 2y^2$ has no solution in positive integers, i.e. $\sqrt{2}$ is irrational.*

First proof. Assume there is a solution in positive integers x, y. Let $2^a \mid x$, $2^b \mid y$ for the highest $a, b \geqslant 0$, so that $x = 2^a u$, $y = 2^b v$ for odd integers u, v. Then $x^2 = 2y^2$ becomes $2^{2a}u^2 = 2^{2b+1}v^2$, so that $2a = 2b + 1$, a contradiction! So there is no such solution x, y.

Second proof. We use Fermat Descent. Again assume that there is a solution x, y in positive integers. Define the size of the solution to be $x + y$. Choose a solution of smallest size (not necessarily unique – that doesn't matter). It follows from $2 \mid 2y^2 = x^2$ that $2 \mid x^2$, and so $2 \mid x$. Put $x = 2x_1$, so that $(2x_1)^2 = 2y^2$, or $y^2 = 2x_1^2$. Hence we have another solution y, x_1 of the original equation. But its size is $y + x_1 < y + x$, contradicting the assumption that we started with a solution of smallest size. Hence the assumption that there was a solution must be wrong. □

We next look at a more complicated example. The principle of proving that there is no solution is just the same, however.

17.3 A 4-variable quadratic equation with no nonzero integer solution

Theorem 17.2. *Let p and q be odd primes such that at least one of $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ is -1. Then the equation*

$$x^2 + pqy^2 = pz^2 + qw^2 \tag{13}$$

has no solution in positive integers x, y, z, w.

Proof. In fact we'll prove the slightly stronger assertion that (13) has no solution in nonnegative integers x, y, z, w not all 0.

Suppose that say $\left(\frac{p}{q}\right) = -1$ and there is such a solution (x, y, z, w). Clearly we can assume that x, y, z, w are all $\geqslant 0$. Define the **size** of such a solution by

$$s(x, y, z, w) \ = \ x + y + z + w \geqslant 1$$

Among all such solutions (x, y, z, w), we choose one that has size $s(x, y, z, w)$ as small as possible.

Considering (13) mod q, we have that $x^2 \equiv pz^2 \bmod q$. If $z \not\equiv 0 \bmod q$, we would have $(xz^{-1})^2 \equiv p \bmod q$, contradicting $\left(\frac{p}{q}\right) = -1$. Hence $q \mid z$, and so also $q \mid x$. Thus we can write $x = qx_1$, $z = qz_1$, and so from (13) we have

$$(qx_1)^2 + pqy^2 = p(qz_1)^2 + qw^2.$$

Dividing by q and reordering the terms, we have

$$w^2 + pqz_1^2 = py^2 + qx_1^2,$$

which gives a new solution (w, z_1, y, x_1) of (13). Now x and z can't both be 0, as then (13) would give $py^2 = w^2$. This is impossible, as y and w aren't both 0, and so the LHS is exactly divisible by an odd power of p while the RHS is exactly divisible by an even power of p. Hence either $0 < z_1 < z$ or $0 < x_1 < x$ (or both!), so we have $s(w, z_1, y, x_1) = w+z_1+y+x_1 < w + z + y + x = s(x, y, z, w)$. So we have found a solution of smaller size, contradicting the fact that we started with one of minimal size. Hence no solution can exist.

Of course if, instead, $\left(\frac{q}{p}\right) = -1$, then we simply swap the rôles of p and q in the above argument. □

Corollary 17.3. *If both p and q are primes* $\equiv -1 \bmod 4$ *then* (13) *has no solution in positive integers.*

Proof. In this case quadratic reciprocity tells us that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, so that one of these Legendre symbols is -1. Hence the condition that at least one of $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ is -1 in Theorem 17.2 applies. □

Notes.

1. If both $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$, then (13) can have a nonzero solution. For instance, when $p = 5$, $q = 11$ we have $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$, from Quadratic Reciprocity. And indeed the equation $x^2 + 55y^2 = 5z^2 + 11w^2$ has the nonzero solutions
$$(x, y, z, w) \;=\; (4, 0, 1, 1)\ ,\ (3, 1, 2, 2)\ ,\ (7, 1, 1, 3)\ .$$

2. Theorem 17.2 can be strengthened to show that (13) has no solutions in nonnegative integers not all 0. To see this, you follow the proof as above, but the size of the new solution obtained, $w + z_1 + y + x_1$, is $< w + z + y + x$ only if x and z are not both 0. In this case the proof goes through as before.

   However, if $x = z = 0$ then (13) gives $py^2 = w^2$. But this has no nonzero solution, as is easily seen by replacing '2' by 'p' in Proposition 17.1 – the proof is just the same. Hence the case $x = z = 0$ cannot occur.

Our third example has a trickier proof, but again the underlying 'descent' method is the same.

17.4 Fermat's Last Theorem for exponent 4

Fermat's Last Theorem is that the Diophantine equation

$$x^n + y^n \;=\; z^n$$

can be solved by integers $x, y, z \geqslant 1$ only for $n = 1, 2$. (For $n = 2$ we have the Pythagorean Triples). The theorem was first claimed by Fermat in 1637 in the margin of Diophantus's **Arithmetica**, although "the margin of the book was too large to accommodate the proof". So it was downgraded to the **Fermat Conjecture**. The conjecture was sensationally proved by Sir Andrew Wiles in 1994. On YouTube you can see the marvellous 1996 BBC TV film about what is now officially **Fermat's Last Theorem**.

Theorem 17.4. *The equation*

$$x^4 + y^4 = z^2 \tag{14}$$

has no solution in positive integers x, y, z.

Corollary 17.5 (Fermat's Last Theorem for exponent 4)**.** *The equation* $x^4 + y^4 = z^4$ *has no solution in positive integers* x, y, z.

This corollary is simply the special case of Theorem 17.4 where z is assumed to be a square.

Proof of Theorem 17.4. (From H. Davenport, **The higher arithmetic. An introduction to the theory of numbers**, Longmans 1952, p.162). Suppose that (14) has such a solution. We can clearly assume that $z \neq 1$, i.e., that $z > 1$. We measure the size of a solution simply by z. Assume we have a solution with z minimal. If $d = \gcd(x, y) > 1$ we can divide by d^4, replacing x by x/d, y by y/d and z by z/d^2 in (14), obtaining a solution with z smaller. So we must have $\gcd(x, y) = 1$ for our minimal solution.

Now from Corollary 7.9 we know that

$$X^2 + Y^2 = Z^2$$

has general solution (with $\gcd(X, Y) = 1$), possibly after interchanging X and Y of

$$X = p^2 - q^2 \qquad Y = 2pq \qquad Z = p^2 + q^2,$$

where $p, q \in \mathbb{N}$ and $\gcd(p, q) = 1$, so

$$x^2 = p^2 - q^2 \qquad y^2 = 2pq \qquad z = p^2 + q^2.$$

As a square is $\equiv 0$ or $1 \bmod 4$, and x is odd (because $\gcd(x, y) = 1$), we see that p is odd and q is even, say $q = 2r$. So

$$x^2 = p^2 - (2r)^2 \qquad \left(\frac{y}{2}\right)^2 = pr.$$

Since $\gcd(p, r) = 1$ and pr is a square, we have $p = v^2$ and $r = w^2$ say, so

$$x^2 + (2w^2)^2 = v^4.$$

Note that, as $\gcd(p, q) = 1$, we have $\gcd(x, q) = 1 = \gcd(x, 2w^2)$. Hence, on applying Corollary 7.9 again, we have

$$x = p_1^2 - q_1^2 \qquad 2w^2 = 2p_1q_1 \qquad v^2 = p_1^2 + q_1^2,$$

where $\gcd(p_1, q_1) = 1$ and not both are odd. Say p_1 odd, q_1 even. Thus $w^2 = p_1q_1$, giving $p_1 = v_1^2$, $q_1 = r_1^2$, say. Hence

$$v^2 (= p_1^2 + q_1^2) = v_1^4 + r_1^4,$$

which is another solution of (14)! But

$$v^2 = p = \sqrt{z - q^2} < \sqrt{z},$$

giving $v < z^{1/4}$, so certainly $v < z$ (as $z > 1$), contradicting the minimality of z. □

Main Points from Lecture 17:

- Diophantine equations without solutions
- Irrationality of $\sqrt{2}$
- Fermat's method of descent
- Fermat's Last Theorem for $n = 4$.

18 Representation of integers as sums of two squares (19.11.2015)

Which $n \in \mathbb{Z}$ can be represented as a sum of two squares

$$n = x^2 + y^2 \text{ for } x, y \in \mathbb{Z} \ ?$$

Obviously need $n \geqslant 0$. Can clearly assume that x and y are $\geqslant 0$.

Here is what happens for low values of n

$$\begin{array}{l} 0 = 0^2 + 0^2 \ , \ 1 = 0^2 + 1^2 \ , \ 2 = 1^2 + 1^2 \ , \ 3 \neq x^2 + y^2 \ , \ 4 = 0^2 + 2^2 \ , \\ 5 = 1^2 + 2^2 \ , \ 6 \neq x^2 + y^2 \ , \ 7 \neq x^2 + y^2 \ , \ 8 = 2^2 + 2^2 \ , \ 9 = 0^2 + 3^2 \ , \\ 10 = 1^2 + 3^2 \ , \ 11 \neq x^2 + y^2 \ , \ 12 \neq x^2 + y^2 \ , \ 13 = 2^2 + 3^2 \ , \ 14 \neq x^2 + y^2 \ , \dots \ . \end{array}$$

There is no apparent pattern.

Gauss was the first to observe that the question of expressing an integer as a sum of two squares is closely related to the properties of complex numbers with integer real and imaginary parts. The **modulus** of a complex number $z = a + ib$ $(a, b \in \mathbb{R})$ is the nonnegative real number

$$\|z\| = \sqrt{a^2 + b^2} \geqslant 0 \ .$$

The product of two complex numbers $z = a + ib$, $w = c + id$ is

$$zw = (a + ib)(c + id) = ac - bd + i(ad + bc)$$

with modulus

$$\begin{aligned} \|zw\| &= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = \|z\| \, \|w\| \ . \end{aligned}$$

A **Gaussian integer** is a complex number of the form

$$z = a + ib$$

with $a, b \in \mathbb{Z}$. It is clear that the sum of Gaussian integers is a Gaussian integer

$$(a+ib)+(c+id) \;=\; (a+c)+i(b+d) \;.$$

An integer $m \in \mathbb{N}$ is a sum of squares $m = a^2 + b^2$ of integers $a, b \in \mathbb{N}$ if and only if it is the square of the modulus (called the **norm**) of a Gaussian integer $a + ib$

$$m \;=\; \|a+ib\|^2 \;=\; a^2+b^2 \;.$$

Proposition 18.2 below states that the product of sums of two squares is a sum of two squares:

$$(a^2+b^2)(c^2+d^2) \;=\; (ac-bd)^2+(ad+bc)^2$$

which is immediate from the product rule $\|zw\| = \|z\|\,\|w\|$ for the modulus of the product of complex numbers: the product of Gaussian integers is a Gaussian integer with the product norm. The Wikipedia article on Gaussian integers is a brief introduction to the interesting algebraic and geometric properties of the Gaussian integers. You might even wish to take a Stroll through the Gaussian primes.

So the question of expressing an integer as a sum of two squares is reduced to the expression of prime powers as sums of two squares.

Certainly every power of 2 is a sum of squares:

$$2^{2k} \;=\; (2^k)^2+0^2 \;,\; 2^{2k+1} \;=\; (2^k)^2+(2^k)^2 \;.$$

It will turn out that every power of an odd prime $p \equiv 1(\text{mod})$ is a sum of two squares, and that only the even powers of odd prime $p \equiv 3(\bmod 4)$ are sums of two squares. It will follow that an integer $n \geqslant 1$ is a sum of two squares if and only if the the highest exponents of the primes $q \mid n$ with $q \equiv -1(\bmod 4)$ are even - a theorem of Fermat (who pre-dated Gauss).

Important note:

$$(2k)^2 \equiv 0 \bmod 4 \text{ and } (2k+1)^2 \;=\; 8\binom{k+1}{2}+1 \equiv 1 \bmod 8$$

so that

$$(\text{even})^2 \equiv 0 \;(\text{mod}, 4) \;,\; (\text{odd})^2 \;\equiv\; 1 \;(\text{mod}, 4) \;.$$

The sum $n = x^2 + y^2$ of two squares is

$$\begin{array}{ll} \text{either} & (\text{even})^2{+}(\text{even})^2 \equiv 0 \bmod 4 \\ \text{or} & (\text{odd})^2{+}(\text{odd})^2 \equiv 2 \bmod 4 \\ \text{or} & (\text{even})^2{+}(\text{odd})^2 \equiv 1 \bmod 4. \end{array}$$

If the sum n is odd then only the last case applies, so it must be $n \equiv 1 \bmod 4$.

18.1 The case $n = p$, odd prime

Which primes are the sum of two squares?

