MAS330 FULL NOTES

Week 1. Euclidean Algorithm, Linear congruences, Chinese Remainder Theorem

Elementary Number Theory studies modular arithmetic (i.e. counting modulo an integer n), primes, integers and equations.

This week we review modular arithmetic and Euclidean algorithm.

1. Introduction

1.1. **What is Number Theory?** Not trying to answer this directly, let us mention some typical questions we will deal with in this course.

Q. What is the last decimal digit of 3^{1000}?
A. The last decimal digit of 3^{1000} is 1. This is a simple computation we'll do using Euler's Theorem in Week 4.

Q. Is there a formula for prime numbers?
A. We don't know if any such formula exists. P. Fermat thought that all numbers of the form $F_n = 2^{2^n} + 1$ are prime, but he was mistaken! We study Fermat primes F_n in Week 6.

Q. Are there any positive integers (x, y, z) satisfying $x^2 + y^2 = z^2$?
A. There are plenty of solutions of $x^2 + y^2 = z^2$, e.g. $(x, y, z) = (3, 4, 5), (5, 12, 13)$. In fact, there are infinitely many of them. Ancient Greeks have written the formula for all the solutions! We'll discover this formula in Week 8.

Q. How about $x^n + y^n = z^n$ for $n \geq 3$?
A. There are no solutions of $x^n + y^n = z^n$ in positive integers! This fact is called Fermat's Last Theorem and we discuss it in Week 8.

Q. Which terms of the Fibonacci sequence $u_n = \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots\}$ are divisible by 3?
A. Every fourth term starting from $u_4 = 3$ is divisible by 3. We study the Fibonacci sequence and its amazing properties in Week 9.

Q. What is a good rational approximation for $\sqrt{2}$?
A. We use continued fractions in Week 10 to show that one good approximation is

$$\sqrt{2} \approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = \frac{41}{29}.$$

1.2. **Where does Number Theory come from and what is it good for?** Number Theory has been originally created by the Ancient Greeks in the quest for pure knowledge and then taken further by P. Fermat in the 17th century with no relation to other branches of science or real world applications whatsoever.

Some of the greatest mathematicians of all time, L. Euler and C. F. Gauss created large parts of Number Theory as we know it today, with strong connections to other branches of mathematics. For example the triumphant 1995 A. Wiles' proof of Fermat's Last Theorem would have been impossible without input from Algebra, Geometry and Analysis!

What about applications of Number Theory? American number-theorist Leonard Dickson once said "Thank God that number theory is unsullied by any application". Nowadays this is not true: Number Theory is used in Computer Science and Cryptography (RSA cryptosystem, elliptic cryptography).

2. Prime factorization

We use the following number systems:

$$\text{Integers: } \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$
$$\text{Positive integers: } \mathbb{N} = \{0, 1, 2, 3, \dots\}$$
$$\text{Prime numbers: } \mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

Theorem 1 (**The Fundamental Theorem of Arithmetic**). *Every nonzero integer number $n \in \mathbb{Z}$ is the unique (up to order) product of primes:*

$$n = \pm \prod_{p \in \mathbb{P}} p^{n_p} \tag{1}$$

where $n_p \in \mathbb{N}$ and $n_p = 0$ for almost all p.

["Almost all" means: for all except finitely many.]

Example 2. $-12 = -2^2 \cdot 3$, $100 = 2^2 \cdot 5^2$.

Divisibility. Let m, n be two integers. Write

$$m = \pm \prod_{p \in \mathbb{P}} p^{m_p}$$
$$n = \pm \prod_{p \in \mathbb{P}} p^{n_p}$$

as their prime factorizations. It is clear that m divides n if and only if all exponents m_p in the prime factorization of m are no larger than those for n:

$$m_p \leq n_p$$

for all $p \in \mathbb{P}$. To express in symbols that m divides n we use the notation:

$$m \mid n.$$

Coprime pairs. We say that m, n are **coprime** if $\gcd(m, n) = 1$, i.e. there is no integer $d > 1$ which is a common divisor of both m and n. Factoring m and n as before we see that m and n are coprime if and only if they have no common prime factors. Sometimes one says **relatively prime**, and this is the same as coprime.

Example 3. *The two consecutive integers n and $n+1$ are coprime, can you prove that? How about n and $n+2$? What could be* $\gcd(n, n+2)$*?*

Some properties of divisibility.

(1) If p is prime and p divides a product $n_1 \cdot \cdots \cdot n_r$, then p divides at least one of the n_i.
(2) If m is divisible by each of the $n_1, \ldots, n_r$ and every pair n_i, n_j, $i \neq j$ is coprime, then m is divisible by the product $n_1 \cdot \cdots \cdot n_r$.

Can you prove these?

Greatest common divisor and least common multiple. Prime factorization is useful in computing the greatest common divisor (gcd) and the least common multiple (lcm):

- $\gcd(m, n) = \prod_{p \in \mathbb{P}} p^{\min(n_p, m_p)}$
- $\operatorname{lcm}(m, n) = \prod_{p \in \mathbb{P}} p^{\max(n_p, m_p)}$

For example:

- $\gcd(12, 100) = \gcd(2^2 \cdot 3, 2^2 \cdot 5^2) = 2^2$
- $\operatorname{lcm}(12, 100) = \gcd(2^2 \cdot 3, 2^2 \cdot 5^2) = 2^2 \cdot 3 \cdot 5^2$

The following theorem about prime numbers and its proof by contradiction are due to Euclid. You most likely have seen before.

Theorem 4 (**Infinitude of prime numbers**). *The set $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$ of prime numbers is infinite.*

Proof. Assume, on the contrary, that $\mathbb{P}$ is finite. Thus $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$. Let

$$N = 1 + p_1 \cdot p_2 \cdot \cdots \cdot p_n.$$

Consider q, a prime divisor of N.

Can we have $q = p_i$ for some i? No. If $q = p_i$, then q divides both N and $p_1 \cdot p_2 \cdot \cdots \cdot p_n$, hence it also divides

$$1 = N - p_1 \cdot p_2 \cdot \cdots \cdot p_n.$$

Thus q is a prime and q is NOT in the list $p_1, p_2, \ldots, p_n$. We get a contradiction and the proof is finished. □

3. Euclidean algorithm and Linear congruences

Example 5. *Given two buckets: a 3 liter one and a 5 liter one, is it possible to measure exactly one liter of water? Sure.* $1 = 2 \times 3 - 1 \times 5$. *Another solution is* $1 = 2 \times 5 - 3 \times 3$. *Solutions exist because 3 and 5 are coprime:* $\gcd(3, 5) = 1$.

Theorem 6 (**Representation of** *gcd*). *Given positive integers m, n it is always possible to express $gcd(m, n)$ as an integer linear combination*

$$gcd(m, n) = m \cdot x + n \cdot y$$

for some $x, y \in \mathbb{Z}$.

Proof of the Theorem "Representation of gcd". The proof is called Euclidean algorithm: at each step we replace our pair $m > n \geq 0$ by a smaller pair $n > r \geq 0$, with the same gcd. This process is an instance of Infinite Descent, which will show up again later in the module when we solve other types of equations.

Let us assume that $m > n > 0$; we perform division with remainder:

$$m = kn + r,\ 0 \leq r < n$$

and notice that

$$d = \gcd(m, n) = \gcd(kn + r, n) = \gcd(r, n).$$

The last equality holds because any common of the pair (r, n) is also a common divisor of the pair $(kn + r, n)$ and conversely any common divisor of the pair $(kn + r, n)$ is a common divisor of the pair (r, n).

Now if we can write d as a combination of r and n then we also can write d as a combination of m and n because $r = m - kn$:

$$d = r \cdot x + n \cdot y = (m - kn)x + ny = (m + n)x + ny.$$

This infinite descent process will terminate as soon as we reach a pair $(d, 0)$ in which case the combination is simply $d = 1 \cdot d + 0 \cdot 0$. □

Example 7. *Find x and y such that $\gcd(86, 20) = 86x + 20y$. We take the larger number, 86 and find the remainder when divided by 20, and then repeat the process:*

$$\begin{aligned} 86 &= 4 \cdot \underline{20} + \underline{6} \\ 20 &= 3 \cdot \underline{6} + \underline{2} \\ 6 &= 3 \cdot \underline{2}. \end{aligned}$$

Thus we deduce that $\gcd(86, 20) = 2$. To find its representation we apply the above steps backwards:

$$\begin{aligned} 2 &= \underline{20} - 3 \cdot \underline{6} = \\ &= \underline{20} - 3 \cdot (\underline{86} - 4 \cdot \underline{20}) = \\ &= -3 \cdot \underline{86} + 13 \cdot \underline{20}. \end{aligned}$$

Underlying the numbers as I do helps distinguishing them from coefficients.

Example 8. *Find x and y such that $\gcd(86, 19) = 86x + 19y$. We compute:*

$$\begin{aligned} 86 &= 4 \cdot \underline{19} + \underline{10} \\ 19 &= 1 \cdot \underline{10} + \underline{9} \\ 10 &= 1 \cdot \underline{9} + 1. \end{aligned}$$

Thus 86 and 19 are coprime. To find the representation we compute:

$$\begin{aligned} 1 &= \underline{10} - \underline{9} = \underline{10} - (\underline{19} - \underline{10}) = \\ &= 2 \cdot \underline{10} - \underline{19} = 2 \cdot (\underline{86} - 4 \cdot \underline{19}) - \underline{19} = \\ &= 2 \cdot \underline{86} - 9 \cdot \underline{19}. \end{aligned}$$

Understanding Euclidean algorithm will be important for the rest of this course.

Definition 9. *Let $a, b, n \in \mathbb{Z}$. We write*

$$a \equiv b \pmod{n}$$

and say that a is **congruent** *to b modulo n if*

$$n \mid a - b$$

i.e. n divides $a - b$. We call n the **modulus** *of the congruence.*

Example 10. *We have:* $12 \equiv 5 \pmod 7$ *and* $5 \equiv -2 \pmod 7$.

Properties of congruences are easily established:

Lemma 11. *Let* $a, b, c, d, n \in \mathbb{Z}$. *Then:*

(1) *reflective:* $a \equiv a \pmod n$
(2) *symmetric:* $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$
(3) *transitive:* $a \equiv b \pmod n$, $b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$
(4) $a \equiv b \pmod n$, $c \equiv d \pmod n \Rightarrow \begin{cases} a + c \equiv b + d \pmod n, \\ a - c \equiv b - d \pmod n, \\ ac \equiv bd \pmod n \end{cases}$
(5) $a \equiv b \pmod n$, $c \in \mathbb{N} \Rightarrow ca \equiv cb \pmod{cn} \Rightarrow ca \equiv cb \pmod n$
(6) $ca \equiv cb \pmod{cn}$ *and* $c > 0 \Rightarrow a \equiv b \pmod n$
(7) $ca \equiv cb \pmod n$ *and* $\gcd(c, n) = 1 \Rightarrow a \equiv b \pmod n$

Parts (i)-(iii) of the Lemma tell us that $\equiv$ is an equivalence relation on the set of integers $\mathbb{Z}$. The set of equivalence classes of integers under congruence modulo n is denoted by $\mathbb{Z}_n$. This set consists of classes

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Arithmetic operations can be performed in $\mathbb{Z}_n$: for instance in $\mathbb{Z}_5$ we have $\overline{2} + \overline{4} = \overline{1}$, $-\overline{3} = \overline{2}$ and so on. We will often be interested in existence of multiplicative inverses in $\mathbb{Z}_n$. For instance in $\mathbb{Z}_7$ we have $\overline{2} \cdot \overline{4} = \overline{1}$, hence we may write this fact as $\overline{2}^{-1} = \overline{4}$. In general finding inverse elements will have to do with solving linear congruences which are in turn solved using Euclid's algorithm.

A **linear congruence** is an equation

$$ax \equiv b \pmod n$$

where $a, b, n \in \mathbb{Z}$ and $n > 1$ are given and $x \in \mathbb{Z}$. Equivalently we may think of a linear congruence as an equation

$$\overline{a}x = \overline{b} \in \mathbb{Z}_n$$

where $\overline{a}, \overline{b} \in \mathbb{Z}_n$ and $x \in \mathbb{Z}_n$.

As already mentioned above we use Euclidean algorithm to solve linear congruences.

Example 12. *We explain how to find a solution of the linear congruence* $19x \equiv 1 \pmod{86}$.

Our congruence is equivalent to the equation

$$19x = 1 + 86y$$

or

$$19x - 86y = 1,$$

i.e. we are trying to represent 1 *as a linear combination of* 19 *and* 86. *This is done using Euclidean algorithm. As we found in Example 8:*

$$1 = 2 \cdot 86 - 9 \cdot 19,$$

so that $x = -9$ *is a solution. Of course, adding/subtracting from* x *multiples of* 86 *still gives a solution. For a complete solution we get:*

$$x \equiv -9 \pmod{86}.$$

Example 13. *Let us now find a solution of the linear congruence* $19x \equiv 3 \pmod{86}$.

As we found in Example 12, $x_0 = -9$ *is a solution of*

$$19x_0 \equiv 1 \pmod{86}.$$

Multiplying both sides by 3 *we get*

$$19(3x_0) \equiv 3 \pmod{86}.$$

Now $x = 3 \cdot (-9) = -27$ *is a solution of*

$$19x \equiv 3 \pmod{86}.$$

Furthermore, the complete solution is

$$x \equiv -27 \pmod{86}.$$

Theorem 14 (On linear congruences with coprime a and n). *If* $\gcd(a, n) = 1$*, then the linear congruence*

$$ax \equiv b \pmod{n}$$

always has a solution. Furthermore, if x_0 *is a solution, then all the solutions are given by*

$$x \equiv x_0 \pmod{n}$$

Proof. We first solve the congruence $ax \equiv 1 \pmod{n}$, the solution exists by Theorem about representation of gcd since $\gcd(a, n) = 1$. Now multiplying both sides of the congruence above by b we get

$$a(bx) \equiv b \pmod{n},$$

thus solutions to the congruence $ax \equiv b \pmod{n}$ also exist.

If x_0 and x are both solutions of $ax \equiv b \pmod{n}$, then

$$ax - ax_0 \equiv n - n = 0 \pmod{n},$$

so that n divides $a(x - x_0)$. However since $\gcd(a, n) = 1$, n divides $x - x_0$ so that $x \equiv x_0 \pmod{n}$. □

If $\gcd(a, n) > 1$, the situation is more complicated. One thing that may happen is that the linear congruence has no solutions:

Example 15. *Solve* $20x \equiv 1 \pmod{86}$. *Here* $\gcd(a, n) = \gcd(20, 86) = 2$. *The corresponding equation is*

$$20x - 1 = 86y.$$

There are no solutions: the LHS is odd, and the RHS is even.

Theorem 16 (On linear congruences). *The linear congruence*

$$ax \equiv b \pmod{n}$$

has a solution if and only if $\gcd(a, n) \mid b$*. Furthermore if* x_0 *is a solution, then all other solutions are given by*

$$x \equiv x_0 \left(\bmod \frac{n}{\gcd(a, n)} \right).$$

Proof. Throughout the proof we use that the congruence $ax \equiv b \pmod{n}$ is equivalent to the equation in $ax + ny = b$ in two variables $x, y \in \mathbb{Z}$.

If $\gcd(a,n) \mid b$, then $ax \equiv b \pmod{n}$ can be seen to be equivalent to $\frac{a}{\gcd(a,n)}x \equiv \frac{b}{\gcd(a,n)} \left(\mathrm{mod}\ \frac{n}{\gcd(a,n)}\right)$ and the claim about existence and characterization of of solutions follows from Theorem 14 since this time the terms $\frac{a}{\gcd(a,n)}$ and $\frac{n}{\gcd(a,n)}$ are coprime.

Now conversely, if $ax \equiv b \pmod{n}$ has a solution then every common divisor of a and n is also a divisor of b. Therefore we must have $\gcd(a,n) \mid b$. □

Example 17. *We solve* $20x \equiv 2 \pmod{86}$. *The corresponding equation is*

$$20x - 2 = 86y$$

or

$$20x - 86y = 2.$$

We apply Euclidean algorithm to find $\gcd(20, 86)$ *and the linear representation. In fact, this already has been done in Example 7:* $\gcd(86, 20) = 2$ *and*

$$2 = -3 \cdot 86 + 13 \cdot 20.$$

Thus $x = 13$ *is a solution. To find all solutions we apply Theorem 16. Here* $n = 86, a = 20, \gcd(86, 20) = 2$*, so all solutions are given by*

$$x \equiv 13 \pmod{43}.$$

Corollary 18. *An element* $\overline{a} \in \mathbb{Z}_n$ *has a multiplicative inverse if and only if* $\gcd(a, n) = 1$.

Proof. By definition a multiplicative inverse to $\overline{a} \in \mathbb{Z}_n$ is an element $\overline{x} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{x} = \overline{1} \in \mathbb{Z}_n$; in other words we require

$$ax \equiv 1 \pmod{n},\ x \in \mathbb{Z}.$$

By the Theorem above a solution to this congruence exists if and only if $\gcd(a, n) \mid 1$ which is of course equivalent to $\gcd(a, n) = 1$. □

4. Chinese Remainder Theorem

In the third century AD, the Chinese mathematician Sun-Tsu asked the following question:

- Can a number be found which leaves remainders $2, 3, 2$ when divided by $3, 5, 7$ respectively? In other words, do the congruences

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

  have a simultaneous solution?

Theorem 19 (Chinese Remainder Theorem). *Let* $n_1, \ldots, n_r$ *be integers* > 1 *such that* $\gcd(n_i, n_j) = 1$ *for* $i \neq j$.

Then the congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \cdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

have a simultaneous solution.

Furthermore, if x_0 is a simultaneous solution, then the complete solution is

$$x \equiv x_0 \pmod{n_1 n_2 \dots n_r}.$$

Remark 20. *We can put Chinese Remainder Theorem in a concise form by saying that for any factorization $N = n_1 \cdots n_r$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$, the map*

$$\begin{aligned} \mathbb{Z}_N &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \\ \overline{a} &\mapsto (\overline{a} \pmod{n_1}, \dots, \overline{a} \pmod{n_r}) \end{aligned}$$

is a bijection. Indeed the existence part of the Chinese Remainder Theorem is equivalent to surjectivity of this map, whereas the uniqueness part is equivalent to injectivity.

The proof below is constructive: it explains the algorithm of finding a solution.

Proof of the CRT. We introduce complementary products

$$N_i = \prod_{j \neq i} n_j.$$

This means that

$$\begin{aligned} N_1 &= n_2 \cdot n_3 \cdot n_4 \cdot \dots \\ N_2 &= n_1 \cdot n_3 \cdot n_4 \cdot \dots \\ N_3 &= n_1 \cdot n_2 \cdot n_4 \cdot \dots \end{aligned}$$

and so on.

I claim that for each i, n_i and N_i are coprime. Indeed, if p was a prime factor of N_i, it has to divide one of the factors in the product $N_i = \prod_{j \neq i} n_j$:

$$p \mid n_j$$

for some $j \neq i$. Since $\gcd(n_i, n_j) = 1$ is required in the Theorem, p can not divide n_i.

Thus n_i and N_i are coprime, and using Theorem 6 we can represent their gcd as

$$1 = s_i N_i + t_i n_i$$

for every i. Taking this modulo n_i we obtain

$$s_i N_i \equiv 1 \pmod{n_i} \tag{2}$$

Now I claim that

$$x_0 = s_1 N_1 a_1 + s_2 N_2 a_2 + \cdots + s_r N_r a_r$$

is a solution of our system of congruences. To see this take $x_0 \pmod{n_i}$ for every i:

$$\begin{aligned} x_0 &= s_1 N_1 a_1 + s_2 N_2 a_2 + \cdots + s_r N_r a_r \equiv \\ &\equiv s_i N_i a_i \pmod{n_i} \quad [\text{since all } N_j \text{ are divisible by } n_i \text{ for } i \neq j] \\ &\equiv a_i \pmod{n_i} \quad [\text{using (2)}] \end{aligned}$$

Thus x_0 satisfies every congruence in the system.

To find all the solutions we use the same argument as for linear systems of equations. Let x be an arbitrary solution of our system of congruences. This means that

$$x \equiv a_i \pmod{n_i}$$

for every i. Since our solution x_0 satisfies the same system of congruences, we have

$$x - x_0 \equiv 0 \pmod{n_i},$$

so that $x - x_0$ is divisible by every n_i. Since the n_i are coprime with each other, it follows that $x - x_0$ is divisible by their product $N = n_1 \cdot n_2 \dots n_r$:

$$x \equiv x_0 \pmod{n_1 \cdot n_2 \dots n_r}$$

and this is what we had to prove: every other solution is congruent to our solution x_0. □

Example 21. *We solve the system of congruences*

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

using the method given in the proof above.

Three numbers

$$n_1 = 3, n_2 = 5, n_3 = 7$$

are coprime, so we may use the Chinese Remainder Theorem. We have

$$N_1 = n_2 \cdot n_3 = 35,$$
$$N_2 = n_1 \cdot n_3 = 21,$$
$$N_3 = n_1 \cdot n_2 = 15.$$

We need to find $s_i, t_i \in \mathbb{Z}$ such that

$$s_i N_i + t_i n_i = 1$$

for $i = 1, 2, 3$. Generally this is done using Euclidean algorithm, but in this case it is easy guesswork:

$$-1 \cdot 35 + 12 \cdot 3 = 1 \implies s_1 = -1$$
$$1 \cdot 21 - 4 \cdot 5 = 1 \implies s_2 = 1$$
$$1 \cdot 15 - 2 \cdot 7 = 1 \implies s_3 = 1.$$

We obtain one solution as

$$x_0 = -1 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 2 = 23.$$

All solutions are congruent to this one modulo $N = 3 \cdot 5 \cdot 7 = 105$. The answer is:

$$x \equiv 23 \pmod{105}.$$

(Check that 23 satisfies the original system of congruences!)

Week 2. Fermat's Little Theorem RSA cryptosystem

The subject of number theory was created by Pierre Fermat (1601 - 1665) a French lawyer who studied mathematics in his free time. The profound influence of Fermat on development of mathematics is clear from the quote "I had a hint of this method from Fermat's way of drawing tangents, and by applying it to abstract equations, directly and invertedly, I made it general" by Isaac Newton, about the invention of Differential Calculus.

5. Fermat's Little Theorem

We begin with explaining an efficient way of computing powers in modular arithmetic. Let's say we'd like to compute

$$5^9 \pmod{14}$$

without relying on a calculator and by using as little multiplications as possible. Instead of multiplying 5 with itself 9 times we start by computing consecutive squares:

$$\begin{aligned} 5^2 &= 25 \equiv 11 \pmod{14} \\ 5^4 &= (5^2)^2 \equiv 11^2 = 121 = (140 - 19) \equiv -19 \equiv 9 \pmod{14} \\ 5^8 &= (5^4)^2 \equiv 9^2 = 81 \equiv 11 \pmod{14}. \end{aligned}$$

Now we notice that

$$5^9 = 5^{8+1} = 5^8 \cdot 5^1 \equiv 11 \cdot 5 = 55 \equiv -1 \pmod{14}.$$

Thus we have finished the computation using only four multiplication operations!

There are other power taking tricks. For example we can factor the exponent and do

$$5^9 = (5^3)^3 \equiv 125^3 \equiv (-1)^3 = -1 \pmod{14}.$$

Fermat's Little Theorem (for a prime modulus) and Euler's Theorem (for an arbitrary modulus, Week 4) will further simplify power computations.

Example 22. *We compute* $a^6 \pmod 7$ *for* $a = 1, 2, 3, 4, 5, 6, 7$. *We have*

$$\begin{aligned} 1^6 &= 1 \\ 2^6 &= (2^3)^2 = 8^2 \equiv 1^2 = 1 \pmod 7 \\ 3^6 &= (3^3)^2 = 27^2 \equiv 6^2 = 36 \equiv 1 \pmod 7 \\ 4^6 &\equiv (-3)^6 \equiv 3^6 \equiv 1 \pmod 7 \\ 5^6 &\equiv (-2)^6 \equiv 2^6 \equiv 1 \pmod 7 \\ 6^6 &\equiv (-1)^6 = 1 \pmod 7 \\ 7^6 &\equiv 0^6 = 0 \pmod 7. \end{aligned}$$

Obviously this pattern repeats and we notice that for any integer a *not divisible by* 7 *we have*

$$a^6 \equiv 1 \pmod 7.$$

This is an instance of Fermat's little theorem.

