Introduction to Number Theory
Lecture Notes

Adam Boocher (2014-5), edited by Andrew Ranicki (2015-6)
& Martin Kalck (2016-7)& Milena Hering (2018)

April 18, 2018

1 Lecture 1: Introduction (16.1.2018)

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

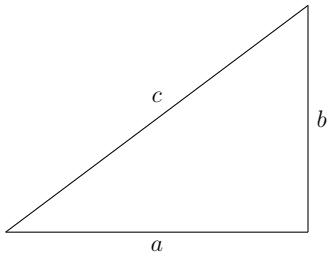
- Elementary Number Theory, by Kenneth H. Rosen, 6th Edition, 2011, Pearson. Library: QA241Ros
- A friendly introduction to number theory by J. H. Silverman, Prentice Hall, 2013.Library: QA241Sil

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

We start with the classical theorem of Pythagoras[1].

Theorem 1.1. *Let a, b, c be the side lengths of a right triangle, (c being the hypotenuse)*



then

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

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

In this lecture we shall study the following

Question 1.2. *What are the natural number (= positive integers* $1, 2, 3 \ldots$*) solutions* (a, b, c) *to the equation* $a^2 + b^2 = c^2$*? Such a solution is called a* **Pythagorean triple (PT)**.

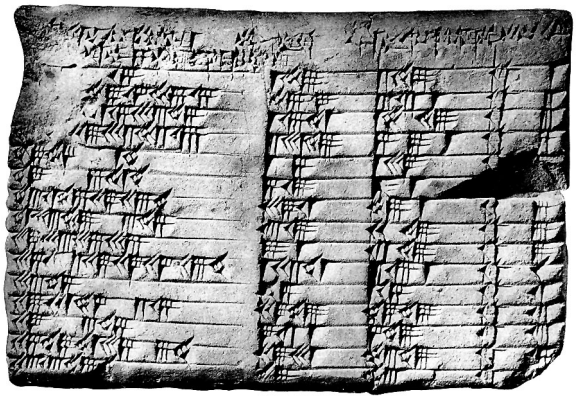
Remark 1.3. *This is a typical question/problem in number theory and also in many other areas of maths. More precisely, we could ask:*

- *are there any solutions at all? (existence question)*
- *how many solutions are there? Finitely many? Infinitely many?*
- *if there are solutions can we write them all down? (classification question)*

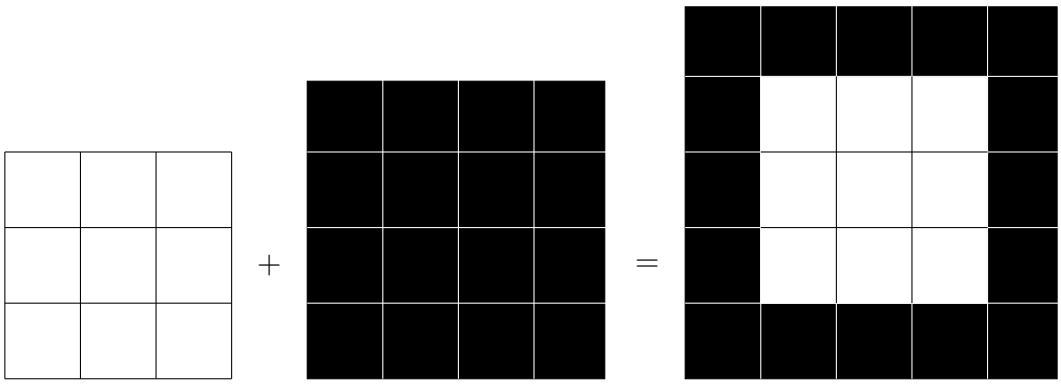
The following example shows that there are Pythagorean triples.

Example 1.4. *Some easy-to-remember Pythagorean triples are e.g.* $(3, 4, 5), (5, 12, 13), (8, 15, 17)$.

Remark 1.5. *Pythagorean triples have been studied already in Babylonean times almost* 4000 *years ago, as documented by the clay tablet see "Plimpton 322" for general explanations and here for how to read it.*



Here is a visualisation of $3^2 + 4^2 = 5^2$



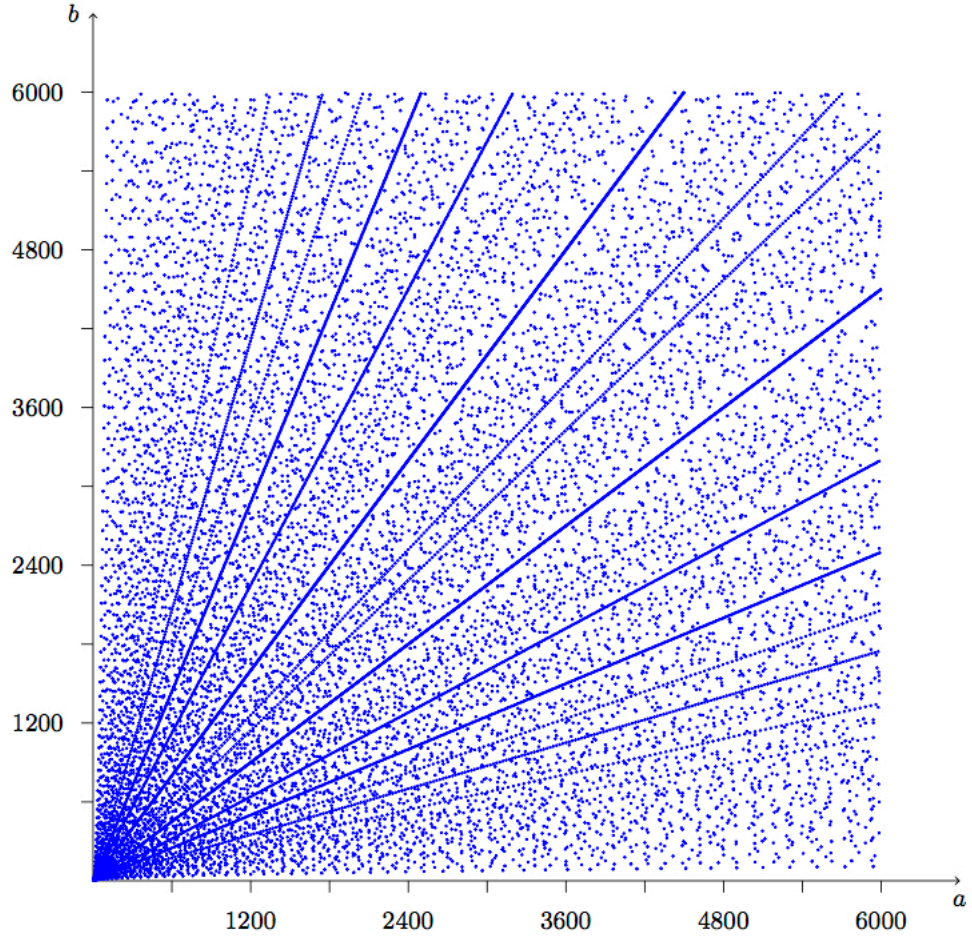
Remark 1.6. *One can show that the same thing does NOT work if we replace squares by cubes. More generally, Fermat's Last Theorem*[2] *states that for all integers $n > 2$ there are no natural number solutions (x, y, z) to the equation*

$$x^n + y^n = z^n. \tag{1}$$

We will treat the case $n = 4$ in Lecture 17 following Fermat's original "method of descent" [3].

Remark 1.7. *The Pythagorean triple $(3, 4, 5)$ has been used by carpenters, masons, ... throughout history to construct and check right angles – this is often called rule of 3-4-5 and is based on Pythagoras' Theorem 1.1.*

We plot the points (a, b) appearing in Pythagorean triples (a, b, c) with $a \leqslant 6000$ and $b \leqslant 6000$.



[2] which has a very fascinating and over 350 year long history, see wikipedia.

[3] It turns out that this method does not work for all n and it is quite unlikely that Fermat had a correct proof for his "last theorem".

Studying this picture carefully, might lead us to the following lemma[4]. It shows that as soon as we have a single solution, we have found infinitely many:

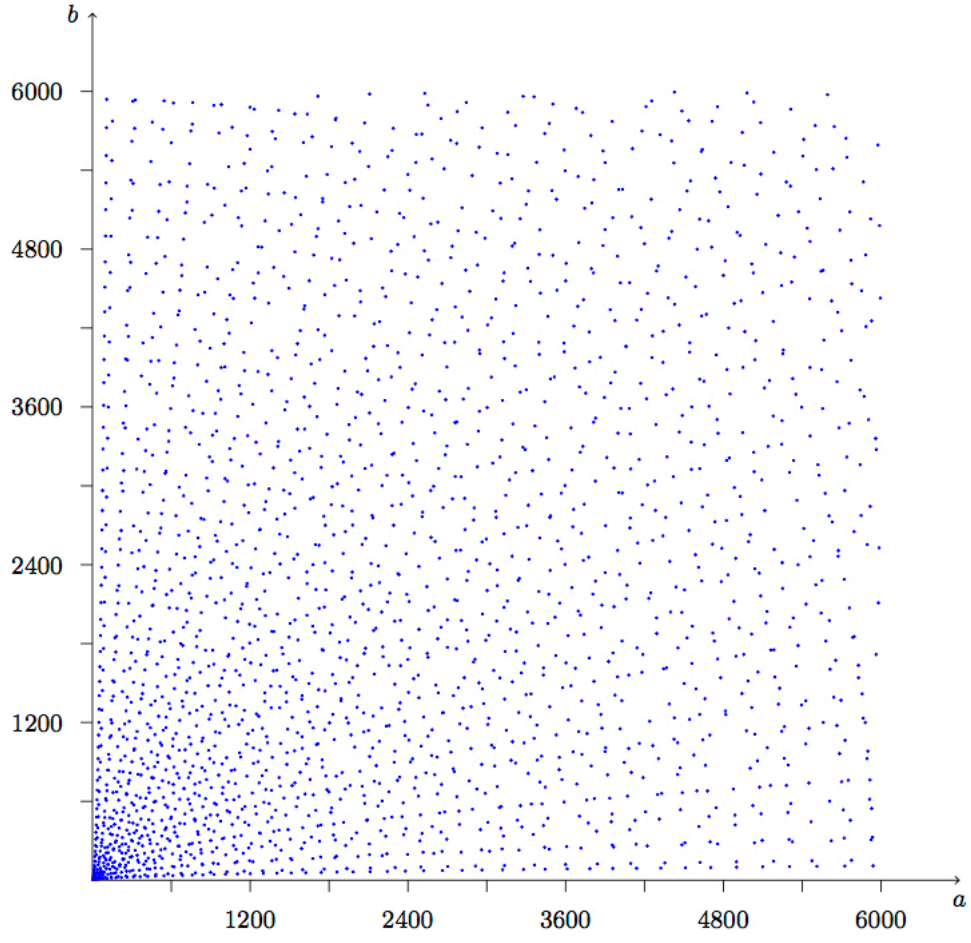
Lemma 1.8. *If (a, b, c) is a Pythagorean triple, and d is any positive integer then so is (da, db, dc). Conversely, if (a', b', c') is a Pythagorean triple and d' is an integer dividing a', b' and c', then $(a'/d', b'/d', c'/d')$ is a Pythagorean triple.*

Proof. Exercise. □

In view of this lemma, we define a **primitive Pythagorean triple (PPT)** to be a Pythagorean triple such that a, b, c have no common factor (for example, the triples in Example 1.4 are all PPTs). This means that there is no natural number d that divides all of a, b, c. We can now rephrase Question 1.2 as:

Question 1.9. *What is the set of PPTs?*

Here is a plot of points (a, b) appearing in primitive Pythagorean triples (a, b, c) with $a \leqslant 6000$ and $b \leqslant 6000$.



[4]What is the connection between the picture and the lemma?

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). 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[5]

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

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! From now on we assume without loss of generality that a is odd.

Hence we can reformulate Question 1.9 as

Question 1.10. *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.*

To answer this question, let's recall two important statements involving primes[6]

Lemma 1.11 (Euclid)**.** *Let a and b be natural numbers and let p be a prime. If p divides the product $a \cdot b$, then p divides a or p divides b (or both a and b!).*

Remark 1.12. *Let (a, b, c) be a PT. 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 Euclid's Lemma 1.11 this means it divides a.*

Euclid's lemma 1.11 is also the key ingredient in proving the so called Fundamental Theorem of Arithmetic (FTA).

Theorem 1.13 (Fundamental Theorem of Arithmetic)**.** *Every natural number $n > 1$ has a unique representation as a product of primes p_i:*

$$n = p_1^{e_1} \cdots p_k^{e_k}, \qquad \text{where } k > 0,\ p_1 < p_2 < \ldots < p_k, \text{ and each } e_j \text{ is a natural number.}$$

Let's get to work! By the discussion above we may assume that a and c are odd and b is even. The **key step** is to observe

[5] These parity considerations are special cases of congruences which we review in Section 4.2.

[6] Recall that a prime number is a natural number $p > 1$, which is only divisible by 1 and p. We'll study prime numbers in more detail in the next lecture and we'll also discuss Lemma 1.11 and Theorem 1.13 there.

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

and to wonder how $(c-b)$ and $(c+b)$ need to be chosen so that we get a PPT (a,b,c). In our situation, it turns out that both $(c-b)$ and $(c+b)$ have to be square numbers (which can be chosen independently as long as they don't have a common prime factor).

To see this we first show that $c-b$ and $c+b$ are relatively prime (so they have no common prime factor). Indeed, suppose that they both shared a common prime factor p, then certainly p should divide their sum and difference. Thus p divides

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

But now b and c have no common prime factor, so using Euclid's Lemma 1.11 again it must be that p divides 2. But p cannot be 2 since $c+b$ is odd! This shows that $c-b$ and $c+b$ are indeed coprime.

From this we see that the only way that their product can be a square is if both factors are squares: the proof relies on the Fundamental Theorem of Arithmetic 1.13. 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[7]. 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 1.14. *Every PPT (a,b,c) with a odd satisfies*

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

where $s > t \geqslant 1$ are odd integers with no common prime factors, which are uniquely determined by (a,b,c).

Conversely, using equations (2), every pair of odd integers $s > t \geqslant 1$ without common prime factors gives rise to a PPT (a,b,c) with a odd.

[7] You may object and say that we've stated the Fundamental Theorem only for natural numbers $n > 1$. So who guarantees that $c-b > 1$? Nobody! This can happen but then $a^2 = c+b$ is automatically a square and $c-b = 1^2$ as well. So we arrive at the same conclusion.

Exercise 1.15. *There are a few things in this Theorem which would be good to double check and clarify for yourself.*

(a) Check the "Conversely, ..." part of the Theorem.

(b) Convince yourself that $s > t$ are indeed uniquely determined by (a, b, c).

(c) Check that (a, b, c) as defined in the Theorem indeed don't have a common prime factor.

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 geometric method which extends a bit more generally, which we will study in the tutorial session.

The theorem may be used to classify all Pythagorean triples as follows:

Corollary 1.16. *Let (a, b, c) be a Pythagorean triple. Then (after possibly swapping a and b) there are odd coprime*[8] *integers $s > t \geqslant 1$ and an integer $d \geqslant 1$ such that*

$$a = dst \ , \ b = d\frac{s^2 - t^2}{2} \ , \ c = d\frac{s^2 + t^2}{2} \tag{3}$$

Conversely, (up to exchanging the roles of a and b) every Pythagorean triple arises in this way.

1.2 A Geometric Derivation

In the first workshop we will explore a geometric method to understand Pythagorean Triples. A detailed solution will be available on LEARN.

Main Points from Lecture 1 and Workshop 1:

- Know how to find infinitely many PPTs
- Have familiarity with basic divisibility arguments.
- Be able to use the geometric method we will discuss in Workshop 1 of using lines with rational slope to find rational points. Memory of this method is important. Memory of the actual formulas is not.

2 Lecture 2: The Primes (19.1.2018)

Notation: $\mathbb{Z}$ = ring of integers $\{0, \pm 1, \pm 2, \dots\}$;
$\mathbb{N}$ = 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.

[8] This is just another way of saying that they don't share a common prime factor.

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**.

Example 2.1. $2, 3, 5, 7, 11, 13, 17, \ldots$ *are primes, whereas* $4, 6, 8, 9, \ldots$ *are composite.*

Theorem 2.2 (Fundamental Theorem of Arithmetic)**.** *Every natural number n has a unique representation as a product of primes p_i:*

$$n = p_1^{e_1} \cdots p_k^{e_k}, \qquad \text{where } k \geqslant 0,\ p_1 < p_2 < \ldots < p_k, \text{ and each } e_j \text{ is a natural number.}$$

[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 nice visualisation of this theorem can be seen at http://www.datapointed.net/visualizations/math/factorization/animated-diagrams/ [9]

Remark 2.3. *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 (in particular, the uniqueness part of the statement!). It shows that prime numbers are the "building blocks" of the natural numbers (if we use multiplication for building them up) and up to reordering the factors we have no choice which building blocks to use. As such prime numbers are very fundamental objects and their definition is elementary. Yet, after over 2000 years of study they are still very mysterious objects and if you ask questions about them it is quite likely that you stumble upon problems which nobody can answer!*

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.

Definition 2.4. *Let n and m be integers. We say that n* **divides** *m if we can write $m = n \cdot d$ for some integer d. We also write $n|m$ in this case.*

The following result known as Euclid's Lemma is the key ingredient in proving the uniqueness part of the Fundamental Theorem of Arithmetic [10].

Lemma 2.5 (Euclid)**.** *Let a and b be natural number and let p be a prime. If p divides the product $a \cdot b$, then p divides a or p divides b (or both a and b!).*

Proof. We assume without loss of generality that p does not divide a. We want to show that p divides b. Since p is a prime number (so only divisible by 1 and p) it follows that the only common divisor of p and a is 1. It follows from Bezout's Lemma 3.10 (which we will prove

[9] Clarify for yourself why this animation is an illustration of the Fundamental Theorem of Arithmetic!

[10] It's a good exercise to try to prove this.

next time) that there are integers x and y such that $px + ay = 1$. Multiplying this equation with b on both sides we obtain

$$bpx + aby = b. \tag{4}$$

Since p divides ab it divides the left side of the equation and therefore it divides b. This completes the proof. □

Remark 2.6. *Other way around, we can characterise prime numbers p as follows: a prime number p is a natural number such that if p divides the product $a \cdot b$ of arbitrary natural numbers a and b, then p divides a or p divides b. Use this to show that 6 is not prime! Try to generalise to an arbitrary composite number.*

Remark 2.7. *Conversely, one can show Euclid's Lemma using the Fundamental Theorem of Arithmetic. This is a good exercise!*

Example 2.8. *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 2.9. *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 procedure is called the **Sieve of Eratosthenes**. For an animation and more information see 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 2.10 (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 the Fundamental Theorem of Arithmetic 2.2 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 $2k+1$ (but this is clear anyway. Why?). One additional exercise on the second homework assignment is to show that there are infinitely many prime numbers of the form $4k+3$. Later in the course we'll be able to treat the case of primes of the form $4k+1$. In fact, these are the special cases $(a,b) = (2,1)$, $(4,3)$ and $(4,1)$ of a much stronger statement:

Theorem 2.11 (Dirichlet's Theorem)**.** *If a and b are positive integers that have no common factors, then there are infinitely many primes of the form $ak+b$ where $k \geqslant 0$ is an integer.*

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[11]. For example it is an open problem, whether there are infinitely many primes of the form n^2+1 with n an integer. 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 2.12. *The sum of the reciprocals of the primes diverges*

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

We will need the following tools[12] for the proof:

0. The Fundamental Theorem of Arithmetic.
1. $1/(1-x) = 1 + x + x^2 + \cdots + x^n + \cdots$. (sometimes called Maclaurin series)
2. $\ln(1-x) = -x - x^2/2 - x^3/3 - \cdots - x^n/n - \cdots$. (this follows from Tool 1 by integration.)
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 $s > 1$.) The idea of the following proof goes back to Leonhard Euler (1737).

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

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

[11] See for example the celebrated Theorem of Green & Tao on arithmetic progressions in the primes for recent progress, closely related to the Theorem of Dirichlet above.

[12] the second tool goes back to Colin Maclaurin who was a maths professor at the University of Edinburgh around 300 years ago.

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 2.2, 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 $\ln \lambda(n) \to \infty$ 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 logarithms. By basic properties of logarithms of products[13] and reciprocals[14], we obtain:[15]

$$\ln(\lambda(n)) = \sum_{\substack{p \leqslant n \\ p \text{ prime}}} -\ln(1 - 1/p).$$

Using Tool 2, we obtain:

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

But then this means that

$$\ln \lambda(n) < \sum_{\substack{p \leqslant n \\ p \text{ prime}}} \frac{2}{p}.$$

[13] $\ln(a \cdot b) = \ln(a) + \ln(b)$

[14] $\ln(x^{-1}) = -\ln(x)$

[15] 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.

Since the left hand side diverges, we have that

$$\sum_{\substack{p \leqslant n \\ p \text{ prime}}} \frac{2}{p}$$

diverges. Division by two yields the result. □

This Theorem is somewhat surprising, since for instance the sum $1+1/4+1/9+1/16+\cdots$ of the reciprocals of squares converges[16], 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, Joseph Bertrand conjectured the following back in 1845:

Conjecture 2.13 ("Bertrand's postulate")**.** *For every natural number $n > 1$ there is a prime p with $n < p < 2n$.*

This conjecture was first proved by Chebyshev in 1852 and later in an elementary and elegant way by Erdös, see Proofs from the Book[17].

In fact, the famous **prime number theorem** discussed below, implies that if we let n go to infinity the number of primes between n and $2n$ also goes to infinity.

To state the prime number theorem, we introduce the function

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

counting all primes $\leqslant n$. E.g. $\pi(5) = 3$, $\pi(100) = 25$, and $\pi(5000) = 669$.

One way of measuring how many prime numbers there are is to consider the fraction $\pi(n)/n$. The prime number theorem says that for large n this fraction approaches $1/\ln(n)$ where $\ln(n)$ is the natural logarithm of n.

Theorem 2.14. *When x 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.

Already in 1850 Chebyshev proved that there exist real numbers C_1, C_2 with $0 < C_1 < 1 < C_2$ such that

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

[16] the limit is $\frac{\pi^2}{6}$ – this result also goes back to Euler (1734) and maybe seen as the starting point for the study of the famous Riemann zeta function.

[17] This is a great book, containing many beautiful and elegant proofs of theorems! It is available for download from within the EASE network.

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

Conjecture 2.16. *(Goldbach Conjecture) Every even integer larger than 2 can be written as a sum of two primes.*

In 2013, the so called **weak Goldbach conjecture** was proved by Harald Helfgott, the proof uses convolutions[18]. We'll study the number theoretic analogue of these convolutions in Lecture 14 (here is an interesting "snapshot" of the proof).

Conjecture 2.17. *(Weak Goldbach Conjecture) Every odd integer $n > 5$ is the sum of three primes.*

Remark 2.18. *One can check that the Goldbach Conjecture implies the weak Goldbach conjecture.*

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

[18] and builds on earlier work by Hardy & Littlewood (1923) and in particular, Vinogradov (1937) who showed that the weak Goldbach conjecture is true for "all sufficiently large numbers". Helfgott's achievement was to show that sufficiently large can be interpreted as larger than 10^{27} and he checked everything below that using computers.

Main Points from Lecture 2:

- Statement of the Fundamental Theorem of Arithmetic.
- Proof of the infinitude of primes and its variants.
- The statement that $\sum 1/p$ diverges.

3 Lecture 3: The greatest common divisor, the lowest common multiple and the Euclidean Algorithm (23.1.2018)

The Euclidean Algorithm dates back at least 2300 years and is one of the oldest algorithms in common use. It's an efficient method to compute the greatest common divisor (see definition below) of two integers and is used in cryptography and error correcting codes. Interestingly, it may also be used to create most rhythms of world music (like Samba, Tango, Bossa Nova, ...), see Euclidean rhythms for a nice introduction and the program for experimenting with these rhythms.

The **greatest common divisor** (gcd) of integers n, m (which are not both zero) is, as the name suggests, the largest positive integer that divides both n and m. Such an integer always exists, as $1 \mid n$ and $1 \mid m$ (so common divisors exist) and further no common divisor can exceed $\min(\mid n \mid, \mid m \mid)$ (so we are taking the maximum over a nonempty finite set). To sum up: $1 \leqslant \gcd(n, m) \leqslant \min(\mid n \mid, \mid m \mid)$.

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

The **least common multiple** (lcm) of $n, m \in \mathbb{N}$ is the smallest natural number that both n and m divide (equivalently, as the name suggests it is the smallest natural number, which is a multiple of both n and m). Again, such an integer exists, as n and m both divide nm. We have inequalities

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

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.*

The following result shows how to compute the gcd of two numbers with known prime factorisation. As you might imagine this builds on the Fundamental Theorem of Arithmetic[19], which was discussed in the previous lecture.

[19] Can you explain why?

Proposition 3.2. *Given $m, n \in \mathbb{N}$ let $p_1, \ldots, p_k$ 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 $\ell = \prod_{i=1}^{k} p_i^{g_i} \cdot \ell'$ say, where ℓ' is a product of primes different from $p_1, \ldots, p_k$, then also $m \mid \prod_{i=1}^{k} p_i^{g_i}$. In other words,

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

so that $e_i \leqslant g_i$. Similarly $n \mid \ell$ gives $f_i \leqslant g_i$. Hence $g_i \geqslant \max(e_i, f_i)$. But 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) Using (iii) for the first equality and Proposition 3.3 below for the second equality, we get

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

□

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 $a = ckd$ and $b = cld$. 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 $c = 1$.

Alternatively, we can use Proposition 3.2 (i) to show this result [20]. □

Remark 3.4. *Actually, a similar argument shows the following: assume $q \mid a$ and $q \mid b$ (so q is a common divisor of a and b but not necessarily the greatest common divisor). Then*

$$\gcd(a/q, b/q) = \frac{\gcd(a,b)}{q} \tag{5}$$

The following result is an important ingredient in the Euclidean algorithm, which we discuss below.