Theorem 18.1. *An odd prime p is a sum of two squares $p = x^2 + y^2$ (of integers) if and only if $p \equiv 1 \bmod 4$.*

Proof. We have already shown that if an odd number is a sum of two squares than it is $\equiv 1 \bmod 4$.
Conversely, assume p is an odd prime and $p \equiv 1 \bmod 4$. Knowing that then $\left(\frac{-1}{p}\right) = 1$ (Thm. 15.3), take $r \in \mathbb{N}$ with $r^2 \equiv -1 \bmod p$. Define $K = \lfloor \sqrt{p} \rfloor$, note that

$$K < \sqrt{p} < K + 1, \tag{15}$$

as $\sqrt{p} \notin \mathbb{Z}$. The function

$$f \ : \ [0, K] \times [0, K] \to \mathbb{F}_p \ ; \ (u, v) \mapsto u + rv \bmod p$$

is from a set with $(K + 1)^2 > p$ elements to a set with p elements, so by the Pigeonhole Principle, there exist $(u_1, v_1) \neq (u_2, v_2)$ for which $f(u_1, v_1) \equiv f(u_2, v_2) \bmod p$. Hence

$$\begin{aligned} u_1 + rv_1 &\equiv u_2 + rv_2 \bmod p \\ u_1 - u_2 &\equiv -r(v_1 - v_2) \bmod p \\ a &\equiv -rb \bmod p, \end{aligned}$$

say, where $a = u_1 - v_1$ and $b = v_1 - v_2$ are not both 0. Hence $a^2 \equiv -b^2 \bmod p$ as $r^2 \equiv -1 \bmod p$, so that $p \mid (a^2 + b^2)$. But $|a| \leqslant K$, $|b| \leqslant K$, giving

$$0 < a^2 + b^2 \leqslant 2K^2 < 2p.$$

So $a^2 + b^2 = p$. □

18.2 The general case

We now look at what happens if a prime $\equiv -1 \bmod 4$ **divides** a sum of two squares.

Proposition 18.2. *Let $q \equiv 3 \bmod 4$ be prime, and $q \mid (x^2 + y^2)$. Then $q \mid x$ and $q \mid y$, so that $q^2 \mid (x^2 + y^2)$.*

Proof. Assume that it is not the case that both x and y are divisible by q, say $q \nmid x$. Then from $x^2 + y^2 \equiv 0 \bmod q$ we get $(yx^{-1})^2 \equiv -1 \bmod q$, contradicting $\left(\frac{-1}{q}\right) = -1$ (Thm. 15.3). □

Proposition 18.3. *If n is a sum of two squares and m is a sum of two squares then so is nm.*

Proof. If $n = a^2 + b^2$ and $m = c^2 + d^2$ then

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

Corollary 18.4. *If $n = A^2 \prod_i n_i$ where $A, n_i \in \mathbb{Z}$ and each n_i is a sum of two squares, then so is n.*

Proof. Use induction on i to get $n/A^2 = \prod_i n_i = a^2 + b^2$ say. Then $n = (Aa)^2 + (Ab)^2$. □

We can now state and prove our main result.

Theorem 18.5 (Fermat)**.** *Write n in factorised form as*

$$n = 2^{f_2} \prod_{p \equiv 1 \bmod 4} p^{f_p} \prod_{q \equiv -1 \bmod 4} q^{g_q},$$

where (of course) all the p's and q's are prime. Then n can be written as the sum of two squares of integers iff all the g_q's are even.

Proof. If all the g_q are even then $n = A^2 \times$(product of some p's) and also $\times 2$ if f_2 is odd. So we have $n = A^2 \times \prod_i (a_i^2 + b_i^2)$ by Theorem 18.1 (using also $2^{f_2} = (2^{(f_2-1)/2})^2 + (2^{(f_2-1)/2})^2$ if f_2 odd). Hence, by Corollary 18.4, n is the sum of two squares.

Conversely, suppose $q \mid n = a^2 + b^2$, where $q \equiv -1 \bmod 4$ is prime. Let q^k be the highest power of q dividing both a and b, so say $a = q^k a_1$, $b = q^k b_1$. Then

$$\frac{n}{q^{2k}} = a_1^2 + b_1^2.$$

Now $q \nmid \dfrac{n}{q^{2k}}$, as otherwise q would divide both a_1 and b_1, by Prop. 18.2. Hence q^{2k} is the highest power of q dividing n, i.e., $g_q = 2k$ is even. Hence all the g_q's are even. □

18.3 Related results

Proposition 18.6. *If an integer n is the sum of two squares of rationals then it's the sum of two squares of integers.*

Proof. Suppose that

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

for some rational numbers a/b and c/d. Then

$$n(bd)^2 = (da)^2 + (bc)^2.$$

Hence, by Thm 18.5, for every prime $q \equiv -1 \bmod 4$ with $q^i | n(bd)^2$, i must be even. But then if $q^\ell | bd$ then $q^{i-2\ell} | n$, with $i - 2\ell$ even. Hence, by Thm 18.5 (in the other direction), n is the sum of two squares of integers. □

Corollary 18.7. *A rational number n/m is the sum of two squares of rationals iff nm is the sum of two squares of integers.*

Proof. If $nm = a^2 + b^2$ for $a, b \in \mathbb{Z}$ then

$$\frac{n}{m} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2.$$

Conversely, if

$$\frac{n}{m} = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

then

$$nm = \left(\frac{am}{b}\right)^2 + \left(\frac{cm}{d}\right)^2.$$

Hence, by Prop. 18.6, nm is the sum of two squares of integers. □

18.4 Finding all ways of expressing a rational as a sum of two rational squares

Now let h be a rational number that can be written as the sum of two squares of rationals. We can then describe **all** such ways of writing h.

Theorem 18.8. *Suppose that $h \in \mathbb{Q}$ is the sum of two rational squares: $h = s^2 + t^2$, where $s, t \in \mathbb{Q}$. Then the general solution of $h = x^2 + y^2$ in rationals x, y is*

$$x = \frac{s(u^2 - v^2) - 2uvt}{u^2 + v^2} \qquad y = -\left(\frac{t(u^2 - v^2) + 2uvs}{u^2 + v^2}\right), \tag{16}$$

where $u, v \in \mathbb{Z}$ and are not both zero.

Proof. We are looking for all points $(x, y) \in \mathbb{Q}^2$ on the circle $x^2 + y^2 = h$. If (x, y) is such a point, then for $x \neq s$ the chord through (s, t) and (x, y) has rational slope $(t - y)/(s - x)$.

Conversely, take a chord through (s, t) of rational slope r, which has equation $y = r(x - s) + t$. Then for the intersection point (x, y) of the chord and the circle we have

$$x^2 + (r(x - s) + t)^2 = h,$$

which simplifies to

$$x^2(1 + r^2) + 2rx(t - rs) + (r^2 - 1)s^2 - 2rst = 0,$$

using the fact that $t^2 - h = -s^2$. This factorises as

$$(x - s)((1 + r^2)x + 2rt + s(1 - r^2)) = 0.$$

For $x \neq s$ we have

$$x = \frac{s(r^2 - 1) - 2rt}{1 + r^2}$$

and

$$\begin{aligned} y &= t + r(x - s) \\ &= -\left(\frac{t(r^2 - 1) + 2sr}{1 + r^2}\right), \end{aligned}$$

on simplification. Finally, substituting $r = u/v$ gives (16). Note that $v = 0$ in (16) (i.e., $r = \infty$) gives the point $(r, -s)$. □

Corollary 18.9. *The general integer solution x, y, z of the equation $x^2 + y^2 = nz^2$ is*

$$(x, y, z) = (a(u^2 - v^2) - 2uvb, b(u^2 - v^2) + 2uva, u^2 + v^2),$$

where $n = a^2 + b^2$, with $a, b, u, v \in \mathbb{Z}$, and u, v arbitrary.

(If n is not the sum of two squares, then the equation has no nonzero solution, by Prop. 18.6.)

In particular, for $n = 1 = 1^2 + 0^2$, we see that the general integer solution to Pythagoras' equation $x^2 + y^2 = z^2$ is

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2).$$

For a socalled **primitive** solution — one with $\gcd(x, y) = 1$ — choose u, v with $\gcd(u, v) = 1$ and not both odd.

The same method works for $Ax^2 + By^2 + Cz^2 = 0$.

18.5 Sums of three squares, sums of four squares

Proposition 18.10. *No number of the form $4^a(8k + 7)$, where a is a nonnegative integer, is the sum of three squares (of integers).*

Proof. Use induction on a. For $a = 0$: Now $n^2 \equiv 0, 1$ or $4 \bmod 8$, so a sum of three squares is $\equiv 1$ or 1 or 2 or 3 or 4 or 5 or 6 mod 8, but $\not\equiv 7 \bmod 8$.

Assume result true for some integer $a \geqslant 0$. If $4^{a+1}(8k + 7) = n_1^2 + n_2^2 + n_3^2$ then all the n_i must be even, and so $= 4(n_1'^2 + n_2'^2 + n_3'^2)$ say. But then $4^a(8k + 7) = n_1'^2 + n_2'^2 + n_3'^2$, contrary to the induction hypothesis. □

In fact (won't prove)

Theorem 18.11 (Legendre 1798, Gauss)**.** *All positive integers except those of the form $4^a(8k + 7)$ are the sum of three squares.*

Assuming this result, we can show

Corollary 18.12 (Lagrange 1770)**.** *Every positive integer is the sum of four squares.*

Proof. The only case we need to consider is $n = 4^a(8k+7)$. But then $n-(2^a)^2 = 4^a(8k+6) = 2^{2k+1}(4k + 3)$, which (being exactly divisible by an odd power of 2) is not of the form $4^{a'}(8k' + 7)$, so is the sum of three squares. □

The Wikipedia article on the Lagrange four-square theorem has much to recommend it.

Main Points from Lecture 18:

- An odd prime p is a sum of two squares iff p mod 1 mod 4
- Fermat: a positive integer n is a sum of two squares iff for every odd prime $q|n$ with $q \equiv -1 \bmod 4$ the highest power of q dividing n is even.
- An integer is a sum of two squares of rationals iff it is a sum of two squares of integers.

19 Primality testing (23.11.2015)

19.1 Introduction

The applications of number theory to cryptography depend both on you being able to recognize large primes, and on other people not being able to recognize them! You need to recognize which numbers are prime in order to encode information, but the security of the data transmission depends on the opposition *not* being able to work out what these primes actually are. For example, in the RSA cryptosystem the public encryption key is the product $n = pq$ of two primes p, q so large that it is not feasible to factor n.

Factorization is concerned with the problem of developing efficient algorithms to express a given positive integer $n > 1$ as a product of powers of distinct primes. With primality testing, however, the goal is more modest: given n, decide whether or not it is prime. If n does turn out to be prime, then of course you've (trivially) factorised it, but if you show that it is not prime (i.e., *composite*), then in general you have learnt nothing about its factorisation (apart from the fact that it's not a prime!).

One way of testing a number n for primality is the following: suppose a certain theorem, Theorem X say, whose statement depends on a number n, is true when n is prime. Then if Theorem X is false for a particular n, then n cannot be prime.

It would be good if we could find a Theorem Y that was true *iff* n was prime, and was moreover easy to test. Then we would know that if the theorem was true for n then n was prime. A result of this type is the following (also on a problem sheet): n is prime iff $a^{n-1} \equiv 1 \bmod n$ for $a = 1, 2, \dots, n-1$. This is, however, not easy to test; it is certainly no easier than testing whether n is divisible by a for $a = 1, \dots, n$.

19.2 Wilson's Theorem and its converse

Here is a theorem which gives a necessary and sufficient condition (hard to verify in practice) for n to be prime.

Theorem 19.1. *A positive integer $n \geqslant 2$ is prime if and only if $(n-1)! \equiv -1 \bmod n$.*

Proof. One way round is just Wilson's Theorem 9.4: if p is prime then $(p-1)! \equiv -1 \bmod p$.

For the converse, assume that n is composite and $(n-1)! \equiv -1 \bmod n$. Let $n = ab$ with $1 < a < n$ and $1 < b < n$, so that $a \mid (n-1)!$. We now have $a \mid n$ and also that $n \mid ((n-1)! + 1)$, so that $a \mid (n-1)! + 1$. Hence

$$a \mid ((n-1)! + 1) - (n-1)! \; = \; 1 \; ,$$

a contradiction. So n is prime. □

Example 19.2. $5! = 120 \not\equiv -1 \bmod 6$, *so* $n = 6$ *is not a prime.*

The application of Theorem 19.1 in practice requires $n-2$ multiplications mod n to calculate $(n-1)!$ mod n, which is $O(n(\log_2 n)^2)$. See https://en.wikipedia.org/wiki/Big_O_notation for the Big O terminology: a numerical function $f(n)$ is $O(g(n))$ if there exist numbers $M, n_0 > 0$ such that $f(n) \leqslant Mg(n)$ for all $n \geqslant n_0$.

19.3 Fermat's Little Theorem (again), and pseudoprimes

Recall Fermat's Little Theorem 9.5: if p is prime then $a^p \equiv a \bmod p$ for every $a \bmod p$. So if for some n have $a^n \not\equiv a \pmod n$ for some $a \not\equiv 0 \bmod n$ then n is not prime.

Example 19.3. *For* $a = 2$ *and* $n = 63$

$$2^{63} \; = \; 2^{60}.2^3 \; = \; 64^{10}.8 \; = \; 8 \not\equiv 2 \bmod 63$$

so that 63 is not prime. (Of course it is easier to just observe 63=7.9).