Theorem 23 (**Fermat's little theorem**). *Let* p *be a prime and* a *an integer. Then*

(1) $a^p \equiv a \pmod p$
(2) *If* p *does not divide* a, *then* $a^{p-1} \equiv 1 \pmod p$

We'll abbreviate Fermat's Little Theorem as FLT. Before we prove the FLT, notice that parts (1) and (2) of it are equivalent to each other. To see this, let a be an integer not divisible by p. If we assume part (2), i.e. that

$$a^{p-1} \equiv 1 \pmod p,$$

then multiplying both sides by a we obtain

$$a^p = a^{p-1} \cdot a \equiv 1 \cdot a = a \pmod p$$

and part (1) follows. Similarly, if we assume part (1):

$$a^p \equiv a \pmod{p},$$

then dividing both sides by a (this is allowed since a and p are coprime, check this!) implies that

$$a^{p-1} \equiv 1 \pmod{p}.$$

Finally, when p divides a, part (1) is obviously true as both sides are $0 \pmod{p}$.

To prove the FLT we will need two Lemmas:

Lemma 24 (**Modular binomial coefficients**). *If p is prime and k an integer $0 < k < p$, then*

$$\binom{p}{k} \equiv 0 \pmod{p}$$

Example 25. *We compute $\binom{7}{1}, \binom{7}{2}, \binom{7}{3} \pmod 7$ to see that Lemma makes sense:*

$$\begin{aligned}\binom{7}{1} &= 7 \equiv 0 \pmod 7\\ \binom{7}{2} &= \frac{7\cdot 6}{2} = 21 \equiv 0 \pmod 7\\ \binom{7}{3} &= \frac{7\cdot 6\cdot 5}{6} = 35 \equiv 0 \pmod 7.\end{aligned}$$

Proof of the Modular binomial coefficients Lemma. We use the definition of the binomial coefficient:

$$\binom{p}{k} = \frac{p\cdot(p-1)\cdot\cdots\cdot(p-k+1)}{k!}$$

Since $p > k$, p does not appear in the prime factorization of $k!$ so that p divides the numerator of the fraction, but not the denominator. Thus p divides the fraction itself:

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

□

Lemma 26 (**Modular binomial theorem**). *For any $a, b \in \mathbb{Z}$ we have*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Proof. We use the Binomial Theorem

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

and notice that by the Modular binomial coefficients Lemma all terms in the sum above are zero modulo p except for the two end terms. We obtain

$$(a+b)^p \equiv a^p + b^p$$

as stated. □

First proof of the FLT. As explained above part (2) would follow from part (1). We prove part (1) by induction. The base of induction is $a = 0$. Then both sides of (1) are zero, and the statement is true. For the induction step $a \mapsto a + 1$ we compute using Modular binomial theorem above:

$$(a + 1)^p \equiv a^p + 1^p = a^p + 1,$$

and now use the induction hypothesis:

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

The induction step is finished, and part (1) is proved. □

We now give a different proof of the FLT:

Second proof of the FLT. Let us prove that if p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

Consider the first $p - 1$ positive multiples of a:

$$a, 2a, 3a, \ldots, (p - 1)a \tag{3}$$

Let us show that none of the numbers (3) is congruent modulo p to any other, nor is any congruent to zero. Let ka, la be two numbers of the sequence (3). Then

$$ka \equiv la \pmod{p} \implies k \equiv l \pmod{p}$$

since $\gcd(a, p) = 1$. Since both $1 \leq k, l \leq p - 1$, we must have $k = l$.

Similarly

$$ka \equiv 0 \pmod{p} \implies k \equiv 0 \pmod{p}$$

which is not possible at all.

We deduce that the above set of integers (3) must be congruent modulo p to

$$1, 2, 3, \ldots, p - 1$$

taken in some order. Thus since all non-zero remainders are present in (3) we get

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p - 1) \pmod{p}.$$

We rewrite the last congruence as

$$a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}.$$

Now since $\gcd((p - 1)!, p) = 1$, we can cancel out $(p - 1)!$ on both sides to obtain

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Example 27. *We calculate* $2641^{4828} \pmod{13}$. *We do long division to find the remainder of* 2641 *modulo* 13*:*

$$2641 \equiv 2 \pmod{13}.$$

Thus

$$2641^{4828} \equiv 2^{4828} \pmod{13}.$$

Next thing we do is reduce 4828 *modulo* $p - 1 = 12$ *(long division again):*

$$4828 = 402 \cdot 12 + 4.$$

By the FLT we have $2^{12} \equiv 1 \pmod{13}$ *and we compute:*

$$2641^{4828} \equiv 2^{4828} = 2^{402 \cdot 12 + 4} = (2^{12})^{402} \cdot 2^4 \equiv 16 \equiv 3 \pmod{13}.$$

Example 28. *We calculate the last decimal digit of* 3^{100}*, i.e.* $3^{100} \pmod{10}$ *Warning:* 10 *is not a prime, and the FLT is not applicable directly! We use prime factorization* $10 = 2 \cdot 5$*, and compute* 3^{100} *modulo* 2 *and modulo* 5 *independently, and then put the results together using the Chinese Remainder Theorem. We have*

$$3^{100} \equiv 1^{100} = 1 \pmod{2}$$

and using the FLT $3^4 \equiv 1 \pmod{5}$*:*

$$3^{100} \equiv 3^{25 \cdot 4} = (3^4)^{25} \equiv 1 \pmod{5}.$$

Both remainders are the same, thus from the uniqueness claim of the Chinese remainder theorem the answer is

$$3^{100} \equiv 1 \pmod{10}.$$

6. RSA cryptosystem

Most of the Internet and banking security today is based on the RSA cryptosystem introduced by young MIT researchers Ron Rivest, Adi Shamir and Leonard Adleman in 1977. The RSA cryptosystem is an example of an open key system: an open (public) key is used to encrypt messages and a closed (private) key is used to decrypt messages.

The basic idea of the RSA is that a message is represented by a sequence of numbers

$$0 \leq a < n,$$

and encryption process consists in taking powers:

$$a \mapsto a^e \pmod{n}.$$

We call the two participants in message exchange Alice and Bob. Alice creates the key, Bob sends messages to Alice using the public key, and finally Alice deciphers Bobs messages using the private key.

Alice creates her keys

- Alice chooses large primes p,q, $n = pq$ and chooses an integer e

$$1 \leq e \leq (p-1)(q-1), \quad \gcd(e, (p-1)(q-1)) = 1$$

- Public key: (n, e)
- Alice solves the congruence

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

[She uses Euclidean algorithm to solve the congruence.]

- Private key: (p, q, d)

Bob sends message to Alice using her public key (n, e)

- Message: $0 \leq a < n$
- Encryption: $b = a^e \pmod{n}$.

Alice decrypts Bob's message b **using the private key** (p, q, d)

Alice received the encrypted message $b = a^e$. She needs to solve for a.

Lemma 29 (RSA). *Let* $n = pq$*,* $de \equiv 1 \pmod{(p-1)(q-1)}$ *as before. If* $b \equiv a^e \pmod{n}$*, then*

$$a \equiv b^d \pmod{n}.$$

Alice received $b = a^e$, she computes the message a with the RSA Lemma:

$$a \equiv b^d \pmod{n}.$$

Proof of the RSA Lemma. We need to show that $a \equiv b^d \pmod{n}$. Since $n = pq$ and p,q are coprime it suffices to check that

$$\begin{aligned} a &\equiv b^d \pmod{p} \\ a &\equiv b^d \pmod{q}. \end{aligned} \tag{4}$$

We compute

$$b^d = (a^d)^e = a^{de}.$$

To compute modulo p we take the exponent modulo $p-1$ (by the FLT), and notice that $de \equiv 1 \pmod{p-1}$. Thus

$$b^d = a^{de} \equiv a^1 = a \pmod{p}.$$

Thus we checked the first congruence in (4), the second one is analogous. □

Example 30. *Alice's public key* $(n = 33, e = 13)$. *Bob's message:* $a = 2 \pmod{33}$. *The encrypted message is*

$$b = 2^{13} \pmod{33}.$$

In order to compute the numerical value of b. *Note that* 33 *is not a prime, and FLT is not directly applicable. Instead we factor* $33 = 3 \times 11$, *and compute* $b = 2^{13}$ *modulo both of these primes using FLT, and then put the results together using Chinese Remainder Theorem just like in Example 28.*

We have

$$b = 2^{13} \equiv (-1)^{13} = -1 \pmod{3}$$

and

$$b = 2^{13} \equiv 2^{10+3} \equiv 2^3 \equiv 8 \pmod{11}.$$

Since $8 \equiv -1 \pmod{3}$ *the Chinese Remainder Theorem gives the answer for the encrypted message:*

$$b \equiv 8 \pmod{33}.$$

Example 31. *Let's demonstrate how Alice would decipher the message* $b = 8$ *she receives in the previous Example. We first figure out Alice's private key. We have*

$$n = 33 = 3 \times 11 \implies p = 3, q = 11$$

and we find d *satisfying*

$$13d \equiv 1 \pmod{20}.$$

using Euclidean algorithm:

$$\begin{aligned} 20 &= 13 + 7 \\ 13 &= 7 + 6 \\ 7 &= 6 + 1 \end{aligned}$$

so that

$$1 = 7 - 6 = 7 - (13 - 7) = -13 + 2 \cdot 7 = -13 + 2 \cdot (20 - 13) = 2 \cdot 20 - 3 \cdot 13.$$

Thus

$$d = -3 \equiv 17 \pmod{20}.$$

By the RSA Lemma Alice has to compute

$$a = b^d = 8^{17} \pmod{33}.$$

As before we do computations for $p = 3$, $p = 11$ independently:

$$a = 8^{17} \equiv (-1)^{17} = -1 \pmod{3}$$

and

$$a = 8^{17} \equiv 8^7 \equiv 8^4 \cdot 8^2 \cdot 8 \equiv 4 \cdot (-2) \cdot 8 = -64 \equiv 2 \pmod{11}.$$

Normally we'd use the algorithm from the Chinese Remainder Theorem here, but here we find the answer directly:

$$a \equiv 2 \pmod{33}.$$

6.1. **RSA cryptosystem: Security.** Roughly speaking the RSA cryptosystem is secure because computing roots in modular arithmetic is hard!

In practice large primes p, q have several hundred digits. If Chuck (a third participant of malicious intent) wants to find $a \pmod n$ from $a^e \pmod n$, he can try **all** values of a one after another. This will take more than 10^{100} years of computer time to decipher a message!

In fact security of the RSA has to do with the Integer Factorization Problem. If Chuck can recover the factorization $n = pq$, then he also can find d and decipher Bob's messages the same way as Alice does.

Is there a fast algorithm to factor large integers? The estimate for existing factorization algorithms: it will take thousands of years of computer time to factor integers with several hundred digits.

Note that the keys have to be chosen carefully. See Problem Sheet 2 for examples of weak RSA keys.

Week 3. Arithmetic functions σ, τ, μ, ϕ Möbius Inversion Formula

This week we do arithmetic and multiplicative functions. These functions provide a convenient language for studying divisibility and divisors of integers.

Two of these functions, ϕ and σ will appear again later in this course. The Euler ϕ-function will play a central role in Week 4 when introducing Euler's theorem and primitive roots.

The σ-function will show up again in Week 6 when studying perfect numbers.

7. Arithmetic functions and multiplicativity

Definition 32. *An* **arithmetic function** *is a function f with domain of definition $\mathbb{N} = \{1, 2, 3, \dots\}$.*

Definition 33. *Let $n > 0$ be an integer. Then:*

- $\tau(n) =$ *(number of divisors of n)* $= \sum_{d|n} 1$
- $\sigma(n) =$ *(sum of divisors of n)* $= \sum_{d|n} d$

Throughout this week by a divisor $d \mid n$ we always mean a positive divisor d of a positive integer n.

Example 34. *Divisors of 15 are $1, 3, 5, 15$. Thus*

$$\begin{aligned} \tau(15) &= 4, \\ \sigma(15) &= 1 + 3 + 5 + 15 = 24. \end{aligned} \tag{5}$$

Example 35. *If n, is a prime power*

$$n = p^k,$$

then it is very easy to compute $\tau(n)$, $\sigma(n)$. Indeed, divisors of n are

$$1, p, p^2, \ldots, p^k,$$

so that

$$\tau(p^k) = k + 1$$

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

(geometric series).

Example 36. *If we compute the number of divisors or the sum of divisors of $n = 15$, we notice the following:*

$$\tau(15) = 4 = 2 \cdot 2 = \tau(3)\tau(5)$$
$$\sigma(15) = 24 = 4 \cdot 6 = \sigma(3)\sigma(5).$$

On the other, hand for $n = 25$, this works differently:

$$\tau(25) = 3 \neq 2 \cdot 2 = \tau(5)\tau(5)$$
$$\sigma(25) = 31 \neq 6 \cdot 6 = \sigma(5)\sigma(5).$$

Definition 37. *An arithmetic function f is called* **multiplicative** *if*

$$f(mn) = f(m)f(n)$$

for all $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$.

Lemma 38. *If f is multiplicative, then to compute $f(n)$ one may use prime factorization:*

$$n = p_1^{k_1} \cdots p_r^{k_r} \implies f(n) = f(p_1^{k_1}) \cdots f(p_r^{k_r}).$$

Proof. This is essentially obvious. One may give an easy proof by induction on r. □

Theorem 39. *1. The functions τ and σ are multiplicative.*
2. In particular, if $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$\tau(n) = (k_1 + 1) \cdots (k_r + 1)$$
$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Proof. We first prove part (2) of the Theorem. If

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

what are divisors of n? These are

$$d = p_1^{a_1} \cdots p_r^{a_r}$$

with $0 \leq a_j \leq k_j$ for all j. We immediately see that the total number of all divisors, i.e. the number of choices for the a_j's is

$$\tau(n) = (k_1 + 1) \cdots (k_r + 1).$$

In order to figure out the value of $\sigma(n)$ we compute

$$\sigma(n) = \sum_{a_1, \ldots, a_r} p_1^{a_1} \cdots p_r^{a_r}$$

where the sum goes over all $0 \leq a_j \leq k_j$. The associativity of multiplication tells us that

$$\sigma(n) = \sum_{a_1,\ldots,a_r} p_1^{a_1} \cdots p_r^{a_r} = \Big(\sum_{a_1=0}^{k_1} p_1^{a_1}\Big) \cdots \Big(\sum_{a_r=0}^{k_r} p_r^{a_r}\Big).$$

Finally we use the geometric sequence formula $1 + p + p^2 + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$ and deduce that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

To prove part (1) of the Theorem we need to check that τ and σ are multiplicative. Let m, n be coprime integers; write their prime factorizations

$$n = p_1^{k_1} \cdots p_r^{k_r}$$
$$m = q_1^{l_1} \cdots q_s^{l_s}.$$

Since we assume m, n to be coprime, all the primes q_i are different for the p_j's. We use prime decomposition for mn:

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$$
$$\tau(mn) = (k_1 + 1) \cdots (k_r + 1) \cdot (l_1 + 1) \cdots (l_s + 1).$$

Finally we compare $\tau(mn)$ with $\tau(m)\tau(n)$:

$$\tau(n) = (k_1 + 1) \cdots (k_r + 1)$$
$$\tau(m) = (l_1 + 1) \cdots (l_s + 1)$$
$$\tau(m)\tau(n) = (k_1 + 1) \cdots (k_r + 1) \cdot (l_1 + 1) \cdots (l_s + 1)$$

Since $\tau(mn) = \tau(m)\tau(n)$ we see that τ is multiplicative. The argument for σ is completely analogous.

□

Example 40. *Theorem 97 allows for an efficient computation of $\tau(n)$, $\sigma(n)$. For example, let $n = 180$. Then we factor n as*

$$n = 180 = 18 \cdot 10 = 2 \cdot 9 \cdot 2 \cdot 5 = 2^2 \cdot 3^2 \cdot 5.$$

Thus we compute

$$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18$$
$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 13 \cdot 6 = 546.$$

Alternatively, we can factor 180 as a product of two (or more) relatively prime factors, e.g.

$$180 = 9 \cdot 20,$$

and use multiplicativity of τ and σ. Divisors of 9 are $1, 3, 9$ and divisors of 20 are $1, 2, 4, 5, 10, 20$. Thus

$$\tau(9) = 3, \tau(20) = 6 \implies \tau(180) = 3 \cdot 6 = 18$$
$$\sigma(9) = 13, \sigma(20) = 42 \implies \sigma(180) = 13 \cdot 42 = 546.$$

8. Summation over all divisors

Theorem 41 (**Multiplicativity Theorem**). *If f is a multiplicative function, then*

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

is a multiplicative function.

Proof. Let m and n be coprime. We compute

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \quad \text{[by definition of } F\text{]} \\ &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \quad \text{[by Lemma below]} \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \quad \text{[multiplicativity of } f\text{]} \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \quad \text{[distributive law of multiplication]} \\ &= F(m)F(n) \quad \text{[again by definition of } F\text{]}. \end{aligned}$$

□

Lemma 42. *If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1|m$, $d_2|n$; furthermore all these products are distinct.*

Proof. Let $D(m)$ denote the set of divisors of m:

$$D(m) = \{d \mid m\}.$$

We construct a map between the sets

$$\Phi : D(m) \times D(n) \to D(mn)$$

which maps

$$\Phi : (d_1, d_2) \in D(m) \times D(n) \mapsto d_1 d_2 \in D(mn).$$

Both domain and codomain have the same number of elements:

$$\#D(mn) = \tau(mn) = \tau(m)\tau(n) = \#D(m) \times \#D(n).$$

We show that Φ is injective:

$$\Phi(d_1, d_2) = \Phi(d_1', d_2') \implies d_1 d_2 = d_1' d_2' \implies d_1 = d_1', d_2 = d_2'$$

since m and n are coprime. By the pigeonhole principle Φ is also surjective.

This is exactly what we had to prove: every divisor d of mn can be written uniquely as a product

$$d = d_1 d_2$$

with $d_1 \mid m$ and $d_2 \mid n$. □

Theorem 41 yields a simple proof of multiplicativity of σ and τ. Indeed, if we let $f(n) = 1$, then

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} 1 = \tau(n)$$

and since $f(n) = 1$ is multiplicative, Theorem 41 implies that $F(n) = \tau(n)$ is multiplicative.

Similarly, if we let $g(n) = n$, then

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

and since $g(n) = n$ is multiplicative, Theorem 41 implies that $G(n) = \sigma(n)$ is multiplicative.

9. Möbius μ-function and Möbius inversion

We define the Möbius μ-function as follows:

Definition 43. *For an integer $n > 0$ we set*

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & p^2 \mid n, \text{ for some } p \\ (-1)^r, & n = p_1 \cdots p_r, \ p_i \text{ distinct primes} \end{cases}$$

Example 44. *If p is a prime, then $\mu(p) = -1$, $\mu(p^r) = 0$, $r \geq 2$. The values of μ-function on small integers are*

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1, ...$$

Theorem 45. *The function μ is multiplicative.*

Proof. The proof is the same as for the multiplicativity of τ and σ (Theorem 97 (2)). □

The function μ and the formula below are due to August Ferdinand Möbius (1790 - 1868), German mathematician and astronomer. He is also famous for the Möbius band and Möbius transformations $z \mapsto \frac{az+b}{cz+d}$ in complex analysis. According to a biographer of Möbius, "The inspirations for his research he found mostly in the rich well of his own original mind. His intuition, the problems he set himself, and the solutions that he found, all exhibit something extraordinarily ingenious, something original in an uncontrived way...".

Theorem 46 (Möbius Inversion Formula). *Let F and f be two arithmetic functions related by the formula*

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

Then

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d).$$

Proof. We first show that the two expressions $\sum_{d|n} \mu(d) F(\frac{n}{d})$ and $\sum_{d|n} \mu(\frac{n}{d}) F(d)$ are identical. This because we have

$$\sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d \cdot d' = n} \mu(d) F(d') = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$$

and we may rename the dummy variable d' back to d in the last expression.

Now we show that $\sum_{d|n} \mu(d) F(\frac{n}{d})$ equals $f(n)$. For that we use the definition F:

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

and obtain a double sum expression in which I change the order of summation:

$$\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(d)\sum_{e|\frac{n}{d}}f(e)=\sum_{ed|n}\mu(d)f(e)=\sum_{e|n}\sum_{d|\frac{n}{e}}\mu(d)f(e)=\sum_{e|n}M(\frac{n}{e})f(e).$$

Here $M(m)=\sum_{d|m}\mu(d)$ and $M(m)=0$ unless $m=1$ by the next Lemma. Thus all terms in the latter expression are zero except the one with $e=n$ so that we get

$$\sum_{e|n}M(\frac{n}{e})f(e)=1\cdot f(n)=f(n).$$

This finishes the proof. □

Lemma 47. *Let $M(n)=\sum_{d|n}\mu(d)$. Then $M(n)=\begin{cases}1, & n=1\\ 0, & n>1\end{cases}$*

Proof. Since the only divisor of 1 is 1, it is obvious that

$$M(1)=\mu(1)=1.$$

Let us assume that $n>1$. We need to show that $M(n)=0$.

We first do the case of n being a power of a prime: if $n=p^k$ its divisors are $d=p^a$ for $0\leq a\leq k$, so that summing over divisors we get

$$M(p^k)=\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^k)=1-1+0+\cdots+0=0$$

and we are done.

Let us now do the general case of $n>1$. Write

$$n=p_1^{k_1}\cdots p_r^{k_r}$$

for the prime factorization of n. By Theorem 45 μ is multiplicative, and using Theorem 41 we deduce that M is a multiplicative function as well. This implies that

$$M(n)=M(p_1^{k_1})\cdots M(p_r^{k_r})=0$$

as every term in the product is zero as we have checked above. □

Example 48. *Recall that the τ-function can be written as*

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

so that the Möbius Inversion Formula implies that

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

For example, let $n=6$, so that its divisors are $d=1,2,3,6$ and we have

$$\mu(6)\tau(1)+\mu(3)\tau(2)+\mu(2)\tau(3)+\mu(1)\tau(6)=1\cdot 1+(-1)\cdot 2+(-1)\cdot 2+1\cdot 4=1$$

in accordance with the formula above.

Example 49. *Recall that the σ-function can be written as*

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

so that the Möbius Inversion Formula implies that

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

As in the previous example, let us now take $n = 6$, so that its divisors are $d = 1, 2, 3, 6$ and we have

$$\mu(6)\sigma(1) + \mu(3)\sigma(2) + \mu(2)\sigma(3) + \mu(1)\sigma(6) = 1 \cdot 1 + (-1) \cdot 3 + (-1) \cdot 4 + 1 \cdot 12 = 6$$

in accordance with the formula above.