Proposition 3.5. *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 3.6. *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* **integer linear combinations of a and b.**

Remark 3.7. *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 Question 3.6 we allow all integers.*

Example 3.8. *What integers are of the form $8x + 12y$?*

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

$$4k = 8(kx_0) + 12(ky_0). \tag{6}$$

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

$$\{8x + 12y, \ \ | x, y \in \mathbb{Z}\} = \{4k \mid k \in \mathbb{Z}\} = 4\mathbb{Z}. \tag{7}$$

[20] Try this as an exercise.

In general the following is true – next time we will construct an algorithm making this result computational.

Theorem 3.9. *The set of integral linear combinations of two integers a and b is equal to the set of multiples of (a, b)*

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \{(a, b)k \mid k \in \mathbb{Z}\} = (a, b)\mathbb{Z}. \tag{8}$$

Proof. As in Example 16, any linear 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, let d be the smallest positive integer that is a linear combination of a and b.[21] Say that $d = am + bn$. In particular, $d \leqslant a$ and $d \leqslant b$. Now by the division algorithm (see (11)), we know that there are natural numbers q and r such that

$$a = dq + r, \ 0 \leqslant r < d. \tag{9}$$

We would like to show that $r = 0$ (so that $d \mid a$). Now

$$r = a - dq = a - (am + bn)q = (1 - qm)a - nqb \tag{10}$$

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 $d = (a, b)$. □

This result has the following important consequence which is known as Bezout's Lemma or Bezout's identity, which we've used in the proof of Euclid's Lemma 2.5 (in turn, Euclid's Lemma is the key ingredient in the proof i=of the FTA).

Corollary 3.10 (Bezout)**.** *If $(a, b) = d$ then there exists $m, n \in \mathbb{Z}$ with $am + bn = d$. Of particular interest and importance is the case $d = 1$.*

Theorem 3.9 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 $a, b \in \mathbb{N}$ our goal is to compute $g = (a, b)$. We assume[22] that $a \geqslant b$. The **Division Algorithm** is the first key ingredient: using this we can first divide a by b to get

$$a \ = \ bq + r \qquad (q \in \mathbb{N}, 0 \leqslant r < b) \ , \tag{11}$$

[21] Why does such a number exist?

[22] Since $(a, b) = (b, a)$ we don't loose anything by assuming this.

with q the **quotient** and r the **remainder**. The **key observation** is

$$(a, b) \;=\; (b, a - bq) \;=\; (b, r) \tag{12}$$

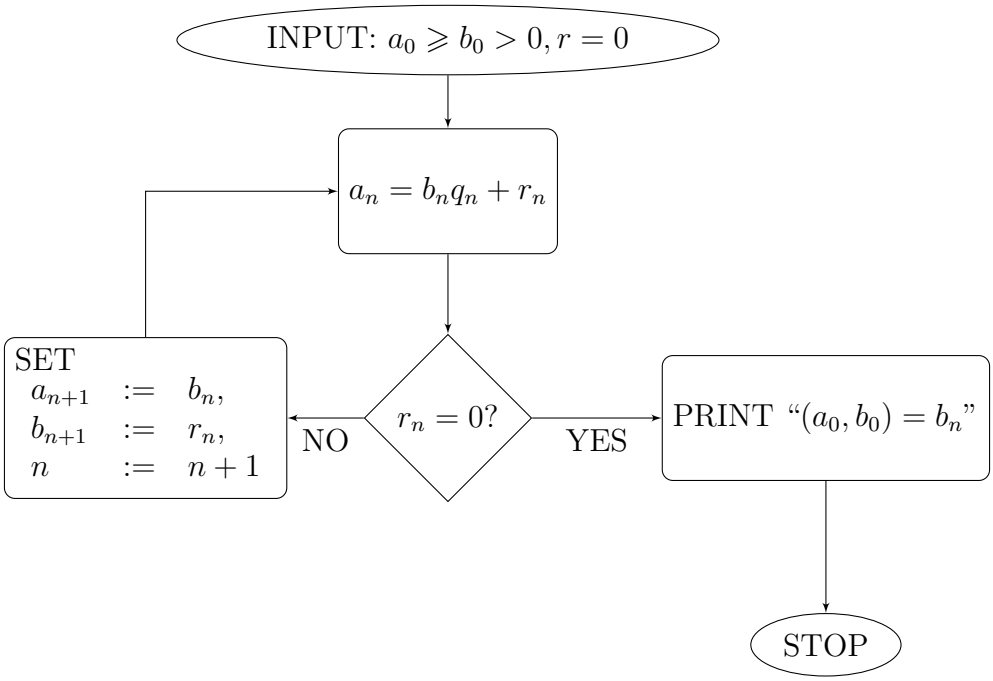
where the first equality comes from $(a, b) = (b, a)$ and Proposition 3.5.

This means if we want to find (a, b) we can now continue with a, b replaced by $a_1 = b$, $b_1 = r$ (note that $a_1 = b \leqslant a$ and $r < b$, so we've simplified our task by reducing the computation to smaller numbers!). Apply the division algorithm again: $a_1 = b_1 q_1 + r_1$ say. Then also $g = \gcd(a_1, b_1) = \gcd(b_1, r_1)$ with $b_1 > r_1$. Continue in this way to obtain a sequence of successively smaller remainders

$$r_0 \;=\; r > r_1 > \cdots > r_k > r_{k+1} \;= 0\ . \tag{13}$$

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 $r_n > r_{n+1}$ as described by the following flowchart :



The following geometric interpretation of the Euclidean algorithm might be helpful too. Can you come up with a similar interpretation for the least common multiple?

Example 3.11. *Use the Euclidean Algorithm to compute* $(87, 51)$*:*

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

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*[23]*:*

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

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 Lecture 4: Linear Diophantine Equations (26.01.2018)

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 $(x, y) \in \mathbb{Z}^2$ [24]. 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 $ax + by = \gcd(a, b)$, in a subsequent lecture. But today we shall concentrate on two questions:

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 $x = (c - by)/a$

[23] In other words this gives a method (an algorithm) for computing the integers m, n predicted by Corollary 3.10. In Lecture 5, we will study an algorithm finding both the gcd and this linear combination in one go.

[24] Do not confuse the ordered pair $(x, y) \in \mathbb{Z}^2$ with the integer $(x, y) = \gcd(x, y) \in \mathbb{Z}$

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

If $ax + by = c$ has an integer solution then c must be an integer multiple of $\gcd(a, b)$.

This is a direct consequence of Theorem 3.9 from the last lecture: the set of linear combinations of two numbers a and b is equal to the set of multiples of $\gcd(a, b)$

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

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 $d = \gcd(a, b)$. 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 "stepping back through the Euclidean Algorithm" will always yield a solution to $d = as + bt$ (see Example 3.11). 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

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

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.[25]

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*

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

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

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

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

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

The Euclidean algorithm for $a = 19$ *and* $b = 5$ *gives*

$$19 = 5 \cdot 3 + 4,$$

$$5 = 4 \cdot 1 + 1$$

Now stepping backwards through this we obtain

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

Finally, multiplying by 100 *yields*

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

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 $(x_1, \ldots, x_n)$:

$$a_1x_1 + \cdots + a_nx_n = b? \tag{14}$$

Important easy cases

1. $g = \gcd(a_1, \ldots, a_n) \nmid b$. Then the LHS of (14) is divisible by g, but the RHS is not, so (14) 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 (14) then determining x_1. Clearly this gives **all** solutions of (14) 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 (14)**:** Make linear changes of variables to successively reduce the minimum modulus of coefficients of (14). 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 (14) in integers:

- Pick the a_i of smallest modulus. If $|a_i| = 1$, can solve (14) as in 2. above.
- Otherwise, when smallest modulus of a_i is $\geqslant 2$: For convenience, we assume that $a_1 > 0$ and a_1 has the smallest modulus among the a_i. 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_j **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 (14) becomes

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

  or

$$a_1u_1 + a_2'x_2 + a_3x_3 \cdots + a_nx_n = b. \tag{15}$$

  This new equation (15) 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 on PIAZZA). 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 think 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 residue 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 is $\{0, 1, 2, 3, 4\}$. Another is $\{-2, -1, 0, 1, 2\}$. Yet another is $\{0, 2016, 27, 3, 10002014\}$.*

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 of Problem 1a on the first Homework sheet. 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:

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

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

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

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 $1! + 2! + 3! + \cdots 100! \bmod 7$

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}.Ho

6. Show that for every integer n there are infinitely many Fibonacci numbers f_k such that n divides f_k. (Hint: Show that the sequence of least positive residues mod n of the fibonacci numbers is a repeating sequence.) (See Homework 2.)

7. If a, b, c, m are integers such that $m > 0$, $d = (c, m)$ and $ac \equiv bc \bmod m$ then $a = b \bmod m/d$. (See Workshop 2.)

Main Points from Lecture 4:

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

5 Lecture 5: The Extended Euclidean Algorithm and Linear Modular Congruences (30.01.2018)

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 our goal is to find the gcd and also a solution to the equation $ax + by = \gcd(a, b)$. We illustrate with an example: $\gcd(91, 77)$. Notice that the following equations hold obviously.

$$E1: \ 91(1) + 77(0) = 91, \quad (1, 0, 91)$$

$$E2: \ 91(0) + 77(1) = 77, \quad (0, 1, 77)$$

We have written the coefficients to the right. Now we run the Euclidean Algorithm in the third coordinate, keeping track of the other coefficients. Notice what happens when we subtract the second equation from the first $E3 = E1 - E2$.

$$E3: \ 91(1) - 77(1) = 14, \quad (1, -1, 14)$$

Now we can set $E4 = E2 - 5 \cdot E3$:

$$E4: \ 91(-5) + 77(6) = 7, \quad (-5, 6, 7).$$

$$E5: \ 91(11) + 77(-13) = 0.$$

What sort of magic is this? 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 5.1. *Compute* $\gcd(561, 306)$ *using the extended Euclidean Algorithm: We begin with the vectors* $v_0 = (1, 0, 561)$ *and* $v_1 = (0, 1, 306)$ *and just subtract one from the other sucessively:*

$$\begin{aligned} v_0 &= (1, 0, 561) \\ v_1 &= (0, 1, 306) \\ v_2 &= (1, -1, 255), \quad (v_2 = v_0 - v_1) \\ v_3 &= (-1, 2, 51), \quad (v_3 = v_1 - v_2) \\ v_4 &= (6, -11, 0), \quad (v_4 = v_2 - 5v_3). \end{aligned}$$

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

For completeness the full algorithm is detailed below.

Proposition 5.2. *Given positive integers $a > b$ and $g = \gcd(a, b)$, we can find integers m, n*

$$ma + nb = d \qquad \textit{(Bézout's Identity 3.10)}$$

as follows:

Put $v_{-2} = (1, 0, a)$, $v_{-1} = (0, 1, b)$. If $(v_{n-2})_3 = q_n(v_{n-1})_3 + r_n$, with $r_n < (v_{n-1})_3$, set

$$v_n = v_{n-2} - q_n v_{n-1},$$

(if v is a vector in $\mathbb{R}^3$, $(v)_3$ denotes the third component of v). At some point the third component of v_{k+1} is 0. Then $v_k = (m, n, g)$ with $ma + nb = g$.

Proof. We will use the same notation here as in the Euclidean Algorithm, see Section 3.1. Note that in the third component we are running the Euclidean Algorithm. Indeed, $(v_{n-2})_3 = a_n, (v_{n-1})_3 = b_n$, and $(v_n)_3 = r_n$. So if k is the smallest number such that the third component of v_{k+1} is zero, then $g = r_k$ is the third component of v_k. Now, v_0 and v_1 lie on the plane $ax + by = z$ in $\mathbb{R}^3$. Further, if v_i and v_{i+1} lie on this plane, then so does $v_{i+2} = v_i - q_* v_{i+1}$ (for some $q_* \in \mathbb{N}$). Hence, by induction, all of $v_0, v_1, v_2, \ldots$ lie on this plane. In particular $v_k = (m, n, g)$ lies on this plane. Hence $ma + nb = g$. □

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

$$ax - ny = c.$$

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, first write

$$d = ax' + ny'$$

Now multiply both sides with the integer (c/d) to get

$$c = (c/d) \cdot d = a(c/d)x' + n(c/d)y' = ax_0 + ny_0$$

with $x_0 = (c/d)x'$ and $y_0 = (c/d)y'$.

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

The set of all solutions is then

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

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*

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

Hence $9 \cdot 2 \equiv 3 \bmod 15$ and thus $9 \cdot 8 \equiv 12 \bmod 15$. 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

$$ax \equiv c \bmod n \tag{16}$$

  is $d = \gcd(a, n)$.
- All solutions of (16) are of the form $x_0 + t(n/d)$ for $t = 0, 1, \ldots, d-1$.

6 Lecture 6: Modular Inverses and the Chinese Remainder Theorem (2.2.2018)

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

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

Beware: such an inverse only exists if $\gcd(a, n) = 1$, see Corollary 5.4.

Also by Corollary 5.4, this solution is unique modulo n. 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 $x \equiv a^{-1}b \bmod n$.

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

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

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 residue class a modulo n has an inverse modulo n (indeed $p \nmid a$ implies $\gcd(a, p) = 1$). For example, we list the inverses modulo 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[26] 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 $x \in \mathbb{Z}$.

Moreover, if x_0 is a solution of this system, then all solutions are of the form

$$x = x_0 + \ell \cdot m_1 \cdot \ldots \cdot m_k,$$

where $\ell \in \mathbb{Z}$. In particular, there is a unique *solution modulo $m_1 \cdot \ldots \cdot m_k$.*

Proof. In fact x can be constructed explicitly. For $i = 1, \ldots, k$ define m_i^* to be the inverse $\bmod m_i$ 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.

We leave the remaining statements as an exercises. □

I think the following exercise is important.

Example 6.4. *Please check the remaining statements of Theorem 6.3.*

Remark 6.5. *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.

[26] Can you say why? What result do we use here?

6.1 Examples and Exercises

See also the text by Adam Boocher, which is available in the background material section on LEARN.

Example 6.6. *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.*

Translating this into a system of equations gives

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

We have $k = 3$ equations, so following the solution in the theorem, we form all products of $k - 1 = 2$ moduli and compute their 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 $3 \cdot 5 \cdot 7 = 105$ all integer solutions are of the form $157 + 105n$. In particular, the smallest positive solution is $x = 52$ (so this is one way of writing the unique solution modulo 105).

There is also an iterative way to find a solution

Example 6.7.

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

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 modulo 6) to obtain

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

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

$$30s + 26 \equiv 3 \bmod 7$$
$$\Leftrightarrow 2s \equiv 5 \bmod 7$$
$$\Leftrightarrow s \equiv 6 \bmod 7.$$

(In the last step we use that $2^{-1} \equiv 4 \mod 7$.) Thus $s = 6$, and $x = 30 \cdot 6 + 26 = 206$.

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 6.8. *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

   (a)

   $$x \equiv 4 \bmod 11$$
   $$x \equiv 3 \bmod 17$$

   (b)

   $$x \equiv 0 \bmod 2$$
   $$x \equiv 0 \bmod 3$$
   $$x \equiv 1 \bmod 5$$
   $$x \equiv 6 \bmod 7.$$

2. (Try to solve this exercise without using Dirichlet's Theorem 2.11 - I find this quite tricky...)

   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:

   $$x \equiv 4 \bmod 6$$
   $$x \equiv 13 \bmod 15$$

   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 Lecture 7: Solving Polynomial Equations and Hensel's Lemma (6.2.2018)

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 mod 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 mod p, what can we say about x mod 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 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 $f(x) \equiv 0 \mod p_i^{e_i}$" if $n = \prod p_i^{e_i}$. In this section we will develop a method for solving polynomial equations of the form $f(x) = 0 \mod p^e$.

Example 7.3. *Continuing Example 7.2, notice that to solve the equation* $2x^3+7x-4 \mod 5$ *we only need to test* $0, 1, 2, 3, 4$. *This is reasonably quick. And we see that all solutions satisfy* $x \equiv 1 \mod 5$. *However, we'd like to avoid check all the numbers* $0, \ldots, 24$ *to solve this equation mod 25. Notice that any solution* x *to*

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

is also a solution mod 5 *(How can we generalise this statement?). Hence* $x \equiv 1 \mod 5$. *Hence* $x = 5t + 1$. *Substituting we see that*

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

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

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

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

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

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

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

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

As you might know (or might have heard) finding solutions of polynomial equations (in one variable x) of degree greater than 4 has been a great challenge for centuries. In the 19. century, mathematicians (see for example wikipedia) were able to show that for polynomials of degree greater than 4 there is (in general) no way of expressing the solutions using only the operations addition/substraction, multiplication/division and taking the n-th root of a number.

Example 7.4. *The solutions of the following polynomial equation cannot be expressed using only the operations addition/substraction, multiplication/division and taking the* n*-th root of a number.*

$$x^5 - 10x + 2 = 0 \tag{17}$$

As we will see later, there is a nice method of finding all solutions of this equation modulo any integer n.[27]

[27] of course one could just try all numbers $0, \ldots, n-1$ but that becomes very inefficient for large n. We'll have to do some trying modulo primes p but once that's done there is a systematic way of doing the remaining work.

A general framework for this type of questions is Galois Theory. One way of finding (better and better approximations to) solutions to polynomial equations numerically is Newton's method discussed below - surprisingly (at least on first sight) this method can be adapted to help with our number theoretic question.

Hensel's Lemma is a number theory version of Newton's calculus method of approximating a solution of a polynomial 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

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

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 different[28] from $(*)$, and proceeds mod prime powers p^k for each prime p separately, and $k = 1, 2, \dots$.

[28] Analysing this led to the theory of p-adic analysis (where p is a prime) which is a powerful technique in modern number theory (for example it was used in the proof of Fermat's last theorem). In p-adic analysis one has the following (on first sight quite strange) notion of distance between integers: two integers x and y are close to each other if their difference $x - y$ is divisible by a high power of p. For example, modulo 3, we have that 1 and 4 are further apart (their difference being 3^1) than 1 and 730 (with difference $3^6 = 729$). With this twisted way of looking at integers, the analogy between the number theoretic version of Newton's method which we'll discuss in the sequel and the original method of Newton in calculus might become clearer...

In the first instance, we only consider one prime p, and how to lift[29] a solution $r \bmod p^{k-1}$ to a solution $s \bmod p^k$, if possible. Of course, we could just try out all the possible lifts $s = s_0 + tp^{k-1} \bmod p^k$ of a solution $s_0 \bmod p^{k-1}$ to find a solution $\pmod{p^k}$ (note that in general there might not exist such a solution - can you think of an easy example of a linear diophantine equation where this happens?) But maybe we can do better...?

Question 7.5. *How can we compute $0 \leqslant t \leqslant p-1$ giving us a lift $s = s_0 + tp^{k-1} \bmod p^k$ of a solution $s_0 \bmod p^{k-1}$?*

To answer this question, we need some input from calculus. Namely, Taylor series of a polynomial $f(x)$ with integer coefficients. Notice that in this case the 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. [30]

Lemma 7.6. *(Integrality Lemma) If $f(x)$ is a polynomial of degree n with integer coefficients then*

$$f(a+b) \;=\; f(a) + f'(a)b + \frac{f''(a)}{2!}b^2 + \cdots + \frac{f^{(n)}(a)}{n!}b^n \tag{18}$$

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

Proof. By the discussion preceeding the Lemma, it remains to show that

$$f(a), f'(a), \frac{f''(a)}{2!}, \ldots, \frac{f^{(n)}(a)}{n!}$$

are polynomials in a with integer coefficients.

To see this consider first the special case of a degree m 'monomial' $f(x) = x^m$. Then

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

For the general case of a degree n polynomial

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

[29] Let r and s be integers. By definition, $s \bmod p^k$ is a **lift** of $r \bmod p^{k-1}$ if $s \equiv r \mod p^{k-1}$ 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.

[30] 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.

we have

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

using that taking derivatives is *linear*, in other words, if f and g are functions and λ, μ are integers, then

$$(\lambda f + \mu g)^{(k)}(x) = \lambda f^{(k)}(x) + \mu g^{(k)}(x).$$

□

Let's check that this Lemma makes sense in an example.

Example 7.7. *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.*

As a consequence, we obtain the following key result which gets us very close to answering Question 7.5.

Corollary 7.8. *Let* p *be a prime and let* $k \geqslant 2$ *and* r, t *be integers. Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *be a polynomial with integer coefficients* $a_i \in \mathbb{Z}$*. Then the following congruence holds*

$$f(r + t \cdot p^{k-1}) \equiv f(r) + f'(r) \cdot t \cdot p^{k-1} \bmod p^k. \tag{19}$$

Proof. Apply (18) to $f(x)$, $a = r$ and $b = t \cdot p^{k-1}$. Then consider this equation modulo p^k. How does the second part of Lemma 7.6 come in to finish the proof? □

Exercise 7.9. *Try to use* (19) *to determine* $t \bmod p$*. When is this possible? What happens in the other cases? This will be answered next time.*

Here is the Wikipedia article on Hensel's Lemma.

Main Points from Lecture 7:

- How to apply the Chinese Remainder Theorem to solving equations mod N via factorization.
- The statement and proof (using Taylor series) of Corollary 7.8.

8 Lecture 8: Hensel's Lemma and Examples (9.2.2018)

Last time we've started to answer the following question:

Question 8.1. *Let n be a natural number and let $f(x)$ be a polynomial with integer coefficients.*

How can we find all solutions $r \bmod n$ to the congruence

$$f(x) \equiv 0 \bmod n \quad ? \tag{20}$$

We have seen that we can use the Chinese Remainder Theorem (in combination with the Fundamental Theorem of Arithmetic) to reduce[31] this question to:

Question 8.2. *Let p be a prime, let $k > 0$ be an integer and let $f(x)$ be a polynomial with integer coefficients.*

How can we find all solutions $r \bmod p^k$ to the congruence

$$f(x) \equiv 0 \bmod p^k \quad ? \tag{21}$$

We've started answering this question, arguing that every solution $s \bmod p^k$ is a *lift* of a solution $r \bmod p^{k-1}$. In other words, if $s \bmod p^k$ is a solution then there exists r such that $s = r + tp^{k-1}$, where t is an integer and $f(r) \equiv 0 \bmod p^{k-1}$ so r is a solution mod p^{k-1}.

So if we assume that we know all solutions $r \bmod p^{k-1}$ already[32], then our question reduces to

Question 8.3. *How can we determine for what values of t*

$$s = r + tp^{k-1} \tag{22}$$

is a solution $\bmod p^k$*?*

Firstly, since we consider $s = r + tp^{k-1}$ modulo p^k, $t = 0$ and $t = p$ will both give $s \equiv r \bmod p^k$ and similarly $t = 1$ and $t = p + 1$ will give equivalent solutions $s \bmod p^k$. This shows that it suffices to determine $t \bmod p$.

We then used ideas from calculus (Taylor series, see the Integrality Lemma 7.6) to show the following formula:

$$f(r + t \cdot p^{k-1}) \equiv f(r) + t \cdot f'(r) \cdot p^{k-1} \bmod p^k. \tag{23}$$

[31] Try to recall how this was done!

[32] To find these solutions, we would then need all solutions $\bmod p^{k-2}$ and so on until we finally arrive at finding all solutions $\bmod p$. For small primes this can even be checked by hand! For larger primes we might need the help of a computer. Also note that we will learn soon that finding solutions of polynomial equations modulo primes p, we can always reduce to finding solutions of polynomials of degree $p-1$ – this very helpful fact is known as Fermat's little Theorem.

Now, we distinguish two cases: $f'(r) \equiv 0 \bmod p$ and $f'(r) \not\equiv 0 \bmod p$.

First case: $f'(r) \equiv 0 \bmod p$

Then $f'(r) = p \cdot u$ for some integer u and therefore, $f'(r) \cdot p^{k-1} \equiv 0 \bmod p^k$.

Hence (23), translates to

$$f(r + t \cdot p^{k-1}) \equiv f(r) + t \cdot 0 \equiv f(r) \bmod p^k. \tag{24}$$

This shows, that we have the following two cases:

(1E) If $f(r) \equiv 0 \bmod p^k$, then EVERY $t \bmod p$ gives a solution $r + t \cdot p^{k-1} \bmod p^k$

(1N) If $f(r) \not\equiv 0 \bmod p^k$, then NO $t \bmod p$ gives a solution $r + t \cdot p^{k-1} \bmod p^k$. In other words, the solution $r \bmod p^{k-1}$ does NOT lift to a solution $s \bmod p^k$.

Before we move on to deal with $f'(r) \not\equiv 0 \bmod p$. We illustrate these two cases with examples.

Example 8.4. (1E) *Let $p = 2$ and $f(x) = x^2 - 1$. Then $r = 1 \in \mathbb{Z}$ is a solution of $f(r) \equiv 0 \bmod 2$, with $f(r) = 0 \in \mathbb{Z}$, $f(r) \equiv 0 \bmod 4$, $f'(r) = 2r \equiv 0 \bmod 2$. 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 $1 \bmod 2$. Thus 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 $s \equiv 3 \bmod 4$.*

(1N) *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 $f(r) = 2 \in \mathbb{Z}$, $f(r) \not\equiv 0 \bmod 4$, $f'(r) = 2r \equiv 0 \bmod 2$. There is no solution $s \in \mathbb{Z}$ of $f(s) \equiv 0 \bmod 4$, let alone one which lifts $1 \bmod 2$.*

Second case: $f'(r) \not\equiv 0 \bmod p$

We are interested in finding $t \bmod p$ such that $f(r + t \cdot p^{k-1}) \equiv 0 \bmod p^k$.