It is known that for all the numbers $1 \leqslant n \leqslant 340$ if $2^n \equiv 2 (\mathrm{mod}\, n)$ then n is prime. But $n = 341$ shows that the converse of Fermat's Little Theorem is false:

Example 19.4. *Let* $n = 341 = 11.31$. *By Fermat's Little Theorem we have* $2^{10} \equiv 1 \bmod 11$, *so that*

$$2^{340} \; = \; (2^{10})^{34} \; = \; 1 (\mathrm{mod}\, 11) \; .$$

Also

$$2^{340} \; = \; (2^5)^{68} \; = \; 32^{68} \; = \; 1 (\mathrm{mod}\, 31) \; .$$

Hence $2^{341} \equiv 2 (\mathrm{mod}\, 341)$, *even though* $n = 341$ *is not a prime.*

There is also a version of Fermat's Little Theorem for a prime p and a coprime to p, in which case $a^{p-1} \equiv 1 \bmod p$. This condition is necessary but not sufficient for a number n to be prime, as shown by the above example.

A number n is a **pseudoprime to base** a if $n \not| a$ and $a^{n-1} \equiv 1 \pmod n$ but n is not actually a prime.

In general, there are far fewer pseudoprimes n to the base a not exceeding a specified bound, than there are primes. For example, there are 455,052,511 primes less than 10^{10}, but only 14,884 pseudoprimes.

19.4 Proving primality of n when $n-1$ can be factored

In general, primality tests can only tell you that a number n either 'is composite', or 'can't tell'. They cannot confirm that n is prime. However, under the special circumstance that we can factor $n-1$, primality can be proved:

Theorem 19.5 (Lucas Test, as strengthened by Kraitchik and Lehmer)**.** *Let $n > 1$ have the property that for every prime factor q of $n-1$ there is an integer a such that $a^{n-1} \equiv 1 \bmod n$ but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$. Then n is prime.*

Proof. Define the subgroup G of $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the subgroup generated by all such a's. Clearly the exponent of G is a divisor of $n-1$. But it can't be a proper divisor of $n-1$, for then it would divide some $(n-1)/q$ say, which is impossible as $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for the a corresponding to that q. Hence G has exponent $n-1$. But then $n-1 \leq \#G \leq \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. Hence $\varphi(n) = n-1$, which immediately implies that n is prime. □

Corollary 19.6 (Pepin's Test, 1877)**.** *Let $F_k = 2^{2^k} + 1$, the kth Fermat number, where $k \geq 1$. Then F_k is prime iff $3^{\dfrac{F_k-1}{2}} \equiv -1 \bmod F_k$.*

Proof. First suppose that $3^{\dfrac{F_k-1}{2}} \equiv -1 \bmod F_k$. We apply the theorem with $n = F_k$. So $n-1 = 2^{2^k}$ and $q = 2$ only, with $a = 3$. Then $3^{\dfrac{F_k-1}{2}} \not\equiv 1 \pmod{F_k}$ and (on squaring) $3^{F_k-1} \equiv 1 \bmod F_k$, so all the conditions of the Theorem are satisfied.

Conversely, suppose that F_k is prime. Then, by Euler's criterion (Proposition 15.2) and quadratic reciprocity (see Chapter 5) we have

$$3^{\dfrac{F_k-1}{2}} \equiv \left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

as 2 is not a square mod3.

□

We can use this to show that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime. It is known that F_k is composite for $5 \leq k \leq 32$, although complete factorisations of F_k are known only for $0 \leq k \leq 11$, and there are no known factors of F_k for $k = 20$ or 24. Heuristics suggest that there may be no more k's for which F_k is prime.

19.5 Carmichael numbers

A *Carmichael number* is a (composite) number n that is a pseudoprime to every base a with $1 \leq a \leq n$ and $\gcd(a, n) = 1$. Since it it immediate that $a^{n-1} \not\equiv 1 \pmod{n}$ when $\gcd(a, n) > 1$, we see that Carmichael numbers are pseudoprimes to as many possible bases as any composite number could be. They are named after the US mathematician Robert Carmichael (1879 – 1967).

[But even *finding* an a with $\gcd(a, n) > 1$ gives you a factor of n. (Imagine that n is around 10^{300} and is a product of three 100-digit primes – such a's are going to be few and far between!)]

Example 1. The number $n = 561 = 3.11.17$ is a Carmichael number. To see this take $a : \gcd(a, 561) = 1$, so that a is coprime to each of 3, 11 and 17. So, by Fermat, we have $a^2 \equiv 1 \bmod 3$, $a^{10} \equiv 1 \bmod 11$ and $a^{16} \equiv 1 \bmod 17$. Now $\operatorname{lcm}(2, 10, 16) = 80$ so that, taking appropriate powers, we have that $a^{80} \equiv 1 \bmod 3.11.17$. Finally $a^{560} = (a^{80})^7 \equiv 1^7 \equiv 1 \bmod 560$, so that indeed $n = 561$ is Carmichael.

For more examples of Carmichael numbers, see Workshop 4.

19.5.1 Properties of Carmichael numbers

Theorem 19.7 (See Qs 14 and 15, Workshop 4)**.** *An integer $n > 1$ is a Carmichael number iff n is squarefree and $p - 1 \mid n - 1$ for each prime p dividing n.*

Proposition 19.8 (See Q 18, Workshop 4)**.** *Every Carmichael number has at least 3 distinct prime factors.*

A curious result is the following.

Theorem 19.9 (See Q 17, Workshop 4)**.** *An integer $n > 1$ has the property that*

$$(a + b)^n \equiv a^n + b^n \bmod n \qquad \textit{for all } a, b \in \mathbb{Z}$$

iff either n is a prime number or n is a Carmichael number.

19.6 Strong pseudoprimes

Given $n > 1$ odd and an a such that $a^{n-1} \equiv 1 \bmod n$, factorise $n - 1$ as $n - 1 = 2^f q$, where q is odd, $f \geq 1$ and consider the sequence

$$\mathcal{S} = [a^q, a^{2q}, a^{4q}, \ldots, a^{2^f q} \equiv 1],$$

taken $\pmod{n}$. If n is prime then, working left to right, either $a^q \equiv 1 \bmod n$, in which case $\mathcal{S}$ consists entirely of 1's, or the number before the first 1 must be -1. This is because the number following any x in the sequence is x^2, so if $x^2 \equiv 1 \bmod n$ for n prime, then $x \equiv \pm 1 \bmod n$. (Why?) A composite number n that has this property, (i.e., is a pseudoprime to base a and for which either $\mathcal{S}$ consists entirely of 1's or the number before the first 1 in $\mathcal{S}$ is -1) is called a *strong pseudoprime to base a.*

Clearly, if n is a prime or pseudoprime but not a strong pseudoprime, then this stronger test proves that n isn't prime. This is called the *Miller-Rabin Strong Pseudoprime Test.*

Example 2. Take $n = 31621$. It is a pseudoprime to base $a = 2$, as $2^{n-1} \equiv 1 \bmod n$ but $5^{n-1} \equiv 12876 \bmod n$ (so n not prime). We have $n - 1 = 2^2 \cdot 7905$, $2^{7905} \equiv 31313 \bmod n$ and $2^{15810} \equiv 2^{31620} \equiv 1 \bmod n$, so n is not a strong pseudoprime to base 2.

19.7 Strong pseudoprimes to the smallest prime bases

It is known that

- 2047 is the smallest strong pseudoprime to base 2;
- 1373653 is the smallest strong pseudoprime to both bases 2, 3;
- 25326001 is the smallest strong pseudoprime to all bases 2, 3, 5;
- 3215031751 is the smallest strong pseudoprime to all bases 2, 3, 5, 7;
- 2152302898747 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11;
- 3474749660383 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11, 13;
- 341550071728321 is the smallest strong pseudoprime to all bases 2, 3, 5, 7, 11, 13, 17.

(In fact 341550071728321 is also a strong pseudoprime to base 19.)

Hence any odd $n < 341550071728321$ that passes the strong pseudoprime test for all bases 2, 3, 5, 7, 11, 13, 17 must be prime. So this provides a cast-iron primality test for all such n.

19.8 Factorising weak pseudoprimes

Let us call a pseudoprime to base a that is not a strong pseudoprime to base a a *weak pseudoprime to base a*.

Theorem 19.10. *An odd weak pseudoprime n to base a can be factored into $n = n_1 n_2$, where $n_1, n_2 > 1$.*

Proof. When the strong pseudoprime test detects n as being composite, what happens is that some $x \in \mathcal{S}$ is a solution to $x^2 \equiv 1 \bmod n$ with $x \not\equiv \pm 1 \pmod n$ because $x \equiv 1 \bmod n_1$ and $x \equiv -1 \bmod n_2$ for some coprime n_1, n_2 with $n_1 n_2 = n$. And then both $g_- := \gcd(x - 1, n)$ (divisible by n_1) and $g_+ := \gcd(x+1, n)$ (divisible by n_2) are nontrivial factors of n. Further, $2 = (x+1) - (x-1) = k_+ g_+ - k_- g_-$ say, for some integers k_+, k_-. So, because n is (assumed) odd, g_+ and g_- are coprime. As they are also factors of n, they must actually *equal* n_1 and n_2 respectively. □

Example 2 revisited. Take $n = 31621$.Then $x = 31313$ and $\gcd(n, 31312) = 103$ and $\gcd(n, 31314) = 307$, giving the factorisation $n = 103 \cdot 307$.

Note that if $n = n_1 n_2$ where n_1 and n_2 are coprime integers, then by the Chinese Remainder Theorem we can solve each of the four sets of equations

$$x \equiv \pm 1 \bmod n_1 \qquad\qquad x \equiv \pm 1 \bmod n_2$$

to get four distinct solutions of $x^2 \equiv 1 \bmod n$. For instance, for $n = 35$ get $x = \pm 1$ or ± 6. For the example $n = 31621$ above, we have $31313 \equiv 1 \bmod 103$ and $31313 \equiv -1 \bmod 307$, so that four distinct solutions of $x^2 \equiv 1 \bmod 31621$ are ± 1 and ± 31313.

19.9 Primality testing in 'polynomial time'

In 2002 the Indian mathematicians Agrawal, Kayal and Saxena invented an algorithm, based on the study of the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[x]$, that was able to decide whether a given n was prime in time $O((\log n)^{6+\varepsilon})$. (Here the constant implied by the 'O' depends on ε and so could go to infinity as $\varepsilon \to 0$.) (Search for 'AKS algorithm' on web.)

19.10 The Lucas-Lehmer primality test for Mersenne numbers

Given an odd prime p, let $M_p = 2^p - 1$, a *Mersenne number* (and a Mersenne prime iff it is prime). [It is an easy exercise to prove that if p is composite, then so is M_p.] See section 13 fro an an introduction to Mersenne numbers.

Define a sequence $S_1, S_2, \dots, S_n, \dots$ by $S_1 = 4$ and $S_{n+1} = S_n^2 - 2$ for $n = 1, 2, \dots$. so we have

$$S_1 = 4, S_2 = 14, S_3 = 194, S_4 = 37634, S_5 = 1416317954, \dots.$$

There is a very fast test for determining whether or not M_p is prime.

Theorem 19.11 (Lucas-Lehmer Test)**.** *For an odd prime p, the Mersenne number M_p is prime iff M_p divides S_{p-1}.*

So $M_3 = 7$ is prime as $7 \mid S_2$, $M_5 = 31$ is prime as $31 \mid S_4, \dots$. In this way get M_p prime for $p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, \dots$ (47th) 43112609. There may be others between the 41st and 47th. [as at October 2012.]

For the proof, we need two lemmas.

Lemma 19.12. *Put $\omega = 2 + \sqrt{3}$ and $\omega_1 = 2 - \sqrt{3}$. Then $\omega\omega_1 = 1$ (immediate) and*

$$S_n = \omega^{2^{n-1}} + \omega_1^{2^{n-1}}$$

for $n = 1, 2, \dots$.

The proof is a very easy induction exercise.

Lemma 19.13. *Let r be a prime $\equiv 1 \bmod 3$ and $\equiv -1 \bmod 8$ (i.e., $\equiv 7 \bmod 24$). Then*

$$\omega^{\dfrac{r+1}{2}} \equiv -1 \bmod r.$$

(So it's equal to $a + b\sqrt{3}$ where $a \equiv -1 \bmod r$ and $b \equiv 0 \bmod r$.)