10. Euler's ϕ-function

Definition 50. *For an integer $n > 0$, the Euler function $\phi(n)$ is defined as*

$$\phi(n) = (\#\ \textit{of integers}\ 1 \leq a \leq n\ \textit{such that}\ \gcd(a, n) = 1).$$

Example 51. *We have $\phi(p) = p - 1$ if p prime. The values of the Euler ϕ-function on small integers are:*

$$\phi(1) = 1$$
$$\phi(2) = 1$$
$$\phi(3) = 2$$
$$\phi(4) = 2$$
$$\phi(5) = 4$$
$$\phi(6) = 2$$
$$\phi(7) = 6.$$

Proposition 52. *For $n = p^k$ we have*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

Proof. We need to count integers $1 \leq a \leq p^k$ which are coprime to p^k. In this case it is easier to count integers which are *not coprime* to p^k. Note that

$$a \text{ not coprime to } p^k \iff a \text{ and } p^k \text{ have a common factor} \iff p \mid a.$$

Thus integers which are not coprime to p^k have the form

$$a = p \cdot b.$$

What are the bounds for b? The lower bound is $b \geq 1$. For the upper bound we have

$$a \leq p^k \implies p \cdot b \leq p^k \implies b \leq p^{k-1}.$$

Thus there are p^{k-1} choices for b to make up an a which is divisible by p. Finally we deduce that

$$\phi(p^k) = p^k - (\#\text{ of integers } 1 \leq a \leq n \text{ such that } p \mid a) = p^k - p^{k-1}.$$

□

Theorem 53. (1) *Euler's ϕ-function is multiplicative.*

(2) *If $n = p_1^{k_1} \cdots p_r^{k_r}$, then*

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) = n \cdot (1 - 1/p_1) \cdots (1 - 1/p_r).$$

Proof. (1): Let m and n be coprime. We need to show that

$$\phi(mn) = \phi(m)\phi(n).$$

Let us recall the notation $\mathbb{Z}_n$ for integers modulo n and also introduce

$$\mathbb{Z}_n^\star = \{\overline{a} \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

We've seen that $\mathbb{Z}_n^\star$ consists of elements in $\mathbb{Z}_n$ which admit multiplicative inverse. In this notation $\phi(n)$ is simply the number of elements in $\mathbb{Z}_n^\star$: $\phi(n) = |\mathbb{Z}_n^\star|$.

That is to check multiplicativity of $\phi(n)$ we need to compare $\mathbb{Z}_{mn}^\star$ with $\mathbb{Z}_m^\star$ and $\mathbb{Z}_n^\star$. We employ the Chinese Remainder Theorem which is a bijection:

$$\mathbb{Z}_{mn} \leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n.$$

Now an integer a is coprime to mn if and only if it is coprime to both m and n. This is because m and n are coprime. Thus we also get a bijection:

$$\mathbb{Z}_{mn}^\star \leftrightarrow \mathbb{Z}_m^\star \times \mathbb{Z}_n^\star.$$

Counting the number of elements on both sides gives

$$\phi(mn) = \phi(m)\phi(n).$$

(2): This follows from (1) and Proposition 52. □

Example 54. *We use Theorem 53 to compute* $\phi(180)$*. Similarly to what we did in Example 40 when computing* $\sigma(180)$ *and* $\tau(180)$ *there are different ways to compute* $\phi(180)$*. We can use prime factorization of* n*:*

$$180 = 2^2 \cdot 3^2 \cdot 5 \implies \phi(180) = (2^2 - 2) \cdot (3^2 - 3) \cdot (5 - 1) = 2 \cdot 6 \cdot 4 = 48.$$

or we can factor $n = 180$ *into a product of arbitrary relatively prime factors:*

$$180 = 9 \cdot 20 \implies \phi(180) = \phi(9)\phi(20).$$

By proposition 52 We have $\phi(9) = 9 - 3 = 6$ *and to compute* $\phi(20)$ *we may use the definition and list numbers between* 1 *and* 20 *relatively prime to* 20*:*

$$1, 3, 7, 9, 11, 13, 17, 19.$$

There are 8 *of these, so that putting everything together we get the same answer as above:*

$$\phi(180) = \phi(9)\phi(20) = 6 \cdot 8 = 48.$$

Exercise 55. *Check that* $\phi(120) = 32$*.*

Proposition 56 (Summing values of ϕ-function over divisors)**.** *We have*

$$\sum_{d|n} \phi(d) = n$$

Proof. We employ the usual strategy: since ϕ is multiplicative (Theorem 53), the sum over divisors function

$$\Phi(n) := \sum_{d|n} \phi(d) = n$$

is also multiplicative by Multiplicativity Theorem 41. Let $n = p^k$, a power of a prime. Then

$$\Phi(p^k) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^k) = 1 + (p - 1) + (p^2 - p) + \cdots + (p^k - p^{k-1}),$$

this is a telescoping sum giving

$$\Phi(p^k) = p^k.$$

Now since $\Phi(n)$ is multiplicative we have $\Phi(n) = n$ for all n. □

Week 4. Euler's theorem
The group $\mathbb{Z}_n^\star$
Primitive roots
Quadratic residues and non-residues
Euler's criterion

This week we continue exploring modular arithmetic. We use a new tool, Euler's function $\phi(n)$ and review Group Theory.

The most important theorem this week is Euler's Theorem which generalizes Fermat's Little Theorem. Its proof is an easy application of Lagrange's Theorem from group theory. We then proceed to discussing orders of elements modulo n, culminating with primitive roots ("generators mod n"). Finally we study quadratic residues ("squares mod. n") and characterize them in terms of orders in the Euler Criterion.

Two theorems in this chapter have Euler's name attached to them. Swiss mathematician Leonhard Euler (1707 - 1783), one of the most influential mathematicians of all time, developed large parts of modern number theory, in particular on the properties of primes and the Riemann zeta-function. Amusingly, here is what Euler himself told us about primes: "Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate."

11. Euler's Theorem

If n is not a prime, then Fermat's Little Theorem does not hold: $a^{n-1} \not\equiv 1 \pmod{n}$. For example: for $n = 4$, $a = 3$ we have

$$a^{n-1} = 3^3 = 27 \equiv -1 \not\equiv 1 \pmod{4}.$$

Theorem 57 (Euler's Theorem). *If n is a positive integer and $\gcd(a, n) = 1$ then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Remark 58. *Euler's theorem implies Fermat's Little Theorem: by putting $n = p$, a prime, we have $\phi(n) = p - 1$, and*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Example 59. *Let $n = 10$, so that $\phi(n) = \phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$. We compute $a^4 \pmod{10}$ for $a = 1, 3, 7, 9$:*

$$1^4 = 1$$
$$3^4 = 9^2 = 81 \equiv 1$$
$$7^4 \equiv (-3)^4 \equiv 3^4 \equiv 1$$
$$9^4 \equiv (-1)^4 = 1$$

All these are congruent to 1 modulo 10, in accordance with Euler's Theorem.

We could have proven Euler's Theorem by induction using factorization $n = p_1^{k_1} \cdots p_r^{k_r}$; in such a proof Fermat's Little Theorem would serve as the base of induction. Instead we will give a very short (almost one line) proof of Euler's Theorem using standard facts from Group Theory.

12. Review of Group Theory

Definition 60. *A* **group** *is a set G together with an operation $* : G \times G \to G$ and an element $e \in G$ satisfying:*

1. *Associativity: $a * (b * c) = (a * b) * c$*
2. *Neutral element: $e * a = a * e = a$*
3. *Inverses exist: $a * a^{-1} = a^{-1} * a = e$*

A group G is called **commutative** *(or* **abelian***) if $a * b = b * a$*
If G is a finite set, then its cardinality is the **order** *of the group. Notation for the order: $|G|$.*

Example 61. *Here are some examples and non-examples:*

- *$(\mathbb{Z}, +)$ is a group;*
- *$(\mathbb{Z}_n, +) = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$ is a group of order n. Here and below we put bars on top of numbers to distinguish elements of $\mathbb{Z}/n$ from elements of $\mathbb{Z}$.*
- *$(\mathbb{Q}, \times)$ is* **not** *a group: 0 does not have an inverse;*
- *$(\mathbb{Q} - \{0\}, \times)$ is a group*

Definition 62. *Let G be a group. A subset $H \subset G$ is a subgroup if*

1. *$e \in H$*
2. *$a, b \in H \implies a * b \in H$*
3. *$a \in H \implies a^{-1} \in H$*

Example 63. *$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.*

Let us consider subgroups **generated** by one element. Any element $g \in G$ generates a subgroup as follows:

$$\langle g \rangle := \{g^k : k \in \mathbb{Z}\},$$

i.e. we look at the set of all powers of g, and this set is a subgroup (check this!).

Order of an element $g \in G$ is defined as $\mathrm{ord}_G(g) = \min(k > 0 : g^k = e)$, and the order of g coincides with the order of subgroup it generates:

$$\mathrm{ord}_G(g) = |\langle g \rangle|. \tag{6}$$

The last thing we need to recall about groups is Lagrange's theorem.

Theorem 64 (Lagrange's theorem). *Let G be a finite group.*

1. *If $H \subset G$ is a subgroup, then $|H|$ divides $|G|$*
2. *If $g \in G$, then $\mathrm{ord}(g)$ divides $|G|$.*
3. *For any $g \in G$ we have*

$$g^{|G|} = e.$$

13. Group $\mathbb{Z}_n^\star$ of invertible elements modulo n

Definition 65. *The group of invertible elements modulo n is*

$$\mathbb{Z}_n^\star = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

Example 66. *Here are examples of invertible elements modulo 5 and modulo 10:*

- *$\mathbb{Z}_5^\star = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$*
- *$\mathbb{Z}_{10}^\star = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$*

Theorem 67. *$(\mathbb{Z}_n^\star, \times)$ is a commutative group of order $\phi(n)$.*

Proof. All group axioms are obvious, except for existence of inverses. For this we notice, that

$$\overline{a} \cdot \overline{b} = \overline{1} \iff a \cdot b \equiv 1 \pmod{n}.$$

Since we include elements relatively prime to n in our group, for each a there exists a corresponding b. □

Example 68. *Multiplying modulo* 5*, we see that the group* $\mathbb{Z}_5^\star$ *has the following multiplication table:*

	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

As always, for a multiplication table of a group, each element appears once in each row and in each column, a bit like in Sudoku.

The inverses work as follows:

$$\overline{1}^{-1} = \overline{1}$$
$$\overline{2}^{-1} = \overline{3}$$
$$\overline{3}^{-1} = \overline{2}$$
$$\overline{4}^{-1} = \overline{4}.$$

Example 69. *Let* $G = \mathbb{Z}_{25}^\star$*, and take an element* $g = \overline{7} \in G$*.* $\langle g \rangle = \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\}$*,* $\operatorname{ord}(g) = 4$*.*

We use Lagrange's theorem applied to $\mathbb{Z}_n^\star$ to get an easy proof of Euler's theorem.

Proof of Euler's Theorem. The group of invertible elements $\mathbb{Z}_n^\star$ has order $\phi(n)$. Thus by Lagrange's Theorem 64 (3) for any $\overline{a} \in \mathbb{Z}_n^\star$ we have

$$\overline{a}^{\phi(n)} = \overline{1}$$

or equivalently

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Example 70. *We compute orders of all elements in* $\mathbb{Z}_7^\star$*. This is a group of order six. By Lagrange's Theorem 64 (2), any element has order dividing* 6*, i.e.*

$$\operatorname{ord}(\overline{a}) \in \{1, 2, 3, 6\}.$$

Only the neutral element $\overline{1}$ *has order* 1*. For the other* 5 *elements, we check whether the order is* 2,3 *or* 6*. When computing the last three rows of the table we keep in mind that* $\overline{4} = \overline{-3}$*,* $\overline{5} = \overline{-2}$ *and* $\overline{6} = \overline{-1}$*.*

$a \pmod 7$	$a^2 \pmod 7$	$a^3 \pmod 7$	$a^6 \pmod 7$	$\operatorname{ord}(a)$
$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	1
$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{1}$	3
$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	6
$\overline{4}$	$\overline{2}$	$\overline{1}$	$\overline{1}$	3
$\overline{5}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	6
$\overline{6}$	$\overline{1}$	$\overline{6}$	$\overline{1}$	2

14. Primitive roots

We need to recall a notion of a generator of a group. This is analogous to a basis element of a vector space. In the same way as a basis helps exploring a vector space, a generator helps exploring a group!

Definition 71. *Let G be a group. We call an element $g \in G$ a* **generator** *of G if $G = \langle g \rangle$, i.e. if G consists only of powers of g. If G has a generator, then G is called a* **cyclic group**.

Theorem 72. *Let G be a finite group. Then $g \in G$ is a generator if and only if* $\mathrm{ord}_G(g) = |G|$.

Proof. Let H denote the subgroup generated by g:

$$H = \langle g \rangle \subset G.$$

From (6) we know that

$$\mathrm{ord}_G(g) = |H|.$$

Thus we have

$$\mathrm{ord}_G(g) = |G| \iff |H| = |G| \iff H = G \iff g \text{ is a generator of } G.$$

□

Definition 73. *An integer a such that* $\gcd(a, n) = 1$ *is called a* **primitive root modulo** *n if $\overline{a}$ is a generator of $\mathbb{Z}_n^\star$.*

From Theorem 72 it follows that a is a primitive root modulo n if and only if $\mathrm{ord}(a) = \phi(n)$.

Example 74. *We find all primitive roots modulo 7. From Example 70 we know the orders of elements in $\mathbb{Z}_7^\star$. Among them primitive roots are elements of order 6 (i.e. the maximal order); these are $\overline{3}$ and $\overline{5}$.*

Example 75. *We will now see that there is no primitive root modulo 8. The group $\mathbb{Z}_8^\star$ consists of 4 elements:*

$$\mathbb{Z}_8^\star = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

Thus a primitive root must have order 4. However all elements have order at most two:

$$\overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}.$$

Given a primitive root a modulo n we may ask which powers a^k are primitive roots, or more generally what is the order of a^k? The next Theorem provides the answers.

Theorem 76. *Let a be a primitive root modulo n. Then*

1. $\mathrm{ord}(a^k) = \frac{\phi(n)}{\gcd(k, \phi(n))}$
2. *a^k is a primitive root if and only if* $\gcd(k, \phi(n)) = 1$
3. *There are $\phi(\phi(n))$ primitive roots modulo n.*

For the proof we need a couple of lemmas.

Lemma 77 (Which powers of a group element give the neutral element). *Let G be a group, $g \in G$ an element of order c. Then we have*

$$g^k = e \iff k \equiv 0 \pmod{c}.$$

Proof. It is easy to see that $k \equiv 0 \pmod{c} \implies g^k = e$:

$$k \equiv 0 \pmod{c} \implies k = lc, l \in \mathbb{Z} \implies g^k = g^{lc} = (g^c)^l = e^l = e.$$

We also need to prove that $g^k = e \implies k \equiv 0 \pmod{c}$. This is also not too hard: let $k = lc + r$, with the remainder $0 \leq r < c$. We'd like to show that $r = 0$. We have:

$$g^k = e \implies g^{lc+r} = e \implies g^r = e.$$

By definition of what *order* is, this is only possible when $r = 0$ (otherwise the order of g is not c, but a smaller $0 < r < c$). □

Lemma 78. *Let G be a group, $g \in G$ an element of order c. Then for any $k \in \mathbb{N}$ the order of g^k is*

$$\operatorname{ord}(g^k) = \frac{c}{\gcd(k, c)}$$

Proof. To see what the order is, we consider l'th power of g^k ($l \in \mathbb{N}$). We use Lemma 1:

$$(g^k)^l = g^{kl} = e \iff c \mid kl \iff \frac{c}{\gcd(k, c)} \mid l.$$

Thus the smallest l for which this is possible is $l = \frac{c}{\gcd(k,c)}$. □

Proof of Theorem 76. It is easy to show that (1) implies (2):

$$a^k \text{ is a primitive root} \iff \operatorname{ord}(\overline{a}^k) = \phi(n) \iff \frac{\phi(n)}{\gcd(k, \phi(n))} = \phi(n) \iff \gcd(k, \phi(n)) = 1.$$

Now (2) implies (3): we need to count elements $\overline{b} \in \mathbb{Z}_n^*$ which are primitive roots, i.e. generators. Since a itself is a generator, any $\overline{b} \in \mathbb{Z}_n^*$ has the form:

$$\overline{b} = \overline{a}^k, \ k = 0, 1, 2, \ldots, \phi(n) - 1.$$

By part (2) of the Theorem, an element $b = a^k$ is a primitive root if and only if

$$\gcd(k, \phi(n)) = 1.$$

There are precisely $\phi(\phi(n))$ such k's.

Finally part (1) follows from Lemma 78 with $G = \mathbb{Z}_n^\star$, $g = \overline{a}$, $c = \phi(n)$. □

15. Existence of primitive roots modulo primes

Theorem 79 (Primitive roots mod. p). *If p is prime, then $\mathbb{Z}_p^\star$ has a primitive root.*

Furthermore, there are precisely $\phi(p-1)$ primitive roots.

Remark 80. *Another way to say that there exits a primitive modulo p is to say that $\mathbb{Z}_p^\star$ is a cyclic group.*

For the proof we need the following lemma:

Lemma 81 (Roots of unity in $\mathbb{Z}_p^*$). *For every divisor n of $p-1$ the number of solutions of the equation $x^n = \overline{1}$ in $\mathbb{Z}_p$ is equal to n.*

Proof. First of all note that if $f(x)$ is any polynomial of degree n, then it has no more than n distinct roots – this is because $\mathbb{Z}_p = \mathbb{F}_p$ is a field.

Now let $p-1 = nm$ and let us factor $x^{p-1} - \overline{1}$:

$$x^{p-1} - \overline{1} = x^{nm} - \overline{1} = (x^n - \overline{1})(x^{n(m-1)} + x^{n(m-2)} + \cdots + x^n + \overline{1}),$$

The polynomial $x^{p-1} - \overline{1}$ on the left has $p-1$ distinct roots in $\mathbb{Z}_p$: all non-zero elements of $\mathbb{Z}_p$ are its roots by Fermat's Little Theorem.

If $x^n - 1$ has less than n roots, then the other factor (that has degree $n(m-1) = nm - n = p-1-n$) will have more than $p-1-n$ roots, which is impossible. □

Lemma 81 is telling us something quite interesting about orders of elements in $\mathbb{Z}_p$. Without saying directly how many elements of a given order n dividing $p-1$ are there, it says how many elements whose order *dividing* n there are: indeed by Lemma 77 applied to $x \in \mathbb{Z}_p$ we see that the order of x *divides* n if and only x is a solution of $x^n = \overline{1}$. We rely on this argument in Theorem 79 below to deduce *existence* of primitive roots in $\mathbb{Z}_p$.

Example 82. *It's instructive to look at what Lemma 81 says for particular values of* $n \mid p-1$*:*

- $n = 1$*: there is one element of order* 1*,* $x = \overline{1}$*.*
- $n = p-1$*: all* $p-1$ *elements of* $\mathbb{Z}_p$ *satisfy* $x^{p-1} = \overline{1}$*. This is FLT.*
- $n = 2$ *(assuming* $p > 2$ *to satisfy* $n \mid p-1$*): there are two elements of order dividing* 2*: these are* $\pm\overline{1}$*.*

Proof of Theorem 79. Apart from basic facts we established in this chapter, the proof also relies on the Theory of Arithmetic functions from Week 3, including the unexpected application of the Möbius Inversion!

Let $\psi(n)$ denote the number of elements in $\mathbb{Z}_p$ of order equal n:

$$\psi(n) = (\#\text{ of } x \in \mathbb{Z}_p\text{: } \mathrm{ord}(x) = n).$$

Note that by this definition we have $\psi(n) = 0$ as soon as n does not divide $p-1$, because orders of elements divide order of the group.

Now to see that there is a primitive root we need to show that there is an element of order $p-1$, in other word we need to show that $\psi(p-1) \neq 0$. In fact we show that $\psi(p-1) = p-1$, establishing the claim on existence and the number roots at the same time!

We use the summation over divisors approach for every n and define:

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

For every $n \mid p-1$ we compute the value $F(n)$ as follows:

$$\begin{aligned} F(n) &= \sum_{d|n} (\#\text{ of elements of } \mathbb{Z}_p \text{ of order equal to } d) \text{ [by Definition of } \psi] = \\ &= (\#\text{ of elements of } \mathbb{Z}_p \text{ of order dividing } n) \text{ [by Lemma 77]} = \\ &= (\#\text{ of solutions of } x^n = 1 \text{ in } \mathbb{Z}_p) = n \text{ [by Lemma 81].} \end{aligned}$$

Now by Möbius Inversion Formula applied to $F(n)$, for every divisor n of $p-1$ we have

$$\psi(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(d) \frac{n}{d}$$

and the last expression is equal to

$$\sum_{d|n} \mu(d)\frac{n}{d} = \phi(n)$$

by the Möbius Inversion applied to the Euler function $\sum_{d|n} \phi(d) = n$.

That is we found

$$\psi(n) = \phi(n)$$

for all n dividing $p-1$. In particular we have:

$$\psi(p-1) = \phi(p-1),$$

that is we have precisely $\phi(p-1)$ primitive roots modulo p.

Note that for the Euler function we always have $\phi(p-1) \geq 1$, thus there is always at least one primitive root. □

Remark 83. *Composite numbers n often do not have primitive roots in $\mathbb{Z}_n^\star$. For instance, there is no primitive root modulo $2^k, k \geq 3$. However, there are primitive roots modulo $2p$. Both of these statements are proven in the Problem Sheet for this week.*

16. Quadratic residues and Euler's criterion

We start by giving a definition:

Definition 84. *Let $p > 2$ be a prime and $\gcd(a,p) = 1$. If the congruence*

$$x^2 \equiv a \pmod{p}$$

has a solution, then a is said to be a **quadratic residue** *modulo p. Otherwise, a is called a* **quadratic nonresidue** *modulo p.*

Example 85. *To find quadratic residues modulo $p = 5$ we look at the squares:*

$$1^2 = 1$$
$$2^2 = 4$$
$$3^2 = 9 \equiv 4$$
$$4^2 = 16 \equiv 1.$$

Thus quadratic residues are $1, 4$ and quadratic nonresidues are $2, 3$. (Note that $a = 0$ is excluded by definition - it is neither a residue nor nonresidue.)

Example 86. *Let us find quadratic residues modulo $p = 7$:*

$$1^2 = 1$$
$$2^2 = 4$$
$$3^2 = 9 \equiv 2$$
$$4^2 \equiv (-3)^2 \equiv 2$$
$$5^2 \equiv (-2)^2 \equiv 4$$
$$6^2 \equiv (-1)^2 \equiv 1$$

We see that quadratic residues modulo 7 are $1, 2, 4$ and quadratic nonresidues are $3, 5, 6$.

Example 87. *We now do quadratic residues modulo* $p = 11$*:*

$$1^2 = 1$$
$$2^2 = 4$$
$$3^2 = 9$$
$$4^2 = 16 \equiv 5$$
$$5^2 = 25 \equiv 3$$

We did not square $6, 7, 8, 9, 10$*, since we have* $6 \equiv -5, 7 \equiv -4, \ldots$*, so that we won't get new squares this way! We see that quadratic residues modulo* 11 *are*

$$1, 3, 4, 5, 9$$

and the other 5 *elements of* $\mathbb{Z}_{11}^\star$ *are quadratic nonresidues:*

$$2, 6, 7, 8, 10.$$

In the three examples 85, 86, 87 above we had the half of our $p-1$ elements in $\mathbb{Z}_p^\star$ as quadratic residues and the other half as quadratic nonresidues. This is a general phenomenon:

Theorem 88. *Let* $p > 2$ *be a prime. Among the numbers* $1, 2, \ldots, p-1$ *there are* $\frac{p-1}{2}$ *quadratic residues, and the same number of quadratic nonresidues modulo* p*.*

Warning: this Theorem is not applicable to $p = 2$. Neither are most of the Theorems that follow next week. Be careful with $p = 2$, which is the only even prime!

Proof. We look at all the nonzero squares modulo p:

$$1^2, 2^2, 3^2, \ldots, (p-1)^2 \pmod{p}.$$

Which elements of this list are the same? Let's see.

$$a^2 \equiv b^2 \pmod{p} \implies (a-b)(a+b) \equiv 0 \pmod{p} \implies p \mid (a-b)(a+b) \implies$$
$$a \equiv b \pmod{p} \quad \text{or} \quad a \equiv -b \pmod{p}.$$

Thus in our original list of squares modulo p we have

$$\frac{p-1}{2}$$

(i.e. the half) distinct elements. Thus there are $\frac{p-1}{2}$ quadratic residues, and the number of quadratic nonresidues is:

$$p - 1 - \frac{p-1}{2} = \frac{p-1}{2}.$$

□

There is a relation between quadratic residues and *orders* we've studied earlier. Recall that by Fermat Little Theorem we have

$$a^{p-1} \equiv 1 \pmod{p}$$

for $\gcd(a, p) = 1$ but sometimes we have

$$a^k \equiv 1 \pmod{p}$$

for $k < p - 1$. In Euler's Criterion we look at $k = \frac{p-1}{2}$.