By (23), this translates to

$$f(r) + t \cdot f'(r) \cdot p^{k-1} \equiv 0 \bmod p^k \Leftrightarrow f(r) + t \cdot f'(r) \cdot p^{k-1} = p^k \ell \text{ for some integer } \ell. \tag{25}$$

By our assumption $f(r) \equiv 0 \bmod p^{k-1}$. Thus p^{k-1} divides $f(r)$. Then dividing the right equation in (25) by p^{k-1} gives[33]

$$f(r)/p^{k-1} + t \cdot f'(r) = p\ell \text{ for some integer } \ell \Leftrightarrow f(r)/p^{k-1} + t \cdot f'(r) \equiv 0 \bmod p \tag{26}$$

This yields the following linear modular congruence

$$f'(r) \cdot t \equiv -f(r)/p^{k-1} \bmod p \tag{27}$$

[33] Note that these equations are actually equivalent to (23).

with $f'(r) \not\equiv 0 \bmod p$ by our assumption. Therefore, there exists an inverse $f'(r)^* \bmod p$ of $f'(r) \bmod p$ (see paragraph below Example 6.1). Multiplying both sides of (27) with $f'(r)^*$ yields a unique solution $t \bmod p$

$$t \equiv -f(r)/p^{k-1} \cdot f'(r)^* \bmod p \tag{28}$$

So we've answered Question 8.3. Namely t can be taken to be the integer $-f(r)/p^{k-1} \cdot f'(r)^*$. In combination with (22), we obtain the following formula for the unique[34] lift $s \bmod p^k$ of $r \bmod p^{k-1}$

$$s = r + t \cdot p^{k-1} = r - f(r)/p^{k-1} \cdot f'(r)^* \cdot p^{k-1} = r - f(r) \cdot f'(r)^* \bmod p^k. \tag{29}$$

Before we sum up our findings in a Theorem let's give an example for this case as well.

Example 8.5. *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 $f(r) = 2 \in \mathbb{Z}$, $f'(r) = 1 \not\equiv 0 \bmod 2$. The inverse $(\bmod 2)$of $f'(r)$ is $f'(r)^* \equiv 1 \bmod 2$, so $s = r - f(r) \cdot f'(r)^* = 1 - 2 = -1 \equiv 3 \bmod 4$ is the unique solution of $f(s) \equiv 0 \bmod 4$ lifting $1 \bmod 2$.*

As promised here is a summary of our discussion.

Theorem 8.6. (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 we have the following cases:*

1. $\mathbf{f'(r) \equiv 0 \bmod p}$.

   (1E) *if $\mathbf{f(r) \equiv 0 \bmod p^k}$, then 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 lifts $s = r + tp^{k-1} \bmod p^k$ $(0 \leqslant t \leqslant p-1)$*

   (1N) *$f(r) \not\equiv 0 \bmod p^k$, 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 $r \bmod p^{k-1}$.*

2. $\mathbf{f'(r) \not\equiv 0 \bmod p}$. *Then there is a unique solution $s \bmod p^k$ of $f(s) \equiv 0 \bmod p^k$ lifting $r \bmod p^{k-1}$. This solution is given by*

$$s \equiv r - f(r) \cdot f'(r)^* \bmod p^k. \tag{30}$$

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

   Since $s \equiv r \bmod p$, we obtain $f'(s) \equiv f'(r) \not\equiv 0 \bmod p$. Therefore, applying this Theorem again, we can lift s to a unique solution $u \bmod p^{k+1}$. Continuing in this way, we get solutions $r_k \bmod p^k$ for all $k \geqslant 1$.

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

[34] which gives a solution

Corollary 8.7. *Suppose that r is a solution to $f(r) \equiv 0 \bmod p$ where p is prime. If $f'(r) \not\equiv 0 \bmod p$ 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 $r_2 \bmod p^2$ with $r_2 = r + tp$ with $t = -f'(r)^*(f(r)/p) \bmod p$. 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 8.8. *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

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

is the unique solution mod 25.

Example 8.9. *Here's the polynomial from last time[35]: $f(x) = x^5 - 10x + 2$ Let's try to find all solutions of*

$$f(x) \equiv 0 \bmod 98 \tag{31}$$

First note that $98 = 2 \cdot 7^2$. So by the chinese remainder theorem, we have to consider the system of congruences

$$f(x) \equiv 0 \bmod 2$$
$$f(x) \equiv 0 \bmod 49$$

As we've discussed in the lecture (and one can check directly) the first equation has the unique solution $x \equiv 0 \bmod 2$.

[35] remember that it was an example of a polynomial where there is no formula for the solutions

For the second equation, we use Hensel's Lemma. So we first consider the equation mod7. *One can check that the only solutions are* $r_1 \equiv 1 \bmod 7$ *and* $r_2 \equiv 2 \bmod 7$. *Now* $f'(x) = 5x^4 - 10$. *So* $f'(1) = -5 \equiv 2 \not\equiv 0 \bmod 7$ *and* $f'(2) = 70 \equiv 0 \bmod 7$. *Since* $f(2) = 14 \not\equiv 0 \bmod 49$ *the solution* $r_2 \equiv 2$ *does not lift to a solution* mod49. *It remains to compute the lift* s_1 *of* r_1.

$$s_1 = r_1 - f(r_1) \cdot f'(r_1)^* = 1 - f(1)f'(r_1)^* = 1 - (-7)4 = 29 \bmod 49 \tag{32}$$

So we apply the chinese remainder theorem to

$$x \equiv 0 \bmod 2$$
$$x \equiv 29 \bmod 49$$

The formula from the chinese remainder theorem shows that the unique solution of (31) *is*

$$x = 0 \cdot 49^{-1} \cdot 49 + 29 \cdot 2^{-1} \cdot 2 = 29 \cdot 25 \cdot 2 = 1450 \equiv 78 \equiv -20 \bmod 98. \tag{33}$$

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 $x^5 + x - 6 \equiv 0 \bmod 144$?

8.2 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 8.7 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 $f(4) = 25 \equiv 0 \bmod 25$ 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 8:

- The method and proof of Hensel's Lemma.

9 Lecture 9: The finite field $\mathbb{F}_p$ (13.2.2018)

For the next two weeks we will be studying in detail the set of integers modulo p, where p is prime. The set of congruence classes mod p forms a field, this is an important and great notion which we now review.

9.1 Groups, Rings and Fields

We know the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. These are sets (of numbers) with addition $+$ and multiplication $\cdot$ which satisfy certain rules, also called *axioms* (we've probably used most of these rules without thinking too much about them for most of our lives). It turns out to be very useful[36] to clarify these rules for oneself. This leads to the notion of a *field*[37], which is a special case of a *ring*, which in turn is a special case of a *group* – see Definitions below.

First, we recall the notion of a group. Examples include the set of all integers $\mathbb{Z}$ together with the usual addition of integers as group operation and the set of all symmetries of a geometric object with composition of symmetries as group operation, see Symmetry groups.

Definition 9.1. *A* **group** G *is a set together with an operation*

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

and an identity element $e \in G$ *such that*

- *the operation is associative* $(gh)i = g(hi) \in G$ *for all* $g,h,i \in G$,
- $ge = eg = g \in G$ *for each* $g \in G$,
- *for each* $g \in G$ *there exists an inverse* $g^* \in G$ *such that* $gg^* = g^*g = e \in G$.

[36] This can save us a lot of work! Instead of showing statements for each example (like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...) separately, we can try to deduce the statement from the general rules. This has to be done only once in general and can then be applied in all the special cases/examples. Moreover, once we've clearly formulated the rules we might be able to find more examples satisfying all the axioms – this turns out to be the case as we shall see in this lecture where we find a field $\mathbb{F}_p$ for every prime p.

[37] The most important structures building on fields are *vectorspaces*. But fields show up in many other places throughout maths, for example, when studying (solutions of) polynomial equations, see Galois Theory.

Definition 9.2. *A group G is called* **abelian** *if $gh = hg \in G$ for all $g, h \in G$.*

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

Next, we take an abelian group $(R, +)$ and add another operation $\cdot\colon R \times R \to R$ to define a *ring*. The sets of integers $\mathbb{Z}$, rationals $\mathbb{Q}$, reals $\mathbb{R}$ and complex numbers $\mathbb{C}$ together with the usual addition and multiplication operations are examples of rings.

Definition 9.3. *A* **ring** *R is a set together with two operations*

$$+\colon R \times R \to R$$

(called addition*) and*

$$\cdot\colon R \times R \to R$$

(called multiplication*) such that the following properties hold:*

- *The set R together with addition $+$ is an abelian group. We call the identity element of this abelian group 0 and write $-a$ for the inverse of an element $a \in R$.*
- *The set R satisfies the following properties with respect to multiplication $\cdot$:*
  - *There exists a* multiplicative identity element *(called 1) such that $r \cdot 1 = 1 \cdot r = r$ for all $r \in R$.*
  - *Multiplication is* associative*, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.*
- *Addition and multiplication are compatible in the following sense (*distributive laws*):*
  - *$a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.*
  - *$(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.*

A field is a special case of a ring. As we said above, examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. The integers $\mathbb{Z}$ are an example of a ring, which is NOT a field[38].

Definition 9.4. *A* **field** *F is a ring, such that additionally:*

- *As a ring, F has an additive identity element 0 and a multiplicative identity element 1. We require $0 \neq 1$.*
- *Multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in F$.*
- *Set $F^\times := F \setminus \{0\}$. For every $x \in F^\times$, there exists an $x^{-1} \in F$ such that*

$$x \cdot x^{-1} = 1.$$

Remark 9.5. *The definition of a field says that the multiplication $\cdot$ defines the structure of an abelian group on $F^\times$. So a field combines two abelian groups $(F, +)$ and $(F^\times, \cdot)$ which interact well by the distributive laws.*

[38] Why not?

As a consequence of these rules, you can prove[39]

Proposition 9.6. *Let F be a field. For $a, b \in F$ we have*

1. $a \cdot 0 = 0$;
2. $a \cdot (-b) = -(a \cdot b)$;
3. *if $a \cdot b = 0$ then $a = 0$ or $b = 0$ (or both).*

As further examples of fields, we are now introducing[40] a field $\mathbb{F}_p$ for every prime p. In contrast to the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ we already know, these fields have only finitely many elements!

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 $3 \cdot 5 = 15 \equiv 1 \bmod 7$, 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 $f(x) = \sum_{i=0}^{m} a_i x^i$ in x with coefficients $a_i \in F$, for variable $m \geqslant 0$. The set $F[x]$ has both addition and multiplication

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

but not division. (In fact one can check that $F[x]$ is an example of a ring as defined in Definition 9.3. It is often called *polynomial ring* (with coefficients in F)). The **degree** of a

[39] this is a good exercise to get familiar with fields.

[40] actually this is essentially just a reformulation of things we already know, using the new "language of fields"

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

$$\text{degree}(f(x)+g(x)) \leqslant \max(\text{degree}(f(x)), \text{degree}(g(x))) \ ,$$
$$\text{degree}(f(x)g(x)) \;=\; \text{degree}(f(x)) + \text{degree}(g(x)) \ .$$

We now restrict to congruences modulo a prime p, and consider solutions of equations $f(x) = 0$ for $f(x) \in \mathbb{F}_p[x]$ and $x \in \mathbb{F}_p$. Note that this is equivalent solving $f(x) \equiv 0 \bmod p$ for $x \in \{0, 1, 2, \ldots, p-1\}$ and for $f(x) \in \mathbb{Z}[x]$, see also Lectures 7 and 8 on Hensel's Lemma.

Theorem 9.7. *A nonzero polynomial $f \in \mathbb{F}_p[x]$ of degree n has at most n roots x in $\mathbb{F}_p$. In fact the proof shows that the same statement is true if we replace $\mathbb{F}_p$ by any field F.*

Proof. Use induction on the degree n of f: for $n = 1$, $f(x) = ax + b$ say, with $a \neq 0$, whence $f(x) = 0$ has the unique solution $x = -a^{-1}b$ in $\mathbb{F}_p$. So the statement is true in this case.

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 we can divide the polynomial $f(x)$ by $(x - b)$, (i.e., one step of the Euclidean algorithm for polynomials) to get

$$f(x) = (x - b)f_1(x) + r(x) \tag{34}$$

say, where f_1 is of degree n, and $r(x) \in \mathbb{F}_p[x]$ has degree less than $\text{degree}(x - b) = 1$. So $r(x)$ has degree 0. In other words, $r(x) = c$ for some constant c. Putting $x = b$ in (34) shows that $c = 0$, so $r(x)$ is the zero polynomial. 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[41] 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 $n \geqslant 1$. □

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 9.8. *Note that this theorem is not true if we work modulo 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!

Exercise 9.9. *Find examples of degree 2 polynomials $f(x)$ modulo a prime p, which either*

1. *have no roots $x \in \mathbb{F}_p$,*
2. *have just one root $x \in \mathbb{F}_p$,*
3. *have two roots $x_1, x_2 \in \mathbb{F}_p$.*

[41] What are we using here?

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 9.10 (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 9.11 (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. □

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 proof of Wilson's Theorem
- Statement (and your favorite proof) of Fermat's Little Theorem

10 Lecture 10: Primitive Roots and the Structure of $\mathbb{F}_p$ (16.2.2018)

10.1 A Warmup for Things to Come:

We start today with defining the **Euler φ-function**[42]:

Definition 10.1. *For a natural number n, we define*

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

This yields a function $\varphi\colon \mathbb{N} \to \mathbb{N}$, which is called **Euler φ-function** *or* **Euler's totient function**.

Remark 10.2. *Here is one way of rephrasing Definition 10.1:*

$$\varphi(n) = \textit{ number of } \text{invertible } \textit{residue classes } \text{mod } n\ .$$

The Euler φ-function shows up in many areas of mathematics and has applications in cryptography. At the age of 19, Gauß famously observed[43] *that a regular n-gon is constructible using only a compass and a straightedge if and only if $\varphi(n) = 2^t$ for some $t \geqslant 0$. This solved an over 2000 year old problem, see wikipedia for more details.*

Example 10.3. *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, which will be important to show that the group $(\mathbb{F}_p^\times, \cdot)$ is cyclic, see Theorem 10.17 :

Theorem 10.4. *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. Here is a good **strategy**[44] to show something like this is to establish a bijection between the numbers $\{1, \ldots, n\}$ and the things you are trying to count.

[42] This is an example of a multiplicative function a notion which we are going to introduce next time.

[43] apparantly, before getting out of bed one morning...

[44] Like proof by induction or proof by contradiction, this is a very useful general strategy! The more of these proof and problem solving strategies you know the more problems you'll be able to solve by yourself – in some sense learning methods and strategies like this one is at least as important as learning the "real" mathematical content.

For each integer $1 \leqslant a \leqslant n$, by definition, the greatest common divisor (a, n) divides n. Therefore, for every integer a with $1 \leqslant a \leqslant n$ there is a unique divisor d of n such that a is contained in the set

$$\{1 \leqslant a \leqslant n \mid (a, n) = d\}.$$

It follows that

$$\bigcup_{d|n} \{1 \leqslant a \leqslant n \mid (a, n) = d\} = \{1, \ldots, n\} \tag{35}$$

with a *disjoint* union on the left hand side.

We claim that $\{1 \leqslant a \leqslant n \mid (a, n) = d\}$ has exactly $\varphi(n/d)$ elements. By Proposition 3.3[45], $(a, n) = d$ is equivalent to $(a/d, n/d) = 1$. Use this to prove our claim[46]. In combination with (35), we have shown that

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

Now whether we sum $\varphi(d)$ or $\varphi(n/d)$ we should get the same thing[47]. This finishes the proof. □

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

Example 10.5. *In this table for each divisor $d|12$ the second row groups together all the numbers $1 \leqslant a \leqslant 12$ such that the greatest common divisor $(a, 12) = d$:*

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

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

[45] This shows only one direction. Try to fill in the other direction yourself.

[46] Again establishing a bijection is the key.

[47] Can you say why? Find a bijection!

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

We are now going to explore the structure of the field $\mathbb{F}_p$, using the rudiments of group theory[48].

Today, we are mainly interested in a very special kind of abelian groups – so called cyclic groups.

Definition 10.6. *Let G be a group with identity element e. We say that an element $g \in G$* **generates** *G if the set of all powers of g and g^{-1} are equal to all of G. In other words, we have an equality of sets*[49]

$$G = \{\ldots, g^{-n}, g^{-n+1}, \ldots, g^{-1}, g^0 = e, g^1, \ldots, g^{n-1}, g^n, \ldots\} \tag{36}$$

If such a g exists, we say that G is **cyclic** *and we write $G = \langle g \rangle$.*

Remark 10.7. *Note that a cyclic group G is necessarily abelian. Indeed, by definition elements $x, y \in G$ may be written as $x = g^n$ and $y = g^m$ for some integers n, m. Therefore,*

$$yx = g^m g^n \;=\; g^{m+n} \;=\; g^{n+m} \;=\; g^n g^m = xy \in G$$

shows that G is abelian. In the middle of this chain of equations, we've used that addition in $\mathbb{Z}$ is abelian. In other words a cyclic group is abelian since $\mathbb{Z}$ is.

Definition 10.8. *If $g \in G$, we say that the* **order** *of g is the smallest positive integer n such that $g^n = e$, or infinity if $g^n \neq e$ for all $n \geqslant 1$.*

Note that if G is finite, then for every element $g \in G$, there is a power m such that $g^m = e$. Indeed, since G is finite, we must have $g^\ell = g^n$ for some $\ell > n$. Then $g^{\ell - n} = e$.

Example 10.9. (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.*

Proposition 10.10. *Let G be a finite group and $g \in G$. Then the order of g divides the order of G.*

Proof. We present two proofs here. The first one uses Lagrange's theorem from Fundamentals of Pure Mathematics. The second one applies only to $\mathbb{F}_p^\times$, which is the only case we need, and it uses the methods we have developed in this course.

1. Using Lagrange's theorem. Let d be the order of g. Consider the subgroup $H = \{e, g, g^2, \ldots, g^{d-1}\}$ of G. By Lagrange's Theorem, we have $d = |H| \mid |G|$.

[48] Recall from last time that any field F is build up from two abelian groups $(F, +)$ and $(F^\times, \cdot)$, which interact well (distributive laws)

[49] It is important to note that the set on the right hand side can be finite – namely, if $g^n = e$ for some integer $n \neq 0$.

2. For $\mathbb{F}_p^\times$, using factorisations of polynomials and Fermat's little theorem.

   Let $g \in \mathbb{F}_p^\times$ be an element of order d. In particular, $g^d - 1 = 0$. By the Division algorithm (11), there are integers q and $0 \leqslant r < d$ such that $p - 1 = qd + r$. Then we have

$$(x^{p-1} - 1) = (x^d - 1)Q(x) + (x^r - 1), \tag{37}$$

   where $Q(x) = x^{(p-1)-d} + x^{(p-1)-2d} + \cdots + x^{(p-1)-qd}$. (Check this by simplifying the right hand side). Consider this as an equation in $\mathbb{F}_p[x]$. Setting $x = g$ and using that $g^{p-1} - 1 = 0$ in $\mathbb{F}_p$ by Fermat, and our assumption that $g^d - 1 = 0$, we see that $g^r = 1$. Since $r < d$ and g has order d we get that $r = 0$ hence $d \mid p - 1$.

□

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

Proposition 10.11. *Let G be an arbitrary group with identity element e and let k be an integer. If $g \in G$ has finite order n, then $g^k \in G$ has order $n/(n,k)$.*

Proof. By Definition, the order of g^k is the smallest integer $j > 0$ such that $(g^k)^j = e \in G$. It follows that $g^{kj} = e$. The Division Algorithm (11) applied to kj and n yields $kj = nq + r$ for integers q and $0 \leqslant r < n$. It follows that

$$e = g^{nq+r} = (g^n)^q g^r = eg^r = g^r. \tag{38}$$

So $r = 0$, since $n > r$ is the smallest positive integer with $g^n = e$. This means that $n \mid kj$, so $\operatorname{lcm}(n,k) \mid kj$. On the other hand, $(g^k)^{\frac{\operatorname{lcm}(n,k)}{k}} = e$, so it follows that

$$kj = \operatorname{lcm}(n,k) = k \cdot n/(n,k) \tag{39}$$

and the claim follows. □

This has the following consequence which will be important later.

Corollary 10.12. *Let G be a group.*

If $g \in G$ has order n, then there are precisely $\varphi(n)$ elements of order n in the sequence $g^0, g^1, \ldots, g^{n-1}$.

Proof. Use Proposition 10.11, the fact that $g^0, g^1, \ldots, g^{n-1}$ are pairwise different and the definition of φ. □

Note that 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 $(F^\times, cdot)$, 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**. Here are some examples.

Example 10.13. ***Some orders of elements in*** $(\mathbb{F}_7, +)$ ***and*** $(\mathbb{F}_7^\times, \cdot)$

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 $\times$	1	3	6	3	6	2

Example 10.14. ***Some orders of elements in*** $(\mathbb{F}_{11}, +)$ ***and*** $(\mathbb{F}_{11}^\times, \cdot)$

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 $\cdot$	1	10	5	5	5	10	10	10	5	2

Example 10.15. ***Some orders of elements in*** $(\mathbb{F}_{13}, +)$ ***and*** $(\mathbb{F}_{13}^\times, \cdot)$

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 $\cdot$	1	12	3	6	4	12	12	4	3	6	12	2

Hopefully the pattern in the table for the operation $+$ is clear.

Exercise 10.16. *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 $\cdot$ 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 10.17. *Let p be a prime. $\mathbb{F}_p^\times$ is a finite cyclic group of order $p-1$.*

We will prove this theorem at the end of the lecture. Note that our proof won't tell us how to find a generator of $\mathbb{F}_p^\times$. We'll only prove that a generator exists. Finding generators turns out to be a non-trivial problem in general.

First we need some preparation.

Definition 10.18. *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 a primitive root 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.

Theorem 10.19. *For all $d \mid p-1$, the number of elements of order d in $\mathbb{F}_p^\times$ is $\varphi(d)$.*

Proof. Let $N(d)$ denote the number of elements of order d in $\mathbb{F}_p^\times$. We proceed in two steps. First we show that $N(d) \leqslant \varphi(d)$. If $N(d) = 0$ we are done, since $0 \leqslant \varphi(d)$. So now suppose that $N(d) > 0$. This means that 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 modulo p. Now these guys are all roots of the equation $x^d - 1$. (Why?) So now if x is some element of order d then it also must be a solution to $x^d - 1$, and hence it is one of the elements a^k. However, an element of the form a^k has order d if and only if $(k, d) = 1$. (Why?)

Thus we have shown that the elements of order d are precisely those elements a^k with $(k, d) = 1$. In other words, there are $\varphi(d)$ of them.

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

$$p - 1 = \sum_{d|p-1} N(d) \leqslant \sum_{d|p-1} \varphi(d)$$

where the inequality follows from Step 1. But now by Theorem 10.4, 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. □

Now we are ready to show that $\mathbb{F}_p^\times$ is cyclic[50]

[50]For field and group enthusiasts: our proof actually shows

Proof of Theorem 10.17. Theorem 10.19 shows that the number of elements of order $p-1$ in $\mathbb{F}_p^\times$ is $\varphi(p-1) > 0$, 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. □

Actually, Theorem 10.19 gives a bit more.

Corollary 10.20. *The special case $d = p-1$ of Theorem 10.19 shows that $\mathbb{F}_p^\times$ has exactly $\varphi(p-1)$ 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 10.21. *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. Since g is a primitive root, we may write $B = g^b$ and $X = g^x$. So our equation becomes $g^{nx} = g^b$, giving $nx \equiv b \bmod p-1$. Hence, using our results on linear congruences, this has a solution x if and only if $\gcd(n, p-1) \mid b = \log_p B$. In this case we know that the number of solutions x is $\gcd(n, p-1)$ (see Theorem 5.3) and therefore we get $\gcd(n, p-1)$ solutions $X = g^x$. □

Remark 10.22.

- *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.,*
- *The special case $n = 2$ (this corresponds to taking square roots in $\mathbb{F}_p$) will be studied in Lectures 15 and 16 including the celebrated so called* quadratic reciprocity law[51] *due to Gauss.*

Theorem. *Let F be any field. Let $G \subseteq (F \setminus \{0\})$ be a* finite *subgroup. Then G is cyclic.*

Do you see how/why?

[51] this law will help us to compute whether or not there exist square roots of an integer B modulo p without using the discrete logarithm. However, it won't tell us what the square roots are in case they exist.

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 Lecture 11: Multiplicative Functions (27.2.2018)

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[52] in general.

11.1 Arithmetic functions - more about φ

Arithmetic functions are functions $f : \mathbb{N} \to \mathbb{C}$ usually having some arithmetic significance. An important subclass of such functions are the **multiplicative functions**:

Definition 11.1. *An arithmetic function f is called* **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, $f(1) = 1$.

Remark 11.2. *Why do we have the convention $f(1) = 1$? 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 $f(1) = 1$. This justifies our convention.*

Proposition 11.3. *If f is multiplicative and $n_1, \ldots, n_k$ are pairwise coprime ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) then*

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

This is readily proved by induction. Using the Fundamental Theorem of Arithmetic we get:

Corollary 11.4. *Let n be a natural number. Write $n = p_1^{e_1} \ldots p_k^{e_k}$ for distinct primes p_i. Then*

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

[52] We'll see some beautiful applications to a certain kind of prime numbers (so called *Mersenne primes*) in Lecture 13 and multiplicative functions are in the background in Lectures 15 and 16 too.

In particular, multiplicative functions f are completely determined by their values on prime powers p^k.

On first sight, it might seem that there aren't too many multiplicative functions. This intuition is wrong. The following example lists a few and later today we'll see how to produce an infinite number of multiplicative functions from a single multiplicative function!

Example 11.5. *Some examples of multiplicative functions are*[53]

- *The identity function:* $\mathrm{id}(n) = n$*;*
- *The constant function* $c(n) = 1$*;*
- *The '1-detecting' function* $\Delta(n)$*, defined by* $\Delta(1) = 1$ *and* $\Delta(n) = 0$ *for all* $n \in \mathbb{N} \setminus \{1\}$*;*
- *For each integer* $k > 0$ *we have a multiplicative function* $g_k(n) = \gcd(k, n)$*. This gives an infinite number of multiplicative functions!* [54] g_1 *is just the constant function* $c(n) = 1$ *from above.*

We define two more arithmetic functions σ and τ. Later we'll show that they are multiplicative too.

Definition 11.6.
- $\tau(n) = \sum_{d|n} 1$*, is the function counting the number of divisors of a natural number* n*;*
- $\sigma(n) = \sum_{d|n} d$*, is the function computing the sum of the divisors of* n*.*

We can imagine that number theorists are very interested in studying τ and σ. Let's start with an example.