Proof. Put

$$\tau = \frac{1+\sqrt{3}}{\sqrt{2}} \qquad \text{and} \qquad \tau_1 = \frac{1-\sqrt{3}}{\sqrt{2}}.$$

Then we immediately get $\tau\tau_1 = -1$, $\tau^2 = \omega$ and $\tau_1^2 = \omega_1$. Next, from $\tau\sqrt{2} = 1 + \sqrt{3}$ we have $(\tau\sqrt{2})^r = (1+\sqrt{3})^r$, so that

$$\begin{aligned} \tau^r 2^{\frac{r-1}{2}}\sqrt{2} &= 1 + \sum_{j=1}^{r-1}\binom{r}{j}(\sqrt{3})^j + 3^{\frac{r-1}{2}}\sqrt{3} \\ &\equiv 1 + 3^{\frac{r-1}{2}}\sqrt{3} \bmod r, \end{aligned} \tag{17}$$

as $r \mid \binom{r}{j}$. Since $r \equiv -1 \bmod 8$ we have

$$2^{\frac{r-1}{2}} \equiv \left(\frac{2}{r}\right) = (-1)^{\frac{r^2-1}{8}} \equiv 1 \bmod r,$$

using Euler's Criterion, and Prop. 5.3. Further, since $r \equiv 1 \bmod 3$ and $r \equiv -1 \bmod 4$ we have

$$3^{\dfrac{r-1}{2}} \equiv \left(\frac{3}{r}\right) = \left(\frac{r}{3}\right)(-1)^{\dfrac{r-1}{2}\cdot\dfrac{3-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1) \equiv -1 \bmod r,$$

using Euler's Criterion again, and also Quadratic Reciprocity (Th. 5.1). So, from (17), we have successively

$$\begin{aligned} \tau^r\sqrt{2} &\equiv 1 - \sqrt{3} \bmod r \\ \tau^r &\equiv \tau_1 \bmod r \\ \tau^{r+1} &\equiv \tau\tau_1 = -1 \pmod r \\ \omega^{\frac{r+1}{2}} &\equiv -1 \bmod r, \end{aligned}$$

the last step using $\tau^2 = \omega$. □

Proof of Theorem 19.11. $\mathbf{M_p}$ **prime** $\Rightarrow$ $\mathbf{M_p \mid S_{p-1}}$. Assume M_p prime. Apply Lemma 19.13 with $r = M_p$, which is allowed as $M_p \equiv -1 \bmod 8$ and $M_p \equiv (-1)^p - 1 \equiv 1 \bmod 3$. So

$$\omega^{\dfrac{M_p+1}{2}} = \omega^{2^{p-1}} \equiv -1 \bmod M_p \tag{18}$$

and, using Lemma 19.12, including $\omega_1^{-1} = \omega$, we have

$$S_{p-1} = \omega^{2^{p-2}} + \omega_1^{2^{p-2}} = \omega_1^{2^{p-2}} \left(\left(\omega_1^{-1}\right)^{2^{p-2}} \omega^{2^{p-2}} + 1 \right) = \omega_1^{2^{p-2}} \left(\omega^{2^{p-1}} + 1 \right) \equiv 0 \bmod M_p, \quad (19)$$

the last step using (18).

$\mathbf{M_p \mid S_{p-1} \Rightarrow M_p}$ **prime**. Assume $M_p \mid S_{p-1}$ but M_p composite. We aim for a contradiction. Then M_p will have a prime divisor q (say) with $q^2 \leq M_p$.

Now consider the multiplicative group $G = \left(\frac{\mathbb{Z}[\sqrt{3}]}{(q)}\right)^{\times}$ of units of the ring $\frac{\mathbb{Z}[\sqrt{3}]}{(q)}$. Then G has coset representatives consisting of numbers $a+b\sqrt{3}$ with $a, b \in \{0, 1, 2, \ldots, q-1\}$ that are also invertible $\pmod q$. So G is a group of size (order) at most $q^2 - 1$, with multiplication defined modulo q. From $\omega(\omega_1 + q\sqrt{3}) \equiv 1 \bmod q$ we see that $\omega = 2 + \sqrt{3}$ is invertible, and so $\omega \in G$. [Strictly speaking, the coset $\omega \pmod q \in G$.]

Now, using $M_p \mid S_{p-1}$ we see that (19) holds even when M_p is composite, so we have successively that $\omega^{2^{p-1}} + 1 \equiv 0 \bmod M_p$, $\omega^{2^{p-1}} \equiv -1 \bmod q$ and $\omega^{2^p} \equiv 1 \bmod q$. Hence the order of ω in G is 2^p. Then $2^p \mid \#G \leq q^2 - 1 \leq M_p - 1 = 2^p - 2$, a contradiction. Hence M_p must be prime.

□

In practice, to test M_p for primality using Theorem 19.11, one doesn't need to compute $S_j (j = 1, 2, \ldots, p-1)$, but only the much smaller (though still large!) numbers $S_j \pmod{M_p} (j = 1, 2, \ldots, p-1)$.

Main Points from Lecture 19:

- The converse of Wilson's theorem is true
- The converse of Fermat's Little Theorem is false
- Pseudoprimes
- Carmichael numbers

20 Integer Factorisation (26.11.2015)

In this chapter we review the historic techniques of Trial Division, the Sieve of Eratosthenes, and Fermat's factorisation method. We then study two simply-programmable integer factorisation algorithms, both due to Pollard.

20.1 Trial Division

Given $n > 1$, try dividing n successively by the primes $2, 3, \ldots,$ up to the largest prime $\leq \sqrt{n}$. If any such prime divides n, then of course you have found a factor, and you can continue the process by applying the same procedure to n/p. On the other hand, if none of these primes divides n, then n itself is prime. Why?

Lemma 20.1. *If $n > 1$ is composite then it is divisible by a prime $\leq \sqrt{n}$.*

Proof. Say $n = n_1 n_2$, where $n_1, n_2 > 1$. If both were $> \sqrt{n}$ then $n = n_1 n_2$ would be $> \sqrt{n}^2 = n$, a contradiction. Hence one of n_1 or n_2, say n_1, is $\leq \sqrt{n}$. Then any prime factor p of n_1 certainly divides n, and so $p \leq n_1 \leq \sqrt{n}$, as required. □

Trial division requires knowledge of all primes $\leq \sqrt{n}$. How to find them?

20.2 The Sieve of Eratosthenes

To find all primes up to N (e.g., for $N = \lfloor \sqrt{n} \rfloor$), write down $2, 3, 4, 5, 6, \ldots, N$ and

- cross off all multiples of 2, except 2 itself. Then the first uncrossedout number (3) is prime.

- cross off all multiples of 3, except 3. Then the first uncrossedout number (5) is prime.

Proceed in this way until you have crossed out all multiples of p, except p itself, for all primes $\leq \sqrt{N}$. Then the uncrossedout numbers consist of all the primes $\leq N$. This is because, by Lemma 20.1, all composite numbers $\leq N$ are divisible by a prime $\leq \sqrt{N}$, and so have been crossed out.

Thus to apply trial division on n you would need to apply the Sieve of Eratosthenes with $N \approx n^{1/4}$ in order to find all primes up to $n^{1/2}$.

20.3 Fermat's factorisation method

Take $n > 1$ and odd. Fermat's idea is to try to write n as $n = x^2 - y^2$, as then $n = (x+y)(x-y)$. So if $x > y + 1$ we get a nontrivial factorisation of n.

We successively try $x = \lceil \sqrt{n} \rceil$, $\lceil \sqrt{n} \rceil + 1$, $\lceil \sqrt{n} \rceil + 2, \ldots$, until $x^2 - n$ is a square, $= y^2$ say. Then $x^2 - n = y^2$, or $n = (x+y)(x-y)$. (This process will eventually terminate, as for $x = (n+1)/2$ we have $x^2 - n = ((n-1)/2)^2$. But this only give the trivial factorisation $n = n \cdot 1$.)

Example 1. $n = 2479$, $\lceil \sqrt{n} \rceil = 50$, $50^2 - n = 21$, $51^2 - n = 122$, $52^2 - n = 225 = 15^2$, giving $n = 52^2 - 15^2 = (52+15)(52-15) = 67 \cdot 37$.

Example 2. $n = 3953$, $\lceil \sqrt{n} \rceil = 63$, $63^2 - n = 16 = 4^2$, giving $n = 63^2 - 4^2 = (63+4)(63-4) = 67 \cdot 59$.

This method works well if n has two factors close together (so that y is small), but is otherwise slow. However, the idea of trying to write n as a difference of two squares is a factorisation idea used in several other factorisation algorithms, for instance in the Quadratic Sieve algorithm.

20.4 Pollard's $p-1$ method

Take $n > 1$ and odd, and suppose that n has a prime factor p. Then, if $p - 1 \mid k!$ for some k, say $k! = (p-1)q$, then

$$2^{k!} = (2^q)^{p-1} \equiv 1 \bmod p,$$

by Fermat's Little Theorem, so that $p \mid 2^{k!} - 1$. Hence $p \mid \gcd(2^{k!} - 1, n)$. So long as this gcd isn't n, we obtain a nontrivial (i.e., not 1 or n) factor of n.

So algorithm is:

Compute modulo n $2, 2^{2!} = 2^2, 2^{3!} = {2^{2!}}^3, 2^{4!} = {2^{3!}}^4, \ldots, 2^{k!} = {2^{(k-1)!}}^k$ until $n > \gcd(n, 2^{k!} - 1) > 1$. Then $\gcd(n, 2^{k!} - 1)$ is a nontrivial factor of n.

Maple code for Pollard $p-1$:

```
r:=2;g:=1;
for k to n while g=1 or g=n do
r:=r^k mod n; g:=gcd(r-1,n);
end do;
print(g,k);
```

At worst k could be near $(n-1)/2$, but is sometimes much smaller. It is generally large when all prime factors p of n are such that $p-1$ has a large prime factor. It is small when n has a prime factor p for which all prime factors of $p-1$ are small.

Example 1 again. $n = 2479$. Here $k = 6$ is enough, as $37 - 1 = 36 \mid 6!$, showing that $p = 37$ is a factor.

Example 2 again. $n = 3953$. Here $k = 11$ is enough, as $67 - 1 = 66 \mid 11!$, showing that $p = 67$ is a factor.

20.5 Pollard rho

The idea: for some function $f : \mathbb{N} \to \mathbb{N}$ define an integer sequence, starting with a 'seed' x_0, and defining $x_{k+1} \equiv f(x_k) \bmod n$ for $k \geq 0$. if these numbers are fairly random (mod n) then we'd expect to need about $\sqrt{n}$ of them before two will be equal (mod n). [Compare the 'Birthday Paradox' in Probability Theory, where 23 people chosen at random have, under standard assumptions, a 50% probability of containing a pair that share a birthday.] However, if p is the smallest prime factor of n, and p is much smaller than n, we'd expect that roughly $\sqrt{p}$ of the x_i are needed before two are equal (mod p). Then if indeed $x_i \equiv x_j \bmod p$ we have $p \mid \gcd(x_i - x_j, n)$. Provided that $x_i \not\equiv x_i \pmod n$, this will yield a proper factor of n.

The name 'Pollard rho' comes from the ρ-shaped diagram you can draw, consisting of a path from x_0 to x_1, x_1 to x_2, and so on, until the path curls around to intersect itself with $x_j \equiv x_i \bmod p$.

In practice we can take $x_0 = 2$ and $f(x) = x^2 + 1$. If $x_i \equiv x_j \bmod p$ with $0 < i < j$, then

$$x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \bmod p.$$

Proceeding in this way, we have

$$x_{i+s} \equiv x_{j+s} \bmod p \qquad \text{for } s = 1, 2, 3, \ldots . \tag{20}$$

Also

$$x_i \equiv x_j \equiv f^{j-i}(x_i) \equiv f^{j-i}(x_j) \equiv x_{j+(j-i)} \equiv x_{2j-i},$$

where f^{j-i} is the $(j-i)$-fold iterate of f. Hence we can add $j-i$ to the index repeatedly, to obtain

$$x_i \equiv x_j \equiv x_{j+(j-i)} \equiv x_{j+2(j-i)} \equiv \ldots \bmod p.$$

Thus, by if necessary replacing j by j + (a multiple of $j-i$), we can make j as large as we like. In particular, we can assume that $j \geq 2i$.

Now take $s = j - 2i$ in (20), giving $x_{j-i} \equiv x_{2(j-i)} \bmod p$. So in fact we just need to find some k such that

$$n > \gcd(x_{2k} - x_k, n) > 1.$$

(So we do not need to compare x_j with all previous x_i's for $i < j$.)

Maple code for Pollard rho:

```
g:=1;x[0]:=2;
for k to 100 while g=1 or g=n do
x[k]:=x[k-1]^2+1 mod n;
if k mod 2 = 0 then g:=gcd(x[k]-x[k/2],n); end if;
end do;
k:=k-1;
print(k,g);
```

(The choice of 100 as the maximum value for k is somewhat *ad hoc*, and can of course be increased.)

Example 1 yet again. $n = 2479$. Here $k = 6$, and $g = 37$ is a factor.

Example 2 yet again. $n = 3953$. Here $k = 12$, and $g = 59$ is a factor.

Example 3. $n = 1009^2$. Here $k = 98$ and $g = 1009$ is a (prime) factor.

This last example shows that the algorithm does not work so well (i.e., k is large) if the prime factors of n are large.

20.6 Final remarks.

- To specify a factoring algorithm, it's enough to have a general method that, for a given composite n, factors n as $n = n_1 n_2$, where both $n_1, n_2 > 1$. For then you can test n_1 and n_2 for primality and, if either is composite, recursively apply your algorithm to them. In this way you will eventually be able to write n as a product of powers of distinct primes. So your algorithm does not need to explicitly specify how to do this.

- In order to factor n, it's enough to find k: $1 < \gcd(k, n) < n$, as then $\gcd(k, n)$ is a nontrivial factor of n, with $n = n_1 n_2$, where $n_1 = \gcd(k, n)$ and $n_2 = n/\gcd(k, n)$.

  But if say $n = pq$ where p, q are primes $\approx 10^{300}$, then $\varphi(n) = (p-1)(q-1) = n-p-q+1 \approx 10^{600}$, and $n-\varphi(n) = p+q-1 \approx 2\cdot 10^{300}$. So a random $k \in \{1, 2, \ldots, n\}$ has a probability of $\approx 2 \cdot 10^{-300}$ of having $\gcd(k, n) > 1$ – vanishingly small!

- If we can find a solution x to the equation $x^2 \equiv 1 \bmod n$ that's not $x = \pm 1$ then we can factor n. This is because such a solution will produce $n = n_1 n_2$ where $n_1 = \gcd(x-1, n)$ and $n_2 = \gcd(x+1, n)$. For more details see also the end of Chapter 6, where this method is applied to factorise a 'weak pseudoprime'.