Theorem 89 (Euler's criterion for quadratic residues). *Let $p > 2$ be a prime, and a an integer not divisible by p. Then:*

(1) $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$
(2) *a is a quadratic residue mod. p* $\iff a^{(p-1)/2} \equiv 1 \pmod{p}$
(3) *a is a quadratic nonresidue mod. p* $\iff a^{(p-1)/2} \equiv -1 \pmod{p}$

Proof. (1) This is true because $x = a^{(p-1)/2}$ satisfies $\overline{x}^2 = 1$. By Lemma 78 (see Example 82) we have $x = \pm\overline{1}$.

(2) Let a be a quadratic residue mod. p. Then $\overline{a} = \overline{b}^2$ for some integer b and we have

$$\overline{a}^{\frac{p-1}{2}} = (\overline{b}^2)^{\frac{p-1}{2}} = \overline{b}^{p-1} = \overline{1}$$

by the FLT.

We see that the set of quadratic residues is contained in the set of elements satisfying $a^{(p-1)/2} = \overline{1}$. Now these set have the same number of elements: by Lemma 78 applied to $n = \frac{p-1}{2}$ there $\frac{p-1}{2}$ solutions to $a^{(p-1)/2} = \overline{1}$, and by Theorem 88 there are $\frac{p-1}{2}$ quadratic residues. Therefore the two sets are equal: a is a quadratic residue iff it satisfies $a^{(p-1)/2} = \overline{1}$.

(3) This formally follows from parts (1) and (2). Indeed, as two statements from (2) are equivalent, their negations are also equivalent:

$$a \text{ is NOT a quadratic residue mod. } p \iff a^{(p-1)/2} \not\equiv 1 \pmod{p}$$

Simplifying this using (1) yields

$$a \text{ is a quadratic nonresidue mod. } p \iff a^{(p-1)/2} \equiv -1 \pmod{p},$$

as stated. □

Example 90. *Let us see how this works for $p = 7$. According to Example 86, quadratic residues modulo 7 are*

$$1, 2, 4$$

and quadratic nonresidues are

$$3, 5, 6.$$

In Euler's criterion we need to look at $\frac{p-1}{2}$th, i.e. 3rd powers:

$$\begin{aligned} 1^3 &= 1 \\ 2^3 &= 8 \equiv 1 \pmod{7} \\ 4^3 &= (2^3)^2 \equiv 1^2 = 1 \pmod{7}. \end{aligned}$$

On the other hand:

$$\begin{aligned} 3^3 &= 27 \equiv -1 \pmod{7} \\ 5^3 &= 5^2 \cdot 5 \equiv 25 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv -1 \pmod{7} \\ 6^3 &= 6^2 \cdot 6 \equiv 36 \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod{7}. \end{aligned}$$

We continue studying quadratic residues next week.

Week 5. Quadratic congruences
Legendre's symbol
Gauss' quadratic reciprocity

The third key figure in number theory, following Fermat and Euler was German mathematician Carl Friedrich Gauss (1777-1855), also one of the most important mathematicians of all time. Gauss is famous for his quote "Mathematics is the queen of the sciences and number theory is the queen of mathematics."

Another nice quote from Gauss: "You know that I write slowly. This is chiefly because I am never satisfied until I have said as much as possible in a few words,and writing briefly takes far more time than writing at length." Quadratic reciprocity law that we study this week is a clear demonstration of this principle: the quadratic reciprocity law is a very concise and yet very powerful statement allowing us to answer the question whether an element a is a quadratic residue modulo p.

Beware that quadratic reciprocity - due its counterintuitive nature and complex proofs - is one the harder topics we study in this module.

17. Quadratic Congruences

Let's say we need to solve a **quadratic congruence**

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad (\star)$$

As with usual quadratic equations, the most important thing is the discriminant

$$d = b^2 - 4ac.$$

The first thing we can do about our congruence is to complete the square. We assume

$$\gcd(2a, p) = 1$$

(i.e. p is odd and p does not divide a) and multiply the congruence $(\star)$ by $4a$:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

Now we notice that

$$(2ax + b)^2 = 4a^2x^2 + 4abx + b^2,$$

so that my quadratic congruence can be rewritten as

$$4a^2x^2 + 4abx + 4ac = (2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{p}.$$

or equivalently

$$(2ax + b)^2 \equiv b^2 - 4ac = d \pmod{p}.$$

Thus if we denote $y = 2ax + b$ we have a system of congruences:

$$\begin{cases} y^2 \equiv d & \pmod{p} \\ 2ax + b \equiv y & \pmod{p} \end{cases}$$

The first is a simple quadratic congruence, and the second is a linear congruence. We can go one step further and write all solutions as in the real case as follows:

$$\overline{2a}\overline{x} + \overline{b} = \overline{y} \implies \overline{x} = \frac{-\overline{b} + \overline{y}}{2\overline{a}} = \frac{-\overline{b} \pm \sqrt{\overline{d}}}{2\overline{a}} \in \mathbb{Z}_p.$$

Here division by $\overline{2a}$ means multiplication by $\overline{2a}^{-1}$. This is well defined since $\gcd(2a, p) = 1$ by assumption so that $\overline{2a}$ is invertible.

Example 91. *Let us solve* $5x^2 - 6x + 2 \equiv 0 \pmod{13}$. *We compute the discriminant:*

$$d = 36 - 4 \cdot 20 = -4 \equiv 9 \pmod{13}$$

so that the formula for the roots reads

$$x = \frac{\overline{6} \pm \overline{3}}{\overline{10}} = \overline{4} \cdot (\overline{6} \pm \overline{3})$$

which gives solutions $x \equiv 10, 12 \pmod{13}$.

We wrote $\sqrt{\overline{d}}$ and pretended that this makes sense in $\mathbb{Z}_p$. So here is the main question we investigate this week:

Question 92. *Which square roots exist modulo p?*

We will develop powerful tools (Legendre's symbol and Gauss Reciprocity) to study this question.

18. Legendre's symbol

Recall that last week we introduced the following definition: a is a *quadratic residue* (QR) modulo p if $x^2 = a$ has a solution in $\mathbb{Z}_p^\star$, and a *quadratic nonresidue* (QNR) otherwise.

For instance we saw that 1 and 4 are QRs and 2 and 3 are QNRs modulo 5.

Definition 93. *Let* $p > 2$ *be a prime, and* a *an integer not divisible by* p. *Then*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

Remark 94. *We* **do not define and do not use** *the symbol* $\left(\frac{a}{2}\right)$.

Example 95. *We can neatly express QRs and QNRs modulo* $p = 5$ *by stating that*

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = +1$$

and

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Remark 96. *By definition we have*

$$a \equiv b \pmod{p} \implies \overline{a} = \overline{b} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

In terms of the Legendre symbol Euler's Criterion takes the form:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{7}$$

Indeed, both sides are $+1$ or -1 depending on whether a is quadratic residue or not. Formula (7) is beautiful and important, but can not be considered as an effective computational tool if the prime p is large.

Indeed if we had to answer whether $a = 38$ is a quadratic residue modulo $p = 67$, we would have to compute $38^{\frac{67-1}{2}} = 38^{33}$ modulo 67 which does seem like a very pleasant thing to do.

Here is one helpful fact to compute $\left(\frac{a}{p}\right)$:

Theorem 97 (**Multiplicativity of the Legendre symbol**). *Let a and b be integers not divisible by p. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Proof. By Euler's Criterion (7) we have:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$
$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$$

Similarly we have:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$$

which we can further rewrite as

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since in both LHS and RHS I have a $+1$ or -1, and they are congruent modulo $p > 2$, this implies that LHS = RHS:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

as required. □

19. Gauss' Quadratic Reciprocity

The most important tool in computing Legendre's symbol is Gauss' Reciprocity. Morally speaking, Gauss' Reciprocity gives us the permission to flip a Legendre symbol

$$\left(\frac{p}{q}\right)$$

where both p and q are primes:

$$\left(\frac{p}{q}\right) = \pm \left(\frac{q}{p}\right)$$

where the $\pm$ sign is governed by $p, q \pmod 4$ (as usual $p = 2$ works a bit differently).

Theorem 98 (**Gauss' Quadratic Reciprocity**). (1) *If $p \neq q > 2$ are two primes then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right)$$

(2) *If $p > 2$ is a prime then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Warning: Gauss' Reciprocity applies only to primes! Before you apply it, check that your p and q are primes!

We have complicated looking signs in the Gauss Reciprocity. The following two Lemmas give the rules for these signs:

Lemma 99. *Let $p, q > 2$ be primes. Then*

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1, & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Proof. Since p, q are odd primes, each of them is 1 or 3 modulo 4. We consider all the possibilities:

$$p = 4k+1, q = 4l+1 \implies \frac{p-1}{2}\cdot\frac{q-1}{2} = 4kl \text{ is even} \implies (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = +1.$$

$$p = 4k+1, q = 4l+3 \implies \frac{p-1}{2}\cdot\frac{q-1}{2} = 2k(2l+1) \text{ is even} \implies (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = +1.$$

$$p = 4k+3, q = 4l+1 \implies \frac{p-1}{2}\cdot\frac{q-1}{2} = (2k+1)2l \text{ is even} \implies (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = +1.$$

$$p = 4k+3, q = 4l+3 \implies \frac{p-1}{2}\cdot\frac{q-1}{2} = (2k+1)(2l+1) \text{ is odd} \implies (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1.$$

We looked at all the possible cases and they are in compliance with what we had to prove. □

Lemma 100. *Let $p > 2$ be a prime. Then*

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof. Since p is an odd prime, possible remainders of $p \pmod 8$ are

$$1,$$
$$3,$$
$$5 \equiv -3,$$
$$7 \equiv -1.$$

In each case I check what $(-1)^{\frac{p^2-1}{8}}$ is:

$$p = 8k \pm 1 \implies p^2 - 1 = 64k^2 \pm 16k \implies \frac{p^2-1}{8} = 8k^2 \pm 2k \text{ is even} \implies (-1)^{\frac{p^2-1}{2}} = +1$$

and

$$p = 8k \pm 3 \implies p^2 - 1 = 64k^2 \pm 48k + 8 \implies \frac{p^2-1}{2} = 8k^2 \pm 6k + 1 \text{ is odd} \implies (-1)^{\frac{p^2-1}{2}} = -1.$$

□

Example 101. *Consider $\left(\frac{5}{3}\right)$. Since $5 \equiv 1 \pmod 4$, I flip Legendre's symbol without introducing an extra sign:*

$$\left(\frac{5}{3}\right) = \left(\frac{3}{5}\right)$$

(both values are -1).

Now consider $\left(\frac{7}{3}\right)$. Since both

$$7 \equiv 3 \equiv 3 \pmod 4,$$

we change sign when flipping the symbol:

$$\left(\frac{7}{3}\right) = -\left(\frac{3}{7}\right)$$

(Can you find the value of each of these symbols? One of them is $+1$, the other is -1.)

Now let's do some real fun calculations.

Example 102. *We've seen that checking whether $a = 38$ is a quadratic residue modulo $p = 67$ is not very convenient using Euler's Criterion.*

Let us use Gauss' Reciprocity instead. We compute $\left(\frac{38}{67}\right)$ as follows: 38 is not a prime, and we factor it

$$38 = 2 \cdot 19.$$

By multiplicativity Theorem 97 we compute

$$\left(\frac{38}{67}\right) = \left(\frac{2}{67}\right) \cdot \left(\frac{19}{67}\right).$$

I compute the first symbol:

$$\left(\frac{2}{67}\right) = -1$$

using Gauss Reciprocity, part 2 together with Lemma 100 since $67 \equiv 3 \pmod 8$. Thus

$$\left(\frac{38}{67}\right) = -\left(\frac{19}{67}\right) = \left(\frac{67}{19}\right).$$

(Here we notice that both 19 and 67 are prime, so we use Gauss Reciprocity, part 1 together with Lemma 99 and $67 \equiv 19 \equiv 3 \pmod 4$.) To continue we reduce 67 modulo 19:

$$\left(\frac{67}{19}\right) = \left(\frac{10}{19}\right)$$

and now we use multiplicativity again:

$$\left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right).$$

We compute each of these symbols:

$$\left(\frac{2}{19}\right) = -1$$

by Gauss Reciprocity, part 2 again, and

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = +1$$

(here we used Gauss Reciprocity, part 1, then reduced 19 modulo 5, and noticed that 4 is a quadratic residue).

Finally we obtain

$$\left(\frac{38}{67}\right) = (-1)(+1) = -1.$$

Done! We see that 38 is a QNR modulo 67.

The following two Lemmas are essential in proving Gauss Reciprocity. You need to know how to apply these Lemmas as well as Gauss Reciprocity itself. See problem sheet week 5.

Lemma 103 (Gauss' Lemma). *If $p > 2$ is a prime and a an integer not divisible by p, then*

$$\left(\frac{a}{p}\right) = (-1)^m$$

where m is the number of elements in the list

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

whose remainder modulo p exceeds $\frac{p}{2}$.

Proof. The proof is a bit obscure. The basic idea is to compute $(\frac{p-1}{2})! \pmod p$ in two different ways.

We introduce two sets:

$$T = \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\} \subset \mathbb{Z}_p$$

and

$$S = \{\overline{a}, \overline{2a}, \ldots, \overline{\frac{p-1}{2}a}\} \subset \mathbb{Z}_p.$$

Both sets consist of $\frac{p-1}{2}$ elements, but S and T are possibly different subsets of $\mathbb{Z}_p$. The proof will consist in comparing S and T and then comparing the values

$$\prod_{t\in T} t = \overline{(\frac{p-1}{2})!} \in \mathbb{Z}_p$$

with

$$\prod_{s\in S} s = \overline{(\frac{p-1}{2})!} \cdot \overline{a}^{\frac{p-1}{2}} = \overline{(\frac{p-1}{2})!} \cdot \left(\frac{a}{p}\right) \in \mathbb{Z}_p,$$

where in the last equality we used Euler's Criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

To control the difference between S and T let us write $S = S_1 \cup S_2$ where

$$S_1 = \{s \in S : s < \frac{p}{2}\}$$
$$S_2 = \{s \in S : s > \frac{p}{2}\}$$

The number of elements in S_2 is what we call m in the statement of the Lemma. We claim that $S_1 \cap S_2 = \emptyset$ (this is obvious) and that $S_1 \cap -S_2 = \emptyset$. Here $-S_2$ is

$$-S_2 = \{-s | s \in S_2\}.$$

To see that $S_1 \cap -S_2 = \emptyset$, take elements $\overline{ja} \in S_1$ and $\overline{ka} \in S_2$, with $1 \le j, k \le \frac{p-1}{2}$. We have

$$\overline{ja} = -\overline{ka} \iff \overline{(j+k)a} = 0 \iff p \mid (j+k)a \iff p \mid j+k,$$

which is impossible since $0 \le i + j \le p - 1$.

We now look at the following set:

$$S_1 \cup -S_2 = \{s \in S_1\} \cup \{-s | s \in S_2\} \subset \mathbb{Z}_p.$$

We claim that $S_1 \cup -S_2 = T$. This is because T is made up of elements whose remainders mod. p do not exceed $\frac{p-1}{2}$, so that T is contained in the list above, and the two sets have the same number of elements!

Now comes the key computation:

$$\begin{aligned}(\frac{p-1}{2})! &\equiv \prod_{t\in T} t \equiv \\ &\equiv \prod_{s\in S_1} s \cdot \prod_{s\in S_2} (-s) = \\ &= (-1)^m \prod_{s\in S} s = \\ &= (-1)^m \prod_{k=1}^{\frac{p-1}{2}} ka = \\ &= (-1)^m (\frac{p-1}{2})! \cdot a^{\frac{p-1}{2}} \pmod p .\end{aligned}$$

Canceling out $(\frac{p-1}{2})!$ on both sides we see that

$$(-1)^m a^{\frac{p-1}{2}} \equiv 1 \pmod p ,$$

and since both terms are equal to ± 1, it follows using Euler's criterion that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^m \pmod p$$

and that

$$\left(\frac{a}{p}\right) = (-1)^m.$$

□

Proof of the part (2) of Quadratic Reciprocity. This is a relatively straightforward computation: according to the Gauss Lemma applied to $a = 2$, we have $\left(\frac{2}{p}\right) = (-1)^m$, where m is the number of elements in the list

$$S = \{2, 4, 6, \ldots, \frac{p-1}{2}\} = \{2k,\ k = 1, 2, \ldots, \frac{p-1}{2}\}$$

whose remainder modulo p exceeds $\frac{p}{2}$. However since all the numbers in the list are less than p, they are already reduced modulo p. Hence we just need to compute how many integers in S exceed $\frac{p}{2}$. We have

$$2k > \frac{p}{2} \iff k > \frac{p}{4} \iff k > \left[\frac{p}{4}\right]$$

(the last equivalence holds since $\frac{p}{4}$ is not an integer). Thus m is the number of integers $k = 1, 2, \ldots, \frac{p-1}{2}$ exceed $[\frac{p}{4}]$ and we see that

$$m = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

We need to verify that $(-1)^m$ is the same sign as $(-1)^{\frac{p^2-1}{8}}$. We use the formula of Lemma 100:

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

That is there are four cases to consider:

- $p = 8k + 1$: $m = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k - \left[\frac{8k+1}{4}\right] = 8k - 2k = 6k \implies m$ is even

- $p = 8k-1$: $m = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k-1-\left[\frac{8k-1}{4}\right] = 4k-1-(2k-1) \implies m$ is even
- $p = 8k+3$: $m = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k+1-\left[\frac{8k+3}{4}\right] = 4k+1-2k \implies m$ is odd
- $p = 8k-3$: $m = \frac{p-1}{2} - \left[\frac{p}{4}\right] = 4k-2-\left[\frac{8k-3}{4}\right] = 4k-2-(2k-1) \implies m$ is odd

We see that in every case the sign $(-1)^m$ is the same as that in Gauss reciprocity, part (2):

$$\left(\frac{2}{p}\right) = (-1)^m = (-1)^{\frac{p^2-1}{8}}.$$

□

The proof is based on the following Lemma:

Lemma 104 (**Eisenstein's Lemma**). *If $p > 2$ is a prime and a an odd integer not divisible by p, then*

$$\left(\frac{a}{p}\right) = (-1)^m, \;\; m = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ak}{p}\right] = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{p-1}{2}\frac{a}{p}\right]$$

I do not type the proof of this Lemma, it relies on ideas similar to the proof of the Gauss Lemma. See Burton's book in the syllabus for details.

We finish this chapter with the final proof:

Proof of the part (1) of Quadratic Reciprocity. We are given odd primes $p \neq q$, and we need to compare $\left(\frac{p}{q}\right)$ to $\left(\frac{q}{p}\right)$. Applying Eisenstein's Lemma to *both* of these symbols we see that:

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right]}$$
$$\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]}$$

and multiplying these together we obtain

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]}.$$

Now to show that Quadratic Reciprocity part (1) holds it will be sufficient to check the following equality:

$$(*) \quad \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

We use an unexpected geometric argument to show the equality $(*)$. Consider a rectangle $R = [0, p/2] \times [0, q/2]$ in the xy-plane.

We count the number of points with integral coordinates strictly inside R, that is not lying on its boundary. We will simply call these points integral points inside R. Their coordinates $x, y \in \mathbb{Z}$ satisfy

$$0 < x < \frac{p}{2}, \; 0 < y < \frac{q}{2}$$

and since both p and q are odd, and x and y are integers, we can write these bounds as

$$1 \leq x \leq \frac{p-1}{2}, \; 1 \leq y \leq \frac{q-1}{2}.$$

That is the number of integral points inside R equals

$$\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Now let us count the number of integral points in R in a different way. Let us split the rectangle into two triangles by the diagonal connecting $(0,0)$ to $(p/2,q/2)$. It's helpful to draw the picture now.

It's important for the argument that none of the integral points lie on the diagonal of the rectangle. Indeed, the diagonal has the equation $y=\frac{q}{p}\cdot x$, or $py=qx$, and this is not satisfied by any $1\leq x\leq\frac{p-1}{2}, 1\leq y\leq\frac{q-1}{2}$ simply because p and q are coprime. Therefore the number of integral points inside R equals to the sum of the number of integral points lying *below* diagonal and of the number of integral points lying *above* the diagonal.

To count the integral points in R below the diagonal we may sum while grouping the points with the same x-coordinate. This way we get:

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right],$$

as we need to allow various $x=k$ coordinates in the range $1\leq k\leq\frac{p-1}{2}$, and we require the y-coordinate to be bounded by the diagonal line with slope q/p.

Now swapping the roles of x and y we get that the number of integral points in R lying above the diagonal equals to

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right].$$

Putting everything together we get $(*)$, and this finishes the proof. □

Week 6. Perfect numbers
Mersenne primes
Fermat primes

20. Perfect numbers

Definition 105. *An integer $n\in\mathbb{N}$ is called a* **perfect number** *if*

$$\sigma(n)=2n.$$

That is to say, n is perfect if n is equal to the sum of positive divisors of n excluding n itself:

$$n=\sigma(n)-n\iff\sigma(n)=2n.$$

Example 106. $6=1+2+3$ *and* $28=1+2+4+7+14$ *are the first two perfect numbers.*

Exercise 107. *Compute $\sigma(496)$ to show that $n=496$ is perfect.*

Perfect numbers have been introduced in Ancient Greece. Nicomachus, "*Indroductio Arithmeticae*" (circa 100 A.D.) defined a perfect number as a number "equal to the sum of its parts". He also listed the first 4 perfect numbers:

$$P_1=6, P_2=28, P_3=496, P_4=8128.$$

Based on this evidence Nicomachus stated that [**Caution: this is not quite true**]:

(1) All perfect numbers are even
(2) The last digit alternates: $6, 8, 6, 8, \ldots$
(3) The n'th perfect number P_n contains exactly n digits

Even perfect numbers. It turns out that the first four perfect numbers have very specific form:

$$P_1 = 6 = 2 \cdot 3 = 2^1 \cdot (2^2 - 1)$$
$$P_2 = 28 = 2^2 \cdot 7 = 2^2 \cdot (2^3 - 1)$$
$$P_3 = 496 = 2^4 \cdot 31 = 2^4 \cdot (2^5 - 1)$$
$$P_4 = 8128 = 2^6 \cdot 127 = 2^6 \cdot (2^7 - 1)$$

All these have the form $2^{k-1}(2^k - 1)$. These considerations motivate one of the most important theorems of this week:

Theorem 108. *If $2^k - 1$ is prime, then*

$$n = 2^{k-1}(2^k - 1)$$

is perfect and every even perfect number is of this form.

Before reading the proof you may want to review properties of the σ-function we studied in Week 3.

Proof. There are two things to prove here. First let's prove that if

$$n = 2^{k-1}(2^k - 1),$$

and $2^k - 1$ is prime, then n is perfect. This is done by computing $\sigma(n)$ using multiplicativity:

$$\sigma(n) = \sigma(2^{k-1})\sigma(2^k - 1) = \frac{2^k - 1}{2 - 1}(2^k) = 2^k \cdot (2^k - 1) = 2n.$$

This proves the first claim (all numbers given by the formula are perfect).

The second thing to prove is that if n is even and perfect, then n is given by the above formula for some k. This takes more effort.

First of all we factor n using the Fundamental Theorem of Arithmetic:

$$n = 2^{k-1} \cdot x, \ k \geq 1$$

to give it a look like in the formula we want to prove. Here x is some odd number, not necessarily prime.