Example 11.7. *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.*

[53] convince yourself that these functions are indeed multiplicative!

[54] Check that they are indeed all different.

In the example, we've seen that τ is multiplicative in a special case. This turns out to be true in general

Lemma 11.8. *The divisor counting function $\tau(n)$ is multiplicative.*

Proof. If a and b are coprime integers, then any divisor of $a \cdot b$ can be written as a product of a divisor of a times a divisor of b in a unique way[55]. Conversely, every product of divisors of a and b is a divisor of $a \cdot b$. Hence the number of divisors of $a \cdot b$ is equal to the number of divisors of a times the number of divisors of b. This proves the claim. □

Example 11.9. *Notice that the Lemma 11.8 is not true is if a and b fail to be coprime. For instance if $a = 4, b = 12$ then the divisor $d = 4$ 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 of Lemma 11.8 is that if a and b are coprime, then there's exactly one way to do this!

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

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

$\widehat{f}$ 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 $f = \mathrm{id}$ then

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

Exercise 11.11. *For further practice, check that $\widehat{c} = \tau$, where c is the constant function $c(n) = 1$ for all n.*

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

Proposition 11.12. *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

$$F(ab) = F(a)F(b), \tag{40}$$

[55] Can you say why this is true?

given that $f(ab) = f(a)f(b)$. By definition, the left hand side of (40)

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

Now by the proof of Lemma 11.8 , we know that every divisor d of ab can be written uniquely as a product $d = nm$ of divisors n of a and and m of b. Hence,

$$F(ab) = \sum_{\substack{n|a \\ m|b}} f(nm) = \sum_{\substack{n|a \\ m|b}} f(n)f(m) \tag{41}$$

where the last equality uses that f is multiplicative[56].

Let's try to compute the right hand side of (40). The definition shows

$$F(a)F(b) = (\sum_{n|a} f(n))(\sum_{m|b} f(m)). \tag{42}$$

Using distributive laws this can be rewritten as

$$F(a)F(b) = (\sum_{n|a} f(n))(\sum_{m|b} f(m)) = \sum_{\substack{n|a \\ m|b}} f(n)f(m). \tag{43}$$

Now, the right hand side of (43) equals the right hand side of (41). This completes the proof.

□

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 $\mathrm{id}(n) = n$ and $c(n) = 1$.

The following exercise shows that given a multiplicative function we can use the "hat"-operation to get infinitely many (pairwise different) multiplicative functions.

Exercise 11.13. *Let f_0 be an arithmetic function and define recursively $f_{i+1} = \widehat{f_i}$ for all $i \geqslant 0$. Show that the arithmetic functions f_1, f_2, ..., are pairwise different.*

To close our tour of multiplicative functions for today, let's have a look at our friend φ, the Euler φ-function from last time again. Recall that it was 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!

[56] Clarify for yourself why this works.

Proposition 11.14. *If p is prime and k is a positive integer then*

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}) = p^{k-1}(p-1). \tag{44}$$

In particular[57]*, $\varphi(p) = p - 1$.*

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 which 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 11.15. *Euler's φ function is multiplicative.*

Before we prove this result let's look at some consequences and examples.

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 Proposition 11.14 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 11.16. *If n is an integer, then*

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

Remark 11.17. *Notice that this is quite a nice formula, but in practice it's probably easiest to just remember the formula $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ and use the fact that φ is multiplicative to compute φ.*

Example 11.18.

$$\varphi(300) = \varphi(3)\varphi(4)\varphi(25) = (3-1)(4-2)(25-5) = 2 \cdot 2 \cdot 20 = 80.$$

Proof of Theorem 11.15. Take n and n' coprime, and let

$$\{1 \leqslant i \leqslant n \mid \gcd(i, n) = 1\} = \{a_1 < a_2 < \cdots < a_{\varphi(n)}\}, \tag{45}$$

the **invertible residue classes** (mod n). Similarly, let

$$\{1 \leqslant j \leqslant n' \mid \gcd(j, n') = 1\} = \{a'_1 < a'_2 < \cdots < a'_{\varphi(n')}\}. \tag{46}$$

[57] We've seen this in the last lecture already

Let's outline the idea of the proof: numbers that are coprime to nn' are obtained by combining pairs of numbers (a_i, a'_j) (where a_i is from the set (45) and a'_j is from the set (46)) using the Chinese Remainder Theorem. It follows that the number of integers coprime to nn' is equal to the size of the first set (which by definition is $\varphi(n)$) multiplied by the size of the second set (which is $\varphi(n')$).

Let's implement this idea. If $x \in \{1, 2, \ldots, nn'\}$ and $\gcd(x, nn') = 1$ then $\gcd(x, n) = 1 = \gcd(x, n')$, so that

$$x \equiv a_i \bmod n \qquad\qquad x \equiv a'_j \bmod n' \tag{47}$$

for some pair (a_i, a'_j) from the sets (45) and (46) above . Conversely, given such a pair (a_i, a'_j) we can solve (47) using the CRT to get a solution $x \in \{1, 2, \ldots, nn'\}$ with[58] $\gcd(x, nn') = 1$. Thus we have a bijection between such x and such pairs (a_i, a'_j). Hence

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

□

Main Points from Lecture 11:

- Definition and basic properties of multiplicative functions.
- $\tau(n)$ is a multiplicative function.
- f multiplicative implies $\widehat{f}$ multiplicative.
- Euler φ-function is multiplicative and
- $\varphi(p^k) = p^k - p^{k-1}$.

12 Lecture 12: The multiplicative group of units mod n, Euler's Theorem and more about Primitive Roots (2.3.2018)

Aim: Study what happens with the constructions and results from Lecture 10 if we replace the prime p by an arbitrary natural number n.

It turns out that a few things "carry over" (for example, Euler's theorem 12.10 beautifully generalises Fermat's little theorem 9.11. This involves Euler's φ-function which we are now able to compute (see last lecture). Also, we will generalise the definition of primitive roots to this setup – however, primitive roots $\pmod n$ do NOT always exist!) while others break down in general (existence of primitive roots, group of units is cyclic).

We begin with a definition, which is just a new name for a thing we already know.

[58] Please make sure you understand why this works.

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

$$ax \equiv 1 (\mathrm{mod}\, n)$$

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

The following Proposition rewords and summarises things we already know (part (i) was done in Lectures 5 and 6) and I encourage you to think about part (ii) – the things we need to check aren't really new.

Proposition 12.2. *We have*

(i) a is a unit $\mathrm{mod}\, n$ *if and only if a, n are coprime.*

(ii) The set of units mod n forms a finite abelian group using the usual multiplication $\mathrm{mod}\, n$*. We call it the* **group of units** $\mathrm{mod}\, n$ *and denote*[59] *it by $\mathbb{Z}/n\mathbb{Z}^\times$. The group $\mathbb{Z}/n\mathbb{Z}^\times$ has order*[60] *$\varphi(n)$.*

Example 12.3. *1. We've seen that if $n = p$ is a prime then $\mathbb{Z}/n\mathbb{Z}^\times$ is a cyclic group of order $\varphi(p) = p - 1$ (indeed, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and thus $\mathbb{Z}/p\mathbb{Z}^\times = \mathbb{F}_p^\times$, which is cyclic by Theorem 10.17).*

2. Let's look at some examples for n not prime.

(a) Take $n = 4$, then $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, is the set of integers modulo 4. The units are the numbers coprime to 4, which are

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

This is a group of order two. Every group of order two is cyclic[61]*. Let's make this explicit. Since $3^2 \equiv 1 \bmod 4$, we've shown that 3 is a generator of the group $\mathbb{Z}/4\mathbb{Z}^\times$ and also that 3 has order $\varphi(4) = 2$, so we see again that $\mathbb{Z}/4\mathbb{Z}^\times$ is cyclic.*

(b) For $n = 6$, we get $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$ and

$$\mathbb{Z}/4\mathbb{Z}^\times = \{1, 5\}.$$

Which is again cyclic. This time 5 is the generator.

[59] 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.

[60] meaning number of elements

[61] in fact there is just one such group up to isomorphism (meaning up to "renaming the elements")

(c) *For $n = 8$ we have $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$, the integers modulo 8, with units*

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

This is a group of order $\varphi(8) = 4$. Now something surprising happens: the 3 elements $3, 5, 7 \in \mathbb{Z}/8\mathbb{Z}^\times$ all have order 2. So $\mathbb{Z}/8\mathbb{Z}^\times$ is not cyclic – indeed that would require an element of order 4! Instead, $\mathbb{Z}/8\mathbb{Z}^\times$ turns out to be (isomorphic to) the **Klein four-group** *V, the only*[62] *non-cyclic finite group of order 4. Another way to think of this group is as a product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ with addition defined component-wise (in particular, $(0, 0)$ is the identity element).*

(d) *Try $n = 9$, 10, 12 and 16 for yourself. What do you expect? Make a prediction for what happens for $n = 32, 64, 128, \ldots$.*

The examples show that for general n, $\mathbb{Z}/n\mathbb{Z}^\times$ need not be cyclic but there are composite numbers n for which it is cyclic, see Theorem 12.12 below for precise conditions. This motivates the following revision of the definition of a primitive root[63]. This time we define it for natural numbers n in general[64] (see Definition 10.18 for the corresponding definition for $n = p$ prime).

Definition 12.4. *We say that a is a* **primitive root modulo** *n if $\gcd(a, n) = 1$ and the following $\varphi(n)$ numbers*

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

are distinct modulo n. In other words, a is a primitive root mod$n$ *if it is a generator of the group of units $\mathbb{Z}/n\mathbb{Z}^\times$. In particular, primitive roots exist*[65] *if and only if $\mathbb{Z}/n\mathbb{Z}^\times$ is a cyclic group*[66].

Exercise 12.5. *Decide if there are primitive roots for the (composite) numbers in Example 12.3 above and if there are any write them down.*

Given an integer $n \geqslant 1$ and a residue $a \pmod n$ it is easy to check if a is a unit mod 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 $a \pmod p$ is non-zero[67].) We will also learn how to check if n has primitive roots - see Theorem 12.12 below.

[62] again up to isomorphism

[63] Like so much else in number theory, primitive roots were first studied by Gauss, in the early 19th century. The Wikipedia articles 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!

[64] of course, only because we can define it in general this does NOT mean that it EXISTS in general

[65] we also say that n has a primitive root

[66] this is always true for $n = p$ prime and therefore we always have primitive roots in that situation

[67] Why does this work?

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 $m = 1, 2, \ldots$ such that $a^m \equiv 1 (\mathrm{mod}\, n)$, and see if it is $m = \varphi(n)$. Of course, some ways of doing this are more efficient than others. For example, we can use Euler's Theorem 12.10 below to show that only certain natural numbers occur as orders of elements in $\mathbb{Z}/n\mathbb{Z}^\times$. This can save a lot of calculation!

Here is a table of elements of the groups $\mathbb{Z}/n\mathbb{Z}^\times$ and a list of primitive roots 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

Table 1: Units modulo n

What's the relationship between $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$?

The following result is a consequence of the chinese remainder theorem and tells us that understanding the structure of $\mathbb{Z}/n\mathbb{Z}^\times$ reduces to understanding the structure of $\mathbb{Z}/p^k\mathbb{Z}^\times$ for p prime. It also shows (again) that the φ-function is multiplicative.

Theorem 12.6. *Let n be an integer and write $n = m_1 m_2 \ldots m_k$ as a product of pairwise coprime numbers m_i (i.e. $\gcd(m_i, m_j) = 1$ for all $i \neq j$). Then the group $\mathbb{Z}/n\mathbb{Z}^\times$ of units modulo n is a product of groups*

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

Proof. Consider the map

$$\begin{aligned} &\psi \colon \mathbb{Z}/n\mathbb{Z}^\times \to \mathbb{Z}/m_1\mathbb{Z}^\times \times \mathbb{Z}/m_2\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}^\times \;: \\ &a \bmod n \mapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k). \end{aligned}$$

This map is well-defined, since $a \in \mathbb{Z}/n\mathbb{Z}$ is a unit mod n if and only if[68] each $a \in \mathbb{Z}/m_i\mathbb{Z}$ is a unit mod m_i. The uniqueness part of the Chinese remainder theorem shows that ψ is injective and the existence part of the chinese remainder theorem shows that ψ is surjective.

[68] Indeed, $\gcd(a, n) = 1$ if and only if $\gcd(a, m_i) = 1$ for all i

Summing up, the chinese remainder theorem shows that we've defined a bijection ψ between sets.

Using the formula from the chinese remainder theorem, we can write down the inverse map

$$\mathbb{Z}/m_1\mathbb{Z}^\times \times \mathbb{Z}/m_2\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times \ ;$$

$$(a_1, a_2, \ldots, a_k) \mapsto \sum_{i=1}^{k} a_i m_1 m_2 \ldots m_{i-1} m_i^* m_{i+1} \ldots m_k \ .$$

where as in the Chinese Remainder Theorem m_i^* is defined to be the multiplicative inverse of $m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$ modulo m_i.

Component-wise multiplication turns $\mathbb{Z}/m_1\mathbb{Z}^\times \times \mathbb{Z}/m_2\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}^\times$ into a group. We know that multiplying residue classes a mod m and b mod m is done by multiplying the corresponding integers in $\mathbb{Z}$ and then taking the residue class ab mod m. Summing up, this shows that

$$\begin{aligned}\psi(ab) &= (ab \bmod m_1, ab \bmod m_2, \ldots, ab \bmod m_k) \\ &= (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k) \cdot (b \bmod m_1, b \bmod m_2, \ldots, b \bmod m_k) \\ &= \psi(a)\psi(b)\end{aligned}$$

We say that ψ is a homomorphism of groups. Since it is also a bijection of sets, we say that it is an isomorphism of groups. □

Feel free to ignore the next remark.

Remark 12.7. *Here is a "highbrow proof" of Theorem 12.6. One can rephrase the Chinese remainder theorem by saying that*

$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \ ;$$

$$a \bmod n \mapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_k)$$

defines an isomorphism of rings. For any ring R with multiplicative identity 1, we can define it's unit group

$$R^\times = \{r \in R \mid \text{ there exists an } s \in R \text{ with } rs = 1 \text{ and } sr = 1\}. \tag{48}$$

In general[69]*, an isomorphism of rings $\iota\colon R \to S$ restricts to an isomorphism $\iota^\times\colon R^\times \to S^\times$ between the unit groups $R^\times$ and $S^\times$ respectively. Also the unit group construction behaves well under taking products of rings $R_1 \times R_2$ (with component-wise addition and multiplication):*

$$(R_1 \times R_2)^\times = R_1^\times \times R_2^\times \tag{49}$$

Applying these general results to the map ρ above shows that $\rho^\times$ (which is just our ψ from the Theorem above) is an isomorphism of groups.

[69] the even "higher brow" reason behind this is that the operation sending a ring R to its group of units $R^\times$ is a *functor* from the category of rings to the category of groups.

Maybe you know/remember the following important result due to Lagrange.

Theorem 12.8 (Lagrange)**.** *Let G be a finite group and $U \subseteq G$ be a subgroup. Then the order $|U|$ of U divides the order $|G|$ of G.*

What's important for us is the following consequence.

Corollary 12.9. *Let G be a finite group with identity e and let $g \in G$ be an element.*

1. *The order* ord(g) *of g divides $|G|$.*
2. *$g^{|G|} = e$.*

Proof. 1. Check that $U = \{g^0 = e, g^1, \dots g^{\mathrm{ord}(g)-1}\}$ is a subgroup of G. It has $\mathrm{ord}(g)$ elements. So Lagrange 12.8 tells us that indeed $\mathrm{ord}(g)$ divides $|G|$.

2. By part 1., $|G| = \mathrm{ord}(g) \cdot k$ for some integer k. Therefore, $g^{|G|} = g^{\mathrm{ord}(g)\cdot k} = (g^{\mathrm{ord}}(g))^k = e^k = e$ as claimed.

□

Applying this result to our situation ($G = \mathbb{Z}/n\mathbb{Z}^\times$) shows a famous result due to Euler.

Theorem 12.10 (Euler's Theorem)**.** *If n is a positive integer then $a^{\varphi(n)} \equiv 1 \bmod n$ for every a with $\gcd(a, n) = 1$. In particular, if d is the order of a, then $d \mid \phi(n)$.*

Proof. Use Corollary 12.9, 12.2 (ii), and the definition of φ. □

Remark 12.11. *1. Euler's Theorem is a generalization of Fermat's Little Theorem 9.11, since $\varphi(p) = p - 1$. Note that the proof of Euler's Theorem also gives us an alternative proof for Fermat's Little Theorem.*

2. Corollary 12.9 applied to $\mathbb{Z}/n\mathbb{Z}^\times$ is useful when checking whether some element $x \in \mathbb{Z}/n\mathbb{Z}^\times$ is a primitive root. It tells us that it suffices to check x^d where d runs over all the divisors of $\varphi(n)$. Sometimes it's even better and it turns out that some of the divisors of $\varphi(n)$ cannot occur as orders of x. See the "Lifting a primitive root mod$p$ *to a primitive root* modp^2*" part of the proof of Theorem 12.12 for an example of this phenomenon.*

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 then 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, not always, but sometimes there is. The following theorem states exactly which integers n have primitive roots. We will only sketch a proof. The statement of this theorem is important to know, though. Compare it with table 12.

Theorem 12.12. *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. A complete proof can be found in Section 9.3 of Rosen, posted in the Background Material folder on LEARN.

In Example 12.3 above, we have seen already that 4 has a primitive root, and we have also shown that p has a primitive root for all primes p. What remains is to show that in the remaining cases p^k $(k > 1)$ and $2p^l$ $(l \geqslant 1)$ there is indeed a primitive root (see the sketch for p^2 below), and that also all other composite numbers lack a primitive root[70].

Here's a sketch of how one might go about showing that there are primitive roots modulo p^2. The general case p^k can be done similarly.

Lifting a primitive root mod$p$ **to a primitive root** modp^2 Let p be an odd prime and let x be a primitive root mod$p$, so $x^{p-1} \equiv 1 \bmod p$. We can ask ourselves whether x (which after all is just an integer) is also a primitive root modp^2 – in other words, whether x has order $\varphi(p^2) = p(p-1)$ modulo p^2.

If $x^{p-1} \equiv 1 \bmod p^2$ we know immediately that x is not a primitive root modp^2 (In this case, one can show in a way similar to what we do below that $x + p$ is a primitive root modp^2). So let's assume

$$x^{p-1} \not\equiv 1 \bmod p^2. \tag{50}$$

Let k be the order of $x \bmod p^2$, so $x^k \equiv 1 \bmod p^2$. But this implies $x^k \equiv 1 \bmod p$ and therefore $p-1 \mid k$ since x has order $p-1$ modulo p (see eg the proof of Proposition 10.11 for the latter).

Now list all divisors of $\varphi(p^2) = p(p-1)$. They are all of the form d or dp where d is a divisor of $p-1$. By Corollary 12.9 (i), we know that the order k of x modulo p^2 is among these numbers but by the above we also know that $p-1 \mid k$. It follows that k is either $p-1$ or $p(p-1)$. We've excluded the former, so x has order $p(p-1)$ modulo p^2. and is therefore a primitive root modp^2. □

We've seen a version of the following theorem and its proof in Lecture 10 for $n = p$ prime already.

Theorem 12.13. *If n has a primitive root then it has $\varphi(\varphi(n))$ primitive roots.*

[70] It can be deduced from Theorem 12.6 (or alternatively use Exercise 6(c) on Workshop sheet 4) that primitive roots mod$n$ can only exist if n is a prime power q^k or of the form $2\cdot p^l$ with p an odd prime. It remains to exclude the powers 2^t with $t \geqslant 3$. Example 12.3 is already a good start. Another thing one can show (how?) is that if there is a primitive root modulo 2^t, then there is a primitive root modulo 2^{t-1}. Combining this with Example Example 12.3 finishes the proof that primitive roots can only exists if n is as in the statement of the Theorem.

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 by definition 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 12.14 below).

The result now follows. □

Lemma 12.14. *If G is a cyclic group of order m then G has $\varphi(m)$ many generators.*

Proof. 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. By Corollary 10.12 g^k has order m if and only if $\gcd(k, m) = 1$. By definition of φ there are $\varphi(m)$ such integers k between 1 and m. This finishes the proof. □

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 Lecture 13: Perfect numbers and Mersenne primes (6.3.2018)

13.1 Perfect numbers

Given a natural number n we can look at the sum

$$s(n) = \sum_{\substack{d|n \\ d \neq n}} d \tag{51}$$

of all its (proper[71]) divisors.

Question 13.1. *How large/small is $s(n)$ compared to n?*

Let's look at some examples:

[71] a natural number d is a *proper* divisor if $d \mid n$ and $d \neq n$

Example 13.2.

- *For $n = 3$ we a have $s(n) = 1$, so $n > s(n)$ in this case. In fact, we see that more generally*
- *For $n = p$ prime, we have $p > s(p) = 1$.*
- *More generally, for prime powers $n = p^k$, we also have*[72] *$n > s(n)$ and we might start to wonder whether $n > s(n)$ for all natural numbers n.*
- *The example $n = 6$ with $s(n) = 1 + 2 + 3 = 6$ shows that this is not the case. Numbers with $n = s(n)$ are called* perfect numbers. *They've been studied and known by many cultures for thousands of years (see for example wikipedia). They've lots of nice properties*[73] *but are very rare.*
- *The example $n = 12$ shows that also $n < s(n)$ can occur. Indeed, $s(12) = 16$.*

In the Euclid-Euler Theorem 13.10 below we'll relate the even perfect numbers to another group of famous numbers called Mersenne primes. The proof will use the multiplicativity of the sum of divisor function $\sigma(n)$ which we've seen in Lecture 11 as a consequence of the "hat" - operation for multiplicative functions. For this it is useful to note the following lemma which follows directly from the definition of a perfect number.

Lemma 13.3. *A natural number n is perfect if and only if $\sigma(n) = 2n$.*

13.2 Mersenne primes

For any natural number n define the **Mersenne number**

$$M_n \;=\; 2^n - 1 \;.$$

Example 13.4. $M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, ...

Question 13.5. *When is M_n prime?*

As a partial answer to this, Problem 4 on Homework sheet 1 shows that if M_p is prime, then p has to be prime. Note that the converse is not true. Indeed, there are primes p for which M_p is not prime, e.g. $p = 11$ (we've also checked that in Problem 4 on Homework sheet 1).

Definition 13.6. *Primes of the form M_p are called* **Mersenne primes**.

Mersenne primes are named 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!

[72] Do you see why?

[73] For example, the Euclid-Euler Theorem 13.10 below shows that all even perfect numbers are triangular numbers and hexagonal numbers.

Example 13.7.

- *The first four Mersenne primes*

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

have been known since ancient times.

- *Also, the largest known prime number*[74] *is a Mersenne prime – namely,* $M_{77,232,917}$*, which has* $23,249,425$ *decimal digits.*

Mersenne made a conjecture stating which primes p would give Mersenne primes M_p. This conjecture turned out to be wrong however. An attempt to fix this is known as New Mersenne conjectures:

Conjecture 13.8. *Let p be an odd prime. If any two of the following statements are true then so is the third.*

1. $p = 2^k \pm 1$ *or* $p = 4^k \pm 3$ *for some natural number k.*
2. $2^p - 1$ *is prime (a Mersenne prime).*
3. $(2^p + 1)/3$ *is prime (a so called Wagstaff prime).*

Remark 13.9. *It is also conjectured that there are infinitely many Mersenne primes (Lenstra–Pomerance–Wagstaff conjecture).*

There is a relatively efficient algorithm (called *Lucas-Lehmer test*) to check whether a number of the form $M_p = 2^p - 1$ is prime. A good source of information on Mersenne numbers is
http://primes.utm.edu/mersenne/index.html

GIMPS, the Great Internet Mersenne Prime Search
GIMPS on wikipedia,
http://www.mersenne.org/primes/?press=M57885161
is a collective effort to hunt down Mersenne primes. Here is a listing of the 49 known (as of January 2016) 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, 37156667, 42643801, 43112609, 57885161, 74207281.
See www.mersenne.org/primes.

[74] As of April 2018.

13.3 Euclid-Euler theorem: a surprising relation between (even) perfect numbers and Mersenne primes.

The following Theorem shows how the (even) perfect numbers are related to Mersenne primes. It turns out that there is exactly one Mersenne prime for every perfect number and vice versa.

Theorem 13.10 (Euclid and Euler)**.** *Let $n \in \mathbb{N}$ be an even number. Then the following statements are equivalent*

(a) n is perfect,

(b) $n = M_p(M_p+1)/2$ for a Mersenne prime M_p,

(c) $8n+1$ is a square number and $M_p = (\sqrt{8n+1}-1)/2$ is a Mersenne prime.

Proof. We start with the implication (b) $\Rightarrow$ (a), which is due to Euclid. Let $M_p = 2^p - 1$ be a Mersenne prime and consider

$$n = \frac{M_p(M_p+1)}{2} = (2^p-1)2^{p-1} \tag{52}$$

By Lemma 13.3, to show (a), we have to show that $\sigma(n) = 2n$, where σ denotes the sum of divisor function, which is multiplicative by Proposition 11.12. Since (2^p-1) is odd, we have $\gcd(2^p-1, 2^{p-1}) = 1$ and therefore,

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

Let's compute the two factors:

$$\sigma(2^{p-1}) = \; 1+2+2^2+\cdots+2^{p-1} \;=\; 2^p-1\;, \tag{53}$$

$$\sigma(M_p) = \; M_p+1 \qquad\qquad \text{since } M_p \text{ is prime by assumption.} \tag{54}$$

Thus we indeed get

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

showing that n is perfect.

Conversely, to show the Euler's implication (a) $\Rightarrow$ (b) suppose that n is an even perfect number, so

$$\sigma(n) = 2n. \tag{55}$$

Again we want to use that σ is a multiplicative function. In order to do this let's write $n = 2^k \cdot t$ where t is an odd number and $k \geqslant 1$ (so now n is a product of coprime numbers). Substituting this into (55) and using the multiplicativity of σ gives

$$2^{k+1}t = \sigma(2^k t) = \sigma(2^k)\sigma(t) = (2^{k+1}-1)\sigma(t) \tag{56}$$

where we've used (53) again. Since 2^{k+1} and $2^{k+1}-1$ are coprime, (56) implies that $2^{k+1} \mid \sigma(t)$, so we have $\sigma(t) = 2^{k+1}s$ for some natural number s. Substituting this into (56) and canceling shows

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

To show (b), our goal becomes to show $k+1 = p$ and $s = 1$.