  Conversely, any nontrivial factorisation $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$ gives rise to four solutions of $x^2 \equiv 1 \bmod n$. This is because we can use the Chinese Remainder Theorem to solve the equations $x \equiv -1 \bmod n_1$, $x \equiv 1 \bmod n_2$. Then x and $-x$ are both solutions of $x^2 \equiv 1 \bmod n$, and neither is either of ± 1.

- Other factorisation methods:

  - The Quadratic Sieve – the best general algorithm for numbers up to 10^{100};
  - The General Number Field Sieve – best for larger n (not of a special form).

  For more factorisation methods see Wikipedia "integer_factorization".

ADDITIONAL TOPICS
Notes by Prof. Chris Smyth
Not lectured on in 2015

21 Dirichlet series

For an arithmetic function f, define its **Dirichlet series** $D_f(s)$ by

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Here $s \in \mathbb{C}$ is a parameter. Typically, such series converge for $\Re s > 1$, and can be meromorphically continued to the whole complex plane. However, we will not be concerned with analytic properties of Dirichlet series here, but will regard them only as generating functions for arithmetic functions, and will manipulate them formally, without regard to convergence.

The most important example is for $f(n) = 1 \quad (n \in \mathbb{N})$, which gives the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Also, taking $f(n) = n \quad (n \in \mathbb{N})$ gives $\zeta(s-1)$. (Check!).

Proposition 21.1. *If f is multiplicative then*

$$D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots + \frac{f(p^k)}{p^{ks}} + \ldots\right) = \prod_p D_{f,p}(s), \tag{21}$$

say.

Proof. Expanding the RHS of (21), a typical term is

$$\frac{f(p_1^{e_1})f(p_2^{e_2})\ldots f(p_r^{e_r})}{p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}} = \frac{f(n)}{n^s}$$

for $n = \prod_{i=1}^r p_i^{e_i}$, using the fact that f is multiplicative. □

Such a product formula $D_f(s) = \prod_p D_{f,p}(s)$ over all primes p is called an **Euler product** for $D_f(s)$.

For example

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{ks}} + \ldots\right) = \prod_p \left(\frac{1}{1-p^{-s}}\right),$$

on summing the Geometric Progression (GP). Hence also

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - p^{-s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = D_\mu(s),$$

on expanding out the product.

Proposition 21.2. *We have*

$$\left(\sum_k \frac{a_k}{k^s}\right)\cdot\left(\sum_\ell \frac{b_\ell}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} a_k b_{n/k}$.

Proof. On multiplying out the LHS, a typical term is

$$\frac{a_k}{k^s}\cdot\frac{b_\ell}{\ell^s} = \frac{a_k b_{n/k}}{n^s},$$

where $k\ell = n$. So all pairs k, ℓ with $k\ell = n$ contribute to the numerator of the term with denominator n^s. □

Corollary 21.3. *We have* $D_F(s) = D_f(s)\zeta(s)$.

Proof. Apply the Proposition with $a_k = f(k)$ and $b_\ell = 1$. □

Corollary 21.4 (Möbius inversion again)**.** *We have* $f(n) = \sum_{d|n} \mu(n/d)F(d)$ *for all* $n \in \mathbb{N}$.

Proof. From Corollary 21.3 we have

$$D_f(s) = D_F(s)\cdot\frac{1}{\zeta(s)} = \left(\sum_k \frac{F(k)}{k^s}\right)\cdot\left(\sum_\ell \frac{\mu(\ell)}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} F(k)\mu(n/k)$. But $D_f(s) = \sum_{n=1}^\infty \frac{f(n)}{n^s}$, so, on comparing coefficients, $f(n) = \sum_{k|n} F(k)\mu(n/k)$. □

We now compute the Dirichlet series for a few standard functions. [Part (a) is already proved above.]

Proposition 21.5. *We have*

(a) $D_\mu(s) = \frac{1}{\zeta(s)}$*;*

(b) $D_\varphi(s) = \frac{\zeta(s-1)}{\zeta(s)}$*;*

(c) $D_\tau(s) = \zeta(s)^2$*;*

(d) $D_\sigma(s) = \zeta(s-1)\zeta(s)$.

Proof. (b) Now

$$\begin{aligned}
D_\varphi(s) &= \prod_p \left(1 + \frac{\varphi(p)}{p^s} + \frac{\varphi(p^2)}{p^{2s}} + \cdots + \frac{\varphi(p^k)}{p^{ks}} + \dots\right) \\
&= \prod_p \left(1 + \frac{p-1}{p^s} + \frac{p^2-p}{p^{2s}} + \cdots + \frac{p^k - p^{k-1}}{p^{ks}} + \dots\right) \\
&= \prod_p \left(1 + \frac{p-1}{p^s} \cdot \frac{1}{1-p^{1-s}}\right), \qquad \text{on summing the GP} \\
&= \prod_p \left(\frac{1-p^{-s}}{1-p^{-(s-1)}}\right), \qquad \text{on simplification} \\
&= \frac{\zeta(s-1)}{\zeta(s)}.
\end{aligned}$$

(c) Now

$$\begin{aligned}
D_\tau(s) &= \prod_p \left(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \cdots + \frac{\tau(p^k)}{p^{ks}} + \dots\right) \\
&= \prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \cdots + \frac{k+1}{p^{ks}} + \dots\right) \\
&= \prod_p \frac{1}{(1-p^{-s})^2} \qquad \text{using } (1-x)^{-2} = \sum_{k=0}^{\infty} (k+1)x^k \\
&= \zeta(s)^2
\end{aligned}$$

(d) This can be done by the same method as (b) or (c) – a good exercise! But, given that we know the answer, we can work backwards more quickly:

$$\zeta(s-1)\zeta(s) = \left(\sum_k \frac{k}{k^s}\right) \cdot \left(\sum_\ell \frac{1}{\ell^s}\right) = \sum_n \frac{\sum_{k|n} k \cdot 1}{n^s} = D_\sigma(s),$$

using Prop. 21.2

□

22 Some Analytic Results about primes and the divisor function

22.1 The Prime Number Theorem

How frequent are the primes? At the end of the eighteenth century, Gauss and Legendre suggested giving up looking for a formula for the nth prime, and proposed instead estimating the number of primes up to x. So, define the prime-counting function $\pi(x)$ by

$$\pi(x) = \sum_{\substack{p \leqslant x \\ p \text{ prime}}} 1.$$

Gauss conjectured on computational evidence that $\pi(x) \sim \frac{x}{\log x}$. This was proved by independently by Hadamard and de la Vallée Poussin in 1896, and became known as

Theorem 22.1 (The Prime Number Theorem)**.** *We have $\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$.*

It turns out to be more convenient to work with

$$\theta(x) = \sum_{\substack{p \leqslant x \\ p \text{ prime}}} \log p,$$

which is called **Chebyshev's θ-function**. In terms of this function it can be shown (not difficult) that the Prime Number Theorem is equivalent to the statement $\theta(x) \sim x \quad (x \to \infty)$.

We won't prove PNT here, but instead a weaker version, and in terms of $\theta(x)$:

Theorem 22.2. *As $x \to \infty$ we have*

$$(\log 2)x + o(x) < \theta(x) < (2\log 2)x + o(x),$$

so that

$$0.6931x + o(x) < \theta(x) < 1.3863x + o(x).$$

22.2 Proof of Theorem 22.2

22.2.1 The upper bound

Proposition 22.3. *We have $\theta(x) < (2\log 2)x + O(\log^2 x)$.*

Proof. Consider $\binom{2n}{n}$. By the Binomial Theorem, it is less than $(1+1)^{2n} = 4^n$. Also, it is divisible by all primes p with $n < p \leqslant 2n$, so

$$4^n > \binom{2n}{n} \geqslant \prod_{n < p \leqslant 2n} p = e^{\theta(2n) - \theta(n)}.$$

Hence $\theta(2n) - \theta(n) \leqslant 2n \log 2$.

Now if $2n \leqslant x < 2n + 2$ (i.e., $n \leqslant x/2 < n + 1$) then $\theta(x/2) = \theta(n)$ and

$$\theta(x) \leq \theta(2n) + \log(2n+1) \leqslant \theta(2n) + \log(x+1),$$

so that, for each x,

$$\begin{aligned}\theta(x) - \theta(x/2) &\leqslant \theta(2n) + \log(x+1) - \theta(n)\\ &\leqslant 2n\log 2 + \log(x+1)\\ &\leqslant x\log 2 + \log(x+1).\end{aligned}$$

So (standard telescoping argument for $x, x/2, x/2^2, \dots, x/2^k$ where $x/2^{k-1} \geqslant 2$, $x/2^k < 2$, $\theta(x/2^k) = 0$):

$$\begin{aligned}\theta(x) &= \left(\theta(x) - \theta\left(\frac{x}{2}\right)\right) + \left(\theta\left(\frac{x}{2}\right) - \theta\left(\frac{x}{2^2}\right)\right) + \left(\theta\left(\frac{x}{2^2}\right) - \theta\left(\frac{x}{2^3}\right)\right) + \dots \left(\theta\left(\frac{x}{2^{k-1}}\right) - \theta\left(\frac{x}{2^k}\right)\right)\\ &\leqslant \log 2\left(x + \frac{x}{2} + \dots + \frac{x}{2^{k-1}}\right) + k\log(x+1)\\ &\leqslant 2x\log 2 + \lfloor \log_2 x\rfloor \log(x+1)\\ &\leqslant 2x\log 2 + O(\log^2 x).\end{aligned}$$

□

22.2.2 The lower bound

To obtain an inequality in the other direction, we look at

$$d_n = \operatorname{lcm}(1, 2, \dots, n) = e^{\sum_{p^m \leqslant n} \log p}.$$

Define

$$\psi(x) = \sum_{\substack{p^m \leqslant x\\ p \text{ prime}}} \log p;$$

(i.e., $\log p$ to be counted m times if p^m is the highest power of p that is $\leqslant x$). So $d_n = e^{\psi(n)}$.

Lemma 22.4. *We have $\psi(x) < \theta(x) + 2x^{1/2}\log x + O(\log^2 x)$.*

Proof. Now

$$\begin{aligned}\psi(x) &= \sum_{p\leqslant x} \log x + \sum_{p^2 \leqslant x} \log x + \sum_{p^3\leqslant x} \log x + \dots\\ &= \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \dots + \theta(x^{1/k}),\end{aligned}$$

where k is greatest such that $x^{1/k} \geqslant 2$, i.e., $k = \lfloor \log_2 x\rfloor$

$$\begin{aligned}&< \theta(x) + \log_2 x\, \theta(x^{1/2})\\ &< \theta(x) + 2x^{1/2}\log x + O(\log^2 x), \qquad\qquad \text{using Prop. 22.3.}\end{aligned}$$

□

Curious note: this k is the same one as in the proof of Prop. 22.3, though they have apparently different definitions.

We can now prove

Proposition 22.5. *We have* $\theta(x) \geqslant x\log 2 + O(x^{1/2}\log x)$.

Proof. Consider the polynomial $p(t) = (t(1-t))^n$ on the interval $[0,1]$. As $t(1-t) \leq \frac{1}{4}$ on that interval (calculus!), we have

$$0 \leqslant p(t) \leq \frac{1}{4^n} \qquad \text{on } [0,1].$$

Writing $p(t) = \sum_{k=0}^{2n} a_k t^k \in \mathbb{Z}[t]$, then

$$\frac{1}{4^n} \geqslant \int_0^1 p(t)dt = \sum_{k=0}^{2n} \frac{a_k}{k+1} = \frac{N}{d_{2n+1}} \geq \frac{1}{d_{2n+1}},$$

for some $N \in \mathbb{N}$, on putting the fractions over a common denominator. Hence we have successively

$$\begin{aligned} d_{2n+1} &\geqslant 4^n \\ \psi(2n+1) &\geqslant 2n\log 2 && \text{on taking logs} \\ \theta(2n+1) &\geqslant 2n\log 2 - 2\log(2n+1)\sqrt{2n+1} && \text{by Lemma 22.4} \\ \theta(x) &\geqslant x\log 2 + O(x^{1/2}\log x). \end{aligned}$$

□

Combining Propositions 22.3 and 22.5, we certainly obtain Theorem 22.2.

22.3 Some standard estimates

Lemma 22.6. *For* $t > -1$ *we have* $\log(1+t) \leqslant t$, *with equality iff* $t = 0$.

For $n \in \mathbb{N}$ *we have* $n\log(1+\frac{1}{n}) < 1$.

Proof. The first inequality comes from observing that the tangent $y = t$ to the graph of $y = \log(1+t)$ at $t = 0$ lies above the graph, touching it only at $t = 0$. The second inequality comes from putting $t = 1/n$ in the first inequality. □

Lemma 22.7 (Weak Stirling Formula)**.** *For* $n \in \mathbb{N}$ *we have*

$$n\log n - n < \log(n!) \leqslant n\log n.$$

Proof. Now for $j \geqslant 2$ we have

$$\begin{aligned} \log j &= j\log j - (j-1)\log(j-1) - (j-1)\log\left(1 + \frac{1}{j-1}\right) \\ &= j\log j - (j-1)\log(j-1) - \delta_j, \end{aligned}$$

where $0 < \delta_j < 1$, using Lemma 22.6 for $n = j - 1$. So, on summing for $j = 2, \ldots, n$ we get

$$\begin{aligned}\log(n!) &= \sum_{j=2}^{n} \log j \\ &= \sum_{j=2}^{n} j \log j - (j-1)\log(j-1) - \delta_j \\ &= n \log n - \sum_{j=2}^{n} \delta_j \\ &= n \log n - \Delta,\end{aligned}$$

where $0 < \Delta < n$, since $1 \log 1 = 0$ and all the other $j \log j$ terms apart from $n \log n$ telescope. □

Proposition 22.8. *We have*

$$\sum_{n \leqslant x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma = 0.577\ldots$, **the Euler-Mascheroni constant**.