Now we compute using multiplicativity of σ:

$$\sigma(n) = \sigma(2^{k-1})\sigma(x) = \frac{2^k - 1}{2 - 1}\sigma(x) = (2^k - 1)\sigma(x).$$

On the other hand since n is perfect, we have by definition

$$\sigma(n) = 2n = 2^k x.$$

We equate the two expressions for $\sigma(n)$:

$$(2^k - 1)\sigma(x) = 2^k x \quad (\star)$$

The equation $(\star)$ is our condition for our integer $n = 2^{k-1} \cdot x$ to be a perfect number. We will play with this condition until we get the result.

Since the LHS of $(\star)$ is divisible by 2^k-1, the RHS must also be divisible by 2^k-1, however since $\gcd(2^k, 2^k-1)=1$, we must have

$$2^k-1 \mid x \implies x=(2^k-1)y,\ y\in\mathbb{N}.$$

We get

$$n=2^{k-1}x=2^{k-1}(2^k-1)y.$$

This is a formula for our even perfect number n which is very close to what we need to prove. In fact, what we need to prove is that $y=1$.

We summarize what we have:

$$\begin{cases} x=(2^k-1)y \\ \sigma(x)=y\cdot 2^k \end{cases}$$

Here the second formula follows from equation $(\star)$ after substituting $x=(2^k-1)y$.

Let us prove that this is only possible when $y=1$ and 2^k-1 is a prime. Indeed, since y and $x=(2^k-1)y$ are divisors of x (possibly there are other divisors) we have:

$$\sigma(x)\geq x+y=(2^k-1)y+y=2^ky=\sigma(x).$$

Since the first and the last terms are the same, all inequalities are in fact equalities:

$$\sigma(x)=x+y=(2^k-1)y+y=2^ky=\sigma(x).$$

This implies that x and y are the **only** divisors of x. A number with only two divisors is a prime number, and then its divisors are 1 and itself:

$$x=(2^k-1)y \text{ is prime}$$

and

$$y=1, x=2^k-1.$$

Finally we see that

$$n=2^{k-1}x=2^{k-1}(2^k-1)y=2^{k-1}(2^k-1)$$

and 2^k-1 is prime, as desired.

□

Theorem 108 allows us to list as many perfect numbers as we want.

Exercise 109. *Compute the fifth and the sixth perfect numbers P_5 and P_6 to see that assertions (2) and (3) of Nicomachus are incorrect. (Answer: $P_5=33,550,336$, $P_6=8,589,869,056$). You may use a calculator here.*

Furthermore Theorem 108 may be used to find out about different properties of even perfect numbers. For example, we have a statement, correcting Nicomachus' assertion (2):

Theorem 110. *An even perfect number n ends in the digit 6 or 8; that is*

$$n\equiv 6 \pmod{10} \quad \text{or} \quad n\equiv 8 \pmod{10}.$$

Proof. Let n be an even perfect number. By Theorem 108, it has the form:

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

By the Chinese Remainder Theorem to obtain the remainder of n modulo 10 we need to work out $n \pmod 2$ and $n \pmod 5$. Since n is even, $n\equiv 0 \pmod 2$. We now need to compute the remainder of n modulo 5.

We make a little table based on the value of $s = 2^{k-1} \pmod 5$. In terms of s we have

$$n = 2^{k-1}(2^k - 1) = s(2 \cdot 2^{k-1} - 1) = s(2s - 1).$$

So here is our table:

$s \pmod 5$	$2s - 1 \pmod 5$	$n = s(2s-1) \pmod 5$
1	1	1
2	3	1
3	0	N/A
4	2	3

I have not listed $s \equiv 0 \bmod 5$, since $s = 2^{k-1}$ is never divisible by 5. I also wrote N/A (not applicable) in the third row, since $2^k - 1 = 2s - 1$ is a prime by assumption, hence is never divisible by 5.

The summary is that possible remainders of n modulo 5 are

$$n \equiv 1, 3 \pmod 5.$$

Putting this together with $n \equiv 0 \pmod 2$ implies by the Chinese Remainder Theorem

$$n \equiv 6, 8 \pmod{10}.$$

□

Unsolved problems on perfect numbers. We do not know the answers to following questions:

(1) Do **odd** perfect numbers exist?
- They either do not exist or are very rare
- No odd perfect numbers in the range $1 \leq n \leq 10^{1500}$
- Odd perfect numbers (if they exist) have at least 101 prime factors

(2) Are there **infinitely many** perfect numbers?
- By Theorem 108 even perfect numbers are in bijection with primes $2^k - 1$ (these are called Mersenne primes, see next section)
- Are there infinitely many such primes?

21. Mersenne primes

Lemma 111. *If $a^k - 1$ is prime ($a > 0$ and $k \geq 2$), then $a = 2$ and k is also a prime.*

Proof. We first prove that if $a^k - 1$ is a prime, then $a = 2$. I factor:

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

Thus if $a - 1 > 1$, i.e. $a > 2$, we have a non-trivial divisor

$$(a-1) \mid (a^k - 1).$$

I proved that if $a > 2$, then $a^k - 1$ is composite, this is the contrapositive for our statement; so we are done.

Now I prove that if $a^k - 1$ is prime, then k is prime. Again, I do contrapositive: assuming that k is composite, I prove that $a^k - 1$ is composite. We assume $k = mn,\ m, n > 1$. Then we compute:

$$a^k - 1 = a^{mn} - 1 = (a^m)^n - 1 = (a^m - 1)((a^m)^{n-1} + \cdots + (a^m)^2 + a^m + 1),$$

leading to $a^k - 1$ being a composite number. □

Definition 112. *The numbers $M_k = 2^k - 1$ ($k \geq 1$) are called* **Mersenne numbers**. *Primes among the M_k's are called* **Mersenne primes**.

Mersenne primes. By Lemma 111 we know that

$$M_k \text{ prime} \implies k \text{ prime}.$$

The first Mersenne primes are

$$M_2 = 3, M_3 = 7, M_5 = 31, M_{13} = 8191$$

but **not all** M_p are prime:

$$M_{11} = 23 \times 89, \quad M_{23} = 47 \times 178,481.$$

It is not known if there are infinitely many of the Mersenne primes. Only 48 Mersenne primes have been found. The largest one, $M_{57,885,161}$, found on Jan. 25, 2013, contains more than 17 million digits. This is also the largest prime known as of today. Google: Great Internet Mersenne Prime Search (GIMPS).

Divisors of the Mersenne numbers M_p.

Theorem 113. *If p is an odd prime, then any divisor of M_p is of the form*

$$d = 2kp + 1, k \in \mathbb{N}.$$

Proof. We need to show:

$$d \equiv 1 \pmod{2p}.$$

We factor $d = q_1^{k_1} \cdots q_r^{k_r}$. If we show that for any q_i, which are also divisors of M_p the condition is satisfied, i.e. we have

$$q_i \equiv 1 \pmod{p},$$

this would imply that the condition is also satisfied for d:

$$d \equiv q_1^{k_1} \cdots q_r^{k_r} \equiv 1^{k_1} \cdots 1^{k_r} \equiv 1.$$

Thus, we may assume $d = q$ is a prime divisor of M_p. The crucial point in the proof is this:

$$q \mid M_p \iff q \mid (2^p - 1) \iff 2^p \equiv 1 \pmod{q}.$$

This turns to be the question about the order of 2 modulo q. We have learnt quite a bit about orders in Week 4. In particular:

$$2^p \equiv 1 \pmod{q} \iff (\text{ord}(2)) \mid p.$$

(see "Which powers of a group element give the neutral element" Lemma in Week 4).

Since p is a prime and $\text{ord}(2) \neq 1$, in fact we have

$$\text{ord}(2) = p.$$

(all the orders in this proof are taken in $\mathbb{Z}_q^\star$). Very good.

Another fact we may use is that orders of elements in $\mathbb{Z}_q^\star$ divide $q - 1$ (see Lagrange's Theorem in Week 4):

$$p = \text{ord}(2) \mid q - 1.$$

This is the same as

$$q - 1 = mp, \ m \in \mathbb{Z},$$

i.e.

$$q = mp + 1.$$

This is very close to what we want. To get the desired expression, let's note that m is even (otherwise, if m was odd, we would have an odd number $+1$ in the RHS, which would imply q is even, i.e. $q = 2$, but this is not a divisor of M_p, since M_p itself is odd).

We have

$$m = 2k \implies q = 2kp + 1.$$

□

In the next three examples we use the Theorem to find out whether M_{11}, M_{13} and M_{23} are prime.

Example 114. *According to Theorem 113 divisors of $M_{11} = 2047$ have the form*

$$d = 22k + 1.$$

The first candidate is $d = 23$, and we check that

$$2047 = 23 \times 89$$

is the prime factorization of M_{11}.

Example 115. *According to Theorem 113 divisors of $M_{13} = 2^{13} - 1$ have the form*

$$d = 26k + 1 = 27, 53, 79, 105, \ldots$$

We need to check primes up to $\sqrt{M_{13}}$, and without using a calculator a reasonably good bound for the square root may be computed as

$$\sqrt{M_{13}} = \sqrt{2^{13} - 1} < \sqrt{2^{13}} = 2^{\frac{13}{2}} = 2^6\sqrt{2} < 2^6 \cdot 1.5 = 96.$$

Thus either M_{13} is prime, or it is divisible by one of the smaller primes:

$$q = 53, 79.$$

To test each of the two primes we compute $2^{13} \pmod q$. One can find out that

$$2^{13} \equiv 30 \not\equiv 1 \pmod{53}$$
$$2^{13} \equiv 55 \not\equiv 1 \pmod{79}$$

and see thus M_{13} is not divisible by $q = 53, 79$, implying that M_{13} is prime.

Example 116. *According to Theorem 113 divisors of $M_{23} = 2^{23} - 1$ have the form*

$$d = 46k + 1 = 47, 93, 139, 185, \ldots$$

Among these first four candidates only 47 and 139 are primes.

We need to check primes up to $\sqrt{M_{23}}$, and without using a calculator a reasonable bound for the square root may be computed as

$$\sqrt{M_{23}} = \sqrt{2^{23} - 1} < \sqrt{2^{23}} = 2^{\frac{23}{2}} = 2^{11}\sqrt{2} < 2047 \cdot 1.5 < 3071.$$

This is quite a large bound, so let's just hope M_{23} will be divisible by one of the smaller primes

$$47, 139.$$

In fact a computation shows that

$$2^{23} \equiv 1 \pmod{47}$$

so that

$$47 \mid 2^{23} - 1,$$

and M_{23} is composite.

Remark 117. *One can simplify some of the computations in the examples above using Euler's criterion for quadratic residues from Week 5:*

$$a^{\frac{p-1}{2}} = \pm 1$$

using the Legendre symbol

$$\left(\frac{a}{p}\right).$$

Do you see how this works?

22. Fermat Numbers

We continue our quest for primes given by specific formulas.

Lemma 118. *If $n = 2^m + 1$ is a prime, then $m = 2^k$, i.e.*

$$n = 2^{2^k} + 1.$$

Proof. This is very similar to Lemma 111. I prove the contrapositive: if $m \neq 2^k$, then $n = 2^m + 1$ is composite. What does it mean $m \neq 2^k$? It means that m has an odd prime divisor:

$$m = p \cdot m'.$$

I will rely on factorization:

$$x^p + 1 = (x+1)(x^{p-1} - x^{p-2} + \cdots \pm 1) \quad (\star)$$

which holds for every odd number p (in particular, for an odd prime p).

Now I factor my number $n = 2^m + 1$ using $(\star)$:

$$n = 2^m + 1 = (2^{m'})^p + 1 = (2^{m'} + 1)((2^{m'})^{p-1} - (2^{m'})^{p-2} + \cdots \pm 1)$$

which implies that n is composite.

□

Lemma 118 indicates the importance of the numbers $2^{2^k} + 1$: some of them might be primes!

Definition 119. *Numbers of the form*

$$F_k = 2^{2^k} + 1,\ k \geq 0$$

are called **Fermat numbers**. *Those of the F_k's that are prime are called* **Fermat primes**.

The first 5 Fermat numbers

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65,537$$

are all prime. In fact Fermat himself thought, that all F_k are primes. In a letter to Mersenne, he wrote: "*I have a found that numbers of the form $2^{2^n} + 1$ are always prime numbers...*".

It took Euler (1732) to prove that Fermat was mistaken:

$$641 \mid F_5 = 2^{2^5} + 1 = 4,294,967,297 \implies F_5 \text{ composite!}$$

It follows from the definition that there is a recursion for Fermat's numbers:

$$F_{n+1} = (F_n - 1)^2 + 1. \tag{8}$$

Indeed, the RHS can be computed as:

$$(F_n - 1)^2 + 1 = (2^{2^n} + 1 - 1)^2 + 1 = (2^{2^n})^2 + 1 = 2^{2 \cdot 2^n} + 1 = 2^{2^{n+1}} + 1 = F_{n+1}.$$

There is another recursive formula for the Fermat numbers:

Lemma 120.

$$F_n = F_0 \cdot F_1 \cdots F_{n-1} + 2.$$

Proof. This is a classical proof by induction. Induction base is the $n = 1$ case:

$$5 = F_1 = F_0 + 2 = 3 + 2 = 5.$$

Assume the induction hypothesis:

$$F_n = F_0 \cdot F_1 \cdots F_{n-1} + 2 \quad (\star)$$

and let's prove the same statement with n replaced by $n + 1$.

I subtract 2 from both sides of $(\star)$:

$$F_n - 2 = F_0 \cdot F_1 \cdots F_{n-1},$$

multiply both sides by F_n:

$$(F_n - 2)F_n = F_0 \cdot F_1 \cdots F_{n-1} \cdot F_n,$$

and add 2 to both sides:

$$(F_n - 2)F_n + 2 = F_0 \cdot F_1 \cdots F_{n-1} \cdot F_n + 2.$$

Now in the RHS we have what we wanted. What stands in the LHS?

$$\begin{aligned}(F_n - 2)F_n + 2 &= (F_n^2 - 2F_n + 1) + 1 = \\ &= (F_n - 1)^2 + 1 = \\ &= F_{n+1}\end{aligned}$$

using formula (8). We are done! □

An interesting property of Fermat numbers:

Theorem 121. *For Fermat numbers F_n, F_m with $m \neq n \geq 0$ we have*

$$\gcd(F_m, F_n) = 1.$$

Proof. We do the proof by contradiction. Assume that a prime p divides both F_m and F_n. Note that by definition Fermat numbers are all odd, hence p is also an odd prime.

Assume that $n > m$ and apply Lemma 120:

$$F_n = F_0 \cdot F_1 \cdots F_m \cdots F_{n-1} + 2,$$

and rewrite this as

$$2 = F_n - F_0 \cdot F_1 \cdots F_m \cdots F_{n-1}.$$

Since p divides F_n and F_m, it divides both terms in the RHS, hence

$$p \mid 2.$$

This is not possible: p is an odd prime!

□

Remark 122. *This property of the Fermat numbers is quite intriguing and can lead to unexpected results. For example, we can deduce Euclid's Theorem on infinitude of primes. Indeed, let*

$$p_n \mid F_n, \quad n = 0, 1, 2, \ldots$$

be any prime divisor. Then by the Theorem

$$n \neq m \implies p_n \neq p_m.$$

Now the sequence

$$p_0, p_1, p_2, \dots$$

is an infinite sequence of primes!

It is also interesting to mention that for large values of n we can't actually compute what p_n is. For example, we do not know the value of p_{33} (see below).

Unsolved questions on Fermat numbers.

- Are there infinitely many Fermat primes?
- In fact, only F_0, F_1, F_2, F_3, F_4 are known to be primes.
- Is F_k composite for $k \geq 5$?
- As of 2014 it is only known that F_k is composite for $5 \leq k \leq 32$.

Week 8. Diophantine equations
Pythagorean triples
Fermat last theorem
Representing integers as sums of squares

23. Diophantine equations

Definition 123. *A Diophantine equation is an equation*

$$P(x_1, \dots, x_n) = 0$$

where P is a polynomial with integer coefficients and $x_1, \dots, x_n \in \mathbb{Z}$.

Diophantine equations are named after the Greek mathematician Diophantus (200-300 AD). The major work of Diophantus on algebra and equations, *"Arithmetica"*, which deals in particular with equations of this sort, gave inspiration to P. Fermat in his work on Number Theory.

Example 124. *Linear congruence $ax \equiv b \pmod{p}$ is the same as a linear Diophantine equation in two variables:*

$$ax \equiv b \pmod{p} \iff ax + py = b.$$

Example 125. *Pythagorean triangle equation: $x^2 + y^2 = z^2$.*

Example 126. *Fermat's equation: $x^n + y^n = z^n$.*

Example 127. *Representing an integer m as a sum of two squares can be thought of Diophantine equation $m = x^2 + y^2$.*

We will see another example (Pell's equation) later in this course.

There is no general method for solving Diophantine equations. Furthermore, it is known that such method could not exist! Roughly speaking it is known that any problem or question about a sequence of numbers can be written in a form of a Diophantine equation. Since we know that there are questions that are not possible to decide upon, this implies that we can not solve general Diophantine equations![1]

However, even though there is no general method, some equations can be solved and lead to extremely rich theory. A lot of Number Theory has been developed in attempts to solve Diophantine equations.

[1]Look up Hilbert's 10th problem in the Internet.

24. Pythagorean triples

Definition 128. *A Pythagorean triple is a triple of integers*

$$(x, y, z), \quad x, y, z > 0$$

satisfying

$$x^2 + y^2 = z^2.$$

Example 129. *We have* $3^2 + 4^2 = 5^2$ *and also* $5^2 + 12^2 = 13^2$.

Pythagorean triples appeared in Ancient Greece. The first observation we make is that there are infinitely many Pythagorean triples.

Example 130. *There is a sequence of solutions due to Pythagoras:*

$$(x_n, y_n, z_n) = (2n(n+1), 2n+1, (n+1)^2 + n^2), n \in \mathbb{N}. \tag{9}$$

When we plug in $n = 1, 2$ *into (9) we get the two Pythagorean triples* $(4, 3, 5)$ *and* $(12, 5, 13)$ *of Example 129. I leave it as an exercise for you to check that* $x_n^2 + y_n^2 = z_n^2$ *for* $n \in \mathbb{N}$*, i.e. that*

$$(2n(n+1))^2 + (2n+1)^2 = ((n+1)^2 + n^2)^2.$$

Example 131. *Plato gave another set of solutions:*

$$(x_n, y_n, z_n) = (2n, n^2 - 1, n^2 + 1), \quad n \geq 2. \tag{10}$$

For example, when we plug in $n = 2, 3$ *into (10) the Pythagorean triples we get are*

$$(4, 3, 5), (6, 8, 10).$$

In general we have:

$$x_n^2 + y_n^2 = 4n^2 + (n^2 - 1)^2 = n^4 + 2n^2 + 1 = z_n^2.$$

However, neither (9) nor (10) accounts for all Pythagorean triples. Complete solution is given in Theorem 136 below and depends on two integer parameters.

It is important to make the following remark: if (x, y, z) is a Pythagorean triple and $d \in \mathbb{N}$, then

$$(d \cdot x, d \cdot y, d \cdot z)$$

is also a Pythagorean triple:

$$(dx)^2 + (dy)^2 = d^2(x^2 + y^2) = d^2 z^2 = (dz)^2.$$

Definition 132. *A Pythagorean triple* (x, y, z) *is called* **primitive** *if*

$$\gcd(x, y, z) = 1.$$

[There is no connection to primitive roots here.]

The point is that when we only consider primitive Pythagorean triples we do not loose much:

Lemma 133 (All Pythagorean triples come from primitive ones). *Any Pythagorean triple* (x, y, z) *has the form*

$$(x, y, z) = (d \cdot x_0, d \cdot y_0, d \cdot z_0)$$

where $d \geq 1$ *and* (x_0, y_0, z_0) *is a primitive Pythagorean triple.*

Proof. Let

$$d = \gcd(x, y, z) \text{ and } x_0 = \frac{x}{d},\ y_0 = \frac{y}{d},\ z_0 = \frac{z}{d}.$$

Then (x_0, y_0, z_0) is also a Pythagorean triple:

$$x_0^2 + y_0^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_0^2.$$

Furthermore it is primitive:

$$\gcd(x_0, y_0, z_0) = 1$$

and

$$(x, y, z) = (d \cdot x_0, d \cdot y_0, d \cdot z_0).$$

as required. □

Lemma 134 (**gcd for primitive Pythagorean triples).** *For any primitive Pythagorean triple* (x, y, z) *we have*

$$\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1.$$

Proof. This is because if say $p \mid x, y$, then $z^2 = x^2 + y^2$ implies $p \mid z$, and then (x, y, z) is not primitive as $\gcd(x, y, z) \geq p$.

The considerations for $\gcd(y, z)$ and $\gcd(x, z)$ are similar. □

Lemma 135. *For any primitive Pythagorean triple* (x, y, z) *exactly one of the* x*,* y *is even and the other is odd.*

Proof. We do a proof by contradiction. Assume that x and y are both even or both odd.

If both x and y are even, then the defining equation $z^2 = x^2 + y^2$ implies that z is also even, in which case

$$\gcd(x, y, z) \geq 2$$

which contradicts to our assumption that (x, y, z) is primitive.

If both x and y are odd, we will get a contradiction by considering remainders modulo 4. The only non-zero square modulo 4 is $\overline{1}$, so that

$$x^2, y^2 \equiv 1 \pmod 4.$$

This implies that

$$z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4.$$

This is a contradiction since $\overline{2}$ is not a square modulo 4.

□

Now we formulate and prove the main theorem on Pythagorean triples. In conjunction with Lemmas 133, 135 it describes all of them.

Theorem 136 (**Parametrization for Pythagorean triples).** *All primitive Pythagorean triples* (x, y, z) *with* x *even and* y *odd are given by the formulas*

$$\begin{cases} x = 2st \\ y = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

where

- $s, t \in \mathbb{N}$ *such that* $s > t > 0$*,*
- $\gcd(s, t) = 1$*,*

- $s \not\equiv t \pmod 2$.

The latter condition on s, t should be read as: one of the s,t is even and the other is odd.

For the proof we will need the following lemma, describing "rational Pythagorean triples":

Lemma 137. *Solutions of $u^2 + v^2 = 1$, $u, v \in \mathbb{Q}$ are parametrized by*

$$u = \frac{2s}{s^2+1}, \quad v = \frac{s^2-1}{s^2+1}, \quad s \in \mathbb{Q} \cup \{\infty\}.$$

(Note that when $s = \infty$, we take u, v as their limiting values: $u = 0, v = 1$.)

Proof. Let $(u, v) \in \mathbb{Q}^2$ be a solution of $u^2+v^2 = 1$, i.e. a point on a circle with rational coordinates. Make a line L through (u, v) and $(0, 1)$, another point on the same circle, and let us call $(s, 0)$, $s \in \mathbb{Q}$ the intersection point of L with the horizontal axis (make a drawing!).

This establishes the bijection between solutions (u, v) and the set $\mathbb{Q} \cup \{\infty\}$ (the $s = \infty$ corresponds to the case when $L_{u,v}$ does not intersect the horizontal axis, so L is the horizontal tangent line to the circle at $(u, v) = (0, 1)$).