If $s > 1$ then t clearly has $1, s, t$ as factors. Thus

$$\sigma(t) \geqslant 1 + t + s = 1 + (2^{k+1}s - s) + s = 1 + 2^{k+1}s > 2^{k+1}s$$

but this is a contradiction, because we know that $\sigma(t) = 2^{k+1}s$.

Hence $s = 1$ and we have that $\sigma(t) = 2^{k+1}$, now Equation (56) says that

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

Together we see that $\sigma(t) = t + 1$ which can only happen if t is prime, which we know implies[75] that $k + 1 = p$ is prime. So $t = M_p$ is a Mersenne prime and

$$n = 2^k \cdot t = 2^{p-1} \cdot (2^p - 1) = \frac{2^p \cdot (2^p - 1)}{2} = \frac{(M_p + 1) \cdot M_p}{2} \tag{57}$$

as required.

A computation (using the binomial formula) shows that (b) and (c) are equivalent.

□

Combining this Theorem with Example 13.7 above gives the first 4 perfect numbers.

$$\begin{aligned}
M_2(M_2+1)/2 &= 3 \cdot 4/2 = 1 + 2 + 3 = 6 \\
M_3(M_3+1)/2 &= 7 \cdot 8/2 = \ 1 + 2 + 4 + 7 + 14 \ = 28, \\
M_5(M_5+1)/2 &= 31 \cdot 32/2 = \ 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \ = 496, \\
M_7(M_7+1)/2 &= 127 \cdot 128/2 \\
&= 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 \ = 8128.
\end{aligned}$$

Main Points from Lecture 13:

- Definition of Mersenne prime M_p.
- Definition of perfect number.
- The Euclid-Euler Theorem.

[75] see Problem 4 on Homework sheet 1

14 Lecture 14: The Möbius function $\mu(n)$, Möbius inversion and the convolution $f * g$ (9.3.2018)

Recall from Chapter 11 that an arithmetic function $f\colon \mathbb{N} \to \mathbb{C}$ is **multiplicative** if

$$f(mn) \;=\; f(m)f(n) \text{ for all } \textbf{coprime} \text{ integers } m, n \geqslant 1.$$

It follows that $f(1) = 1$ provided f is not the zero function $f(n) = 0$ for all $n \in \mathbb{N}$. Recall also the **summatory function** of f

$$\widehat{f}(n) \;=\; \sum_{d|n} f(d)\ . \tag{58}$$

In Proposition 11.12 it was proved that if $f(n)$ is multiplicative, then so is $\widehat{f}(n)$. The classic formula of Möbius Inversion recovers any[76] arithmetic function $f(n)$ from the function $\widehat{f}(n)$ using the Möbius function $\mu(n)$. The **main result** of today shows

$$f(n) \text{ is multiplicative if and only if } \widehat{f}(n) \text{ is multiplicative.} \tag{59}$$

The relationship between $f(n)$ and $\widehat{f}(n)$ is seen to be a special case of the **convolution**[77]

$$(f * g)(n)$$

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 f be any arithmetic function (not necessarily multiplicative). Using Definition (58), let's write down $\widehat{f}(n)$ for small natural numbers n and let's see what we get:

$$\begin{aligned}
\widehat{f}(1) &= f(1)\\
\widehat{f}(2) &= f(1) + f(2)\\
\widehat{f}(3) &= f(1) + f(3)\\
\widehat{f}(4) &= f(1) + f(2) + f(4)\\
\widehat{f}(5) &= f(1) + f(5)\\
\widehat{f}(6) &= f(1) + f(2) + f(3) + f(6)
\end{aligned}$$

[76] in particular, we don't have to assume that f is multiplicative

[77] This is sometimes also called **Dirichlet convolution** or **number theoretic convolution** to distinguish it from the convolution used in Fourier analysis, which however is closely related in spirit.

Now let's assume that we know $\widehat{f}(n)$ for all natural numbers n but that we've forgotten about f.
AIM: We would like to use the equations above to recover f from $\widehat{f}(n)$.

The following discussion may be a bit lengthy (but the calculations and concepts are really quite elementary). If you are impatient you can jump to Definition 14.2 directly. However, without the discussion that definition might look quite ad hoc...

Solving the equations for $f(n)$ in terms of $\widehat{f}(n)$, we see

$$\begin{aligned} f(1) &= \widehat{f}(1) \\ f(2) &= \widehat{f}(2) - \widehat{f}(1) \\ f(3) &= \widehat{f}(3) - \widehat{f}(1) \\ f(4) &= \widehat{f}(4) - \widehat{f}(2) \\ f(5) &= \widehat{f}(5) - \widehat{f}(1) \\ f(6) &= \widehat{f}(6) - \widehat{f}(2) - \widehat{f}(3) + \widehat{f}(1). \end{aligned}$$

Let's do this a bit more systematically. As we've seen in previous lectures it is always a good idea to study what happens for primes p and then also for prime powers p^k.

From

$$\widehat{f}(p) = f(1) + f(p),$$

we get

$$f(p) = \widehat{f}(p) - \widehat{f}(1).$$

Let's see what happens for p^2:

$$\widehat{f}(p^2) = f(1) + f(p) + f(p^2),$$

this shows

$$f(p^2) = \widehat{f}(p^2) - (f(1) + f(p)) = \widehat{f}(p^2) - \widehat{f}(p)$$

where we use our result for primes from above. Using induction one can show that

$$f(p^k) = \widehat{f}(p^k) - \widehat{f}(p^{k-1}) \tag{60}$$

for all natural numbers k.

Remark 14.1. *These formulas might look familiar. Recall that we've seen in Proposition 11.14 that*

$$\varphi(p^k) = p^k - p^{k-1}. \tag{61}$$

Note also that $\widehat{\varphi}(n) = \mathrm{id}(n) = n$ by Theorem 10.4. Using this, the formula (61) can be recovered from the general formula (60). So it seems we are on the right way!

Experimentally, it seems that

$$f(n) \;=\; \sum_{d|n} \mu_{n,d} \cdot \widehat{f}(d)$$

where $\mu_{n,d}$ seems to be either $0, 1$ or -1. From our formulas above, we can determine some of the $\mu_{n,d}$:

$$\mu_{p^k,p^k} = 1, \mu_{p^k,p^{k-1}} = -1 \textbf{ and } \mu_{p^k,p^l} = 0 \textbf{ for all } l < k-1 \tag{62}$$

using (60). More generally, one can check that

$$\mu_{n,n} = 1 \tag{63}$$

for all natural numbers n. Next, let p and q be different primes, then we can compute

$$\mu_{pq,q} = -1, \mu_{pq,p} = -1, \mu_{pq,1} = 1 \tag{64}$$

It would be nice to get the $\mu_{n,d}$ from some arithmetic function $\mu(m)$. Let's see what happens if we assume that this function is multiplicative. It's certainly not the zero-function so we would get that $\mu(1) = 1$. Now looking back at (63) shows that $\mu_{n,n} = \mu(1) = \mu(n/n)$ for all n. From there a brave guess leads us to

$$\mu_{n,d} = \mu(n/d).$$

Let's see whether this guess makes any sense. Using (62) would give

$$-1 = \mu_{p^k,p^{k-1}} = \mu(p^k/p^{k-1}) = \mu(p) \tag{65}$$

$$0 = \mu_{p^k,p^l} = \mu(p^k/p^l) = \mu(p^{k-l}) \text{ for } 0 \leqslant l < k-1 \tag{66}$$

$$= \mu(p^m) \text{ for } m > 1 \tag{67}$$

Let's see what we would get out of (62)

$$-1 = \mu_{pq,p} = \mu(pq/p) = \mu(p)$$
$$1 = \mu_{pq,1} = \mu(pq/1) = \mu(pq)$$

This is consistent with our previous equations! In both cases, we get $\mu(p) = -1$ and if μ was multiplicative this would imply $\mu(pq) = \mu(p)\mu(q) = (-1)(-1) = 1$, which agrees with what we know to be true. If we assume that μ is multiplicative and using equations (65) to (67) we get the following definition of an important multiplicative function:

Definition 14.2. *The* **Möbius**[78] **function** $\mu(n)$ *is defined as*

$$\mu(n) \;=\; \begin{cases} 0 & \text{if } p^2 \mid n \text{ for some prime } p; \\ (-1)^k & \text{if } n = p_1 p_2 \dots p_k \text{ for pairwise different primes } p_i. \end{cases}$$

[78] August Möbius who is also the discoverer of the famous Möbius strip was a student of Gauss and of Gauss's supervisor Pfaff. His function μ will be the main character of today's lecture.

Remark 14.3. *In particular,* $\mu(1) = 1$ *(this follows since* μ *is a non-zero multiplicative function) and* $\mu(p) = -1$ *for a prime* p*.*

Remark 14.4. *Integers with* $\mu(n) \neq 0$ *are called* **squarefree** *(since they don't have any factors of the form* p^2 *where* p *is prime). On Homework sheet 4 there is an exercise showing that the so called* Carmichael numbers *are squarefree.*

The following result is one of the reasons why the Möbius function μ is important.

Proposition 14.5. *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 $\sum_{k|n} \mu(k) = \Delta(n)$. Since μ is multiplicative, it follows from Proposition 11.12 that $\widehat{\mu}$ is multiplicative. Therefore and since $\Delta(n)$ is multiplicative too, 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. □

The Möbius function arises in many kinds of so called **inversion** formulae, see wikipedia for more information. The fundamental one is the following – which after our discussion preceeding Definition 14.2 won't come as a surprise[79]

Proposition 14.6. (**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. By definition of the $\widehat{\ }$operation, we have

$$\sum_{d|n} \mu(n/d) F(d) \;=\; \sum_{d|n} \mu(n/d) \sum_{k|d} f(k) \quad (n \in \mathbb{N}).$$

[79] indeed, we were guided to the Definition of μ by trying to get this formula. Here we'll check that using our construction of μ it really works.

Setting $e = n/d$ it follows that $d = n/e$ and therefore we get

$$\begin{aligned}\sum_{d|n} \mu(n/d) \sum_{k|d} f(k) &= \sum_{e|n} (\mu(e) \sum_{k|(n/e)} f(k)) \\ &= \sum_{e|n} (\sum_{k|(n/e)} \mu(e) \cdot f(k)) \ .\end{aligned}$$

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 those pairs with $k \mid n$ and $e \mid (n/k)$. So we continue our calculation as

$$\begin{aligned}\sum_{e|n} (\sum_{k|(n/e)} \mu(e) \cdot f(k)) &= \sum_{k|n} (\sum_{e|(n/k)} \mu(e) f(k)) \\ &= \sum_{k|n} f(k) \left(\sum_{e|(n/k)} \mu(e) \right) \ .\end{aligned}$$

The inner bracket is $\widehat{\mu}(n/k)$ which by Proposition 14.5 is nonzero if and only if $n = k$. In this case, $\widehat{\mu}(1) = 1$. Hence we have that the sum above reduces to

$$\sum_{k|n} f(k) \left(\sum_{e|(n/k)} \mu(e) \right) = f(n) \cdot 1 = f(n).$$

This completes the proof. □

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. The second will be to show that the converse of Proposition 11.12 holds, see below.

Example 14.7. *By definition,*

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

Möbius inversion gives that

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

Example 14.8. *By definition*

$$\tau(n) \ = \ \widehat{1}(n) \ = \ \sum_{d|n} 1 \ .$$

Möbius inversion gives that

$$1 \ = \ \sum_{d|n} \mu(n/d) \tau(d) \ .$$

Example 14.9. (i) *By Theorem 10.4, we know that the summatory function of the Euler φ-function*

$$\varphi(n) \;=\; \sum_{1\leqslant a\leqslant n,(a,n)=1} 1$$

is

$$\widehat{\varphi}(n) \;=\; \sum_{d|n}\varphi(d) \;=\; \mathrm{id}(n)=n\ .$$

(ii) *Therefore, Möbius inversion expresses $\varphi(n)$ as*

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

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, 12 has 6 divisors: 1,2,3,4,6,12, so

$$\begin{aligned}\varphi(12) \;&=\; \sum_{d|12}\mu(12/d)d\\ &=\; \mu(12/1)1+\mu(12/2)2+\mu(12/3)3+\mu(12/4)4+\mu(12/6)6+\mu(12/12)12\\ &=\; 0+2+0-4-6+12 \;=\; 4\ .\end{aligned}$$

Now we come to the second main use of Möbius inversion, which is the following converse of Proposition 11.12:

Proposition 14.10. *If an arithmetic function $f(n)$ is such that $F(n)=\widehat{f}(n)$ is multiplicative, then $f(n)$ is multiplicative.*

Proof. By the Möbius inversion formula

$$f(m_1m_2) \;=\; \sum_{d|m_1m_2}\mu(d)F(m_1m_2/d)$$

To simplify this we need some preparation[80]. Suppose that m_1,m_2 are coprime integers $\geqslant 1$. If d is a divisor of $m_1\cdot m_2$ then $d=d_1\cdot d_2$ where $d_1\mid m_1$, $d_2\mid m_2$ with d_1,d_2 coprime. Conversely, if d_1 is a divisor of m_1 and d_2 is a divisor of m_2, then $d_1\cdot d_2$ is a divisor of $m_1\cdot m_2$. This shows

$$\sum_{d|m_1m_2}\mu(d)F(m_1m_2/d) = \sum_{d_1|m_1,d_2|m_2}\mu(d_1d_2)F(\tfrac{m_1\cdot m_2}{d_1\cdot d_2})$$

Using the fact that μ and F are multiplicative and the Möbius inversion formula again (in the last step), we continue

$$\begin{aligned}&=\; \sum_{d_1|m_1,d_2|m_2}\mu(d_1)\mu(d_2)F(m_1/d_1)F(m_2/d_2)\\ &=\; \Big(\sum_{d_1|m_1}\mu(d_1)F(m_1/d_1)\Big)\Big(\sum_{d_2|m_2}\mu(d_2)F(m_2/d_2)\Big)\\ &=\; f(m_1)f(m_2)\ .\end{aligned}$$

□

[80] Similar arguments already appeared in Lecture 11.

Conclusion: $f(n)$ is multiplicative if and only if $\widehat{f}(n)$ is multiplicative.

Remark 14.11. *This gives another proof that φ is multiplicative, say from the fact that $\widehat{\varphi} = n$ (Example 14.9 (i)) is multiplicative.*

14.3 Convolution

It is not an accident that an arithmetic function $f(n)$ is multiplicative if and only if the summatory function $\widehat{f}(n)$ is multiplicative!

Definition 14.12. *The* **convolution**[81] *of arithmetic functions $f(n)$, $g(n)$ is the arithmetic function*

$$(f * g)(n) \;=\; \sum_{d|n} f(d)g(n/d)\ .$$

Remark 14.13. *This is the number theory analogue of the convolution of continuous functions $f(x)$, $g(x)$, defined by*

$$(f * g)(x) = \int_{-\infty}^{\infty} f(y)g(x-y)dy,$$

which plays such an important role in functional analysis, e.g. Fourier analysis. From this perspective it should come as no surprise that the convolution of arithmetic functions is important and has good properties, too.

Example 14.14. *We have already seen several examples of convolutions. Let $c(n) = 1$ be the constant function and* $\mathrm{id}(n) = n$
(i) *By Example, 14.7* $\sigma = \mathrm{id} * c$, $\mu * \sigma = \mathrm{id}$.
(ii) *By Example, 14.8* $\tau = c * c$, $\mu * \tau = c$.
(iii) *By Example, 14.9* $\mathrm{id} = \varphi * c$, $\mu * \mathrm{id} = \varphi$.
Can you spot a common feature of (i), (ii) *and* (iii)*?* [82]

Basic properties: the convolution is commutative and associative; for any arithmetic functions $f(n)$, $g(n)$, $h(n)$ one can check that the convolution is *commutative* and *associative*:

$$f * g \;=\; g * f\ ,\ (f * g) * h \;=\; f * (g * h)\ .$$

We have met the unit Δ with respect to the operation $*$ before:

Example 14.15. *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:*

$$f * \Delta \;= f\ .$$

[81] This is sometimes also called **Dirichlet convolution** or **number theoretic convolution** to distinguish it from the convolution of continuous functions, see Remark 14.13.

[82] Yes, if $g = f * c$ then $\mu * g = f$, and in fact $g = \widehat{f}$.

Proposition 14.16. *If $f(n)$ and $g(n)$ are multiplicative functions then so is their convolution $(f*g)(n)$.*

Proof. As in the proof of Proposition 14.10 we have that for coprime integers $m_1, m_2 \geqslant 1$

$$\begin{aligned}(f*g)(m_1m_2) &= \sum_{d_1|m_1, d_2|m_2} f(d_1d_2)g(m_1m_2/d_1d_2) \\ &= \left(\sum_{d_1|m_1} f(d_1)g(m_1/d_1)\right)\left(\sum_{d_2|m_2} f(d_2)g(m_2/d_2)\right) \\ &= (f*g)(m_1)(f*g)(m_2)\ .\end{aligned}$$

□

Remark 14.17. (i) *The summatory function of an arithmetic function $f(n)$ is the convolution with the constant function $c(n) = 1$*

$$\widehat{f} \ = \ f*c\ .$$

Since c is multiplicative Proposition 14.16 recovers Proposition 11.12, that if f is multiplicative then so is $\widehat{f}$.
(ii) *By Proposition 14.5 and part (i) the convolution of the constant function c and the Möbius function $\mu(n)$ is the 1-detecting function*

$$\mu*c \ = \widehat{\mu} = \ \Delta\ .$$

(iii) *From Example 14.15, parts* (i) *and* (ii) *above and the associativity and commutativity of the convolution we have a new proof of the Möbius inversion Proposition 14.6, that we can recover any arithmetic function $f(n)$ from its summatory function $\widehat{f}(n)$ as the convolution with the Möbius function $\mu(n)$*

$$f \ = \ f*\Delta \ = \ f*(c*\mu) \ = \ (f*c)*\mu \ = \ \widehat{f}*\mu\ .$$

Since μ is multiplicative Proposition 14.16 recovers Proposition 14.10, 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.

Main Points from Lecture 14:

- Definition of Möbius function $\mu(n)$
- Möbius inversion formula
- Convolution of arithmetic functions

15 Lecture 15: Quadratic Residues (13.3.2018)

15.1 Motivation

We start with the following question.

Question 15.1. *Let $x \in \mathbb{R}$ be a real number. When is x a* square*? In other words, when can we find an $r \in \mathbb{R}$ such that $x = r^2$?*

We know that the criterion is simple.

Answer 15.2. *x is a square if and only if*[83] *$x \geqslant 0$. In this case, we know that $r = \pm\sqrt{x} \in \mathbb{R}$.*

Today and next time: Study analogous question in the finite field $\mathbb{F}_p$ for an odd[84] prime p. In other words, which integers x are squares mod$p$?

Remark 15.3. *Studying and constructing square roots is a very fruitful and powerful idea throughout the history of mathematics.*

For example, one important motivation to introduce the real numbers was that most positive integers and rational numbers don't have square roots which are integers or rationals but which are reals. Similarly, the complex numbers were introduced in order to provide a natural framework to work with square roots of negative numbers. Both reals and complex numbers quickly developed into powerful tools with wide ranging applications (all natural sciences, engineering...) going very far beyond the original motivation for introducing them.

This is one reason why we might hope that studying today's question might lead to interesting mathematics (and maybe applications). Here are some more thoughts about "Why care about square roots mod$p$*?"*

- *Applications ranging from cryptography to engineering(!) (e.g. in acoustics, there are* sound diffusers *based on the theory we're going to develop).*
- *very useful within number theory:*
  - *Solving quadratic equations* mod$p$ *(see below).*
  - *Showing that there are infinitely many primes of a certain form (eg of the form $4k + 1$ see further below). These are special cases of Dirichlet's Theorem 2.11 which we aren't able to prove in this course unfortunately.*
  - *writing integers as sums of two squares (see Lecture 18).*
  - *testing whether an integer is prime*
- *Moreover, generalisations of these questions led to very deep theories (e.g. "Langlands program", which is related to the proof of Fermat's Last theorem), with many challenging open problems and questions. Surprisingly also (some) theoretical physicists are very interested in these theories and think that they tell us things about our universe.*

[83] $x \geqslant 0$ is necessary since squares of real numbers are $\geqslant 0$. Why does the converse work?

[84] Have a think about what happens for $p = 2$.

Here's a concrete example to show that without theory things are hard to compute/decide:

Example 15.4. *Is* 26 *a square modulo* $p = 107$*, i.e.*

$$26 \equiv r^2 \bmod 107$$

for some integer r*?*

We'll answer this question later today but of course you can try to figure it out without the theory.

15.2 Quadratic residues and nonresidues

We introduce the key notions for this and the next lecture (we've seen them already on the last Workshop and Homework sheets).

Definition 15.5. *Let* p *be an odd prime, and let* $r \in \mathbb{Z}$ *be an integer with* $p \nmid r$*.*

- *If the congruence* $x^2 \equiv r \bmod p$ *has a solution* $x \in \mathbb{Z}$ *then* r *is called a* **quadratic residue (q.r.)** mod$p$*.*
- *If there is no such solution*[85] $x \in \mathbb{Z}$*, then* r *is called a* **quadratic nonresidue (q.n.)** mod$p$*.*

Proposition 15.6. *Take* p *an odd prime, and* g *a primitive root*[86] mod$p$
Then the quadratic residues mod$p$ *are the even powers of* g*, so*

$$\{\textit{quadratic residues} \bmod p\} = \{g^2, g^4, g^6, \ldots, g^{p-1} \bmod p\} \tag{68}$$

while the quadratic nonresidues mod$p$ *are the odd powers of* g*, so*

$$\{\textit{quadratic nonresidues} \bmod p\} = \{g^1, g^3, g^5, \ldots, g^{p-2} \bmod p\} \tag{69}$$

In particular, there are $\frac{p-1}{2}$ *of each.*

Proof. Suppose $r \in \mathbb{F}_p^\times$, since g is a primitive root we know that $r = g^k$ for some integer $1 \leqslant k \leqslant p-1$. If k is even then $r = (g^{k/2})^2$, so that r is a quadratic residue mod$p$.

Conversely, if $x = g^\ell$ (again using that g is a primitive root we can write x like this), with $x^2 = r$, then

$$g^{2\ell} = x^2 = r = g^k$$

and therefore $g^{2\ell-k} = 1$. Since g has order $p-1$ it follows[87] that $2\ell - k$ is a multiple of $p-1$, which is even. So k is even.

[85] Try to find an example where this happens!
[86] we know that this exists from Lecture 10
[87] Do you remember why?

Alternatively, to show that there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues we can also argue as follows (without using primitive roots!). This is a kind of "reverse engineering" – instead of trying to find square roots for given elements $r \in \mathbb{F}_p^\times$ we take squares of all the elements in $\mathbb{F}_p^\times$ and see what we get:

First since p is prime we can write[88] the elements in $\mathbb{F}_p^\times$ as:

$$\mathbb{F}_p^\times = \{-\frac{p-1}{2}, -\frac{p-3}{2}, -\frac{p-5}{2}, \ldots -3, -1, 1, 3, 5, \ldots \frac{p-1}{2}\} \tag{70}$$

This shows that $\mathbb{F}_p^\times$ is built of exactly $(p-1)/2$ pairs of numbers $x, -x$. Now $x^2 = (-x)^2$ in $\mathbb{F}_p^\times$ showing that there are at most $(p-1)/2$ different squares in $\mathbb{F}_p^\times$ (in other words, at most $(p-1)/2$ quadratic residues mod$p$). We want to show that all these $(p-1)/2$ squares are pairwise different so that we get exactly $(p-1)/2$ quadratic residues mod$p$ (which directly implies that the remaining $(p-1)/2$ numbers in $\mathbb{F}_p^\times$ are quadratic nonresidues). So let's consider x, y in $\mathbb{F}_p^\times$ such that

$$x^2 = y^2. \tag{71}$$

Then we get $(xy^{-1})^2 = 1$, which shows $(xy^{-1})^2 - 1 = 0$, so $xy^{-1} = \pm 1$ and by Theorem 9.7 there are no further possiblities for xy^{-1}. But this shows that $x = \pm y$ and therefore the $(p-1)/2$ squares considered above are indeed all different!

□

15.3 The Legendre symbol

We've seen the next Definition on Homework sheet 4 already. Going back to the very beginning of this lecture this piece of notation may be seen as an analogue of the *sign* $\pm$ of a real number.

Definition 15.7. *Let p be an odd prime and let $r \in \mathbb{Z}$ be an integer with $p \nmid r$. Then the* **Legendre symbol** *is defined as*

$$\left(\frac{r}{p}\right) = \begin{cases} 1 \text{ if } r \text{ is a quadratic residue } \bmod p; \\ -1 \text{ if } r \text{ is a quadratic nonresidue } \bmod p. \end{cases}$$

Remark 15.8. *Check that if $r \equiv s \bmod p$ then $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right)$. Therefore, it makes sense to write $\left(\frac{x}{p}\right)$ for residue classes $x \in \mathbb{F}_p^\times$.*

Remark 15.9. *Let g be a primitive root* mod$p$*. Then Proposition 15.6 shows that*

$$\left(\frac{g^k}{p}\right) = \begin{cases} 1 \text{ if } k \text{ is even}; \\ -1 \text{ if } k \text{ is odd}. \end{cases}$$

[88] Make sure to check this!

But the right hand side also equals $(-1)^k$ *so we get*

$$\left(\frac{g^k}{p}\right) = (-1)^k \tag{72}$$

This is a nice formula and will be useful in proofs later on. It also motivates the next result due to Euler. Note however that (72) *does not really help us to compute Legendre symbols in practice as it requires lots of work to write a number in the form* g^k *for some primitive root* g*.*

The following result (which is Exercise 3 on Homework sheet 4), tells us how to compute Legendre symbols without using primitive roots.