Proof. Draw the graph of $y = 1/t$ for t from $0+$ to $N + 1$, where $N = \lfloor x \rfloor$. On each interval $[n, n+1]$ draw a rectangle of height $1/n$, so that these rectangles for $n = 1, 2, \ldots, N$ completely cover the area under the curve from $t = 1$ to $t = N + 1$. The pie-shaped pieces of the rectangles above the curve, when moved to the left to lie above the interval $[0, 1]$, are non-intersecting, and more than half-fill the 1×1 square on that interval. Say their total area is γ_n. Then, as $n \to \infty$, γ_n clearly tends to a limit γ, the Euler-Mascheroni constant.

The sum of the areas of the rectangles above $[n, n + 1]$ for $n = 1, 2, \ldots, N$ is clearly $\sum_{n=1}^{N} 1/n$ (the total area of the parts of the rectangles below the curve). On the other hand, it is $\int_1^{N+1} \frac{dx}{x} = \log(N + 1)$ (the total area of the parts of the rectangles below the curve), plus γ_n (the total area of the parts of the rectangles above the curve). Hence

$$\sum_{n \leqslant x} \frac{1}{n} = \sum_{n=1}^{N} 1/n = \log(N + 1) + \gamma_n.$$

Since $\log(N + 1) - \log x = O\left(\frac{1}{x}\right)$ and $\gamma - \gamma_n = O\left(\frac{1}{x}\right)$ (check!), we have the result. □

22.4 More estimates of sums of functions over primes

Let us put $\mathcal{P}_x = \prod_{p \leqslant x} \frac{1}{1-p^{-1}}$. Then

Proposition 22.9. *We have* $\mathcal{P}_x > \log x$.

Proof. We have

$$\mathcal{P}_x = \prod_{p \leqslant x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n} + \ldots\right).$$

On multiplying these series together, we obtain a sum of terms that includes all fractions $\frac{1}{n}$, where $n \leqslant x$. This is simply because all prime factors of such n are at most x. Hence

$$\mathcal{P}_x > \sum_{n \leqslant x} \frac{1}{n} > \log x,$$

by Prop. 22.8. □

Corollary 22.10. *There are infinitely many primes.*

Proposition 22.11. *We have*

$$\sum_{p \leqslant x} \frac{1}{p} > \log\log x - 1.$$

Proof. We have

$$\begin{aligned}\log \mathcal{P}_x &= \sum_{p \leqslant x} \log \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^k} + \ldots\right)\\ &< \sum_{p \leqslant x} \frac{1}{p} + \sum_{p \leqslant x} \frac{1}{p(p-1)},\end{aligned}$$

on applying Lemma 22.6 with $t = \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^k} + \ldots$, and summing the GP, starting with the $1/p^2$ term,

$$\begin{aligned}&< \sum_{p \leqslant x} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{(n+1)n}\\ &= \sum_{p \leqslant x} \frac{1}{p} + \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1}\right)\\ &= \sum_{p \leqslant x} \frac{1}{p} + 1,\end{aligned}$$

because of the telescoping of $\sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1}\right)$. Hence

$$\sum_{p \leqslant x} \frac{1}{p} > \log \mathcal{P}_x - 1 > \log\log x - 1,$$

using Prop. 22.9. □

Proposition 22.12. *We have*

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + O(1) \qquad \text{as } x \to \infty.$$

Proof. Now from Problem Sheet 1, Q8, we have

$$n! = \prod_{p \leqslant n} p^{\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots},$$

so that (taking logs)

$$\begin{aligned}
\log(n!) &= \sum_{p \leqslant n} \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \right) \log p \\
&= \sum_{p \leqslant n} \left\lfloor \frac{n}{p} \right\rfloor \log p + S_n,
\end{aligned}$$

where

$$\begin{aligned}
S_n : &= \sum_{p \leqslant n} \left(\left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \right) \log p \\
&\leq \sum_{p \leqslant n} \left(\frac{n}{p^2} + \frac{n}{p^3} + \dots \right) \log p \\
&= n \sum_{p \leqslant n} \frac{\log p}{p(p-1)} \\
&< n \sum_{k=1}^{\infty} \frac{\log(k+1)}{(k+1)k} \\
&= nc,
\end{aligned}$$

for some positive constant c, since the last sum is convergent. Hence $nc > S_n > 0$. Also, for $n = \lfloor x \rfloor$ we have

$$\begin{aligned}
n \sum_{p \leqslant x} \frac{\log p}{p} &\geq \sum_{p \leqslant x} \left\lfloor \frac{n}{p} \right\rfloor \log p \\
&> \sum_{p \leqslant x} \left(\frac{n}{p} - 1 \right) \log p \\
&= n \sum_{p \leqslant x} \frac{\log p}{p} - \theta(x).
\end{aligned}$$

Hence

$$n\sum_{p\leqslant x}\frac{\log p}{p}\geqslant\sum_{p\leqslant x}\left\lfloor\frac{n}{p}\right\rfloor\log p>n\sum_{p\leqslant x}\frac{\log p}{p}-O(x),$$

since $\theta(x)=O(x)$, by Theorem 22.2. Now add the inequality $nc>S_n>0$ to the above inequality, to obtain

$$n\sum_{p\leqslant x}\frac{\log p}{p}+nc>\log(n!)>n\sum_{p\leqslant x}\frac{\log p}{p}-O(x).$$

Dividing by n, and using the fact that $\frac{\log(n!)}{n}=\log n-O(1)$ from Prop. 22.7, we have

$$\sum_{p\leqslant x}\frac{\log p}{p}+O\left(1\right)>\log n-O\left(1\right)>\sum_{p\leqslant x}\frac{\log p}{p}-O\left(1\right).$$

Hence

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

□

22.5 The average size of the divisor function $\tau(n)$

The following result is a way of saying that an integer n has $\log n+2\gamma-1$ divisors, on average. Recall that $\tau(n)$ is the number of (positive) divisors of n.

Proposition 22.13. *We have, as $x\to\infty$, that*

$$\sum_{n\leqslant x}\tau(n)=x\log x+(2\gamma-1)x+O\left(\sqrt{x}\right).$$

Proof. Now

$$\begin{aligned}\sum_{n\leqslant x}\tau(n)&=\sum_{n\leqslant x}\sum_{\ell|n}1\\&=\sum_{\ell\leqslant x}\sum_{\substack{n=k\ell\\k\leq\frac{x}{\ell}}}1\\&=\sum_{\ell\leqslant x}\left\lfloor\frac{x}{\ell}\right\rfloor,\end{aligned}$$

on recalling that $\lfloor y \rfloor$ is the number of positive integers $\leqslant y$,

$$\begin{aligned}
&= 2\sum_{\ell \leqslant \sqrt{x}} \left\lfloor \frac{x}{\ell} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 && \text{by Q10, Problem Sheet 1}\\
&= 2\sum_{\ell \leqslant \sqrt{x}} \frac{x}{\ell} - x + O(\sqrt{x})\\
&= 2x\left(\log\sqrt{x} + \gamma + O\left(\frac{1}{\sqrt{x}}\right)\right) - x + O(\sqrt{x}) && \text{using Prop. 22.8}\\
&= x\log x + (2\gamma - 1)x + O(\sqrt{x}).
\end{aligned}$$

□

23 p-adic numbers

23.1 Motivation: Solving $x^2 \equiv a \bmod p^n$

Take an odd prime p, and an integer a coprime to p. Then, as we know, $x^2 \equiv a \bmod p$ has a solution $x \in \mathbb{Z}$ iff $\left(\frac{a}{p}\right) = 1$. In this case we can suppose that $b_0^2 \equiv a \bmod p$. We claim that then $x^2 \equiv a \bmod p^n$ has a solution x for all $n \in \mathbb{N}$.

Assume that we have a solution x of $x^2 \equiv a \bmod p^n$ for some $n \geqslant 1$. Then x is coprime to p, so that we can find $x_1 \equiv \frac{1}{2}(x + a/x) \bmod p^{2n}$. (This is the standard Newton-Raphson iterative method $x_1 = x - f(x)/f'(x)$ for solving $f(x) = 0$, applied to the polynomial $f(x) = x^2 - a$, but modp^{2n} instead of in $\mathbb{R}$ or $\mathbb{C}$.) Then

$$x_1 - x = -\frac{1}{2}\left(x - \frac{a}{x}\right) = -\frac{1}{2x}\left(x^2 - a\right) \equiv 0 \bmod p^n,$$

and

$$\begin{aligned}
x_1^2 - a &= \frac{1}{4}\left(x^2 + 2a + \frac{a^2}{x^2}\right) - a\\
&= \frac{1}{4}\left(x - \frac{a}{x}\right)^2\\
&= \frac{1}{4x^2}(x^2 - a)^2\\
&\equiv 0 \bmod p^{2n}
\end{aligned}$$

Thus, starting with x_0 such that $x_0^2 \equiv a \bmod p^{2^0}$, we get successively x_1 with $x_1^2 \equiv a \bmod p^{2^1}$, x_2 with $x_2^2 \equiv a \bmod p^{2^2}, \ldots$, x_k with $x_k^2 \equiv a \bmod p^{2^k}, \ldots$, with $x_{k+1} \equiv x_k \bmod p^{2^k}$. So, writing the x_i in base p, we obtain

$$\begin{aligned}
&x_0 = b_0 && \\
&x_1 = b_0 + b_1 p && \text{say, specified } \bmod p^2 \\
&x_2 = b_0 + b_1 p + b_2 p^2 + b_3 p^3 && \text{say, specified } \bmod p^4 \\
&x_3 = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 + b_5 p^5 + b_6 p^6 + b_7 p^7 && \text{say, specified } \bmod p^8,
\end{aligned}$$

and so on.

So, in any sense, is $x_\infty = \sum_{i=1}^{\infty} b_i p^i$ a root of $x^2 \equiv a \bmod p^\infty$? It turns out that, yes, it is: x_∞ is a root of $x^2 = a$ in the field $\mathbb{Q}_p$ of p-adic numbers.

23.2 Valuations

In order to define the fields $\mathbb{Q}_p$ of p-adic numbers for primes p, we first need to discuss valuations.

A **valuation** $|\cdot|$ on a field F is a map from F to the nonnegative real numbers satisfying

For each $x \in F$	$\lvert x\rvert = 0$ iff $x = 0$;	(ZERo)
For each $x, y \in F$	$\lvert xy\rvert = \lvert x\rvert \cdot \lvert y\rvert$;	(HOMomorphism)
For each $x, y \in F$	$\lvert x+y\rvert \leqslant \lvert x\rvert + \lvert y\rvert$.	(TRIangle)

If in addition

For each $x, y \in F$	$\lvert x+y\rvert \leqslant \max(\lvert x\rvert, \lvert y\rvert)$,	(MAXimum)

then $|\cdot|$ is called a **nonarchimedean** valuation. A valuation that is not nonarchimedean, i.e., for which there exist $x, y \in F$ such that $|x+y| > \max(|x|, |y|)$, is called **archimedean**. For instance the standard absolute value on $\mathbb{R}$ is archimedean because $2 = |2| = |1+1| > \max(|1|, |1|) = 1$.

Note that MAX is stronger than TRI in the sense that if MAX is true than TRI is certainly true. So to show that a valuation is nonarchimedean we only need to check that ZER, HOM and MAX hold.

Proposition 23.1. *For any valuation $|\cdot|$ on a field F we have $|1| = |-1| = 1$ and for $n \in \mathbb{N}$ (defined as the sum of n copies of the identity of F) we have $|-n| = |n|$ and $|1/n| = 1/|n|$. Further, for $n, m \in N$ we have $|n/m| = |n|/|m|$.*

Proof. We have $|1| = |1^2| = |1|^2$, using HOM, so that $|1| = 0$ or 1. But $|1| \neq 0$ by ZER, so $|1| = 1$.

Also $1 = |1| = |(-1)^2| = |-1|^2$ by HOM, so that $|-1| = 1$ since $|-1| > 0$.

Further, $|-n| = |(-1)n| = |-1| \cdot |n| = 1 \cdot |n| = |n|$, and from $n \cdot (1/n) = 1$ we get $|n| \cdot |1/n| = |1| = 1$, so that $|1/n| = 1/|n|$.

Finally, from $n/m = n \cdot (1/m)$ we get $|n/m| = |n| \cdot |1/m| = |n|/|m|$. □

23.3 Nonarchimedean valuations

From now on we restrict our attention to nonarchimedean valuations.

Proposition 23.2 (Principle of Domination)**.** *Suppose that we have a nonarchimedean valuation $|\cdot|$ on a field F, and that $x, y \in F$ with $|x| \neq |y|$. Then*

$$|x + y| = \max(|x|, |y|).$$

Note the equal sign in this statement!