Now we simply compute which point (u, v) corresponds to the parameter $s \in \mathbb{Q}$. For that we need to make a line through $(0, 1)$ and $(s, 0)$:

$$y = -\frac{x}{s} + 1$$

and intersect this line with the circle $x^2 + y^2 = 1$:

$$\begin{cases} y = -\frac{x}{s} + 1 \\ x^2 + y^2 = 1 \end{cases}$$

After some computation we get an equation for y in terms of s:

$$y^2 - \frac{2s^2}{s^2+1}y + \frac{s^2-1}{s^2+1} = 0,$$

and find that the roots of this equation are $y = 1$ and $y = \frac{s^2-1}{s^2+1}$. This gives rise to our original point $(0, 1)$ and another point on the circle:

$$(u, v) = \Big(\frac{2s}{s^2+1}, \frac{s^2-1}{s^2+1}\Big).$$

We are done because we've seen that rational points (u, v) on the circle correspond to parameters $s \in \mathbb{Q} \cup \{\infty\}$, with the point (u, v) is given by the formula above. The limiting case $s = \infty$ beautifully corresponds to $(0, 1)$. □

Proof of the Theorem about Primitive Pythagorean triples. Let (x, y, z) be a primitive Pythagorean triple. Consider $u = \frac{x}{z}$, $v = \frac{y}{z}$ (note that $z \neq 0$ by assumption). Then dividing the equation $x^2 + y^2 = z^2$ through by z^2 we obtain:

$$x^2 + y^2 = z^2 \iff u^2 + v^2 = 1.$$

Let us introduce the following equivalence relation: $(a, b, c) \sim (a', b', c')$ if $(a', b', c') = (\lambda a, \lambda b, \lambda c)$ for some $0 \neq \lambda \in \mathbb{Q}$. For instance we have:

$$(x, y, z) \sim (\frac{x}{z}, \frac{y}{z}, 1) = (u, v, 1).$$

By the previous Lemma we have a parameter $w \in \mathbb{Q} \cup \{\infty\}$ (we call it w here in order to avoid clash of notation) such that

$$(u, v) = \Big(\frac{2w}{w^2+1}, \frac{w^2-1}{w^2+1}\Big).$$

Note that since u is positive and nonzero same is true for w, so $w = s/t$, $s, t \in \mathbb{N}$, $\gcd(s, t) = 1$. We can write our triple as

$$\begin{aligned}(x, y, z) \sim (u, v, 1) = \Big(\frac{2w}{w^2+1}, \frac{w^2-1}{w^2+1}, 1\Big) \sim \\ \sim (2w, w^2-1, w^2+1) = (2\frac{s}{t}, \frac{s^2}{t^2}-1, \frac{s^2}{t^2}+1) \sim \\ \sim (2st, s^2-t^2, s^2+t^2) \ \text{[here we multiplied every entry by } t^2\text{]}.\end{aligned}$$

If our latter triple is not primitive, then some prime p divides s^2-t^2, s^2+t^2, hence it divides both $2s^2$ (their sum) and $2t^2$ (their difference), so either $p = 2$ or p divides s^2, t^2, in which case it divides both s, t which is impossible as we assumed $\gcd(s, t) = 1$. Thus the only possible common prime divisor of $2st$, s^2-t^2, s^2+t^2 is $p = 2$. This will be the case if s and t are both even (impossible since they are coprime) or s and t are both odd. If s and t are both odd, then we have

$$(x, y, z) \sim (2st, s^2-t^2, s^2+t^2) \sim (st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$$

and since (x, y, z) and $(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$ are primitive equivalent integer triples, they must be equal, in particular $x = st$ is odd, contrary to our assumption.

Thus we see that the only possibility is that one of the s,t is even, the other is odd, and $(2st, s^2-t^2, s^2+t^2)$ is a primitive triple equivalent to our original triple (x, y, z), hence $x = 2st$, $y = s^2-t^2$, $z = s^2+t^2$, and we have our conditions: $s, t > 0$ coprime integers, one even, the other odd. □

Remark 138. *If (x, y, z) are given by the formula in Theorem 136, but the conditions on s, t are not satisfied, then we get a Pythagorean triple, which is not primitive, or has negative entries, or a trivial solution $(x, 0, x)$, $(0, y, y)$. In any case the triple we get for any values of the parameters s, t will be a solution of $x^2+y^2 = z^2$.*

Remark 139. *If one puts $s = n+1, t = n$ (all the three conditions on s, t are satisfied), then*

$$(x, y, z) = (2n(n+1), (n+1)^2-n^2, (n+1)^2+n^2)$$

is a Pythagorean triple of Pythagoras (9).

Remark 140. *Now let us put $s = n, t = 1$. The three conditions on s, t are satisfied as soon as $n > 1$ is even, otherwise we will be getting non-primitive triples. We have:*

$$(x, y, z) = (2n, n^2-1, n^2+1)$$

which is a Pythagorean triple of Plato (10).

Example 141. *We find all primitive Pythagorean triples $(100, y, z)$, $y, z > 0$. We apply Theorem 136. Since 100 is even we consider:*

$$x = 100 = 2st \implies 50 = st \implies (s, t) \in \{(50, 1), (25, 2)\}$$

(recall the conditions on s, t!)

This leads to two primitive Pythagorean triples

$$(s,t) = (50,1) \implies (x,y,z) = (2st, s^2-t^2, s^2+t^2) = (100, 2499, 2501)$$

and

$$(s,t) = (25,2) \implies (x,y,z) = (2st, s^2-t^2, s^2+t^2) = (100, 621, 629)$$

and that's all.

Example 142. *We now find all primitive Pythagorean triples $(x, 21, z)$. Since 21 is odd, x must be even and we apply Theorem 136 as follows:*

$$21 = s^2 - t^2 = (s-t)(s+t).$$

Since $s+t > s-t$ we have two possibilities: either

$$\begin{cases} s+t = 21 \\ s-t = 1 \end{cases}$$

which after adding the equations together implies

$$(s,t) = (11,10)$$

or we have

$$\begin{cases} s+t = 7 \\ s-t = 3 \end{cases}$$

which after adding the equations together implies

$$(s,t) = (5,2).$$

These two pairs lead to two solutions:

$$(s,t) = (11,10) \implies (x,y,z) = (220, 21, 221)$$

and

$$(s,t) = (5,2) \implies (x,y,z) = (20, 21, 29).$$

We are done!

The next example shows how to find all Pythagorean triples containing a prescribed number, not just the primitive ones.

Example 143. *We now use Theorem 136 to find* **all** *Pythagorean triples with $x = 12$. By Lemma 133 any Pythagorean triple $(12, y, z)$ is of the form*

$$(12, y, z) = (d \cdot x_0, d \cdot y_0, d \cdot z_0).$$

Thus

$$d \cdot x_0 = 12.$$

Therefore we need to consider divisors of 12 and look for primitive triples containing $x_0 \mid x$. We may apply Theorem 136 taking into account whether x_0 is even (then we treat it as x) or x_0 is odd (then we treat it as y).

Case $x_0 = 12$, $d = 1$: *We have*

$$x_0 = 2st = 12 \implies st = 6 \implies (s,t) = (3,2), (6,1)$$

(no other possibilities because of the conditions on s, t), which leads to

$$(s,t) = (3,2) \implies (x_0, y_0, z_0) = (2st, s^2-t^2, s^2+t^2) = (12, 5, 13).$$

and

$$(s,t)=(6,1) \implies (x_0,y_0,z_0)=(2st,s^2-t^2,s^2+t^2)=(12,35,37).$$

Case $x_0=6$, $d=2$:

$$x_0=2st=6 \implies st=3 \implies (s,t)=(3,1).$$

This will not give us a primitive triple since $s\equiv t \pmod 2$.

Case $x_0=4$, $d=3$: *We have*

$$x_0=2st=4 \implies st=2 \implies (s,t)=(2,1).$$

which leads to

$$(x_0,y_0,z_0)=(4,3,5) \implies (x,y,z)=(12,9,15).$$

Case $y_0=3$, $d=4$: *Since* 3 *is odd, we treat it as* y*:*

$$3=y_0=s^2-t^2 \implies 3=(s-t)(s+t) \implies \begin{cases} s+t=3, \\ s-t=1 \end{cases} \implies s=2,t=1.$$

In this case we have:

$$(s,t)=(2,1) \implies (x_0,y_0,z_0)=(4,3,5) \implies (x,y,z)=(16,12,20).$$

Case $x_0=2$, $d=6$:

$$x_0=2st=2 \implies st=1.$$

This leads to a trivial solution $(2,0,2)$*. There are no Pythagorean triples with* $x_0=2$*.*

Case $y_0=1$, $d=12$: *There are no Pythagorean triples with* $y_0=1$*. To see this we write*

$$y_0=s^2-t^2 \implies 1=(s-t)(s+t) \implies s-t=1,\ s+t=1.$$

Adding the two equations we get

$$s=1,t=0.$$

We get a trivial triple $(0,1,1)$ *which is not a Pythagorean triple.*

Summary: Pythagorean triples containing 12 *are:* $(12,5,13)$*,* $(12,35,37)$*,* $(12,9,15)$*,* $(16,12,20)$*.*

Theorem 136 makes it very easy to list as many primitive Pythagorean triples as we want: we may simply plug in any s,t satisfying the conditions. Some of the primitive Pythagorean triples are given in the table:

		x	y	z
s	t	$2st$	s^2-t^2	s^2+t^2
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

By looking for divisibility patterns in this table we notice the following facts:

- Exactly one of the x, y is even (Lemma 135).
- Exactly one of the x, y is divisible by 3.
- Exactly one of the x, y, z is divisible by 5.

Can you notice and prove any other divisibility patterns? We prove these and other divisibility properites of Pythagorean triples in the problem sheet.

As we've seen, a lot is known about Pythagorean triples and their properties. We list some unsolved problems:

(1) There are Pythagorean triples which include two primes:

$$(\mathbf{3}, 4, \mathbf{5}),\ (\mathbf{5}, 12, \mathbf{13}),\ (\mathbf{11}, 60, \mathbf{61}),\ (\mathbf{19}, 180, \mathbf{181})\dots$$

Are there infinitely many?

(2) There are Pythagorean triples of the form (x^2-1, y^2-1, z^2-1):

$$(10^2-1, 13^2-1, 14^2-1),\ (265^2-1, 287^2-1, 329^2-1), \dots$$

Are there infinitely many?

(3) There are Pythagorean triples of **triangular numbers** $\frac{n(n+1)}{2}$:

$$(\frac{132\cdot 133}{2}, \frac{143\cdot 144}{2}, \frac{164\cdot 165}{2}).$$

Are there infinitely many?

Exercise 144. *Run a computer search (e.g. using Python) and make a conjecture whether you think there are infinitely many Pythagorean triples as above.*

25. Fermat's Last Theorem

In 1625 P. Fermat left a note on the margin of his copy of Diophantus' "Arithmetica", claiming that he can show that $x^n + y^n = z^n$ has no integer solutions except for the trivial ones (in this case trivial means: one of the x, y, z is zero). Fermat has only written a proof for $n = 4$.

In the several centuries that followed, this problem attracted professionals and amateurs alike. Mathematicians such as Euler, Gauss and Legendre successfully did the cases $n = 3, 4, 5$.

Plenty of incorrect proofs for general n have been given, but some of these were useful as well. In the 19th century, Kummer introduced ideals in number fields after Lamè's incorrect proof of Fermat's Last Theorem using unique factorization in rings more general than $\mathbb{Z}$. This led to a proof of many other cases, in particular, all $n < 100$ except for $n = 37, 59, 67$.

In the 20th century, questions about Diophantine equations, in particular Fermat's Last Theorem became embodied into a field of Arithmetic Geometry. From this perspective the integer solutions of equations like Fermat's equation are treated as a subset of complex or real solutions of the same equation, and thus can be approached by means of geometry. Using these geometric methods a lot of progress has been made. Faltings' 1983 proof of the 1920 conjecture of Mordell implied that the number of non-trivial integer solutions

$$x^n + y^n = z^n$$

is finite! Also, it was known that Fermat's Last Theorem would follow once the so-called Taniyama-Shimura Modularity Conjecture is established.

When Fermat's Last Theorem finally has been settled in 1995 the proof was not simply a smart trick, and not an extension of a methods known to Fermat, Euler or Gauss, but a combination of powerful 20th century techniques in Number Theory, Arithmetic Geometry, Algebra and Analysis.[2]

Theorem 145 (Fermat's Last Theorem, proved by Andrew Wiles 1995)**.** *Let $n > 2$ be an integer. Then the equation*

$$x^n + y^n = z^n$$

has no solution in positive integers x, y, z.

Remark 146. *The theorem is proved, but this is not the end of the story. For example, what happens if instead of looking for solutions of the Fermat equation in $\mathbb{Z}$ we look at other rings?*

$$(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3.$$

In 2004 Frazer Jarvis (Senior Tutor at the School of Mathematics and Statistics) and Paul Meekin have shown that there are no non-zero solutions of

$$x^n + y^n = z^n$$

in $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ when $n > 3$.

26. Representing integers as sums of squares

In this section we answer the following question: which integers can be represented as a sum of two integer squares. For instance we have $1 = 1^2 + 0^2, 2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $8 = 2^2 + 2^2$ but obviously 3, 6 or 7 are not sums of two squares.

To deal with this problem it helps to know that if n is a sum of two squares and m is a sum of two squares, then same is true for their product nm.

Lemma 147 (Product of sums of two squares is a sum of two squares)**.** *We have $(x^2+y^2)(u^2+v^2) = (xu + yv)^2 + (xv - yu)^2$.*

Proof. Proof is a simple direct computation. A better proof though is to use complex numbers and to let $z = x + iy$, $w = u - iv$, so that $zw = (xu + yv) - i(xv - yu)$ and to notice that

$$(xu + yv)^2 + (xv - yu)^2 = |zw|^2 = |z|^2|w|^2 = (x^2 + y^2)(u^2 + v^2).$$

[2]It is worth seeing the BBC - Horizon 1995-1996 Fermat's Last Theorem movie about Andrew Wiles and his proof.

□

Example 148. *We may use the identity in the Lemma to express* $85 = 17 \cdot 5$ *as a sum of two squares:*

$$17 = 4^2 + 1^2$$
$$5^2 = 2^2 + 1^2$$

so we should put $(x, y) = (4, 1)$, $(u, v) = (2, 1)$ *so that*

$$(xu + yv, xv - yu) = (8 + 1, 4 - 2) = (9, 2)$$

and indeed $9^2 + 2^2 = 85$. *Well done!*

Lemma 147 above hints that when studying representations of integers as sums of two squares, it is natural to concentrate on representing primes first:

Lemma 149. *A prime* p *is a sum of two squares if and only if* $p = 2$ *or* $p \equiv 1 \pmod 4$.

Proof. If $p = 2$, then $p = 1^2 + 1^2$, so we may assume that p is odd. Now if $p = x^2 + y^2$, then taking this equality modulo p we see that $x^2 + y^2 = 0$ has a solution in $\mathbb{Z}_p$, hence dividing by y (y and p are coprime!) we deduce that $\left(\frac{-1}{p}\right) = 1$. This implies that $p \equiv 1 \pmod 4$ (see Problem sheet for Week 5).

Conversely, we need to show that if $p \equiv 1 \pmod 4$, then p can be represented as a sum of two squares. We do this by using so-called Infinite Descent. First of all, since $p \equiv 1 \pmod 4$ we have $\left(\frac{-1}{p}\right) = 1$, hence $x^2 \equiv -1 \pmod p$ admits a solution, the fact we'd like to write as:

$$x_0^2 + y_0^2 = kp,\ x_0, y_0 \in \mathbb{Z},\ 0 < k < p.$$

If $k = 1$, we are done. The Infinite Descent method consists in finding a pair of integers (x_1, y_1) which would satisfy $x_1^2 + y_1^2 = k'p$, for $0 < k < k'$, hence after a sequence of steps we would find a solution of $x^2 + y^2 = p$.

We start by replacing x_0, y_0 with their smallest representatives modulo k:

$$x_0 \equiv u \pmod k,\ 0 \le u < k < p$$
$$y_0 \equiv v \pmod k,\ 0 \le v < k < p,$$

and we have $u^2 + v^2 \equiv x_0^2 + y_0^2 = kp \equiv 0 \pmod k$, hence

$$u^2 + v^2 = k'k,$$

with $k' < k$ (since ...). Now we multiply our sums of squares together and use the identity from Lemma 147:

$$(x_0u + y_0v)^2 + (x_0v - y_0u)^2 = (x_0^2 + y_0^2)(u^2 + v^2) = k' \cdot k^2 \cdot p. \tag{11}$$

Now we notice that both terms $x_0u + y_0v$ and $x_0v - y_0u$ are divisible by k:

$$x_0u + y_0v \equiv x_0^2 + y_0^2 \equiv 0 \pmod k$$
$$x_0v - y_0u \equiv x_0y_0 - x_0y_0 \equiv 0 \pmod k$$

and we put

$$x_1 = \frac{x_0u + y_0v}{k},\ x_2 = \frac{x_0v - y_0u}{k}.$$

which now can be seen to satisfy (dividing (11) by k^2)

$$x_1^2 + y_1^2 = k'p.$$

Since $0 < k' < k$ we may proceed with our Infinite Descent until we find a solution of $x^2 + y^2 = p$. □

Theorem 150 (Representing integers as sums of two squares)**.** *The equation*

$$x^2 + y^2 = m$$

has an integer solution if and only if each prime factor of m congruent to 3 modulo 4 occurs to an even power in the prime factorization of m.

Proof. See Problem Sheet. □

Remark 151. *Not every positive integer is a sum of 3 squares. For instance it is easy to verify that 39 not a sum of three squares. However, one can use Infinite Descent to show that every positive integer is a sum of 4 squares. More generally we can ask whether all positive integers can be represented by sums of k'th powers:*

$$m = x_1^k + \cdots + x_g^k$$

and to let $g(k)$ the smallest number of summands that will work for any m. This is known as Waring problem. For instance Waring himself has proved in 1770 that $g(2) = 4$, $g(3) = 9$, $g(4) = 19$. In 1909 Hilbert was first to show that g exists for all k.

Week 9. Generating functions
Fibonacci and Catalan numbers
Partitions

This week we study sequences $a_0, a_1, \ldots$ and their generating functions. In particular we define recursively Fibonacci numbers and Catalan numbers, and obtain formulas for them and their generating functions. Finally we study partition numbers and various partition functions.

The material this week is mostly independent from the rest of the module.

27. Generating functions

Let a_n, $n = 0, 1, 2, \ldots$ be a sequence we'd like to study. One powerful technique is to encode the sequence in a **generating function**

$$A(q) = \sum_{n \geq 0} a_n q^n = a_0 + a_1 q + a_2 q^2 + \ldots$$

Note that we consider the power series above formally, i.e. we do not care whether it actually converges or not.

Example 152. *Let $a_n = 1$ be the constant sequence. Then its generating function is the infinite geometric series:*

$$A(q) = 1 + q + q^2 + \cdots = \sum_{n \geq 0} q^n = \frac{1}{1-q}.$$

Similarly, for a sequence

$$1, 0, 1, 0, 1, 0, \ldots$$

the generating function is

$$1 + q^2 + q^4 + \cdots = \frac{1}{1-q^2}.$$

Note the effect of replacing q by q^2 in the generating series: the terms of the sequence get spread out and put on the even positions, whereas the odd positions have zeros.

We introduce a new piece of notation, $O(q^n)$. This stands for terms of degree n and higher. For instance depending on what we are trying to compute, we may write the familiar Taylor expansions for the geometric series as follows:

$$\frac{1}{1-q} = 1 + O(q)$$
$$\frac{1}{1-q} = 1 + q + O(q^2)$$
$$\frac{1}{1-q} = 1 + q + q^2 + O(q^3)$$

and similarly for the exponential function:

$$e^q = 1 + O(q)$$
$$e^q = 1 + q + O(q^2)$$
$$e^q = 1 + q + \frac{q^2}{2!} + O(q^3)$$

and on. Even though we consider our power series formally, it is useful to imagine that q is small, so that $O(q^n)$ stands for terms of order of magnitude smaller or equal to q^n.

Example 153. *Let us consider the power series* $\frac{1}{(1-q)(1-q^2)}$ *and ask what is the corresponding sequence of coefficients? For that we can start out by finding for instance the first five terms of the sequence, that is we compute the terms of our generating series up to and including* q^4.

We have a product of two geometric series

$$\frac{1}{(1-q)(1-q^2)} = (1 + q + q^2 + q^3 + q^4 + O(q^5))(1 + q^2 + q^4 + O(q^5)) =$$
$$= 1 + q + 2q^2 + 2q^3 + 3q^4 + O(q^5).$$

Note that while making computations we systematically ignore all terms of degree 5 *and above by putting them under* $O(q^5)$.

We see that the sequence of coefficients starts with

$$1, 1, 2, 2, 3, \ldots$$

and we can make a guess what the sequence is. Later in this chapter we actually prove that this guess is correct (see Example 161).

Example 154. *Let* $b_n = \binom{N}{n}$ *for some fixed* N. *Note that by definition* $a_n = 0$ *for* $n > N$. *The generating function for* b_n *is*

$$B(q) = \sum_{n \geq 0} \binom{N}{n} q^n = (1 + q)^N.$$

This is the Binomial Theorem, and the generating series $(1 + q)^N$ *can be used to prove various facts about the binomial coefficients.*

28. Recursive sequences

In this section we show how generating functions allow finding formulas for recursive sequences. We consider two examples: the Fibonacci numbers and the Catalan numbers.

Let u_n be **the Fibonacci sequence** defined by setting

$$u_1 = u_2 = 1$$

and for $n \geq 2$:

$$u_{n+1} = u_n + u_{n-1}.$$

Note that the defining equation holds true for all $n \in \mathbb{Z}$ if we define $u_n = 0$ for $n \leq 0$.

Thus the Fibonacci sequence starts with

$$u_0 = 0, u_1 = 1, u_2 = 1, u_3 = 2, u_4 = 3, u_5 = 5, u_6 = 8, u_7 = 13, u_8 = 21, \ldots. \tag{12}$$

Let $U(q)$ be the generating function for the Fibonacci sequence. It turns out that the recursive definition of the u_n leads to a nice equation for $U(q)$.

Proposition 155. *We have the following expression:*

$$U(q) = \frac{q}{1 - q - q^2}$$

Proof. By definition $U(q)$ is the generating function of the sequence

$$0, 1, 1, 2, 3, \ldots.$$

Let us ask ourselves what is $qU(q)$ the generating function for? All the coefficients get shifted one to the right, so $qU(q)$ is the generating function for

$$0, 0, 1, 1, 2, 3, \ldots.$$

Similarly $q^2U(q)$ is the generating function for

$$0, 0, 0, 1, 1, 2, 3, \ldots.$$

Now let us write the definition of the Fibonacci sequence as an identity for $U(q)$. We'd like to write something like: every term of the sequence is a sum of the two shifted terms, or $U(q) = qU(q) + q^2U(q)$. This is not quite correct though as the first term is an exception. In fact we have:

$$U(q) - q = qU(q) + q^2U(q).$$

Solving this equation for $U(q)$ we get $U(q) = \frac{q}{1-q-q^2}$. □

Using the generating function we deduce Binet's formula (1843) for the Fibonacci numbers:

$$u_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}, \; n \geq 0.$$

Although the formula involves $\sqrt{5}$, each u_n is a nonnegative integer so the $\sqrt{5}$'s cancel out. For example:

$$u_1 = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right) \right\} = \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1.$$

The number

$$\frac{1+\sqrt{5}}{2} = 1.6180339887...$$

is the so-called Golden Ratio. Fibonacci numbers and the Golden ratio are used in painting and architecture to create proportion pleasant to a human eye[3]. The precise relation between the Fibonacci numbers and the Golden ratio is

$$\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \frac{1+\sqrt{5}}{2}.$$

We now consider another recursive sequence, given by the **Catalan numbers** C_n. There are several combinatorial ways to define this sequence. For our purposes we start with the following recursive definition: we set $C_0 = 1$ and

$$C_{n+1} = \sum_{i=0}^{n} C_i \cdot C_{n-i}, \text{ for } n \geq 0.$$

The sequence starts with

$$C_0 = 1, C_1 = 1, C_2 = 2, C_3 = 5, C_4 = 14, C_5 = 42.$$

As with the Fibonacci sequence we may first compute the generating series for the Catalan numbers, and then deduce the formula for C_n. Let $C(q)$ be the generating series.

Proposition 156. *We have the following expression:*

$$C(q) = \frac{1-\sqrt{1-4q}}{2q}.$$

Here the square root is the formal one, that is the one given by its Taylor series

$$\sqrt{1-4q} = \sum_{i\geq 0} \binom{1/2}{i} (-4q)^i$$

where $\binom{1/2}{i} = \frac{1/2\cdot(1/2-1)\cdots(1/2-i+1)}{i!}$.

Using the generating function one can prove the following formula for the Catalan numbers:

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

This formula, as well as proof of Proposition 156 is left to problem sheet.