Proposition 15.10 (Euler's Criterion)**.** *For* p *an odd prime and* $r \in \mathbb{F}_p^\times$ *we have*

$$\left(\frac{r}{p}\right) \equiv r^{\frac{(p-1)}{2}} \bmod p \tag{73}$$

Proof. Let g be a primitive root $\bmod p$. So we can write $r \equiv g^k \bmod p$ for some $1 \leqslant k \leqslant p-1$. We distinguish two cases

$k = 2m$ **even**: Then we see that

$$r^{\frac{p-1}{2}} = (g^{2m})^{\frac{p-1}{2}} = g^{2m\frac{p-1}{2}} = (g^{p-1})^m = 1^m = 1, \tag{74}$$

where in the second last step we used Fermat's little Theorem 9.11. Now Remark 15.9 shows that

$$1 = \left(\frac{g^{2m}}{p}\right) = \left(\frac{r}{p}\right) \tag{75}$$

using Remark 15.8 in the last step. This completes the proof of this case.
$k = 2l+1$ **odd**: Then $r^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \equiv g^{k\cdot\frac{p-1}{2}} \not\equiv 1 \bmod p$ where in the last step we've used that $k \cdot \frac{p-1}{2}$ is not a multiple of $p-1$ if k is odd. However,

$$(r^{\frac{p-1}{2}})^2 \equiv r^{p-1} \equiv 1 \bmod p \tag{76}$$

using Fermat's little Theorem 9.11 in the last step. This implies $r^{\frac{p-1}{2}} \equiv -1 \bmod p$ (as we've excluded the possibility of this being $\equiv 1 \bmod p$). Combining this with Remark 15.9 and $r \equiv g^{(2l+1)} \bmod p$ shows (73) in this case. □

This has the following important consequence

Theorem 15.11. *Let* p *be an odd prime. Taking* $r = -1$ *in Proposition 15.10, we have*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4 \\ -1, & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

Proof. By Proposition 15.10, it remains to check the second equality. This is a good exercise. □

As an application we can show the following special case of Dirichlet's Theorem 2.11

Theorem 15.12. *There are infinitely many primes of the form* $4k+1$.

Proof. Suppose there were only finitely many primes of the form $4k+1$. Call them $p_1, \ldots, p_k$. Then consider the number

$$N = 4(p_1 \cdots p_k)^2 + 1. \tag{77}$$

Now let q be a prime factor of N. Then viewing equation (77) modulo q we see that

$$0 \equiv 4(p_1 \cdots p_k)^2 + 1 \bmod q$$

and thus

$$-1 \equiv (2p_1 \cdots p_k)^2 \bmod q$$

so -1 is a square modulo q. But by Theorem 15.11, we know that -1 is a square $\pmod q$ 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. Therefore, our list of primes that are 1 mod 4 was not complete. Contradiction. So there are infinitely many primes of the form $4k+1$. □

The Legendre symbol is multiplicative in the following sense.

Lemma 15.13. *Let p be an odd prime, and let a, b be integers not divisible by p. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \tag{78}$$

In particular[89], $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1$.

Combining the two results above yields

$$\left(\frac{a^2 b}{p}\right) = \left(\frac{a^2}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right). \tag{79}$$

Proof. Let g be a primitive root mod$p$. Then $\left(\frac{g^k}{p}\right) = (-1)^k$ by (72). Writing $a \equiv g^k$ and $b \equiv g^l$ we get

$$\left(\frac{ab}{p}\right) = \left(\frac{g^k g^l}{p}\right) = \left(\frac{g^{k+l}}{p}\right) = (-1)^{k+l} = (-1)^k (-1)^l = \left(\frac{g^k}{p}\right)\left(\frac{g^l}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \tag{80}$$

as claimed. □

[89] this also follows directly from the definition of Legendre symbols!

Remark 15.14. *Often the definition of the Legendre symbol is extended to* all *integers* $r \in \mathbb{Z}$ *by setting*

$$\left(\frac{r}{p}\right) = 0$$

for all integer multiples $r = kp$*, with* $k \in \mathbb{Z}$*. One can extend Lemma 15.13 to show that for every odd prime* p

$$n \mapsto \left(\frac{n}{p}\right) \tag{81}$$

defines a multiplicative[90] *function in the sense of Lecture 11.*

Let's come back to our Example 15.4 from the beginning:

Example 15.15. *Is* 26 *a square modulo* $p = 107$*?*

Solution: Translating the question into Legendre symbols, we are asked to compute $\left(\frac{26}{107}\right)$*. Using Remark 15.8 and* $26 \equiv -81 \bmod 107$*, we get*

$$\left(\frac{26}{107}\right) = \left(\frac{-81}{107}\right)$$

. Now we can apply Lemma 15.13 (since $81 = 9^2$ *is a square) to obtain*

$$\left(\frac{-81}{107}\right) = \left(\frac{-1}{107}\right) = -1$$

using $107 \equiv 3 \bmod 4$ *and Theorem 15.11 in the last step.*

Summing up, 26 *is* not *a square* mod107*.*

Here's another example

Example 15.16. *Determine whether or not* 90 *is a square mod* 11*.*

Solution: We are asked to compute $\left(\frac{90}{11}\right)$*. By Lemma 15.13 above we see that*

$$\left(\frac{90}{11}\right) = \left(\frac{9}{11}\right)\left(\frac{10}{11}\right) = 1 \cdot \left(\frac{10}{11}\right).$$

(Since $9 = 3^2$ *is a square). Now using Remark 15.8 and* $10 \equiv -1 \bmod 11$*, we have*

$$\left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right)$$

[90] actually it is a completely multiplicative function (meaning that there is no coprime condition needed). See also Exercise 4 on Homework sheet 4 for Dirichlet's generalisation of these functions.

Now by Theorem 15.11, we know that -1 *is a quadratic residue modulo* p *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* mod11. *Thus*

$$\left(\frac{90}{11}\right) = \left(\frac{-1}{11}\right) = -1.$$

This shows that 90 *is not a quadratic residue* mod11.

Outlook: We've seen that computing Legendre symbols is fun and useful (for example it helped us to show that there are infinitely many primes of a certain kind). Therefore, it's natural to ask

Question 15.17. *How can we compute* $\left(\frac{r}{p}\right)$ *in general?*

Lemma 15.13 reduces the problem to the case where $r = p$ is prime. Indeed writing r as a product of primes $r = p_1^{e_1} \cdot \ldots \cdot p_t^{e_t}$, Lemma 15.13 shows that

$$\left(\frac{r}{p}\right) = \left(\frac{p_1}{p}\right)^{e_1} \cdot \ldots \cdot \left(\frac{p_t}{p}\right)^{e_t} \tag{82}$$

So it remains to understand $\left(\frac{q}{p}\right)$ for p and q prime (and using Remark 15.8 we can assume wlog that $q < p$). Of course we could try to use Euler's criterion 15.10 to compute $\left(\frac{q}{p}\right)$ but for large primes p that's a lot of work!

Next time: one of the most famous and celebrated results in number theory the so called **Quadratic Reciprocity Theorem** of Gauss gives a precise, simple(!) and surprising[91] relationship between

$$\left(\frac{p}{q}\right) \text{ and } \left(\frac{q}{p}\right) \text{ for } p, q \text{ prime.} \tag{83}$$

In combination with reductions mod$p$ this gives a powerful and fun method to compute Legendre symbols $\left(\frac{p}{q}\right)$.

[91] Although there are lots of known proofs (Gauss alone wrote down 6 different proofs) of this Theorem, the fact that there is this simple relationship between these Legendre symbols remains slightly mysterious. In current research in number theory people work on vast generalisations of this result. Some of these help to gain a better understanding of why quadratic reciprocity works.

Main Points from Lecture 15:

- Quadratic residues
- The Legendre symbol
- Euler's criterion
- Apply Euler's criterion to compute $\left(\frac{-1}{p}\right)$.
- There are infinitely many primes of the form $4k+1$.

16 Lecture 16: Quadratic Reciprocity (16.3.2018)

Today's lecture sees one of the highlights of this course and of number theory in general! We discuss the so called quadratic reciprocity law and how it links up with what we've seen in the last lecture. Gauss who was the first to prove this result (at the age of 19) called this result the "fundamental theorem" and said that "it must certainly be regarded as one of the most elegant of its type." In his diary, he even called it the "golden theorem"!

16.1 Introduction

Recall that the Legendre symbol $\left(\frac{a}{p}\right)$ is defined for an odd prime p and an integer a coprime to p:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p; \\ -1 & \text{otherwise;} \end{cases} \tag{84}$$

We've seen some rules to compute with Legendre symbols already:

1. if a, b are integers coprime to p, then Lemma 15.13 shows
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
2. Moreover, in Theorem 15.11, we've seen that
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4 \\ -1, & \text{if } p \equiv -1 \bmod 4. \end{cases}$$
3. In particular, combining this with the Fundamental Theorem of Arithmetic, we see that we can reduce the computation of any Legendre symbol to the computation of

$\left(\frac{q}{p}\right)$ where q and p are different primes. Moreover, by reducing modulo p we can assume that $q < p$ (see Remark 15.8).

- The case $q = 2$ is special and will be treated in Lemma 16.9 below.
- Otherwise, q and p are both odd primes. Shockingly, there is a precise relationship (called **quadratic reciprocity law**) between

$$\left(\frac{q}{p}\right) \quad \text{and} \quad \left(\frac{p}{q}\right). \tag{85}$$

  See Theorem 16.1 below. This result was suspected by Euler building on lots of calculations and earlier work of Fermat. The formulation of the relationship was made precise by Legendre who also worked on the proof. The first complete proof however was given by Gauss at the age of 19 in his famous book *Disquisitiones Arithmeticae*. This is often considered to be the starting point for modern number theory!

Theorem 16.1 (Law of Quadratic Reciprocity (Legendre, Gauss))**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

There are now 246 recorded proofs of this result (not all of them different), including six by Gauss – see http://www.rzuser.uni-heidelberg.de/∼hb3/fchrono.html for a list.
Let's see what the Theorem means:

Remark 16.2. *Note that p and q are odd. An odd number n is either $\equiv 1 \bmod 4$ or $\equiv 3 \bmod 4$. In the former case, we have $(-1)^{\frac{n-1}{2}} = 1$ and in the latter case, $(-1)^{\frac{n-1}{2}} = -1$.*

Now by definition Legendre symbols only assume values in $\{1, -1\}$. In combination with the discussion above, this shows that the Theorem says

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \tag{86}$$

UNLESS p and q are both $\equiv -1 \bmod 4$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right). \tag{87}$$

This is a really remarkable result![92] Precise, elegant and simple.

Question 16.3. *How does this help us to compute Legendre symbols $\left(\frac{p}{q}\right)$ for q and p odd primes?*

[92]Indeed a priori it's not clear at all that there should be a relationship between these two symbols. Let alone such a simple one!

Let's look at an example

Example 16.4. *Let's compute* $\left(\frac{5}{19}\right)$. *Note that* $5 \equiv 1 \bmod 4$ *so we are in the case of* (85) *and we get*

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) \tag{88}$$

using Remark 15.8 in the second step. But $4 = 2^2$ *is a square so*

$$\left(\frac{4}{5}\right) = 1 \tag{89}$$

finishing the computation. So 5 *is a square* mod19.

Let's do another example

Example 16.5. *Let's compute* $\left(\frac{7}{19}\right)$. *Note that both* 7 *and* 19 *are* $\equiv 3 \bmod 4$ *so we are in the case of* (87) *and we get*

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) \tag{90}$$

again using reduction mod7 *in the second step (Remark 15.8). Now* 5 *and* 7 *are also odd primes so we can continue the game and "flip them around" again noting that since* $5 \equiv 1 \bmod 4$ *we are in the case of* (85)

$$-\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) \tag{91}$$

Now it seems that we are stuck as 2 *is not odd (see Proposition 16.9 for how to treat this case directly!). But we can use that* $2 \equiv -3 \bmod 5$ *to continue*

$$-\left(\frac{-3}{5}\right) = -\left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{-1}{3}\right) = -(-1). \tag{92}$$

using Theorem 15.11 in the second step and last step, and the law of quadratic reciprocity in the second step.

Remark 16.6. *These examples show a* **strategy** *that actually* **works in general**. *Using the multiplicativity of the Legendre symbol we can always bring ourselves into a situation where we only have to deal with primes* $q < p$. *If both are odd, using quadratic reciprocity we can flip the legendre symbol* $\left(\frac{q}{p}\right)$ *around to get* $\pm\left(\frac{q}{p}\right)$ *where the sign depends on how* q *and* p *look like* mod4. *But now we can reduce* $q \bmod p$ *and continue our computation with Legendre symbols involving smaller numbers. Typically, this process gets down to small numbers quite quickly! Then we can either use Theorem 15.11 or Proposition 16.9 below to finish the computation. I think it's great fun to do these calculations!*

We'll give one of Gauss's proof of Theorem 16.1 below, using the following Lemma for $a = q$ an odd prime number.

Lemma 16.7 (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*

$$a, 2a, 3a, ..., p'a, \tag{93}$$

reduced mod p *to lie in the closed interval $[-p', p']$. Then $\left(\frac{a}{p}\right) = (-1)^\nu$, where ν is the number of negative numbers in the sequence (93).*

Before we look at the proof, let's see what happens in examples

Example 16.8. *Let $p = 11$, then $p' = \frac{p-1}{2} = 5$*

- *take $a = 4$, then (93) from above becomes*[93]

$$a = 4,\ 2a = 8 \equiv -3,\ 3a = 12 \equiv 1,\ 4a = 16 \equiv 5,\ p'a = 5a = 20 \equiv -2 \bmod 11. \tag{94}$$

We count $\nu = 2$ negative numbers in this sequence. Therefore, Gauss's Lemma implies

$$\left(\frac{4}{11}\right) = (-1)^2 = 1.$$

Since $4 = 2^2$ is a square number[94] *this agrees with the Definition (84) of the Legendre symbol recalled above.*

- *take $a = 2$, then (93) from above becomes*

$$a = 2,\ 2a = 4,\ 3a = 6 \equiv -5,\ 4a = 8 \equiv -3,\ p'a = 5a = 10 \equiv -1 \bmod 11. \tag{95}$$

So there are $\nu = 3$ negative numbers in the sequence and Gauss's Lemma implies

$$\left(\frac{2}{11}\right) = (-1)^3 = -1.$$

Let's check whether this makes sense using the rules for computing with Legendre symbols from Lemma 15.13 and Theorem 15.11 in the last step

$$\left(\frac{2}{11}\right) = \left(\frac{-9}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{9}{11}\right) = \left(\frac{-1}{11}\right) \cdot 1 = -1$$

so again Gauss's Lemma gives the correct answer.

[93] note that we've made sure that we choose our numbers mod11 in such a way that they all lie in the interval $[-p', p'] = [-5, 5]$ as required in Gauss's Lemma

[94] in particular it is a q.r. modulo p for any odd prime p

As an application of Gauss's Lemma, the second part of the example above can be generalised to compute $\left(\frac{2}{p}\right)$ for any odd prime.

Proposition 16.9. *For p an odd prime we have* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(Note that the right hand side 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 the value of $p \bmod 8$. We give the details for $p \equiv 3 \bmod 8$, so $p = 8\ell + 3$ for some integer $\ell \geqslant 0$. Then $p' = (p-1)/2 = 4\ell + 1$. Now taking $a = 2$ in Gauss's Lemma, the "unreduced" sequence (93) is

$$2,\ 4,\ 6,\ \ldots,\ 4\ell,\ 4\ell+2,\ \ldots,\ 8\ell+2$$

now passing to equivalent integers $\bmod p$ which lie in the interval $[-p', p'] = [-4\ell - 1, 4\ell + 1]$ this sequence becomes

$$2,\ 4,\ 6,\ \ldots,\ 4\ell,\ -(4\ell+1),\ -(4\ell-1),\ \ldots,\ -3,\ -1 \bmod 8\ell+3.$$

This sequence has 2ℓ positive members and p' members in total. Hence we have

$$\nu = p' - 2\ell = 2\ell + 1$$

negative members. Hence, Gauss's Lemma implies

$$\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1,$$

which shows that

$$\left(\frac{2}{p}\right) = (-1)^{8\ell^2+6\ell+1} = (-1)^{\frac{p^2-1}{8}}$$

as claimed. □

Exercise 16.10. *Do the other three cases in the proof above!*

Let's look at the proof of Gauss's Lemma:

Proof. Since $a \not\equiv 0 \bmod p$ by assumption, each of the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ p'a \tag{96}$$

is congruent to one of $\pm 1,\ \pm 2,\ \ldots,\ \pm p' \bmod p$ (indeed this is a complete list of the $p-1$ different non-zero residue classes $\bmod p$). Let's look at this in more detail. We claim that

- the members of the sequence (96) are pairwise different mod$p$.

  First we look at what happens for $a = 1$. Since $0 < p' < p$, the members of the sequence $1, 2, \cdots, p'$ are pairwise different mod$p$ so the statement is true here. Now

  $$ia \equiv ja \bmod p \Leftrightarrow i \equiv j \bmod p$$

  since a is invertible mod$p$ (see Lectures 5 & 6). This reduces the general statement to the case $a = 1$ which we've already verified.

- none of the members of (96) is minus another member,

  As in the previous argument it suffices to look at the case $a = 1$ since a is invertible[95]. So we have to look at $1 \leqslant i, j \leqslant p'$. If $i \equiv -j \bmod p$ then $i + j \equiv 0 \bmod p$. In other words, $p \mid i + j$ but since

  $$i + j \leqslant 2p' = p - 1 < p$$

  and $i + j > 0$ this is impossible.

Combining the two claims above, we see that (after reordering!!) our sequence (96) is congruent to a sequence

$$\pm 1, \ \pm 2, \ \ldots, \ \pm p' \bmod p,$$

where each of $1, 2, \ldots, p'$ occurs exactly once with a **definite sign**[96]. Using this we get

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot p'a \equiv (\pm 1) \cdot (\pm 2) \cdot \ldots \cdot (\pm p') \bmod p. \tag{97}$$

Recall, that ν was counting the number of negative numbers in our sequence. We can use this to rewrite (97) as follows

$$a^{p'}(p')! \equiv (-1)^{\nu}(p')! \bmod p.$$

Since $0 < p' < p$ and p is prime, we see that $(p')!$ is coprime to p. But this means that $(p')!$ is invertible mod$p$, which implies

$$a^{p'} \equiv (-1)^{\nu} \bmod p.$$

Finally, applying Euler's criterion (Prop. 15.10) to calculate $\left(\frac{a}{p}\right)$ it follows that

$$\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^{\nu} \bmod p.$$

Hence $\left(\frac{a}{p}\right) = (-1)^{\nu}$ as claimed. □

[95] Clarify this for yourself!

[96] If that's confusing look at Example 16.8 again. For $a = 4$, the sequence was $4, -3, 1, 5, -2$ (see (94)), which after reordering is $1, -2, -3, 4, 5$, so indeed of the claimed form. For $a = 2$, the sequence was $2, 4, -5, -3, -1$, which after reordering is $-1, 2, -3, 4, -5$, so also of the claimed form.

In order to prove the Law of Quadratic Reciprocity, we need some more preparation.

Definition 16.11. *We define the* **floor function** *as*

$$\lfloor x \rfloor \ : \ \mathbb{R} \to \mathbb{Z} \ ; \ x \mapsto \lfloor x \rfloor = \textit{largest integer} \leqslant x \ .$$

Using this definition we can rephrase the Division Algorithm (11) as follows

Lemma 16.12. *Let a, b be natural numbers. Then there is a natural number $0 \leqslant r < b$ such that*

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r. \tag{98}$$

We now use Gauss's Lemma 16.7 for $a = q$ an odd prime different from p to prove the Law of Quadratic Reciprocity.

Proof of Theorem 16.1. Take distinct odd primes p and q. For each $k = 1, 2, \ldots, p'$ apply Lemma 16.12 to $a = kq$ and $b = p$ to get

$$kq = q_k p + r_k \tag{99}$$

with $1 \leqslant r_k \leqslant p-1$ (we have $r_k \neq 0$ since q and p are different primes and since $k < p$) and

$$q_k = \left\lfloor \frac{kq}{p} \right\rfloor. \tag{100}$$

Now, working modulo p and using (99) in the first step, we have

$$\{r_1, r_2, \ldots, r_{p'}\} \equiv \{q, 2q, \ldots, p'q\} \equiv \{a_1, a_2, \ldots, a_t\} \cup \{-b_1, -b_2, \ldots, -b_\nu\},$$

where the a_i's are in $(0, p']$ and the $-b_i$'s are in $[-p', 0)$ as in Gauss's Lemma 16.7 (in particular, ν is the same as in Gauss's Lemma too) and the r_i's are in $[1, p-1]$. More precisely, we note that if $r_j \leqslant p'$, then

$$r_j = a_i \quad \text{for some } i \in \{1, \cdots, t\} \tag{101}$$

and if $r_j > p'$, then

$$r_j - p = -b_i \quad \text{for some } i \in \{1, \cdots, \nu\}. \tag{102}$$

Now we set

$$a = \sum_{i=1}^{t} a_i, \qquad\qquad b = \sum_{i=1}^{\nu} b_i.$$

So, by (101), (102) and the definition of ν, we have

$$\sum_{k=1}^{p'} r_k - \nu p = a - b, \tag{103}$$

which is equivalent to

$$\sum_{k=1}^{p'} r_k = a - b + \nu p. \tag{104}$$

In the proof of Gauss's Lemma we saw that

$$\{a_1, a_2, \ldots, a_t\} \cup \{b_1, b_2, \ldots, b_\nu\} = \{1, 2, \ldots, p'\},$$

which we use in the last step of the next chain of equations

$$\frac{p^2-1}{8} = \frac{p'(p'+1)}{2} = 1 + 2 + \cdots + p' = a + b. \tag{105}$$

This gives

$$\begin{aligned} \frac{p^2-1}{8} q &= \sum_{k=1}^{p'} kq && \text{using (105)} \\ &= p \sum_{k=1}^{p'} q_k + \sum_{k=1}^{p'} r_k && \text{using (99)} \\ &= p \sum_{k=1}^{p'} q_k + a - b + \nu p, && \text{using (104)} \end{aligned} \tag{106}$$

Next, subtracting (105) from (106) we get

$$\frac{p^2-1}{8}(q-1) = p \sum_{k=1}^{p'} q_k - 2b + \nu p.$$

Reducing this modulo 2 and using that p and q are odd, we obtain

$$0 \equiv \sum_{k=1}^{p'} q_k - \nu \bmod 2,$$

which gives

$$\nu \equiv \sum_{k=1}^{p'} q_k \bmod 2.$$

Thus Gauss's Lemma gives[97]

$$\left(\frac{q}{p}\right) = (-1)^\nu = (-1)^{\sum_{k=1}^{p'} q_k} = (-1)^{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor},$$

[97] Check for yourself why this works!

using (100) in the last step.

Now, reversing the roles of p and q, we directly get

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor},$$

where $q' = (q-1)/2$, and we've replaced the dummy variable k by ℓ. Summing up, we get

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left\{\sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{q'} \left\lfloor \frac{\ell p}{q} \right\rfloor\right\}}.$$

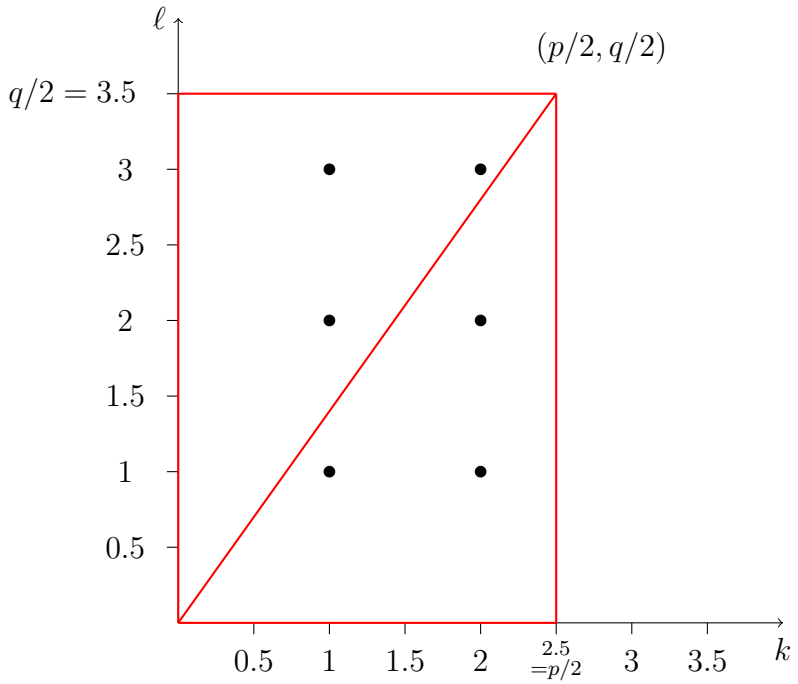
The right hand side equals $(-1)^{p'q'}$ as desired, using the following beautiful geometric argument for a (on first sight) quite horrific looking formula (see Lemma 16.13) □

Lemma 16.13. *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 $\ell = kq/p$, see also the picture below.)

KEY IDEA: We **count** the number of points with **integer** coordinates (k,ℓ) which are strictly inside this rectangle **in two different ways**. One way of counting will give the left hand side of the equation above and the other way of counting will give the right hand side. Here is an illustration for the case $p = 5$ and $q = 7$:



We see that there are $\frac{p-1}{2}\frac{q-1}{2} = 2 \cdot 3 = 6$ points with integer coordinates inside this rectangle, this corresponds to the right hand side of our equation.

Below the diagonal we have $1 = \lfloor 7/5 \rfloor$ point in the first column (namely the point $(1,1)$) and $2 = \lfloor 2 \cdot 7/5 \rfloor$ points in the second column (namely, $(2,1)$ and $(2,2)$). This gives 3 points below the diagonal in total and explains the first summand of the left hand side of our equation.