Proof. Put $s = x + y$, and assume w.l.g. that $|x| < |y|$. Then $|s| \leq \max(|x|, |y|) = |y|$, while

$$|y| = |s - x| \leq \max(|s|, |-x|) = \max(|s|, |x|) = |s|,$$

since otherwise we'd have $|y| \leq |x|$. Hence $|s| = |y| = \max(|x|, |y|)$. □

Corollary 23.3. *Suppose that $x_1, \ldots, x_n \in F$, with $|\cdot|$ nonarchimedean. Then*

$$|x_1 + \ldots, +x_n| \leq \max(|x_1|, \ldots, |x_n|),$$

with equality if $|x_1| > \max(|x_2, \ldots, |x_n|)$.

Proof. Use induction, with the help of MAX, for the inequality. For the equality, put $x_1 = y$ and $x_2 + \cdots + x_n = x$ in the Principle of Domination. □

Corollary 23.4. *For $|\cdot|$ nonarchimedean and $n \in \mathbb{Z}$ we have $|n| \leqslant 1$.*

Proof. Apply the Corollary above with all $x_i = 1$. Then use $|-n| = |n|$. □

Lemma 23.5. *If $|\cdot|$ is a nonarchimedean valuation on F, then so is $|\cdot|^\alpha$ for any $\alpha > 0$.*

Proof. It's easily checked that ZER, HOM and MAX still hold when the valuation we start with is taken to the α-th power. □

[The same does **not** apply to TRI – we need $0 < \alpha \leqslant 1$ for TRI to still always hold.]

23.4 Nonarchimedean valuations on $\mathbb{Q}$

Corollary 23.6. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| = 1$ for all $n \in \mathbb{N}$ then $|\cdot|$ is* **trivial***, i.e., $|x| = 0$ if $x = 0$ while $|x| = 1$ if $x \neq 0$.*

Proof. We then have $|x| = 0$ by ZER, while $|n/m| = |n|/|m| = 1/1 = 1$. □

We'll ignore trivial valuations from now on.

Proposition 23.7. *If $|\cdot|$ is a nonarchimedean valuation on $\mathbb{Q}$ with $|n| < 1$ for some $n \in \mathbb{N}$, then there is a prime p such that $\{n \in \mathbb{N} : |n| < 1\} = \{n \in \mathbb{N} : p$ divides $n\}$.*

Proof. Take the smallest positive integer n_1 such that $|n_1| < 1$. We know that $n_1 > 1$. If n_1 is composite, say $n_1 = n_2 n_3$ with $1 < n_2, n_3 < n_1$, then, by the minimality of n_1, we have $|n_2| = |n_3| = 1$, so that $|n_1| = |n_2| \cdot |n_3| = 1 \cdot 1 = 1$ by HOM, a contradiction. Hence n_1 is prime, $= p$ say.

Then for any n with $|n| < 1$ we can, by the division algorithm, write $n = qp + r$ where $0 \leqslant r < p$. But then $|r| = |n - qp| \leq \max(|n|, |-qp|) = \max(|n|, |-1| \cdot |q| \cdot |p|) < 1$, as $|-1| = 1$, $|q| \leqslant 1$ and $|p| < 1$. By the minimality of p we must have $r = 0$, so that $p \mid n$. □

Next, we show that there is indeed a valuation on $\mathbb{Q}$ corresponding to each prime p. We define $|\cdot|_p$ by $|0| = 0$, $|p|_p = 1/p$ and $|n| = 1$ for $n \in \mathbb{Z}$ and coprime to p, and $|p^k n/m|_p = p^{-k}$ for n and m coprime to p. We call this the **p-adic valuation** on $\mathbb{Q}$.

Proposition 23.8. *The p-adic valuation on $\mathbb{Q}$ is indeed a valuation.*

Proof. The definition of $|\cdot|_p$ ensures that ZER and HOM hold. It remains only to check that MAX holds.

Let $x = p^k n/m$ and $y = p^{k'} n'/m'$,where $n, m, n'm'$ are all coprime to p. Suppose w.l.g. that $k \leqslant k'$. Then $|x|_p = |p^k|_p \cdot |n|_p / |m|_p = p^{-k}$ as $|n|_p = |m|_p = 1$ and $|p|_p = 1/p$. Similarly $|y|_p = p^{-k'} \leq |x|_p$. Hence

$$|x + y|_p = \left| \frac{p^k (nm' + p^{k'-k} n'm)}{mm'} \right|_p = \frac{p^{-k} |nm' + p^{k'-k} n'm|_p}{|mm'|_p} \leqslant p^{-k} = \max(|x|_p, |y|_p).$$

as $|m|_p = |m'|_p = 1$ and $|nm' + p^{k'-k} n'm|_p \leqslant 1$, since $nm' + p^{k'-k} n'm \in \mathbb{Z}$. □

[Note that the choice of $|p|_p = 1/p$ is not particularly important, as by replacing $|\cdot|_p$ by its α-th power as in Lemma 23.5 we can make $|p|_p$ equal any number we like in the interval $(0, 1)$. But we do need to fix on a definite value!]

23.5 The p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$

We first recall how to construct the real field $\mathbb{R}$ from $\mathbb{Q}$, using Cauchy sequences. Take the ordinary absolute value $|\cdot|$ on $\mathbb{Q}$, and define a **Cauchy sequence** to be a sequence $(a_n) = a_1, a_2, \dots, a_n, \dots$ of rational numbers with the property that for each $\varepsilon > 0$ there is an $N > 0$ such that $|a_n - a_{n'}| < \varepsilon$ for all $n, n' > N$. We define an equivalence relation on these Cauchy sequences by saying that two such sequences (a_n) and (b_n) are **equivalent** if the interlaced sequence $a_1, b_1, a_2, b_2, \dots, a_n, b_n, \dots$ is also a Cauchy sequence. [Essentially, this means that the sequences tend to the same limit, but as we haven't yet constructed $\mathbb{R}$, where (in general) the limit lies, we can't say that.] Having checked that this is indeed an equivalence relation on these Cauchy sequences, we define $\mathbb{R}$ to be the set of all equivalence classes of such Cauchy sequences. We represent each equivalence class by a convenient equivalence class representative; one way to do this is by the standard decimal expansion. So, the class π will be represented by the Cauchy sequence $3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \dots$, which we write as $3.14159\dots$. Further, we can make $\mathbb{R}$ into a field by defining the sum and product of two Cauchy sequences in the obvious way, and also the reciprocal of a sequence, provided the sequence doesn't tend to 0.

[The general unique decimal representation of a real number a is

$$a = \pm 10^k(d_0 + d_1 10^{-1} + d_2 10^{-2} + \cdots + d_n 10^{-n} + \dots),$$

where $k \in \mathbb{Z}$, and the digits d_i are in $\{0, 1, 2, \dots, 9\}$, with $d_0 \neq 0$. Also, it is forbidden that the d_i's are all $= 9$ from some point on, as otherwise we get non-unique representations, e.g., $1 = 10^0(1.00000\dots) = 10^{-1}(9.99999\dots)$.]

We do the same kind of construction to define the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$, except that we replace the ordinary absolute value by $|\cdot|_p$ in the method to obtain **p-Cauchy sequences**. To see what we should take as the equivalence class representatives, we need the following result.

Lemma 23.9. *Any rational number m/n with $|m/n|_p = 1$ can be p-adically approximated arbitrarily closely by a positive integer. That is, for any $k \in \mathbb{N}$ there is an $N \in \mathbb{N}$ such that $|m/n - N|_p \leqslant p^{-k}$.*

Proof. We can assume that $|n|_p = 1$ and $|m|_p \leqslant 1$. We simply take $N = mn'$, where $nn' \equiv 1 \bmod p^k$. Then the numerator of $m/n - N$ is an integer that is divisible by p^k. □

An immediate consequence of this result is that **any** rational number (i.e., dropping the $|m/n|_p = 1$ condition) can be approximated arbitrarily closely by a positive integer times a power of p. Thus one can show that any p-Cauchy sequence is equivalent to one containing only those kind of numbers. We write the positive integer N in base p, so that $p^k N = p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r)$ say, where the a_i are base-p digits $\in \{0, 1, 2, \dots, p-1\}$, and where we can clearly assume that $a_0 \neq 0$ (as otherwise we could increase k by 1). We define $\mathbb{Q}_p$, the **p-adic numbers**, to be the set of all equivalence classes of p-Cauchy sequences of elements of $\mathbb{Q}$. Then we have the following.

Theorem 23.10. *Every nonzero element (i.e., equivalence class) in $\mathbb{Q}_p$ has an equivalence class representative of the form*

$$p^k a_0, p^k(a_0 + a_1 p), p^k(a_0 + a_1 p + a_2 p^2), \dots, p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_i p^i), \dots,$$

which we write simply as

$$p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_i p^i + \dots) \qquad [= p^k(\sum_{i=0}^{\infty} a_i p^i)].$$

Here, the a_i are all in $\in \{0, 1, 2, \dots, p-1\}$, with $a_0 \neq 0$.

Thus we can regard p-adic numbers as these infinite sums $p^k(\sum_{i=0}^{\infty} a_i p^i)$. We define the unary operations of negation and reciprocal, and the binary operations of addition and multiplication in the natural way, namely: apply the operation to the (rational) elements of the p-Cauchy sequence representing that number, and then choose a standard equivalence class representative (i.e., $p^k(\sum_{i=0}^{\infty} a_i p^i)$ with all $a_i \in \{0, 1, 2, \dots, p-1\}$, $a_0 \neq 0$) for the result. When we do this, we have

Theorem 23.11. *With these operations, $\mathbb{Q}_p$ is a field, the field of p-adic numbers, and the p-adic valuation $|\cdot|_p$ can be Extended from $\mathbb{Q}$ to $\mathbb{Q}_p$ by defining $|a|_p = p^{-k}$ when $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$. Again, the a_i are all in $\in \{0, 1, 2, \ldots, p-1\}$, with $a_0 \neq 0$.*

We shall skip over the tedious details that need to be checked to prove these two theorems.

Note that, like $\mathbb{R}$, $\mathbb{Q}_p$ is an uncountable field of characteristic 0 (quite unlike $\mathbb{F}_p$, which is a finite field of characteristic p).

We define a **p-adic integer** to be an p-adic number a with $|a|_p \leqslant 1$, and $\mathbb{Z}_p$ to be the set of all p-adic integers.

Proposition 23.12. *With the arithmetic operations inherited from $\mathbb{Q}_p$, the set $\mathbb{Z}_p$ is a ring.*

Proof. This is simply because if a and $a' \in \mathbb{Z}_p$, then $|a|_p \leqslant 1$ and $|a'|_p \leqslant 1$, so that

$$\begin{array}{rll} |a + a'|_p \leq \max(|a|_p, |a'|_p) & \leqslant 1 & \text{by MAX ;} \\ |a \cdot a'|_p = |a|_p \cdot |a'|_p & \leqslant 1 & \text{by HOM ,} \end{array}$$

showing that $\mathbb{Z}_p$ is closed under both addition and multiplication, and so is a ring. □

An p-adic number a is called a **p-adic unit** if $|a|_p = 1$. Then $k = 0$ so that $a = \sum_{i=0}^{\infty} a_i p^i$ with all $a_i \in \{0, 1, 2, \ldots, p-1\}$ and $a_0 \neq 0$. The set of all p-adic units is a multiplicative subgroup of the multiplicative group $\mathbb{Q}_p^{\times} = \mathbb{Q}_p \setminus \{0\}$. This is because if $|a|_p = 1$ then $|1/a|_p = 1/|a|_p = 1$, so that $1/a$ is also a unit.

23.6 Calculating in $\mathbb{Q}_p$

23.6.1 Negation

If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$-a = p^k \left((p - a_0) + \sum_{i=1}^{\infty} (p - 1 - a_i) p^i \right),$$

as can be checked by adding a to $-a$ (and getting 0!). Note that from all $a_i \in \{0, 1, 2, \ldots, p-1\}$ and $a_0 \neq 0$ we have that the same applies to the digits of $-a$.

23.6.2 Reciprocals

If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, then

$$\frac{1}{a} = p^{-k}(a'_0 + a'_1 p + \cdots + a'_i p^i + \ldots)$$

say, where for any i the first i digits $a'_0, a'_1, \ldots, a'_i$ can be calculated as follows: Putting $a_0 + a_1 p + \cdots + a_i p^i = N$, calculate $N' \in \mathbb{N}$ with $N' < p^{i+1}$ such that $NN' \equiv 1 \bmod p^{i+1}$. Then writing N' in base p as $N' = a'_0 + a'_1 p + \cdots + a'_i p^i$ gives $a'_0, a'_1, \ldots, a'_i$.

23.6.3 Addition and multiplication

If $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ and $a' = p^k(\sum_{i=0}^{\infty} a'_i p^i)$ (same k) then $a + a' = p^k((a_0 + a'_0) + (a_1 + a'_1)p + \cdots + (a_i + a'_i)p^i + \dots)$, where then 'carrying' needs to be performed to get the digits of $a + a'$ into $\{0, 1, 2, \dots, p-1\}$. If $a' = p^{k'}(\sum_{i=0}^{\infty} a'_i p^i)$ with $k' < k$ then we can pad the expansion of a' with initial zeros so that we can again assume that $k' = k$, at the expense of no longer having a'_0 nonzero. Then addition can be done as above.