29. Partitions

We consider the following problem: how many ways are there to represent a positive integer n as a sum of positive integers? For instance we have 5 ways of representing 4 as a sum: $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$.

Definition 157. *A partition of $n > 0$ is a sequence $n_1 \geq n_2 \geq \cdots \geq n_r$ of positive integers such that*

$$n = n_1 + n_2 + \cdots + n_r.$$

r is called the number of parts and n is called the weight of the partition.

[3]For examples in classical art see `http://www.goldennumber.net/art-composition-design/` and for use in photography see `http://www.1stwebdesigner.com/design/eight-photography-effects/`

We denote p_n the number of partitions of n, and sometimes refer to p_n's as **partition numbers**. We've seen above that $p_4 = 5$. In the problem sheet we will verify that the first values of p_n are

$$p_1 = 1,\ p_2 = 2,\ p_3 = 3,\ p_4 = 5,\ p_5 = 7,\ p_6 = 11.$$

By convention we have $p_0 = 1$.

In fact there is no formula for p_n and it is hard to say anything about individual p_n: it is much easier to work with the generating function

$$P(q) = \sum_{n\geq 0} p_n q^n = 1 + q + 2q^2 + 3q^3 + 5q^4 + \dots,$$

which we call the **partition function**.

Let us introduce the following version of partition numbers. For any subset $S \subset \mathbb{N}$ we denote by $p_{n,S}$ the number of partitions of n with parts taken from S. For instance $p_{n,\{1,2,3\}}$ is the number of partitions of n into parts 1, 2, 3. The usual partition number is obtained when $S = \mathbb{N}$: $p_n = p_{n,\mathbb{N}}$.

We let $P_S(q) = \sum_{n\geq 0} p_{n,S} q^n$. Our goal is to compute $P_S(q)$ for any set S. We start with the simplest case when S consists of a single element:

Lemma 158. *For a positive integer k and $S = \{k\}$ we have*

$$p_{n,S} = \begin{cases} 1, & k \text{ divides } n \\ 0, & \text{otherwise} \end{cases}$$

and

$$P_S(q) = \frac{1}{1-q^k}.$$

Proof. By definition $p_{n,S}$ counts number of ways to partition n into parts of size k. Thus if k divides n there is one way, otherwise there is none. This is exactly the claimed formula for $p_{n,S}$.

Now for the generating series we get

$$P_S(q) = 1 + q^k + q^{2k} + q^{3k} + \dots = \frac{1}{1-q^k}$$

using the infinite geometric series. □

Lemma 159. *If two sets $S_1, S_2 \subset \mathbb{N}$ do not intersect, then*

$$P_{S_1 \cup S_2}(q) = P_{S_1}(q) \cdot P_{S_2}(q). \tag{13}$$

Proof. The key step in the argument is the formula

$$p_{n,S_1\cup S_2} = \sum_{i+j=n} p_{i,S_1} \cdot p_{j,S_2}.$$

This holds for the following reason: if we count the number of ways to partition n into parts coming from S_1 and S_2 and these two sets are disjoint, then we need to specify the parts that belong to S_1 and the parts that belong to S_2. We can group the parts belonging to S_1 and let them sum up to i and group the parts belonging to S_2 and let them sum up to j. For such partitions the total number is $p_{i,S_1} \cdot p_{j,S_2}$ and then we must sum up over $i + j = n$.

To prove the Lemma let us start at the RHS:

$$\begin{aligned} P_{S_1}(q)\cdot P_{S_2}(q) &= \left(\sum_{i\geq 0} p_{i,S_1}q^i\right)\cdot\left(\sum_{j\geq 0} p_{j,S_2}q^j\right) = \\ &= \sum_{i,j\geq 0} p_{i,S_1}\cdot p_{j,S_2}q^{i+j} = \\ &= \sum_{n\geq 0}\left(\sum_{i+j=n} p_{i,S_1}\cdot p_{j,S_2}\right)q^n = \\ &= \sum_{n\geq 0} p_{n,S_1\cup S_2}q^n = P_{S_1\cup S_2}(q). \end{aligned}$$

□

Lemma 160. *Let N be a positive integer and let $S=\{1,2,\ldots,N\}$. Then for the partition function with parts bounded above by N we have*

$$P_{\{1,2,\ldots,N\}}(q)=\prod_{k=1}^{N}\frac{1}{1-q^k}.$$

Proof. Using inductively the formula (13) we get

$$P_{\{1,2,\ldots,N\}}(q)=P_{\{1\}}(q)P_{\{2\}}(q)\cdots P_{\{N\}}(q)$$

and now by Lemma 158 we obtain

$$P_{\{1,2,\ldots,N\}}(q)=\frac{1}{1-q}\cdot\frac{1}{1-q^2}\cdots\frac{1}{1-q^N}$$

and this is what we had to prove. □

Example 161. *We consider the generating function $\frac{1}{1-q}\cdot\frac{1}{1-q^2}$ from Example 153. According to Lemma 160 with $N=2$ this is the generating function $P_{\{1,2\}}(q)$ for partition numbers $p_{n,\{1,2\}}$ into parts of size 1 and 2.*

We can determine such a partition by specifying how many 2's it contains. For instance we have

$$5=2+2+1=2+1+1+1=1+1+1+1+1$$

having two, one or none 2's and the rest is partitioned into 1's. Thus to specify the sequence $p_{n,\{1,2\}}$ the question we need to answer is this: what's the maximal number of 2's which can enter a partition of n. The answer to this question is $\left[\frac{n}{2}\right]$, and since we allow any number of 2's between zero and $\left[\frac{n}{2}\right]$ we get

$$p_{n,\{1,2\}}=\left[\frac{n}{2}\right]+1$$

and this generates the sequence

$$1,1,2,2,3,3,\ldots$$

we guessed in Example 153.

We now state the result for the partition function, recall that this means that $S=\mathbb{N}$, i.e. we allow arbitrary parts.

Theorem 162. *For the partition function we have*

$$P(q) = \prod_{k\geq 1} \frac{1}{1-q^k}.$$

Remark 163. *The infinite product may look scary: it seems that we have to multiply infinitely many terms. However, for every given coefficient p_n we need to multiply only finitely many terms. For instance for the term up to p_4 we need to compute*

$$P(q) + O(q^5) = \prod_{k\geq 1} \frac{1}{1-q^k} + O(q^5) = \frac{1}{1-q} \cdot \frac{1}{1-q^2} \cdot \frac{1}{1-q^3} \cdot \frac{1}{1-q^4} + O(q^5)$$

which can be rewritten as the product of geometric series

$$(1+q+q^2+q^3+q^4+O(q^5))(1+q^2+q^4+O(q^5))(1+q^3+O(q^5))(1+q^4+O(q^5)).$$

Proof of Theorem 162. Take a positive integer N, and let us show that the formula for the generating function is correct up to $O(q^{N+1})$. By Lemma 160 we have

$$P_{\{1,2,\ldots,N\}}(q) = \prod_{k=1}^{N} \frac{1}{1-q^k}$$

so that

$$\prod_{k=1}^{\infty} \frac{1}{1-q^k} + O(q^{N+1}) = \prod_{k=1}^{N} \frac{1}{1-q^k} + O(q^{N+1}) = P_{\{1,2,\ldots,N\}}(q) + O(q^{N+1})$$

It remains to show that

$$P(q) + O(q^{N+1}) = P_{\{1,2,\ldots,N\}}(q) + O(q^{N+1}).$$

This equality encodes the following fact: if we consider partitioning of integers less than $N+1$ (LHS), then all the parts will also be less than $N+1$ (RHS).

We have shown that for arbitrary $N > 0$ we have

$$P(q) + O(q^{N+1}) = P_{\{1,2,\ldots,N\}}(q) + O(q^{N+1}) = \prod_{k=1}^{\infty} \frac{1}{1-q^k} + O(q^{N+1}).$$

This means that all coefficients of the two power series $P(q)$ and $\prod_{k=1}^{\infty} \frac{1}{1-q^k}$ are equal; and this is just the same as to say that the power series are equal. □

Week 10. Continued Fractions

Continued fractions is a way of representing real numbers. Rational numbers will correspond to finite continued fractions whereas irrational numbers will correspond to infinite ones.

30. Finite continued fractions

Example 164. *Consider the following multiple-decked expression:*

$$2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}}. \tag{14}$$

Evidently, (14) is a rational number, and we can easily compute what this number is:

$$2+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2}}}}=2+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{7/2}}}=2+\cfrac{1}{4+\cfrac{1}{1+2/7}}=$$

$$=2+\cfrac{1}{4+\cfrac{1}{9/7}}=2+\cfrac{1}{4+7/9}=2+\cfrac{1}{43/9}=2+9/43=95/43.$$

The short hand notation for (14) is $[2;4,1,3,2]$. *Thus we have*

$$\frac{95}{43}=[2;4,1,3,2].$$

Definition 165. *By a* **finite continued fraction** *is meant a fraction of the form*

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots a_{n-1}+\cfrac{1}{a_n}}}}, \tag{15}$$

where $a_0,a_1,\ldots,a_n$ *are positive integers.*

Thus a finite continued fraction is a rational number obtained by recursively taking reciprocals and adding positive integers. The notation for continued fraction (15) is

$$[a_0;a_1,a_2,\ldots,a_n].$$

Theorem 166. *Every positive rational number can be represented as a finite continued fraction.*

Proof. A rational number can be written uniquely as

$$\frac{m}{n},\ \ m,n\in\mathbb{Z},\ \ n>0,\ \ \gcd(m,n)=1.$$

I do induction on the denominator n. The base case is $n=1$, so that

$$\frac{m}{n}=m=[a_0]$$

with $a_0=m$.

The induction step: I assume that all rational numbers

$$\frac{m'}{n'},\ \ 0<n'<n$$

have a continued fraction expansion, and I show that the same is true for $\frac{m}{n}$. I write:

$$m=an+r,\ \ 0<r<n$$

so that

$$\frac{m}{n}=\frac{an+r}{n}=a+\frac{r}{n},$$

and I flip the latter fraction:

$$\frac{m}{n} = a + \frac{1}{n/r}.$$

Now since $r < n$, by induction hypothesis $\frac{n}{r}$ has a continued fraction expansion:

$$\frac{n}{r} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{k-1} + \cfrac{1}{a_k}}}}, \quad a_i \in \mathbb{N}$$

which implies that

$$\frac{m}{n} = a + \frac{1}{n/r} = a + \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{k-1} + \cfrac{1}{a_k}}}}.$$

This means that we successfully expressed $\frac{m}{n}$ as a continued fraction. □

Example 167. *We illustrate the proof of the Theorem above by finding continued fraction expansion for* $\frac{19}{51}$.

$$\frac{19}{51} = \frac{1}{\frac{51}{19}} = \frac{1}{2 + \frac{13}{19}} = \frac{1}{2 + \frac{1}{\frac{19}{13}}} = \frac{1}{2 + \frac{1}{1 + \frac{6}{13}}} = \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{13}{6}}}} = \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}}.$$

Thus we found that

$$\frac{19}{51} = [0; 2, 1, 2, 6].$$

31. Convergents of continued fractions

Definition 168. *The continued fraction made from* $[a_0; a_1, \dots a_n]$ *by cutting the expansion after* k*'th partial denominator* a_k *is called* **the k'th convergent** *of the given continued fraction and is denoted by* C_k*; in symbols,*

$$C_k = [a_0; a_1, \dots, a_k] \qquad (0 \le k \le n).$$

Thus we have

$$C_0 = a_0$$

$$C_1 = a_0 + \frac{1}{a_1}$$

$$C_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$$

and so on.

Example 169. *We use continued fraction expansion*

$$\frac{19}{51} = [0; 2, 1, 2, 6]$$

obtained in Example 167. We have

$$\begin{aligned}
C_0 &= [0] = 0 \\
C_1 &= [0; 2] = 0 + \frac{1}{2} = \frac{1}{2} \\
C_2 &= [0; 2, 1] = 0 + \frac{1}{2 + \frac{1}{1}} = \frac{1}{3} \\
C_3 &= [0; 2, 1, 2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{8} \\
C_4 &= [0; 2, 1, 2, 6] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}} = \frac{19}{51}.
\end{aligned}$$

The next theorem is a powerful tool for computing convergents for continued fractions.

Theorem 170 (**Numerators and denominators of partial fractions**). *Given a continued fraction $[a_0; a_1, \ldots, a_n]$, for each $0 \leq k \leq n$ we have $C_k = \frac{p_k}{q_k}$ where the integers p_k and q_k are computed by following procedure:*

$$\begin{aligned}
p_0 &= a_0 \\
p_1 &= a_1 a_0 + 1 \\
&\cdots \\
p_k &= a_k p_{k-1} + p_{k-2}
\end{aligned}$$

and

$$\begin{aligned}
q_0 &= 1 \\
q_1 &= a_1 \\
&\cdots \\
q_k &= a_k q_{k-1} + q_{k-2}.
\end{aligned}$$

Proof. We check the first couple of cases to make sure things are right:

$$\begin{aligned}
C_0 &= a_0 = \frac{p_0}{q_0} \\
C_1 &= a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1} \\
C_2 &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_2 a_1 + 1} = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1} = \frac{p_2}{q_2}.
\end{aligned}$$

We now prove the general case by induction. The base is already checked, let's do the induction step $k \mapsto k + 1$. I use the following trick to reduce the length of my continued fraction:

$$[a_0; a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}].$$

Indeed, these two continued fractions represent the same rational number

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{k-1} + \cfrac{1}{a_k + \cfrac{1}{a_{k+1}}}}}}.$$

I compute using the induction hypothesis

$$[a_0; a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}] = \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}.$$

Here $p_k, p_{k-1}, q_k, q_{k-1}$ depend only on $a_0; a_1, \ldots, a_{k-1}$, hence are the same for

$$[a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}]$$

and

$$[a_0; a_1, \ldots, a_n].$$

I finish the proof by showing that the fraction we obtained evaluates to $\frac{p_{k+1}}{q_{k+1}}$:

$$\frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} = \frac{(a_k a_{k+1} + 1)p_{k-1} + a_{k+1}p_{k-2}}{(a_k a_{k+1} + 1)q_{k-1} + a_{k+1}q_{k-2}} =$$

$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.$$

□

Example 171. *We demonstrate how Theorem 170 works for* $\frac{19}{51} = [0; 2, 1, 2, 6]$ *and check consistency of our results with Examples 167 and 169. We compute p's:*

$$a_0 = 0 \implies p_0 = a_0 = 0$$
$$a_1 = 2 \implies p_1 = a_1 a_0 + 1 = 2 \cdot 0 + 1 = 1$$
$$a_2 = 1 \implies p_2 = a_2 p_1 + p_0 = 1 \cdot 1 + 0 = 1$$
$$a_3 = 2 \implies p_3 = a_3 p_2 + p_1 = 2 \cdot 1 + 1 = 3$$
$$a_4 = 6 \implies p_4 = a_4 p_3 + p_2 = 6 \cdot 3 + 1 = 19$$

and we compute q's:

$$q_0 = 1$$
$$a_1 = 2 \implies q_1 = a_1 = 2$$
$$a_2 = 1 \implies q_2 = a_2 q_1 + q_0 = 1 \cdot 2 + 1 = 3$$
$$a_3 = 2 \implies q_3 = a_3 q_2 + q_1 = 2 \cdot 3 + 2 = 8$$
$$a_4 = 6 \implies q_4 = a_4 q_3 + q_2 = 6 \cdot 8 + 3 = 51.$$

Dividing each p_k *by the corresponding* q_k *we get the convergents:*

$$C_0 = 0, C_1 = \frac{1}{2}, C_2 = \frac{1}{3}, C_3 = \frac{3}{8}, C_4 = \frac{19}{51},$$

in accordance with Example 169.

Remark 172. *The inductive definition for p's and q's given in Theorem 170 should remind you of the Fibonacci sequence u_k. To make this analogy precise, consider the case when the sequence a_k has the form:*

$$a_0 = 0, \quad a_k = 1, \quad k \geq 1,$$

i.e. we consider continued fraction of the form

$$[0; 1, 1, \ldots, 1].$$

Then the p's are given by

$$p_0 = 0, p_1 = 1, p_2 = 1, p_3 = 2, p_4 = 3, \ldots,$$

i.e.

$$p_k = u_{k-1}$$

and the q's are given by

$$q_0 = 1, q_1 = 1, q_2 = 2, q_3 = 3, q_4 = 5, \ldots,$$

i.e.

$$q_k = u_k.$$

Thus the convergents of $[0; 1, 1, \ldots, 1]$ are given by ratios of consecutive Fibonacci numbers:

$$C_k = \frac{p_k}{q_k} = \frac{u_{k-1}}{u_k}.$$

Theorem 173 (p-q relation). *If $C_k = \frac{p_k}{q_k}$ is the k'th convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$, then*

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

The proof of this theorem is done using induction. I leave the proof to the Problem Sheet.

The next Corollary shows that our expressions for convergents

$$C_k = \frac{p_k}{q_k}.$$

have minimal possible denominators.

Corollary 174. *For $1 \leq k \leq n$, p_k and q_k are coprime.*

Proof. According to Theorem 173, any common divisor d of p_k and q_k would also divide

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1} = \pm 1,$$

and this is only possible for $d = 1$, i.e. we have

$$\gcd(p_k, q_k) = 1,$$

meaning that p_k and q_k are coprime. □

Dividing both sides of the formula from Theorem 173 by $q_{k-1}q_k$ we get the following:

Corollary 175. *We have*

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_{k-1}q_k}.$$

32. Infinite continued fractions

We turn to discussing infinite continued fractions. These will be useful in finding rational approximations for irrational numbers, such as the following approximation for π:

$$\pi \approx \frac{355}{113}, \tag{16}$$

which was discovered by Chinese mathematician Tsu Chung-chi (430-501 AD).

Given an infinite sequence $[a_0; a_1, a_2, \dots]$ we would like to define the corresponding infinite continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}, \tag{17}$$

as the limit of convergents

$$[a_0; a_1, a_2, \dots] := \lim_{n\to\infty} C_n = \lim_{n\to\infty} [a_0; a_1, \dots, a_n],$$

and the next theorem shows that this limit exists.

Theorem 176 (**Convergents for infinite partial fractions**). *Let $[a_0; a_1, a_2, \dots]$ be an infinite sequence. Then: 1) The convergents with even subscripts form a strictly increasing sequence; that is,*

$$C_0 < C_2 < C_4 < \dots.$$

2) The convergents with odd subscripts form a strictly decreasing sequence; that is,

$$C_1 > C_3 > C_5 > \dots.$$

3) The limit $\lim_{n\to\infty} C_n$ exists.

Proof. I first prove (1) and (2). For that, I compute using Corollary 175:

$$\begin{aligned} C_{k+2} - C_k &= (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k) = \\ &= \frac{(-1)^{k+1}}{q_{k+1}q_{k+2}} + \frac{(-1)^k}{q_k q_{k+1}} = \\ &= \frac{(-1)^k}{q_{k+1}} \left(-\frac{1}{q_{k+2}} + \frac{1}{q_k} \right) = \\ &= \frac{(-1)^k (q_{k+2} - q_k)}{q_k q_{k+1} q_{k+2}}. \end{aligned}$$

We see that $C_{k+2} - C_k > 0$ for k even and that $C_{k+2} - C_k < 0$ for k odd. This proves (1) and (2).

A standard fact from Analysis/Calculus is that an increasing sequence C_{2j} must have a limit:

$$x := \lim_{j\to\infty} C_{2j}$$

and similarly, a decreasing sequence C_{2j+1} has a limit:

$$x' := \lim_{j\to\infty} C_{2j+1}.$$

Since I have not checked whether the sequences are bounded, a priori it is possible that $x = +\infty$ or $x' = -\infty$. However I will show that $x = x'$, which implies that both limits are finite and equal to each other.

We compare the two limits x, x'. According to Corollary 175 we have

$$C_{2j+1} - C_{2j} = \frac{1}{q_{2j}q_{2j+1}},$$

and the limit of the RHS is zero, thus:

$$x' - x = \lim_{n\to\infty}(C_{2j+1} - C_{2j}) = 0 \implies x = x'.$$

Our sequence C_n consists of two subsequences: one is made of even terms C_{2j}, and the other is made of odd terms C_{2j+1}. Both subsequences have the same limit x, which implies that

$$\lim_{n\to\infty} C_n = x.$$

□

Remark 177. *It follows from the theorem, that if $x = \lim_{n\to\infty} C_n$, then*

$$C_0 < C_2 < C_4 < \cdots < x < \cdots < C_5 < C_3 < C_1,$$

in particular any even convergent is smaller than any odd convergent.

Definition 178. *We define the value represented by an infinite continued fraction to be the limit of convergents:*

$$[a_0; a_1, a_2, \dots] := \lim_{n\to\infty} C_n = \lim_{n\to\infty} [a_0; a_1, \dots, a_n].$$

Theorem 179. *Infinite continued fractions represent irrational numbers and every positive irrational number may be represented by an infinite continued fraction.*

Instead of giving the formal proof of Theorem 179, I give an algorithm to find an infinite continued fraction representation for an irrational number x_0. You may recognize that the procedure I describe is essentially the same as our proof of Theorem 166.

Representing irrational numbers as infinite continued fractions algorithm: Start by considering the sequence [4]

$$x_1 = \frac{1}{x_0 - [x_0]}, \quad x_2 = \frac{1}{x_1 - [x_1]}, \quad x_3 = \frac{1}{x_2 - [x_2]}, \quad \dots \tag{18}$$

and then take

$$a_0 = [x_0], \quad a_1 = [x_1], \quad a_2 = [x_2], \quad \dots. \tag{19}$$

Each a_i is a positive integer. The defining relation for x's may be rewritten as:

$$x_k - [x_k] = \frac{1}{x_{k+1}}$$

or using the definition of a's:

$$x_k = a_k + \frac{1}{x_{k+1}}. \tag{20}$$

[4]Here and below I use the "bracket" notation $[x]$ for the integer part of x. In fact I already used this notation in Week 5 in the formulation of Eisenstein's Lemma. Just to remind you what it does: $[7.54] = 7$, i.e. we take the largest integer not exceeding x.

Now I explain why $a_0, a_1, a_2, \dots$ is the sequence we have been looking for. I repeatedly use relation (20) to compute:

$$x_0 = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \frac{1}{x_3}}} = \dots$$

and one can show that in the limit we have

$$x_0 = [a_0; a_1, a_2, \dots].$$

Example 180. *We start writing out infinite continued fraction expansion for π and compute the first four convergents C_0, C_1, C_2, C_3. I use (18), (19) and I rely on a calculator here:*

$$\begin{aligned}
x_0 = \pi = 3 + (\pi - 3) &\implies a_0 = [x_0] = 3 \\
x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{0.14159265...} = 7.06251330... &\implies a_1 = [x_1] = 7 \\
x_2 = \frac{1}{x_1 - [x_1]} = \frac{1}{0.06251330...} = 15.99659440... &\implies a_2 = [x_2] = 15 \\
x_3 = \frac{1}{x_2 - [x_2]} = \frac{1}{0.99659440...} = 1.00341723... &\implies a_3 = [x_3] = 1 \\
x_4 = \frac{1}{x_3 - [x_3]} = \frac{1}{0.00341723...} = 292.63724... &\implies a_4 = [x_4] = 292.
\end{aligned}$$

Thus the infinite continued fraction expansion for π begins with

$$\pi = [3; 7, 15, 1, 292, \dots].$$

Similarly to decimal expansion, there is no pattern found in the sequence a_k.