Above the diagonal, there are $0 = \lfloor 5/7 \rfloor$ points in the first row (with $\ell = 1$), then $1 = \lfloor 2 \cdot 5/7 \rfloor$ point in the second row (namely, $(1,2)$) and finally $2 = \lfloor 3 \cdot 5/7 \rfloor$ points in the third row (namely, $(1,3)$ and $(2,3)$). So in total we have $1+2 = 3$ points above the diagonal.

Finally, there are NO POINTS on the diagonal.

To sum up, we see that this way of counting the points also gives $6 = 3 + 3$ points in total.

Let's do the general case. First we note that the points with integer coordinates 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 $\frac{p-1}{2} \cdot \frac{q-1}{2}$ points in total, which is the right hand side of our equation

On the other hand, we count separately those points below, above and on the diagonal $\ell = k \cdot q/p$.

Below the diagonal: in the first column with k-coordinate 1 the points

$$(1,1), (1,2), \ldots, (1, \left\lfloor \frac{q}{p} \right\rfloor) \tag{107}$$

are below the diagonal. Using the equation $\ell = k \cdot q/p$ for the diagonal, we see that there are no more points in this column which lie below the diagonal. We continue in this way to look at all other possible columns inside the rectangle. They have k-coordinates $2, 3, \ldots, \frac{p-1}{2}$ and the points

$$(k,1), (k,2), \ldots, (k, \left\lfloor \frac{kq}{p} \right\rfloor) \tag{108}$$

are exactly the ones below the diagonal, using the equation for the diaginal again.

Summing up the number of points below the diagonal for each column, we get

$$\text{number of points below the diagonal} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor. \tag{109}$$

Above the diagonal: we first flip the diagram over, reversing the roles of p and q, and of k and ℓ. Then using (109), we get that the number of points above the diagonal is

$$\text{number of points above the diagonal} = \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor. \tag{110}$$

On the diagonal: 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 $0 < k < p$, so this is impossible.

Summing up, as every point inside the rectangle has to be either above, below or on the diagonal the total number of points is

$$\text{total number of points} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor + 0 \tag{111}$$

which gives the left hand side of the equation. □

16.2 Proofs of Infinitude of Primes

We've seen in the last Lecture that Legendre symbols are useful for showing that there are infinitely many primes of the form $4k + 1$ (see Theorem 15.12). We review this case and others below and see how the results of today's lecture can be used to go beyond this.

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 16.14. *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 all factors were congruent to 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 16.15. *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 a product which is congruent to 1 mod 4. For instance $3 \cdot 7 = 21$.

Last time we've seen how to use quadratic residues to overcome this difficulty (see Theorem 15.12).

Using the results from today we can show that other families of numbers contain infinitely many primes too. Indeed Problem 4 on Workshop sheet 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 $(p_1 \cdots p_k)^2 - 2$. You can also use a similar 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 Lecture 17: Fermat's approach to Diophantine equations (20.3.2018)

17.1 Fermat's method of descent

Recall that in the first lecture, we studied all integer solutions of the polynomial equation

$$X_1^2 + X_2^2 - X_3^2 = 0. \tag{112}$$

These solutions are called **Pythagorean triples**.

More generally, one can study integer solutions of polynomial equations of the form

$$f(X_1, \ldots, X_n) = 0 \quad \text{where } f \text{ is a polynomial in } n\text{-variables with integer coefficients} \tag{113}$$

Such equations 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 an **important 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' one (where "small" has to be defined in a sense suitable for the equation in question). Use this 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.

We illustrate the method with some examples. There will be examples building on the theory of quadratic residues which we've developed in the last two lectures and also the case $n = 4$ of Fermat's famous Last Theorem, which will make use of our knowledge about (primitive) Pythagorean triples from Lecture 1.

17.2 A 2-variable quadratic equation with no nonzero integer solution

Proposition 17.1. *The Diophantine equation*

$$x^2 = 2y^2 \tag{114}$$

has no integers solutions $(x, y) \neq (0, 0)$.

In particular, $\sqrt{2}$ *is irrational (meaning that* $\sqrt{2}$ *is not a rational number, i.e. cannot be written as a fraction of integers).*

First proof. We show that any non-zero integer solution (x, y) would contradict the Fundamental Theorem of Arithmetic. Assume that there is an integer solution $(x, y) \neq (0, 0)$. 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 $2^{2a}u^2 = 2^{2b+1}v^2$. It follows from the Fundamental Theorem of Arithmetic that $2a = 2b + 1$. This is a contradiction as no integer is odd and even at the same time. So there is indeed no such solution x, y.

Second proof using Fermat Descent. First note that if there is an integer solution $(x, y) \neq (0, 0)$, then[98] there is also an integer solution (x', y') with $x' > 0$ and $y' > 0$. So let's assume that there is a solution x, y in positive integers. Define the size of such a solution (x, y) to be $x + y$. Choose a solution of smallest[99] size (this wouldn't necessarily be unique – but that doesn't matter for our proof). 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. □

Exercise 17.2. *What happens in the proofs of Proposition 17.1 if we replace* 2 *by an arbitrary odd prime* p *?*

[98] Check this for yourself!

[99] why does this work?

We next look at a more complicated example of a Diophantine equation, where Fermat's method applies. This time we also make use of the results about quadratic residues from the previous two lectures. Why does this work, how do the congruences come in? This is a simple but **very powerful method** which sometimes helps to attack Diophantine equations: if we have a Diophantine equation

$$f(X_1, \ldots, X_n) = 0 \quad \text{where } f \text{ is a polynomial in } n\text{-variables with integer coefficients} \tag{115}$$

Then we can pick any natural number m and equation (115) yields a congruence[100]

$$f(X_1, \ldots, X_n) \equiv 0 \bmod n \tag{116}$$

If we choose n in a clever way we might hope to arrive at a congruence where one of our techniques and results about congruences applies. From this, we can often deduce that certain **integer** solutions are not possible. Sometimes (as in the Theorem below) we even get that there are no solutions at all!

17.3 A 4-variable quadratic equation with no nonzero integer solution

Theorem 17.3. *Let p and q be odd primes. Assume that at least one of $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ is -1.*

Then the equation

$$x^2 + pqy^2 = pz^2 + qw^2 \tag{117}$$

has no integer solutions (x, y, z, w) apart from $(0, 0, 0, 0)$..

Proof. We first observe that if (x, y, z, w) is a solution of (117), then $(\pm x, \pm y, \pm z, \pm w)$ is also a solution for any choice of signs $\pm$. Therefore, if there is a solution, then there is a solution with all x, y, z, w nonnegative. So let's assume that this is the case. Define the **size** of a nonnegative[101] solution by

$$s(x, y, z, w) \;=\; x + y + z + w.$$

By our assumptions one of x, y, z, w is strictly positive so the size of any solution is at least 1. Among all such solutions, we choose one solution (x, y, z, w) that has size $s(x, y, z, w)$ **as small as possible**.

Suppose further that

$$\left(\frac{p}{q}\right) = -1.$$

Since our equation (117) is symmetric in p and q the case

$$\left(\frac{q}{p}\right) = -1$$

[100] Clarify for yourself why this works!

[101] meaning that all x, y, z, w are nonnegative and at least one is nonzero

can be treated by changing the roles of p and q.

Now, considering the equation (117) modulo q, we have that

$$x^2 \equiv pz^2 \bmod q. \tag{118}$$

If $z \not\equiv 0 \bmod q$, we could invert z to obtain

$$(xz^{-1})^2 \equiv p \bmod q,$$

so that p would be a square mod$q$. But this contradicts our assumption that $\left(\frac{p}{q}\right) = -1$. Hence, $z \equiv 0 \bmod q$ and therefore $x \equiv 0 \bmod q$ by (118). In other words, this shows that $q \mid z$ and $q \mid x$. Thus we can write $x = qx_1$, $z = qz_1$, and so from (117), 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 (117). Following Fermat's method, we would like to show that this solution is smaller than our smallest solution (x, y, z, w) which would lead to a contradiction.

Note first that x and z can't both be 0, as then (117) would imply $py^2 = w^2$, which implies $y = 0 = w$ by the same arguments used to in the proof of Proposition 17.1 (see also Exercise 17.2). So we would get $(x, y, z, w) = (0, 0, 0, 0)$ a solution which we've excluded from the outset. Hence either $0 < z_1 < z$ or $0 < x_1 < x$ (or both!), so we have

$$s(w, z_1, y, x_1) = w + z_1 + y + x_1 < w + z + y + x = s(x, y, z, w),$$

showing that the new solution is indeed of smaller size, contradicting the fact that we started with (x, y, z, w) of minimal size. Hence no solution can exist. □

Corollary 17.4. *If both p and q are primes $\equiv -1 \bmod 4$ then (117) has no integer solution $(x, y, z, w) \neq (0, 0, 0, 0)$.*

Proof. In this case, the quadratic reciprocity law from last lecture 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 17.3 applies. □

Example 17.5. *1. The Diophantine equation $x^2 + 21y^2 = 3z^2 + 7w^2$ has no integer solution $(x, y, z, w) \neq (0, 0, 0, 0)$ by Corollary 17.4.*

2. *If both* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$, *then* (117) *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*

$$(x, y, z, w) \;=\; (4, 0, 1, 1)\ ,\ (3, 1, 2, 2)\ ,\ (7, 1, 1, 3)\ .$$

Our third example is due to Fermat and is in fact one of the most famous cases where his method applies. In the proof we will also make use of our knowledge of (primitive) Pythagorean triples from the very first Lecture!

17.4 Fermat's Last Theorem for exponent 4

Fermat's Last Theorem is the statement that the Diophantine equation

$$x^n + y^n \;=\; z^n$$

can be solved by **non-zero** integers x, y, z only for exponents $n = 1$ and 2. (For $n = 1$, we have a linear Diophantine equation as studied in Lecture 4. Geometrically, the solutions are points with integer coordinates on a plane in $\mathbb{R}^3$ and there are infinitely many such points[102]. For $n = 2$ we have the Pythagorean Triples from the first lecture[103] Geometrically the solutions are points with integer coordinates on a cone in $\mathbb{R}^3$ (see the video on Pythagorean triples on LEARN)).

The theorem above was first claimed by Pierre de Fermat in 1637 in the margin of Diophantus's **Arithmetica**, although he said that "unfortunately, the margin of the book is too small to accommodate the proof". Therefore, we don't know whether Fermat had a proof or not. However, most people believe that he did not have a correct proof. He possibly believed that his strategy which works for $n = 4$ (and with more effort for other exponents n) would do the job in general. This is not true unfortunately. So Fermat's Theorem was "downgraded" to the **Fermat Conjecture**. The conjecture was sensationally proved by Sir Andrew Wiles in 1994 after over 350 years of research by the some of the greatest mathematicians[104]. It is now officially called **Fermat's Last Theorem**.

[102] Do you see why?

[103] and this is one of the reasons which makes Fermat's Last theorem for $n > 2$ interesting. For example for $n = 3$ the Theorem says that it's impossible to find two cubes with integer side length such that one can combine them to build a third cube with integer side length, see Remark 1.6 and the illustration above it.

[104] Not every great mathematician was interested in this problem however. Apparently the great Gauss was pretty unimpressed by the difficulty of Fermat's problem saying that he "could easily find many problems in number theory which are as hard as this." He preferred general theories which could handle many (diophantine) equations/problems at the same time – his "golden quadratic reciprocity theorem" (see last lecture) is an example of such a result. It took a long time and the effort of many great minds to "embed" Fermat's last theorem into a general theory/framework. Wiles's contribution was to show (a special case of) an important conjecture (the Taniyama-Shimura-Weil conjecture – now called *modularity theorem*) in this theory – others

Theorem 17.6. *The equation*

$$x^4 + y^4 = z^2 \tag{119}$$

has no integer solutions (x, y, z) *with* x, y, z *all non-zero.*

As a special case of Theorem 17.6 (assume z to be a square) we obtain.

Corollary 17.7 (Fermat's Last Theorem for exponent 4)**.** *The equation* $x^4 + y^4 = z^4$ *has no integer solutions* (x, y, z) *with* x, y, z *all non-zero.*

Proof of Theorem 17.6. (the presentation of this proof is inspired by the presentation in H. Davenport, **The higher arithmetic. An introduction to the theory of numbers**, Longmans 1952, p.162). Suppose that (119) has an integer solution (x, y, z) with x, y, z all non-zero. Since all exponents are even, it follows (by changing signs if needed) that there is also a solution with x, y, z all *positive*. We can further assume that $z \neq 1$, i.e., that $z > 1$ since x and y are both positive. In this proof, 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 replace x by x/d, y by y/d and z by z/d^2 in (119), obtaining another solution with z smaller. So we must have $\gcd(x, y) = 1$ for our minimal solution.

Setting $X = x^2$, $Y = y^2$ and $Z = z$ our solution to the equation (119) gives a solution of

$$X^2 + Y^2 = Z^2.$$

We've studied this equation in Lecture 1 and Workshop 1. So we know that it has a general integer solution of the following form (after possibly swapping the roles of X and Y)

$$X = p^2 - q^2 \qquad Y = 2pq \qquad Z = p^2 + q^2,$$

where $p > q \in \mathbb{N}$ and $\gcd(p, q) = 1$ (this follows from our classification of Pythagorean triples on the first Workshop sheet (see Exercise (1) part (f))). So substituting back in we get

$$x^2 = p^2 - q^2 \qquad y^2 = 2pq \qquad z = p^2 + q^2. \tag{120}$$

It follows that y is even and therefore x has to be odd because we know that they are coprime. This shows that precisely one of p and q is even and the other is odd. Here comes a nice trick that shows that we don't have a choice: p is odd and q is even!

Indeed look at the equation

$$x^2 = p^2 - q^2 \tag{121}$$

(it's the first in (120) above) and view it as a congruence mod 4. We can check that squares mod4 are congruent 0 or 1 mod 4. Since x is odd $x^2 \equiv 1 \bmod 4$. If p was even and q odd then the right hand side of (121) would be congruent to $0 - 1 \equiv -1 \bmod 4$ which is not

had already shown that this would imply Fermat's last Theorem. Ironically, this theory around Fermat's last Theorem turns out to be part of a larger theory/net of conjectures – the so called Langlands program which in turn is a vast generalisation of Gauss's quadratic reciprocity theorem... so in this sense Gauss was wrong, but with the knowledge of his time this was not really possible to foresee even for someone like Gauss.

congruent to 1 (the result we had for the left hand side). Contradiction. Thus p must be odd and q even, say $q = 2r$.

Using this we can rewrite (120) as follows

$$x^2 = p^2 - (2r)^2 \qquad \left(\frac{y}{2}\right)^2 = pr.$$

Since $\gcd(p, r) = 1$ and $pr = (y/2)^2$ is a square, we see that

$$p = v^2 \tag{122}$$

and $r = w^2$ (using the Fundamental Theorem of Arithmetic). So $q = 2w^2$. Substituting into (121) it follows that

$$x^2 + (2w^2)^2 = (v^2)^2.$$

Note that, as $\gcd(x, y) = 1$ and $y^2 = 2pq$, we have $1 = \gcd(x, q) = \gcd(x, 2w^2)$. Hence, using Workshop sheet 1, Exercise (1) part (f) again, we have

$$x = p_1^2 - q_1^2 \qquad 2w^2 = 2p_1q_1 \qquad v^2 = p_1^2 + q_1^2, \tag{123}$$

where $p_1, q_1 \in \mathbb{N}$ with $\gcd(p_1, q_1) = 1$. It follows that $w^2 = p_1q_1$, giving $p_1 = v_1^2$, $q_1 = r_1^2$ for $v_1, r_1 \in \mathbb{N}$ (again using the fundamental Theorem of Arithmetic). Hence substituting into the last equation of (123) we get

$$v^2 = p_1^2 + q_1^2 = v_1^4 + r_1^4,$$

showing that (v_1, r_1, v) is another positive integer solution of (119)! We show that $v < z$ contradicting our assumption that we had a solution with z minimal: using first (122) and then (120), we get

$$v^2 = p = \sqrt{z - q^2} < \sqrt{z},$$

giving $v < z^{1/4}$, so certainly $v < z$ (as $z > 1$ by remark in beginning). This finishes the proof by Fermat descent. □

Here's a cheap but impressive looking consequence[105].

Corollary 17.8. *Let $k \in \mathbb{N}$. Then the Fermat equation*

$$x^{4k} + y^{4k} = z^{4k} \tag{124}$$

has no integer solutions (x, y, z) with x, y, z all non-zero.

Proof. We can rewrite (124) as

$$(x^k)^4 + (y^k)^4 = (z^k)^4 \tag{125}$$

and use Corollary 17.7. □

[105] How can we generalise this? What does this mean for Fermat's Last Theorem in general?

Main Points from Lecture 17:

- Fermat's method of descent
- Irrationality of $\sqrt{2}$
- Diophantine equations without solutions
- Fermat's Last Theorem for $n = 4$.

18 Lecture 18: Representation of integers as sums of two squares (23.3.2018)

Today we are studying the following classical question.

Question 18.1. *Which integers $n \in \mathbb{Z}$ can be represented as a sum of two squares of integers*

$$n \;=\; x^2 + y^2 \text{ for } x, y \in \mathbb{Z} \; ?$$

Certainly, we need $n \geqslant 0$. Also, we may assume that x and y are $\geqslant 0$.

Let's look at some examples for low values of n

$$0 \;=\; 0^2+0^2 \;,\; 1 \;=\; 0^2+1^2 \;,\; 2 \;=\; 1^2+1^2 \;,\; 3 \;\neq\; x^2+y^2 \;,\; 4 \;=\; 0^2+2^2 \;,$$
$$5 \;=\; 1^2+2^2 \;,\; 6 \;\neq\; x^2+y^2 \;,\; 7 \;\neq\; x^2+y^2 \;,\; 8 \;=\; 2^2+2^2 \;,\; 9 \;=\; 0^2+3^2 \;,$$
$$10 \;=\; 1^2+3^2 \;,\; 11 \;\neq\; x^2+y^2 \;,\; 12 \;\neq\; x^2+y^2 \;,\; 13 \;= 2^2+3^2 \;,\; 14 \;\neq\; x^2+y^2 \;, \ldots \;.$$

There is no apparent pattern. So we need to develop some theory if we want to understand Question 18.1.

Again 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. Indeed we will see below that this reduces the question to prime powers.

Let's introduce the relevant notions from complex numbers. 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

$$\|zw\| = \sqrt{(ac-bd)^2+(ad+bc)^2} \tag{126}$$
$$= \sqrt{a^2c^2+b^2d^2+a^2d^2+b^2c^2} \;=\; \sqrt{a^2+b^2}\sqrt{c^2+d^2} \;=\; \|z\|\,\|w\| \;. \tag{127}$$

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

$$(a + ib) + (c + id) \;=\; (a + c) + i(b + d)\ .$$

To relate this to our question, we observe that 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 18.11 below states that the product of sums of two squares is a sum of two squares:

$$(a^2 + b^2)(c^2 + d^2) \;=\; (ac - bd)^2 + (ad + bc)^2 \tag{128}$$

So using the Fundamental Theorem of Arithmetic, the question of expressing an integer as a sum of two squares is indeed reduced to the expression of prime powers as sums of two squares.

Note that (128) can also be seen from the product rule (126) for the modulus of the product of complex numbers

$$\|zw\| = \|z\|\,\|w\|.$$

Remark 18.2. *The Wikipedia article on Gaussian integers is a brief introduction to the interesting algebraic*[106] *and geometric properties of the Gaussian integers. You might even wish to take a Stroll through the Gaussian primes.*

18.1 Prime powers as sums of squares

We've seen above that our original question 18.1 reduces to

Question 18.3. *Which prime powers can be written as sums of two squares of integers.*

It's a good exercise to see what happens for powers of 2.

Exercise 18.4. *Let $k \geqslant 0$ be an integer. Show that $n = 2^k$ can be written as $n = x^2 + y^2$ for some integers $x, y \in \mathbb{Z}$.*

[106] For example, there is an analogue of the Fundamental Theorem of Arithmetic for the Gaussian integers. Roughly, the reason for this is that (as for the integers) there is a way to do division with remainder in the Gaussian integers. In particular, there is a notion of prime number for Gaussian integers and these are called Gaussian primes.

Every power of 2 is a sum of two squares since

$$2^{2k} = (2^k)^2 + 0^2 \ , \ 2^{2k+1} = (2^k)^2 + (2^k)^2 \ .$$

Let's look at odd primes p. We know that every odd number is congruent to 1 or -1 mod 4.

Exercise 18.5. *Show that if an odd prime p can be written as*

$$p = x^2 + y^2$$

for integers x and y. Then $p \equiv 1 \bmod 4$.

It turns out that the converse statement (in exercise 18.5) is true as well. The proof involves Legendre symbols and results from Lecture 15.

Theorem 18.6. *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. Exercise 18.5 says 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 $p \equiv 1 \bmod 4$. Then Theorem 15.11 shows that $\left(\frac{-1}{p}\right) = 1$. By definition of the Legendre-symbol, this means that there is an $r \in \mathbb{N}$ with $r^2 \equiv -1 \bmod p$. We use the floor function (see Definition 16.11) to define $K = \lfloor \sqrt{p} \rfloor$. Note that

$$K < \sqrt{p} < K + 1, \tag{129}$$

as $\sqrt{p} \notin \mathbb{Z}$. The function

$$f \colon [0, K] \times [0, K] \to \mathbb{F}_p \ ; \ (u, v) \mapsto u + rv \bmod p$$

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 $f(u_1, v_1) \equiv f(u_2, v_2) \bmod p$. Writing this out gives

$$\begin{aligned} u_1 + rv_1 &\equiv u_2 + rv_2 \bmod p \\ u_1 - u_2 &\equiv -r(v_1 - v_2) \bmod p \\ a &\equiv -rb \bmod p, \end{aligned}$$

say, where $a = u_1 - u_2$ and $b = v_1 - v_2$ are not both 0 (since we've taken $(u_1, v_1) \neq (u_2, v_2)$). Hence

$$a^2 \equiv (-rb)^2 \equiv r^2 b^2 \equiv -b^2 \bmod p \tag{130}$$

as we know that $r^2 \equiv -1 \bmod p$. In other words, (130) shows that $p \mid (a^2 + b^2)$. But by construction $|a| \leqslant K$, $|b| \leqslant K$, giving

$$0 < a^2 + b^2 \leqslant 2K^2 < 2p.$$

So $p \mid (a^2 + b^2)$ is only possible if $a^2 + b^2 = p$. □

Combining this with the product rule (128) above shows

Corollary 18.7. *Let p be an odd prime with $p \equiv 1 \bmod 4$ and let $k \geqslant 0$ be an integer. Then p^k is a sum of two squares of integers.*

Example 18.8. *Take the prime $p = 5$. Then $p \equiv 1 \bmod 4$ so we should be able to express 5 as a sum of two squares of integers. Indeed,*

$$5 = 2^2 + 1^2. \tag{131}$$

What happens for $25 = 5^2$? There is a cheap way of doing this

$$25 = 5^2 + 0^2.$$

But we can also use the product formula (128) as follows

$$25 = 5 \cdot 5 = (2^2 + 1^2)(2^2 + 1^2) = (4 - 1)^2 + (2 + 2)^2 = 3^2 + 4^2 = 9 + 16 \tag{132}$$

which might look familiar from the first Lecture on Pythagorean triples.

Try to figure out what happens for 125.

Example 18.9. *Let's write $n = 13 \cdot 17$ as a sum of two squares. Observe that*

$$13 = 2^2 + 3^2 \quad \textit{and} \quad 17 = 4^2 + 1^2.$$

Now using the product formula (128), we get

$$n = 13 \cdot 17 = (2^2 + 3^2)(4^2 + 1^2) = (8 - 3)^2 + (12 + 2)^2 = 5^2 + 14^2.$$

alternatively by swapping 2^2 and 3^2 we get

$$n = 13 \cdot 17 = (3^2 + 2^2)(4^2 + 1^2) = (12 - 2)^2 + (8 + 3)^2 = 10^2 + 11^2.$$

So we've discussed powers of 2 and powers of primes p with $p \equiv 1 \bmod 4$. Now it remains to check what happens for powers of primes q with $q \equiv -1 \bmod 4$. By Exercise 18.5 it follows that q itself is NOT a sum of two squares. On the other hand $q^2 = q^2 + 0^2$ is and so is every power $q^{2k} = (q^k)^2 + 0^2$ with even exponent. This leads to the following statement.

Lemma 18.10. *Let q be prime with $q \equiv -1 \bmod 4$ and let $n \geqslant 0$ be an integer.*

Then q^n is a sum of two squares of integers if and only if n is even.

Proof. We've discussed already that even exponents work. That q^n for n odd is NOT a sum of two squares of integers follows from the following more general Proposition 18.11 (using induction). □

Proposition 18.11. *Let $q \equiv -1 \bmod 4$ be prime, and $q \mid (x^2 + y^2)$. Then $q \mid x$ and $q \mid y$, and therefore $q^2 \mid (x^2 + y^2)$.*

Proof. Assume that it is not the case that both x and y are divisible by q, say $q \nmid x$, so $x \not\equiv 0 \bmod q$ is invertible. Now $q \mid (x^2 + y^2)$ implies $y^2 \equiv -x^2 \bmod q$. And multiplying with x^{-2}, we get $(yx^{-1})^2 \equiv -1 \bmod q$, showing that -1 is a quadratic residue mod$q$. But this contradicts $\left(\dfrac{-1}{q}\right) = -1$ (by Theorem 15.11). So x and y are both divisible by q and therefore $x^2 + y^2$ is divisible by q^2 as claimed. □

18.2 The general case

We want to use the results from the previous section to study which natural numbers n are sums of two squares of integers.

We've seen the following result in Examples 18.8 and 18.9 already.

Proposition 18.12. *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 using (128) we get

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

We can combine this with induction to show.

Corollary 18.13. *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 and Proposition 18.12 to get $n/A^2 = \prod_i n_i = a^2 + b^2$. Then $n = (Aa)^2 + (Ab)^2$. □

We can now state and prove our main result describing precisely which natural numbers are sums of two squares. This is due to Fermat.