Multiplication is similar: multiplying $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ by $a' = p^{k'}(\sum_{i=0}^{\infty} a'_i p^i)$ gives

$$a \cdot a' = p^{k+k'}(a_0 a'_0 + (a_1 a'_0 + a_0 a'_1)p + \cdots + (\sum_{j=0}^{i} a_j a'_{i-j})p^i + \dots),$$

where then this expression can be put into standard form by carrying.

23.7 Expressing rationals as p-adic numbers

Any nonzero rational can clearly be written as $\pm p^k m/n$, where m, n are positive integers coprime to p (and to each other), and $k \in \mathbb{Z}$. It's clearly enough to express $\pm m/n$ as a p-adic number $a_0 + a_1 p + \dots$, as then $\pm p^k m/n = p^k(a_0 + a_1 p + \dots)$.

23.7.1 Representating $-m/n$, where $0 < m < n$

We have the following result.

Proposition 23.13. *Put $e = \varphi(n)$. Suppose that m and n are coprime to p, with $0 < m < n$, and that the integer*

$$m\frac{p^e - 1}{n} \qquad \textit{is written as} \qquad d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$$

in base p. Then

$$-\frac{m}{n} = d_0 + d_1 p + \cdots + d_{e-1}p^{e-1} + d_0 p^e + d_1 p^{e+1} + \cdots + d_{e-1}p^{2e-1} + d_0 p^{2e} + d_1 p^{2e+1} + \dots.$$

Proof. We know that $\frac{p^e-1}{n}$ is an integer, by Euler's Theorem. Hence

$$-\frac{m}{n} = \frac{m\frac{p^e-1}{n}}{1 - p^e} = (d_0 + d_1 p + \cdots + d_{e-1}p^{e-1})(1 + p^e + p^{2e} + \dots),$$

which gives the result. □

In the above proof, we needed $m < n$ so that $m\frac{p^e-1}{n} < p^e$, and so had a representation $d_0 + d_1 p + \cdots + d_{e-1}p^{e-1}$.

23.7.2 The case m/n, where $0 < m < n$

For this case, first write $-m/n = u/(1-p^e)$, where, as above, $u = m \cdot \frac{p^e-1}{n}$. Then

$$\frac{m}{n} = \frac{-u}{1-p^e} = 1 + \frac{p^e-1-u}{1-p^e} = 1 + \frac{u'}{1-p^e},$$

where $u' = p^e - 1 - u$ and $0 \leqslant u' < p^e$. Thus we just have to add 1 to the repeating p-adic integer $u' + u'p^e + u'p^{2e} + \dots$.

Example What is $1/7$ in $\mathbb{Q}_5$?
From $5^6 \equiv 1 \bmod 7$ (Fermat), and $(5^6-1)/7 = 2232$, we have

$$\begin{aligned}-\frac{1}{7} &= \frac{2232}{1-5^6}\\ &= \frac{2+1\cdot 5+4\cdot 5^2+2\cdot 5^3+3\cdot 5^4}{1-5^6}\\ &= (21423)(1+5^6+5^{12}+\dots)\\ &= 214230\,214230\,214230\,214230\,214230\ \dots .\end{aligned}$$

Hence

$$\frac{1}{7} = 330214\,230214\,230214\,230214\,230214\,230214\ \dots ,$$

which is a way of writing $3 + 3\cdot 5^1 + 0 \cdot 5^2 + 2 \cdot 5^3 + \dots$.

23.8 Taking square roots in $\mathbb{Q}_p$

23.8.1 The case of p odd

First consider a p-adic unit $a = a_0 + a_1 p + a_2 p^2 + \dots \in \mathbb{Z}_p$, where p is odd. Which such a have a square root in $\mathbb{Q}_p$? Well, if $a = b^2$, where $b = b_0 + b_1 p + b_2 p^2 + \dots \in \mathbb{Z}_p$, then, working mod p we see that $a_0 \equiv b_0^2 \bmod p$, so that a_0 must be a quadratic residue mod$p$. In this case the method in Section 23.1 will construct b. Note that if at any stage you are trying to construct $b \bmod n$ then you only need to specify $a \bmod n$, so that you can always work with rational integers rather than with p-adic integers.

On the other hand, if a_0 is a quadratic nonresidue, then a has no square root in $\mathbb{Q}_p$.

Example. Computing $\sqrt{6}$ in $\mathbb{Q}_5$. While the algorithm given in the introduction to this chapter is a good way to compute square roots by computer, it is not easy to use by hand. Here is a simple way to compute square roots digit-by-digit, by hand: Write $\sqrt{6} = b_0 + b_1 \cdot 5^1 + b_2 \cdot 5^2 + \dots$. Then, squaring and working mod 5, we have $b_0^2 \equiv 1 \bmod 5$, so that $b_0 = 1$ or 4. Take $b_0 = 1$ (4 will give the other square root, which is minus the one we're computing.)

Next, working mod 5^2, we have

$$\begin{aligned}6 &\equiv (1 + b_1 \cdot 5)^2 \bmod 5^2\\ 6 &\equiv 1 + 10b_1 \bmod 5^2\\ 1 &\equiv 2b_1 \bmod 5,\end{aligned}$$

giving $b_1 = 3$. Doing the same thing mod 5^3 we have

$$\begin{aligned}6 &\equiv (1 + 3 \cdot 5 + b_2 \cdot 5^2)^2 \bmod 5^3\\ 6 &\equiv 16^2 + 32b_2 \cdot 5^2 \bmod 5^3\\ -250 &\equiv 32b_2 \cdot 5^2 \bmod 5^3\\ 0 &\equiv 32b_2 \bmod 5,\end{aligned}$$

giving $b_2 = 0$. Continuing mod 5^4, we get $b_3 = 4$, so that $\sqrt{6} = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \ldots$.

Next, consider a general p-adic number $a = p^k(a_0 + a_1p + \ldots)$. If $a = b^2$, then $|a|_p = |b|_p^2$, so that $|b|_p = |a|_p^{1/2} = p^{-k/2}$. But valuations of elements of $\mathbb{Q}_p$ are integer powers of p, so that if k is odd then $b \notin \mathbb{Q}_p$. But if k is even, there is no problem, and a will have a square root $b = p^{k/2}(b_0 + b_1p + \ldots) \in \mathbb{Q}_p$ iff a_0 is a quadratic residue mod$p$.

23.8.2 The case of p even

Consider a 2-adic unit $a = 1+a_12+a_22^2+\cdots \in \mathbb{Z}_2$. If $a = b^2$, where $b = b_0+b_12^1+b_22^2+\cdots \in \mathbb{Z}_2$, working mod 8, we have $b^2 \equiv 1 \bmod 8$, so that we must have $a \equiv 1 \bmod 8$, giving $a_1 = a_2 = 0$. When this holds, the construction of Section 23.1 will again construct b. On the other hand, if $a \not\equiv 1 \bmod 8$, then a has no square root in $\mathbb{Q}_2$.

For a general 2-adic number $a = 2^k(1 + a_12 + a_22^2 + \ldots)$, we see that, similarly to the case of p odd, a will have a square root in $\mathbb{Q}_2$ iff k is even and $a_1 = a_2 = 0$.

23.9 The Local-Global Principle

The fields $\mathbb{Q}_p$ (p prime) and $\mathbb{R}$, and their finite extensions, are examples of **local fields**. These are **complete** fields, because they contain all their limit points. On the other hand, $\mathbb{Q}$ and its finite extensions are called **number fields** and are examples of **global fields**. [Other examples of global and local fields are the fields $\mathbb{F}(x)$ of rational functions over a finite field $\mathbb{F}$ (global) and their completions with respect to the valuations on them (local).] One associates to a global field the local fields obtained by taking the completions of the field with respect to each valuation on that field.

Suppose that you are interested in whether an equation $f(x, y) = 0$ has a solution x, y in rational numbers. Clearly, if the equation has no solution in $\mathbb{R}$, or in some $\mathbb{Q}_p$, then, since these fields contain $\mathbb{Q}$, the equation has no solution on $\mathbb{Q}$ either.

For example, the equation $x^2 + y^2 = -1$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{R}$. The equation $x^2 + 3y^2 = 2$ has no solution in $\mathbb{Q}$ because it has no solution in $\mathbb{Q}_3$, because 2 is a quadratic nonresidue of 3.

The Local-Global (or Hasse-Minkowski) Principle is said to hold for a class of equations (over $\mathbb{Q}$, say) if, whenever an equation in that class has a solution in each of its completions, it has a solution in $\mathbb{Q}$. This principle holds, in particular, for quadratic forms. Thus for such forms in three variables, we have the following result.

Theorem 23.14. *Let a, b, c be nonzero integers, squarefree, pairwise coprime and not all of the same sign. Then the equation*

$$ax^2 + by^2 + cz^2 = 0 \tag{22}$$

has a nonzero solution $(x, y, z) \in \mathbb{Z}^3$ iff
$-bc$ is a quadratic residue of a; i.e. the equation $x^2 \equiv -bc \bmod a$ has a solution x;
$-ca$ is a quadratic residue of b;
$-ab$ is a quadratic residue of c.

(Won't prove.) The first of these conditions is necessary and sufficient for (22) to have a solution in $\mathbb{Q}_p$ for each odd prime dividing a. Similarly for the other two conditions. The condition that a, b, c are not all of the same sign is clearly necessary and sufficent that (22) has a solution in $\mathbb{R}$. But what about a condition for a solution in $\mathbb{Q}_2$?

23.9.1 Hilbert symbols

It turns out that we don't need to consider solutions in $\mathbb{Q}_2$, because if a quadratic form has no solution in $\mathbb{Q}$ then it has no solution in a positive, even number (so, at least 2!) of its completions. Hence, if we've checked that it has a solution in all its completions except one, it must in fact have a solution in all its completions, and so have a solution in $\mathbb{Q}$. This is best illustrated by using Hilbert symbols and Hilbert's Reciprocity Law.

For $a, b \in \mathbb{Q}$ the Hilbert symbol $(a, b)_p$, where p is a prime or ∞, and $\mathbb{Q}_\infty = \mathbb{R}$, is defined by

$$(a,b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a nonzero solution in } \mathbb{Q}_p; \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert's Reciprocity Law says that $\prod_p (a, b)_p = 1$. (Won't prove; it is, however, essentially equivalent to the Law of Quadratic Reciprocity.) Hence, a finite, even number of $(a, b)_p$ (p a prime or ∞) are equal to -1.

23.10 Nonisomorphism of $\mathbb{Q}_p$ and $\mathbb{Q}_q$

When one writes rational numbers to any (integer) base $b \geqslant 2$, and then forms the completion with respect to the usual absolute value $|\cdot|$, one obtains the real numbers $\mathbb{R}$, (though maybe written in base b). Thus the field obtained ($\mathbb{R}$) is independent of b. Furthermore, b needn't be prime.

However, when completing $\mathbb{Q}$ (in whatever base) with respect to the p-adic valuation to obtain $\mathbb{Q}_p$, the field obtained **does** depend on p, as one might expect, since a different valuation is being used for each p. One can, however, prove this directly:

Theorem 23.15. *Take p and q to be two distinct primes. Then $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are* **not** *isomorphic.*

Proof. We can assume that p is odd. Suppose first that q is also odd. Let n be a quadratic nonresidue mod$q$. Then using the Chinese Remainder Theorem we can find $k, \ell \in \mathbb{N}$ with $1 + kp = n + \ell q$. Hence, for $a = 1 + kp$ we have $\left(\dfrac{a}{p}\right) = \left(\dfrac{1}{p}\right) = 1$ while $\left(\dfrac{a}{q}\right) = \left(\dfrac{n}{q}\right) = -1$. Hence, by the results of Subsection 23.8 we see that $\sqrt{a} \in \mathbb{Q}_p$ but $\sqrt{a} \notin \mathbb{Q}_q$. Thus, if there were an isomorphism $\phi : \mathbb{Q}_p \to \mathbb{Q}_q$ then we'd have

$$\phi(\sqrt{a})^2 = \phi(\sqrt{a}^2) = \phi(a) = \phi(1 + 1 + \cdots + 1) = a,$$

so that $\phi(\sqrt{a})$ **would** be a square root of a in $\mathbb{Q}_q$, a contradiction.

Similarly, if $q = 2$ then we can find $a = 1 + kp = 3 + 4\ell$, so that $\sqrt{a} \in \mathbb{Q}_p$ again, but $\sqrt{a} \notin \mathbb{Q}_2$. so the same argument applies. □

23.11 The b-adic numbers

Note that for any integer $b \geqslant 2$ one can, in fact, define the ring of b-adic numbers, which consists of numbers $p^k(a_0 + a_1 b + a_2 b^2 + \cdots + a_i b^i + \ldots)$, where $k \in \mathbb{Z}$ and all $a_i \in \{0, 1, 2, \ldots, b-1\}$. However, if b is composite, this ring has nonzero zero divisors (nonzero numbers a, a' such that $aa' = 0$), so is not a field — in fact not even an integer domain. The following exercise proves this for $b = 6$.

Exercise. Define the ring of 6-adic numbers as for the p-adic numbers but with 6 replacing p. Show that the 6-adic numbers are not a field by finding a 6-adic number $\alpha \neq 0, -1$ satisfying $\alpha(\alpha + 1) = 0$.

[Suggestion: put $\alpha = 2 + a_1 \cdot 6 + a_2 \cdot 6^2 + a_3 \cdot 6^3 + \cdots$, and solve $\alpha(\alpha + 1) = 0 \bmod 6^k$ for $k = 2, 3, \ldots$ to obtain $a_1, a_2, a_3, \ldots$ and hence α.]