We now compute the convergents using Theorem 170. The fact that we have an infinite continued fraction does not make a difference here, since we work only with its finite approximations. We compute p's:

$$\begin{aligned}
a_0 = 3 &\implies p_0 = a_0 = 3 \\
a_1 = 7 &\implies p_1 = a_1 a_0 + 1 = 22 \\
a_2 = 15 &\implies p_2 = a_2 p_1 + p_0 = 15 \cdot 22 + 3 = 333 \\
a_3 = 1 &\implies p_3 = a_3 p_2 + p_1 = 1 \cdot 333 + 22 = 355
\end{aligned}$$

and we compute q's:

$$\begin{aligned}
q_0 &= 1 \\
a_1 = 7 &\implies q_1 = a_1 = 7 \\
a_2 = 15 &\implies q_2 = a_2 q_1 + q_0 = 15 \cdot 7 + 1 = 106 \\
a_3 = 1 &\implies q_3 = a_3 q_2 + q_1 = 1 \cdot 106 + 7 = 113
\end{aligned}$$

Dividing each p_k by the corresponding q_k we get the convergents:

$$C_0 = 3, C_1 = \frac{22}{7}, C_2 = \frac{333}{106}, C_3 = \frac{355}{113}.$$

If one writes decimal expansion for each of these convergents, one can see that they provide approximations for π of increasing precision:

$$\left|\pi - \frac{22}{7}\right| < 10^{-2}$$
$$\left|\pi - \frac{333}{106}\right| < 10^{-3}$$
$$\left|\pi - \frac{355}{113}\right| < 10^{-6}.$$

The last convergent $C_3 = \frac{355}{113}$ is the approximation (16) used by Tsu Chung-chi.

Remark 181. *In a certain sense, which can be made precise, continued fractions provide the* **best** *rational approximations to irrational numbers. For example,*

$$\pi \approx \frac{355}{113}$$

is the best approximation with a three-digit denominator.

33. Periodic continued fractions

Example 182. *We work out continued fraction expansion for $\sqrt{2}$. The thing to keep in mind is $[\sqrt{2}] = 1$. I use (18), (19):*

$$x_0 = \sqrt{2} = 1 + (\sqrt{2} - 1) \implies a_0 = 1$$
$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1) \implies a_1 = 2$$
$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1) \implies a_2 = 2$$
$$\dots$$

In fact this process continues infinitely and we get $a_k = 2$ for all $k \geq 1$. Thus the infinite continued fraction expansion for $\sqrt{2}$ is

$$\sqrt{2} = [1; 2, 2, 2, 2, \dots].$$

Similarly to the decimal expansion case we write this as

$$\sqrt{2} = [1; \overline{2}].$$

Example 183. *We work out continued fraction expansion for $\sqrt{23}$, keeping in mind that $[\sqrt{23}] = 4$. I use (18), (19):*

$$x_0 = \sqrt{23} = 4 + (\sqrt{23} - 4) \implies a_0 = 4$$
$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{7} = 1 + \frac{\sqrt{23} - 3}{7} \implies a_1 = 1$$
$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{7}{\sqrt{23} - 3} = \frac{7(\sqrt{23} + 3)}{14} = 3 + \frac{\sqrt{23} - 3}{2} \implies a_2 = 3$$
$$x_3 = \frac{1}{x_2 - [x_2]} = \frac{2}{\sqrt{23} - 3} = \frac{\sqrt{23} + 3}{7} = 1 + \frac{\sqrt{23} - 4}{7} \implies a_3 = 1$$
$$x_4 = \frac{1}{x_3 - [x_3]} = \frac{7}{\sqrt{23} - 4} = \sqrt{23} + 4 = 8 + (\sqrt{23} - 4) \implies a_4 = 8.$$

Since $x_5 = x_1$, also $x_6 = x_2$, and so on, which means that the block of integers $1, 3, 1, 8$ repeats indefinitely:

$$\sqrt{23} = [4; 1, 3, 1, 8, 1, 3, 1, 8, \dots] = [4; \overline{1, 3, 1, 8}].$$

Definition 184. *We call an infinite continued fraction*

$$[a_0; a_1, a_2, \dots]$$

periodic *if it has the form*

$$[a_0; a_1, a_2, \dots, a_m, \overline{b_1, \dots, b_r}].$$

Theorem 185 (Periodic continued fractions represent quadratic irrationalities). *Infinite continued fraction expansion $[a_0; a_1, a_2, \dots]$ is periodic if and only if it represents an irrational number of the form*

$$a + b\sqrt{d}$$

for some $a, b \in \mathbb{Q}$, $d \in \mathbb{N}$.

I do not give a proof for this Theorem. Two examples above demonstrate the "if" direction. The next example demonstrates the "only if" direction.

Example 186. *We determine the unique irrational number represented by the infinite continued fraction*

$$x = [3; 6, \overline{1, 4}].$$

In order to do so, I use the following trick:

$$[a_0; a_1, a_2, \dots, a_{n-1}, a_n, \dots] = [a_0; a_1, a_2, \dots, a_{n-1}, y]$$

where

$$y = [a_n; a_{n+1}, \dots].$$

This follows from definitions and works for finite or infinite continued fractions.

Thus let us write

$$x = [3; 6, y],$$

where

$$y = [1; 4, 1, 4, \dots] = [1; 4, y].$$

Then

$$y = 1 + \frac{1}{4 + 1/y} = 1 + \frac{y}{4y + 1} = \frac{5y + 1}{4y + 1},$$

which leads to the quadratic equation

$$4y^2 - 4y - 1 = 0.$$

Since $y > 0$, we take the positive root:

$$y = \frac{1+\sqrt{2}}{2}.$$

From $x = [3; 6, y]$ we then find that

$$x = 3 + \frac{1}{6 + \frac{1}{y}} = 3 + \frac{1}{\frac{6y+1}{y}} = 3 + \frac{y}{6y+1} = \frac{19y+3}{6y+1} =$$

$$\frac{19\frac{1+\sqrt{2}}{2} + 3}{6\frac{1+\sqrt{2}}{2} + 1} = \frac{19(1+\sqrt{2})+6}{6(1+\sqrt{2})+2} = \frac{19\sqrt{2}+25}{6\sqrt{2}+8} =$$

$$\frac{(19\sqrt{2}+25)(6\sqrt{2}-8)}{(6\sqrt{2}+8)(6\sqrt{2}-8)} = \frac{28-2\sqrt{2}}{8} = \frac{14-\sqrt{2}}{4}.$$

Week 11. Pell's Equation

Recall that a Diophantine equation is a polynomial equation to be solved in integers. In Week 8 we studied Diophantine equation $x^2 + y^2 = z^2$. This week we study another Diophantine equation

$$x^2 - dy^2 = 1 \tag{21}$$

with an integer parameter $d \in \mathbb{N}$. Equation (21) is known as **Pell's equation**. Attribution to Pell is due to Euler; this attribution is erroneous as the English mathematician John Pell (1611-1685) had nothing to do with this equation. Presumably Euler confused Pell with Lord William Brouncker of Ireland (1620-1684).

Indeed, it was Brouncker who solved the equation

$$x^2 - 313y^2 = 1$$

in response to a challenge from P. Fermat to his English colleagues.

Before the times of Fermat, Pell's equation has been considered in Greece and in India. In Greece it appeared in an epigram sent from Archimedes to Eratosthenes.

Indian 7th century mathematician Brahmagupta said that a person who can within a year solve the equation

$$x^2 - 92y^2 = 1$$

is a mathematician. So this is what we are up to: becoming mathematicians.

34. Fundamental solution

Notice that if (x, y) is a solution of (21), then $(\pm x, \pm y)$ is also a solution. Also notice that

$$(\pm 1, 0)$$

satisfy the equation, and these may be referred as trivial solutions.

Remark 187. *If d is a perfect square, $d = k^2$, then Pell's equation (21) only has trivial solutions $(\pm 1, 0)$. In order to see this we factor*

$$1 = x^2 - k^2y^2 = (x - ky)(x + ky).$$

Since both $x - ky$ and $x + ky$ are integers, they must be ± 1. Therefore we either have

$$\begin{cases} x - ky &= 1 \\ x + ky &= 1 \end{cases}$$

which after adding / subtracting the two equations leads to $(x, y) = (1, 0)$ or we have

$$\begin{cases} x - ky &= -1 \\ x + ky &= -1 \end{cases}$$

which after adding / subtracting the two equations leads to $(x, y) = (-1, 0)$.

We will see that if d is not a perfect square, Pell's equation will have infinitely many solutions. From now on we will **assume that d is not a perfect square and that $x > 0$.** We allow $y < 0$.

Definition 188. *The fundamental solution of Pell's equation is the positive solution with minimal x and y.*

To find the fundamental solution, we may try possible values of y

$$y = 1, 2, 3, 4, \ldots$$

and stop when $1 + dy^2$ is a perfect square, i.e.

$$1 + dy^2 = x^2.$$

Example 189. *We find the fundamental solution of*

$$x^2 - 2y^2 = 1.$$

We compute:

$$\begin{aligned} y = 1 &\implies 1 + 2y^2 = 3 \ \textit{not a perfect square} \\ y = 2 &\implies 1 + 2y^2 = 9 \ \textit{is a perfect square} \implies x = 3. \end{aligned}$$

We found that $(3, 2)$ is the fundamental solution.

Example 190. *We find the fundamental solution of*

$$x^2 - 5y^2 = 1.$$

We compute:

$$\begin{aligned} y = 1 &\implies 1 + 5y^2 = 6 \ \textit{not a perfect square} \\ y = 2 &\implies 1 + 5y^2 = 21 \ \textit{not a perfect square} \\ y = 3 &\implies 1 + 5y^2 = 46 \ \textit{not a perfect square} \\ y = 4 &\implies 1 + 5y^2 = 81 \ \textit{is a perfect square} \implies x = 9. \end{aligned}$$

We found that $(9, 4)$ is the fundamental solution.

35. Group G_d of solutions

The set of solutions of $x^2 - dy^2 = 1$ can be made into a group:

Theorem 191 (Solutions form a group). *For any $d > 0$ the set of solutions*

$$G_d = \{(x, y) \mid x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - dy^2 = 1\}$$

of Pell's equation is a commutative group under the operation

$$(x, y) \star (x', y') = (xx' + dyy', xy' + x'y)$$

with neutral element

$$(x, y) = (1, 0)$$

and with inverses given by

$$(x, y)^{-1} = (x, -y).$$

Proof. First of all, we need to check that the operation is well defined, i.e. that if (x, y) and (x', y') are solutions of $x^2 - dy^2 = 1$, then

$$(x, y) \star (x', y') = (xx' + dyy', xy' + x'y)$$

is also a solution. We do this computation:

$$(xx' + dyy')^2 - d(xy' + x'y)^2 = x^2x'^2 + 2dxx'yy' + d^2y^2y'^2 - d(x^2y'^2 + 2xx'yy' + x'^2y^2) =$$

$$= x^2x'^2 + d^2y^2y'^2 - d(x^2y'^2 + x'^2y^2) = (x^2 - dy^2)(x'^2 - dy'^2) = 1.$$

We check the axioms of a group now. Commutativity is easy from definition:

$$(x, y) \star (x', y') = (xx' + dyy', xy' + x'y) = (x'x + dy'y, x'y + xy') = (x', y') \star (x, y).$$

Checking associativity

$$((x, y) \star (x', y')) \star (x'', y'') = (x, y) \star ((x', y') \star (x'', y''))$$

is a long and boring computation showing that both sides are equal to

$$(xx'x'' + d(yy' + y'y'' + y''y), xx'y'' + xy'x'' + yx'x'' + dyy'y'').$$

Neutral element is easy:

$$(x, y) \star (1, 0) = (x \cdot 1 + d \cdot y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y).$$

Inverses are interesting:

$$(x, y) \star (x, -y) = (x^2 - dy^2, -xy + yx) = (1, 0)$$

since we assume $x^2 - dy^2 = 1$. □

Remark 192. *You may notice that the product operation in G_d is reminiscent to multiplying complex numbers. In fact the operations on pairs (x, y) in G_d are induced by multiplication of real numbers of the form*

$$x + \sqrt{d} \cdot y.$$

See Problem Sheet for details.

Given a solution of Pell's equation we may use Theorem 191, to find more solutions.

Example 193. *Consider $d = 2$ case, i.e. the equation*

$$x^2 - 2y^2 = 1. \tag{22}$$

We found in Example 189 that the fundamental solution is $(x_1, y_1) = (3, 2)$. Using Theorem 191 we get other solutions by taking powers of (x_1, y_1) in the group G_d. The square of (x_1, y_1):

$$(x_1, y_1)^2 = (x_1, y_1) \star (x_1, y_1) = (3, 2) \star (3, 2) = (3^2 + 2 \cdot 2^2, 6 + 6) = (17, 12).$$

And indeed, $(17, 12)$ is a solution of (22):

$$17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 1.$$

The cube of (x_1, y_1):

$$(x_1, y_1)^3 = (x_1, y_1)^2 \star (x_1, y_1) = (17, 12) \star (3, 2) = (3 \cdot 17 + 2 \cdot 2 \cdot 12, 17 \cdot 2 + 12 \cdot 3) = (99, 70)$$

is another solution. Thus we found three positive solutions

$$(3, 2), (17, 12), (99, 70)$$

and it is clear that continuing working in this fashion we get an infinite sequence of solutions.

We can also take inverses in G_d, but this is not so interesting, as the result is simply the change of sign for y:

$$(x_1, y_1)^{-1} = (3, -2)$$
$$(x_1, y_1)^{-2} = (17, -12)$$
$$(x_1, y_1)^{-3} = (99, -70).$$

It is a natural guess, that taking powers of the fundamental solution of Pell's Equations gives all possible solutions. The next Theorem shows that this is indeed the case.

Theorem 194 (Group of solutions is cyclic). *Let d be not a perfect square and let (x_1, y_1) be the fundamental solution of Pell's equation*

$$x^2 - dy^2 = 1.$$

Then the group of solutions G_d is an infinite cyclic group with generator (x_1, y_1). In particular, all positive solutions are given as

$$(x_k, y_k) = (x_1, y_1)^k, \quad k = 1, 2, 3, \ldots$$

To prove the theorem will need an ordering $<$ on the set of the solutions G_d. We define this relation as

$$(x, y) < (x', y') \iff y < y'.$$

Example 195. *For $x^2 - 2y^2 = 1$ the solutions are ordered as follows*

$$\cdots < (99, -70) < (17, -12) < (3, -2) < (1, 0) < (3, 2) < (17, 12) < (99, 70) < \ldots$$

Recall that we only consider solutions with $x > 0$.

Lemma 196 ($\star$ preserves the ordering). *For any $g, g', h \in G_d$ we have*

$$g < g' \implies g \star h < g' \star h.$$

I leave the proof of Lemma for the Problem Sheet.

Proof of Theorem 194. Assume for the sake of obtaining a contradiction that there is a solution (x, y) which does not coincide with any of the $(x_k, y_k) = (x_1, y_1)^k$. Then comparing the y-coordinates, we may write for some k:

$$(x_1, y_1)^k < (x, y) < (x_1, y_1)^{k+1}.$$

By Lemma 196 we may multiply this through by $(x_1, y_1)^{-k}$ to obtain

$$(1, 0) < (x, y) \star (x_1, y_1)^{-k} < (x_1, y_1).$$

This is a contradiction, since it appears that

$$(x, y) \star (x_1, y_1)^{-k}$$

is a positive solution which is smaller than the fundamental solution. □

Example 197. *In Example 190 we found that $(x_1, y_1) = (9, 4)$ is the fundamental solution of*

$$x^2 - 5y^2 = 1.$$

By Theorem 194, all positive solutions are given as

$$(9, 4), (9, 4)^2, (9, 4)^3, \ldots.$$

For example, we can compute that the second solution is

$$(x_2, y_2) = (9, 4)^2 = (9, 4) \star (9, 4) = (81 + 5 \cdot 16, 9 \cdot 4 + 9 \cdot 4) = (161, 72).$$

Remark 198. *If d is a perfect square, then according to Remark 187 the group G_d of solutions has only one element, the neutral element:*

$$G_d = \{(1, 0)\}.$$

36. Computing solutions via continued fractions

Solutions of Pell's equation $x^2 - dy^2 = 1$ are closely related to the convergents of the continued fraction expansion of $\sqrt{d}$. Recall from Week 10 that the continued fraction expansion of $\sqrt{d}$ is periodic.

Example 199. *Let us revisit Example 189 where we found some solutions of $x^2 - 2y^2 = 1$. We'd like to relate these to the continued fraction expansion of $\sqrt{2}$, which is*

$$\sqrt{2} = [1; 2, 2, 2, \ldots] = [1; \overline{2}].$$

We compute some convergents:

$$C_0 = [1] = 1/1$$
$$C_1 = [1; 2] = 3/2$$
$$C_2 = [1; 2, 2] = 7/5$$
$$C_3 = [1; 2, 2, 2] = 17/12$$

and then we plug in the numerator and the denominator (p_n, q_n) of C_n into Pell's equation and compute $p_n^2 - dq_n^2$:

$$1^2 - 2 \cdot 1^2 = 1 - 2 = -1$$
$$3^2 - 2 \cdot 2^2 = 9 - 8 = 1$$
$$7^2 - 2 \cdot 5^2 = 49 - 50 = -1$$
$$17^2 - 2 \cdot 12^2 = 289 - 288 = 1$$

Note that $(3, 2)$ is the fundamental solution of $x^2 - 2y^2 = 1$, and $(17, 12)$ is the next solution.

In general the situation is the following:

Theorem 200. (1) *If (x, y) is a positive solution of Pell's equation $x^2 - dy^2 = 1$, then $\frac{x}{y}$ is a convergent for the infinite continued fraction expansion of $\sqrt{d}$.*

(2) *If (x, y) is a a convergent for the infinite continued fraction expansion of $\sqrt{d}$, then $x^2 - dy^2 = k$, where $k \in \mathbb{Z}$ satisfies $|k| < 1 + 2\sqrt{d}$.*

Proof. (1) We rely on the following Fact #1: if α is a positive irrational number and $\frac{x}{y}$ is a positive rational number satisfying $|\alpha - \frac{x}{y}| < \frac{1}{2y^2}$, then $\frac{x}{y}$ is a convergent of α. Thus if we show that $|\sqrt{d} - \frac{x}{y}| < \frac{1}{2y^2}$ then (1) will follow. The rest is a straightforward computation. We have $(x - \sqrt{d}y)(x + \sqrt{d}y) = x^2 - dy^2 = 1$ so that

$$\frac{x}{y} - \sqrt{d} = \frac{1}{y(x + \sqrt{d}y)}.$$

Since $x - \sqrt{d}y > 0$ we have $x > \sqrt{d}y$ so that the denominator satisfies

$$y(x + \sqrt{d}y) > 2\sqrt{d}y > 2y,$$

thus we get

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y},$$

and we are done, using Fact #1.

(2) We rely on the following Fact #2: any convergent $\frac{x}{y}$ ($x, y > 0$, $\gcd(x, y) = 1$) of an irrational number α satisfies $|\frac{x}{y} - \alpha| < \frac{1}{y^2}$. We start with

$$|x^2 - dy^2| = |x - \sqrt{d}y||x + \sqrt{d}y|$$

and we estimate both terms. Since $\frac{x}{y} - \alpha| < \frac{1}{y^2}$ we have

$$|x - \sqrt{d}y| < \frac{1}{y}$$

and we also have using the triangle inequality $|a + b| \leq |a| + |b|$ that

$$|x + \sqrt{d}y| = |(x - \sqrt{d}y) + 2\sqrt{d}y| \leq \frac{1}{y} + 2\sqrt{d}y \leq (1 + 2\sqrt{d})y.$$

Altogether this gives

$$|x^2 - dy^2| = |x - \sqrt{d}y||x + \sqrt{d}y| < \frac{1}{y} \cdot (1 + 2\sqrt{d})y = 1 + 2\sqrt{d}.$$

□

Theorem 201 (All solutions from continued fractions). *Let $\frac{p_k}{q_k}$ be the convergents of the continued fraction expansion of $\sqrt{d}$ and let n be the length of the period of the expansion.*

(1) *If n is even, then all positive solutions of $x^2 - dy^2 = 1$ are given by*

$$x = p_{kn-1}, y = q_{kn-1}, \quad (k = 1, 2, 3, \dots).$$

(2) *If n is odd, then all positive solutions of $x^2 - dy^2 = 1$ are given by*

$$x = p_{2kn-1}, y = q_{2kn-1}, \quad (k = 1, 2, 3, \dots).$$

Example 202. *Consider the equation $x^2 - 2y^2 = 1$. Given that $\sqrt{2} = [1, \overline{2}]$ we will find three positive solutions of the equation.*

The period has length one (odd), so that by Theorem 201 (2), the first three positive solutions are

$$(p_1, q_1), (p_3, q_3), (p_5, q_5).$$

Thus we need to compute the convergents $C_0, \ldots, C_5$. According to Problem Sheet Week 10 these are given by

$$p_0 = 1, p_1 = 3, p_2 = 7, p_3 = 17, p_4 = 41, p_5 = 99,$$
$$q_0 = 1, q_1 = 2, q_2 = 5, q_3 = 12, q_4 = 29, q_5 = 70.$$

Thus the first three positive solutions are

$$(3, 2), (17, 12), (99, 70).$$

Note that these are of course the same as the solutions found in Example 193.

Example 203. *We find the fundamental solution of $x^2 - 12y^2 = 1$. To begin with, we need to find a continued fraction expansion for $\sqrt{12}$. To this end, I use the method I described in Week 10:*

$$x_0 = \sqrt{12} = 3 + (\sqrt{12} - 3) \implies a_0 = [\sqrt{12}] = 3$$
$$x_1 = \frac{1}{\sqrt{12} - 3} = \frac{\sqrt{12} + 3}{3} = 2 + \frac{\sqrt{12} - 3}{3} \implies a_1 = 2$$
$$x_2 = \frac{3}{\sqrt{12} - 3} = \frac{3(\sqrt{12} + 3)}{3} = \sqrt{12} + 3 = 6 + (\sqrt{12} - 3) \implies a_2 = 6$$
$$x_3 = \frac{1}{\sqrt{12} - 3} = x_1,$$

so that the continued fraction expansion for $\sqrt{12}$ is

$$\sqrt{12} = [3; \overline{2, 6}].$$

The period has length two (even), so that by Theorem 201 (1), the positive solutions of $x^2 - 12y^2 = 1$ are

$$(p_1, q_1), (p_3, q_3), \ldots$$

The first convergent is

$$\frac{p_1}{q_1} = C_1 = [3; 2] = 3 + \frac{1}{2} = \frac{7}{2}.$$

Thus the fundamental solution of $x^2 - 12y^2 = 1$ is

$$(p_1, q_1) = (7, 2).$$

We also make a table of convergents of $\sqrt{12}$ to illustrate Theorem 200. By part (2) of the Theorem, all convergents p/q will satisfy $|p^2 - 12q^2| < 1 + 2\sqrt{12}$, that is $|p^2 - 12q^2| \leq 7$.

k	a_k	p_k	q_k	$p_k^2 - 12q_k^2$
0	3	3	1	-3
1	2	7	2	1
2	6	45	13	-3
3	2	97	28	1

Example 204. *Given that* $\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}]$ *find the fundamental solution of* $x^2 - 19y^2 = 1$. *The period of the continued fraction expansion is* 6 *(even), thus by Theorem 201 (1), the fundamental solution is*

$$(p_5, q_5).$$

Thus we have to compute

$$C_5 = [4; 2, 1, 3, 1, 2].$$

Since we do not need other convergents, but just C_5*, here is a quick way to go:*

$$\begin{aligned} C_5 = [4; 2, 1, 3, 1, 2] &= [4; 2, 1, 3, 1 + \frac{1}{2}] = \\ &= [4; 2, 1, 3, \frac{3}{2}] = [4; 2, 1, 3 + \frac{2}{3}] = \\ &= [4; 2, 1, \frac{11}{3}] = [4; 2, 1 + \frac{3}{11}] = \\ &= [4; 2, \frac{14}{11}] = [4; 2 + \frac{11}{14}] = \\ &= [4; \frac{39}{14}] = 4 + \frac{14}{39} = \\ &= \frac{170}{39}. \end{aligned}$$

This works basically by the definition of a continued fraction: at each step I flip the rightmost term and add it to the previous term.

We see that the fundamental solution of $x^2 - 19y^2 = 1$ *is* $(p_5, q_5) = (170, 39)$.