Theorem 18.14 (Fermat)**.** *Let n be a natural number. Using the Fundamental Theorem of Arithmetic we can write n as*

$$n = 2^k \cdot \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} p^{f_p} \cdot \prod_{\substack{q \text{ prime} \\ q \equiv -1 \bmod 4}} q^{g_q} \qquad \text{where} \quad k \geqslant 0, f_p \geqslant 0, g_q \geqslant 0. \tag{133}$$

Then n can be written as the sum of two squares of integers if and only if all the exponents g_q in (133) are even.

Proof. It is an exercise to show that if all the g_q's are even, then n is a sum of two squares of integers.

If all the g_q's are even, then n is a sum of two squares of integers using the product formula (128) in combination with Exercise 18.4, Theorem 18.6 and Lemma 18.10.

Conversely, suppose $q \mid n = a^2 + b^2$, where $q \equiv -1 \bmod 4$ is prime. We want to show that g_q is even, where q^{g_q} is the largest power of q dividing n. For this, 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. 18.11 contradicting the maximality of k. 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. □

Let's look at some more examples

Example 18.15. *1. By Theorem 18.14, $n = 30 = 2 \cdot 3 \cdot 5$ is not the sum of two squares of integers as $3 \equiv -1 \bmod 4$ and $g_3 = 1$ is odd.*

2. $n = 90 = 2 \cdot 3^2 \cdot 5$, using the product formula (128) we get

$$n = 90 = (1^2 + 1^2)3^2(1^2 + 2^2) = 3^2((1-2)^2 + (1+2)^2) = 3^2 + 9^2.$$

18.3 Related results

Proposition 18.16. *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

$$n = (a/b)^2 + (c/d)^2$$

for some rational numbers a/b and c/d. Then

$$n(bd)^2 = (da)^2 + (bc)^2.$$

Hence, by Theorem 18.14, for every prime $q \equiv -1 \bmod 4$ and maximal integer i with $q^i | n(bd)^2$, it follows that i must be even. But then if $q^\ell | bd$ then $q^{i-2\ell} | n$, with $i - 2\ell$ even. Hence, by Theorem 18.14 (in the other direction), n is the sum of two squares of integers. □

Corollary 18.17. *Let m be a non-zero integer and n be an integer.*

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 dividing by m^2 gives

$$(n/m) = (a/m)^2 + (b/m)^2.$$

so (n/m) is indeed a sum of squares of rationals.

Conversely, if

$$(n/m) = (a/b)^2 + (c/d)^2$$

then

$$nm = (am/b)^2 + (cm/d)^2.$$

Hence, by Proposition 18.16, 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. We've done this in Exercise 3(a) on the first Homework sheet but we'll recall it here.

Theorem 18.18. *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*

$$x = \frac{s(u^2 - v^2) - 2uvt}{u^2 + v^2} \qquad y = -\left(\frac{t(u^2 - v^2) + 2uvs}{u^2 + v^2}\right), \tag{134}$$

where $u, v \in \mathbb{Z}$ and are not both zero or $(x, y) = (s, t)$ or $(x, y) = (-s, -t)$.

Remark 18.19. *Note that different pairs (u, v) can give rise to the same point (x, y). Indeed if $d = \gcd(u, v)$, then (u, v) and $(u/d, v/d)$ give rise to the same point on the circle $h = x^2 + y^2$ (we've seen this phenomenon in the first workshop. The (algebraic) reason for this is that for each term in (134) the sum of degrees of u and v is always 2, so we can take out a factor $(1/d)^2$ everywhere).*

Proof. We are looking for all points $(x, y) \in \mathbb{Q}^2$ on the circle $x^2 + y^2 = h$. By assumption, we know that the point (s, t) is on this circle (and therefore $(-s, -t)$ is on the circle too). We'll now use a "stereographic projection type argument" as in the first Workshop. If (x, y) is another point (with rational coordinates) on the circle, then for $x \neq s$ the chord through (s, t) and (x, y) has rational slope $(t - y)/(s - x)$.

We now describe the intersection point of the circle and any chord through (s, t) with rational slope. The intersection point turns out to have rational coordinates as well and by the argument above we know that all points on the circle with rational coordinates (x, y) and $x \neq s$ arise in this way. (For $x = s$ we get the given point (s, t) and also $(s, -t)$)

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

$$x^2 + (r(x - s) + t)^2 = h.$$

Using the fact that $t^2 - h = -s^2$ this simplifies to

$$x^2(1 + r^2) + 2rx(t - rs) + (r^2 - 1)s^2 - 2rst = 0.$$

This can be factored as

$$(x - s)((1 + r^2)x + 2rt + s(1 - r^2)) = 0.$$

So either $x = s$ (which corresponds to the points (s, t) and $(s, -t)$) or if $x \neq s$, the right factor has to be zero and solving for x gives

$$x = \frac{s(r^2 - 1) - 2rt}{1 + r^2}. \tag{135}$$

Using the equation of the chord we can calculate y as

$$y = t + r(x - s) \tag{136}$$

$$= -\left(\frac{t(r^2-1)+2sr}{1+r^2}\right), \tag{137}$$

on simplification. Finally, since$r$ is rational, we can write[107] $r = u/v$ for integers u and $v \neq 0$. Substituting into (135) and (136) gives (134) as desired. Note that $v = 0$ in (134) (i.e., $r = \infty$) gives the point $(s, -t)$. □

We can

Corollary 18.20. *Let n be a natural number. Then the diophantine equation*

$$x^2 + y^2 = nz^2 \tag{138}$$

has integer solutions $(x, y, z) \neq (0, 0, 0)$ if and only if $n = s^2 + t^2$ for some integers s and t.

In this case, the integers solutions (x, y, z) are given by

$$(x, y, z) = (s(u^2 - v^2) - 2uvt, t(u^2 - v^2) + 2uvs, u^2 + v^2),$$

where $u, v \in \mathbb{Z}$, and u, v arbitrary.

Proof. Since $(x, y, z) \neq (0, 0, 0)$ we get $z \neq 0$. Dividing (138) by z^2 and using Proposition 18.16 shows the first part.

The formula for the solutions follows from Theorem 18.18. □

Remark 18.21. *In particular, for $n = 1 = 1^2 + 0^2$, we see that (up to changing the roles of x and y the general integer solution to Pythagoras's equation $x^2 + y^2 = z^2$ is*

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2).$$

For a **primitive** *solution — that is one with $\gcd(x, y) = 1$ — choose u, v with $\gcd(u, v) = 1$ and not both odd. This recovers results from the first lecture and workshop.*

The same method works for $Ax^2 + By^2 + Cz^2 = 0$.

18.5 Sums of three squares, sums of four squares

Proposition 18.22. *Let $a, k \geqslant 0$ be integers. Then no natural number of the form $4^a(8k+7)$, is the sum of three squares of integers.*

[107] Here we see that we can choose u and v to be coprime as discussed in Remark 18.19 above.

Proof. Use induction on a. For $a = 0$: we have $n^2 \equiv 0, 1$ or $4 \bmod 8$, which shows that a sum of three squares of integers is $\equiv 0$ or 1 or 2 or 3 or 4 or 5 or $6 \bmod 8$, but $\not\equiv 7 \bmod 8$.

Assume that the result is 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[108], and so

$$4^{a+1}(8k+7) = n_1^2 + n_2^2 + n_3^2 = 4(n_1'^2 + n_2'^2 + n_3'^2)$$

for some integers n_1', n_2', n_3'. But then

$$4^a(8k+7) = n_1'^2 + n_2'^2 + n_3'^2,$$

contrary to the induction hypothesis. □

It turns out that all the other natural numbers are sums of three squares of integers!

Theorem 18.23 (Legendre 1798, Gauss)**.** *All positive integers except those of the form $4^a(8k+7)$ (for integers $a, k \geqslant 0$) are the sum of three squares of integers.*

Assuming this result, we can show

Corollary 18.24 (Lagrange 1770)**.** *Every positive integer is the sum of four squares of integers.*

Proof. By Theorem 18.23, the only case we need to consider is $n = 4^a(8k+7)$ for $a, k \geqslant 0$. But then

$$n - (2^a)^2 = n - 4^a = 4^a(8k+6) = 2^{2a+1}(4k+3),$$

is exactly divisible by an odd power of 2 so it is not of the form $4^{a'}(8k'+7)$. Therefore, $n - (2^a)^2$ is the sum of three squares of integers and adding the square $(2^a)^2$ shows the claim. □

The Wikipedia article on the Lagrange four-square theorem has much to recommend it.

Main Points from Lecture 18:

- Using formula (128) to write natural numbers as sums of two squares of integers (if it's possible).
- An odd prime p is a sum of two squares iff $p \equiv 1 \bmod 4$
- Theorem of 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.
- Natural numbers as sums of three and four squares of integers.

[108] indeed this follows if we look at this equation mod4 and use that $n^2 \equiv 0 \bmod 4$ for n even and $n^2 \equiv 1 \bmod 4$ for n odd.

The rest of these lecture notes (from previous years) are NOT relevant for the exam and I WON'T edit them. I think there's a lot of interesting stuff in there so have a look if you want to learn some more number theory!:) Also, I might choose to change the topics of Lectures 19 and 20.

19 Lecture 19: Primality testing (27.3.2018)

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 $a = 1, 2, \ldots, n-1$. This is, however, not easy to test; it is certainly no easier than testing whether n is divisible by a for $a = 1, \ldots, n$.

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 9.10: 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 $O(n(\ln_2 n)^2)$. 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 9.11: 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 $2^n \equiv 2 (\bmod n)$ 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*

$$2^{340} = (2^{10})^{34} = 1 (\bmod 11) .$$

Also

$$2^{340} = (2^5)^{68} = 32^{68} = 1 (\bmod 31) .$$

Hence $2^{341} \equiv 2 (\bmod 341)$, 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* k*th Fermat number, where* $k \geq 1$*. Then* F_k *is prime iff* $3^{\frac{F_k - 1}{2}} \equiv -1 \bmod F_k$*.*

Proof. First suppose that $3^{\frac{F_k - 1}{2}} \equiv -1 \bmod F_k$. We apply the theorem with $n = F_k$. So $n - 1 = 2^{2^k}$ and $q = 2$ only, with $a = 3$. Then $3^{\frac{F_k - 1}{2}} \not\equiv 1 \pmod{F_k}$ 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 15.10) and quadratic reciprocity (see Chapter 5) we have

$$3^{\frac{F_k - 1}{2}} \equiv \left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

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*

$$(a + b)^n \equiv a^n + b^n \bmod n \qquad \text{for all } a, b \in \mathbb{Z}$$

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 $O((\ln n)^{6+\varepsilon})$. (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 $S_1, S_2, \ldots, S_n, \ldots$ by $S_1 = 4$ and $S_{n+1} = S_n^2 - 2$ for $n = 1, 2, \ldots$. so we have

$$S_1 = 4, S_2 = 14, S_3 = 194, S_4 = 37634, S_5 = 1416317954, \ldots.$$

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 $31 \mid S_4$,.... In this way get M_p prime for $p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, \ldots$ (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 $n = 1, 2, \ldots$.

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*

$$\omega^{\frac{r+1}{2}} \equiv -1 \bmod r.$$

(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

$$\begin{aligned} \tau^r 2^{\frac{r-1}{2}}\sqrt{2} &= 1 + \sum_{j=1}^{r-1} \binom{r}{j} (\sqrt{3})^j + 3^{\frac{r-1}{2}}\sqrt{3} \\ &\equiv 1 + 3^{\frac{r-1}{2}}\sqrt{3} \bmod r, \end{aligned} \tag{139}$$

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

$$3^{\frac{r-1}{2}} \equiv \left(\frac{3}{r}\right) = \left(\frac{r}{3}\right)(-1)^{\frac{r-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1) \equiv -1 \bmod r,$$

using Euler's Criterion again, and also Quadratic Reciprocity (Th. 5.1). So, from (139), 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. **M_p prime $\Rightarrow$ $M_p \mid S_{p-1}$.** 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

$$\omega^{\frac{M_p+1}{2}} = \omega^{2^{p-1}} \equiv -1 \bmod M_p \tag{140}$$

and, using Lemma 19.12, including $\omega_1^{-1} = \omega$, we have

$$S_{p-1} = \omega^{2^{p-2}} + \omega_1^{2^{p-2}} = \omega_1^{2^{p-2}}\left(\left(\omega_1^{-1}\right)^{2^{p-2}}\omega^{2^{p-2}} + 1\right) = \omega_1^{2^{p-2}}\left(\omega^{2^{p-1}} + 1\right) \equiv 0 \bmod M_p, \tag{141}$$

the last step using (140).

$M_p \mid S_{p-1} \Rightarrow M_p$ 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 $q^2 \le M_p$.

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 (141) 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 $2^p \mid \#G \le q^2 - 1 \le M_p - 1 = 2^p - 2$, 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 Lecture 20: Integer Factorisation (30.3.2018)

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

$$x_{i+s} \equiv x_{j+s} \bmod p \qquad \text{for } s = 1, 2, 3, \ldots. \tag{142}$$

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 $j \quad +$ (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 (142), 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*

$$D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots + \frac{f(p^k)}{p^{ks}} + \ldots\right) = \prod_p D_{f,p}(s), \tag{143}$$

say.

Proof. Expanding the RHS of (143), 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 $\pi(x) \sim \frac{x}{\ln x}$. 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 $\pi(x) \sim \frac{x}{\ln x}$ as $x \to \infty$.*

It turns out to be more convenient to work with

$$\theta(x) = \sum_{\substack{p \leqslant x \\ p \text{ prime}}} \ln p,$$

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*

$$(\ln 2)x + o(x) < \theta(x) < (2 \ln 2)x + o(x),$$

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 $\theta(x) < (2 \ln 2)x + O(\ln^2 x)$.*

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 $\theta(2n) - \theta(n) \leqslant 2n \ln 2$.

Now if $2n \leqslant x < 2n + 2$ (i.e., $n \leqslant x/2 < n + 1$) then $\theta(x/2) = \theta(n)$ and

$$\theta(x) \leq \theta(2n) + \ln(2n+1) \leqslant \theta(2n) + \ln(x+1),$$

so that, for each x,

$$\begin{aligned}\theta(x) - \theta(x/2) &\leqslant \theta(2n) + \ln(x+1) - \theta(n)\\ &\leqslant 2n \ln 2 + \ln(x+1)\\ &\leqslant x \ln 2 + \ln(x+1).\end{aligned}$$

So (standard telescoping argument for $x, x/2, x/2^2, \ldots, x/2^k$ where $x/2^{k-1} \geqslant 2$, $x/2^k < 2$, $\theta(x/2^k) = 0$):

$$\begin{aligned}\theta(x) &= \left(\theta(x) - \theta\left(\frac{x}{2}\right)\right) + \left(\theta\left(\frac{x}{2}\right) - \theta\left(\frac{x}{2^2}\right)\right) + \left(\theta\left(\frac{x}{2^2}\right) - \theta\left(\frac{x}{2^3}\right)\right) + \cdots + \left(\theta\left(\frac{x}{2^{k-1}}\right) - \theta\left(\frac{x}{2^k}\right)\right)\\ &\leqslant \ln 2 \left(x + \frac{x}{2} + \cdots + \frac{x}{2^{k-1}}\right) + k \ln(x+1)\\ &\leqslant 2x \ln 2 + \lfloor \ln_2 x \rfloor \ln(x+1)\\ &\leqslant 2x \ln 2 + O(\ln^2 x).\end{aligned}$$

□

22.2.2 The lower bound

To obtain an inequality in the other direction, we look at

$$d_n = \operatorname{lcm}(1, 2, \ldots, n) = e^{\sum_{p^m \leqslant n} \ln p}.$$

Define

$$\psi(x) = \sum_{\substack{p^m \leqslant x \\ p \text{ prime}}} \ln p;$$

(i.e., $\ln p$ 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 $\psi(x) < \theta(x) + 2x^{1/2} \ln x + O(\ln^2 x)$.*

Proof. Now

$$\begin{aligned}\psi(x) &= \sum_{p \leqslant x} \ln x + \sum_{p^2 \leqslant x} \ln x + \sum_{p^3 \leqslant x} \ln x + \ldots\\ &= \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots + \theta(x^{1/k}),\end{aligned}$$

where k is greatest such that $x^{1/k} \geqslant 2$, i.e., $k = \lfloor \ln_2 x \rfloor$

$$\begin{aligned}&< \theta(x) + \ln_2 x \, \theta(x^{1/2})\\ &< \theta(x) + 2x^{1/2} \ln x + O(\ln^2 x), \qquad \text{using Prop. 22.3.}\end{aligned}$$

□

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* $\theta(x) \geqslant x \ln 2 + O(x^{1/2} \ln x)$.

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

$$\begin{aligned} d_{2n+1} &\geqslant 4^n \\ \psi(2n+1) &\geqslant 2n \ln 2 && \text{on taking logs} \\ \theta(2n+1) &\geqslant 2n \ln 2 - 2\ln(2n+1)\sqrt{2n+1} && \text{by Lemma 22.4} \\ \theta(x) &\geqslant x \ln 2 + O(x^{1/2} \ln x). \end{aligned}$$

□

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* $\ln(1+t) \leqslant t$, *with equality iff* $t = 0$.

For $n \in \mathbb{N}$ *we have* $n \ln(1 + \frac{1}{n}) < 1$.

Proof. The first inequality comes from observing that the tangent $y = t$ to the graph of $y = \ln(1+t)$ 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*

$$n \ln n - n < \ln(n!) \leqslant n \ln n.$$

Proof. Now for $j \geqslant 2$ we have

$$\begin{aligned} \ln j &= j \ln j - (j-1)\ln(j-1) - (j-1)\ln\left(1 + \frac{1}{j-1}\right) \\ &= j \ln j - (j-1)\ln(j-1) - \delta_j, \end{aligned}$$

where $0 < \delta_j < 1$, using Lemma 22.6 for $n = j - 1$. So, on summing for $j = 2, \dots, n$ we get

$$\begin{aligned}\ln(n!) &= \sum_{j=2}^{n} \ln j \\ &= \sum_{j=2}^{n} j \ln j - (j-1)\ln(j-1) - \delta_j \\ &= n \ln n - \sum_{j=2}^{n} \delta_j \\ &= n \ln n - \Delta,\end{aligned}$$

where $0 < \Delta < n$, since $1 \ln 1 = 0$ and all the other $j \ln j$ terms apart from $n \ln n$ telescope. □

Proposition 22.8. *We have*

$$\sum_{n \leqslant x} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma = 0.577\dots$, **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 $n = 1, 2, \dots, N$ 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 $n = 1, 2, \dots, N$ 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 $\int_1^{N+1} \frac{dx}{x} = \ln(N+1)$ (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

$$\sum_{n \leqslant x} \frac{1}{n} = \sum_{n=1}^{N} 1/n = \ln(N+1) + \gamma_n.$$

Since $\ln(N+1) - \ln x = O\left(\frac{1}{x}\right)$ 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* $\mathcal{P}_x > \ln x$.

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

$$\mathcal{P}_x > \sum_{n \leqslant x} \frac{1}{n} > \ln x,$$

by Prop. 22.8. □

Corollary 22.10. *There are infinitely many primes.*

Proposition 22.11. *We have*

$$\sum_{p \leqslant x} \frac{1}{p} > \ln \ln x - 1.$$

Proof. We have

$$\begin{aligned}\ln \mathcal{P}_x &= \sum_{p \leqslant x} \ln \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^k} + \ldots\right) \\ &< \sum_{p \leqslant x} \frac{1}{p} + \sum_{p \leqslant x} \frac{1}{p(p-1)},\end{aligned}$$

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

$$\sum_{p \leqslant x} \frac{1}{p} > \ln \mathcal{P}_x - 1 > \ln \ln x - 1,$$

using Prop. 22.9. □

Proposition 22.12. *We have*

$$\sum_{p \leqslant x} \frac{\ln p}{p} = \ln x + O(1) \qquad \text{as } x \to \infty.$$

Proof. Now from Problem Sheet 1, Q8, we have

$$n! = \prod_{p \leqslant n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots},$$

so that (taking logs)

$$\begin{aligned} \ln(n!) &= \sum_{p \leqslant n} \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \right) \ln p \\ &= \sum_{p \leqslant n} \left\lfloor \frac{n}{p} \right\rfloor \ln p + S_n, \end{aligned}$$

where

$$\begin{aligned} S_n :&= \sum_{p \leqslant n} \left(\left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \right) \ln p \\ &\leq \sum_{p \leqslant n} \left(\frac{n}{p^2} + \frac{n}{p^3} + \dots \right) \ln p \\ &= n \sum_{p \leqslant n} \frac{\ln p}{p(p-1)} \\ &< n \sum_{k=1}^{\infty} \frac{\ln(k+1)}{(k+1)k} \\ &= nc, \end{aligned}$$

for some positive constant c, since the last sum is convergent. Hence $nc > S_n > 0$. Also, for $n = \lfloor x \rfloor$ we have

$$\begin{aligned} n \sum_{p \leqslant x} \frac{\ln p}{p} &\geq \sum_{p \leqslant x} \left\lfloor \frac{n}{p} \right\rfloor \ln p \\ &> \sum_{p \leqslant x} \left(\frac{n}{p} - 1 \right) \ln p \\ &= n \sum_{p \leqslant x} \frac{\ln p}{p} - \theta(x). \end{aligned}$$

Hence

$$n\sum_{p\leqslant x}\frac{\ln p}{p}\geqslant\sum_{p\leqslant x}\left\lfloor\frac{n}{p}\right\rfloor\ln p>n\sum_{p\leqslant x}\frac{\ln p}{p}-O(x),$$

since $\theta(x)=O(x)$, by Theorem 22.2. Now add the inequality $nc>S_n>0$ to the above inequality, to obtain

$$n\sum_{p\leqslant x}\frac{\ln p}{p}+nc>\ln(n!)>n\sum_{p\leqslant x}\frac{\ln p}{p}-O(x).$$

Dividing by n, and using the fact that $\frac{\ln(n!)}{n}=\ln n-O(1)$ from Prop. 22.7, we have

$$\sum_{p\leqslant x}\frac{\ln p}{p}+O\left(1\right)>\ln n-O\left(1\right)>\sum_{p\leqslant x}\frac{\ln p}{p}-O\left(1\right).$$

Hence

$$\sum_{p\leqslant x}\frac{\ln p}{p}=\ln x+O(1).$$

□

22.5 The average size of the divisor function $\tau(n)$

The following result is a way of saying that an integer n has $\ln n+2\gamma-1$ 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*

$$\sum_{n\leqslant x}\tau(n)=x\ln x+(2\gamma-1)x+O\left(\sqrt{x}\right).$$

Proof. Now

$$\begin{aligned}\sum_{n\leqslant x}\tau(n)&=\sum_{n\leqslant x}\sum_{\ell\mid n}1\\&=\sum_{\ell\leqslant x}\sum_{\substack{n=k\ell\\k\leq\frac{x}{\ell}}}1\\&=\sum_{\ell\leqslant x}\left\lfloor\frac{x}{\ell}\right\rfloor,\end{aligned}$$

on recalling that $\lfloor y \rfloor$ is the number of positive integers $\leqslant y$,

$$\begin{aligned}
&= 2 \sum_{\ell \leqslant \sqrt{x}} \left\lfloor \frac{x}{\ell} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 && \text{by Q10, Problem Sheet 1} \\
&= 2 \sum_{\ell \leqslant \sqrt{x}} \frac{x}{\ell} - x + O(\sqrt{x}) \\
&= 2x \left(\ln \sqrt{x} + \gamma + O\left(\frac{1}{\sqrt{x}} \right) \right) - x + O(\sqrt{x}) && \text{using Prop. 22.8} \\
&= x \ln x + (2\gamma - 1)x + O(\sqrt{x}).
\end{aligned}$$

□

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

$$\begin{aligned}
&\text{For each } x \in F && |x| = 0 \text{ iff } x = 0; && \text{(ZERo)} \\
&\text{For each } x, y \in F && |xy| = |x| \cdot |y|; && \text{(HOMomorphism)} \\
&\text{For each } x, y \in F && |x + y| \leqslant |x| + |y|. && \text{(TRIangle)}
\end{aligned}$$

If in addition

$$\text{For each } x, y \in F \qquad |x + y| \leqslant \max(|x|, |y|), \qquad \text{(MAXimum)}$$

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 $\{n \in \mathbb{N} : |n| < 1\} = \{n \in \mathbb{N} : p \text{ divides } n\}$.*

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 $(a_n) = a_1, a_2, \ldots, a_n, \ldots$ 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 $a_1, b_1, a_2, b_2, \ldots, a_n, b_n, \ldots$ 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 $3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots$, which we write as $3.14159\ldots$. 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

$$\begin{aligned} |a + a'|_p \leq \max(|a|_p, |a'|_p) &\qquad \leqslant 1 &\qquad &\text{by MAX ;} \\ |a \cdot a'|_p = |a|_p \cdot |a'|_p &\qquad \leqslant 1 &\qquad &\text{by HOM ,} \end{aligned}$$

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 mod n then you only need to specify a mod 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 $\sqrt{6} = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \dots$.

Next, consider a general p-adic number $a = p^k(a_0 + a_1 p + \dots)$. 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 $b = p^{k/2}(b_0 + b_1 p + \dots) \in \mathbb{Q}_p$ iff a_0 is a quadratic residue mod$p$.

23.8.2 The case of p even

Consider a 2-adic unit $a = 1 + a_1 2 + a_2 2^2 + \dots \in \mathbb{Z}_2$. If $a = b^2$, where $b = b_0 + b_1 2^1 + b_2 2^2 + \dots \in \mathbb{Z}_2$, 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 $a = 2^k(1 + a_1 2 + a_2 2^2 + \dots)$, 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*

$$ax^2 + by^2 + cz^2 = 0 \tag{144}$$

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 (144) 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 (144) 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 $\left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) = 1$ while $\left(\frac{a}{q}\right) = \left(\frac{n}{q}\right) = -1$. 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 $p^k(a_0 + a_1 b + a_2 b^2 + \cdots + a_i b^i + \dots)$, where $k \in \mathbb{Z}$ and all $a_i \in \{0, 1, 2, \dots, b-1\}$. 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 $k = 2, 3, \dots$ to obtain $a_1, a_2, a_3, \dots$ and hence α.]