Math 180A

Asaf Ferber

September 7, 2020

Contents

1 A general introduction

1.1 Why number theory?

Number Theory, unsurprisingly, is about the theory of numbers. By "Numbers" we mean the natural numbers $\mathbb{N} := \{1, 2, 3, \ldots\}$, or the set of integers $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. One of the most fundamental reasons to study Number Theory is that the entire math can be built from natural numbers!

For example, in order to build the set of integers $\mathbb{Z}$ from $\mathbb{N}$, one needs to define negation (and zero). To build the set of rational numbers $\mathbb{Q}$ from $\mathbb{Z}$ one needs to define division. To build the real line $\mathbb{R}$ out of $\mathbb{Q}$ one can define Dedekind cuts, and to build the set of complex numbers $\mathbb{C}$ one needs to add $i := \sqrt{-1}$ to the set of real numbers. As the famous 19th cetury German mathematician Leopold Kronecker (1823-1891) once said: *God made the integers, all the rest is the work of man.*

In Number Theory, at large, we are trying to understand non-trivial relationships among different sorts of numbers. Among other examples, we consider the following:

- Odd numbers: $1, 3, 5, 7, \ldots$
- Even numbers: $2, 4, 6, 8, \ldots$
- Squares: $1^2, 2^2, 3^2, 4^2, \ldots$
- Primes: $2, 3, 5, 7, 11, \ldots$
- Composite: $4, 6, 8, 9, 10 \ldots$
- 1 mod 4: $1, 5, 9, 13, 17, \ldots$
- Triangular: $1, 3, 6, 10, \ldots$
- and more.

The type of problems we are interested at are:

- Can the sum of two squares be a square?
- Can the sum of two cubes be a cube?
- How many primes are? How many primes are of the form 1 mod 4? 3 mod 5?
- which numbers are sums of two squares?
- Are there infinitely many twin primes? (that is, are there infinitely many primes p for which $p + 2$ is also a prime?)
- Are there infinitely many primes of the form $n^2 + 1$?

1.2 How to solve?

I found the following summary of George Polya's lessons on few websites (I'm not sure about its origin but I highly recommend you to take a look. I copy pasted from `https://lindseynicholson.org/2018/03/polyas-problem-solving-techniques/`).

In 1945 George Polya published a book How To Solve It, which quickly became his most prized publication. It sold over one million copies and has been translated into 17 languages. In this book he identifies four basic principles of problem solving.

Polya's First Principle: Understand the Problem This seems so obvious that it is often not even mentioned, yet students are often stymied in their efforts to solve problems simply because they don't understand it fully, or even in part. Polya taught teachers to ask students questions such as:

- Do you understand all the words used in stating the problem?
- What are you asked to find or show?
- Can you restate the problem in your own words?
- Can you think of a picture or diagram that might help you understand the problem?
- Is there enough information to enable you to find a solution?

Polya's Second Principle: Devise a Plan Polya mentions that there are many reasonable ways to solve problems. The skill at choosing an appropriate strategy is best learned by solving many problems. You will find choosing a strategy increasingly easy. A partial list of strategies is included:

- Guess and check
- Look for a pattern
- Make an orderly list
- Draw a picture
- Eliminate the possibilities
- Solve a simpler problem
- Use symmetry
- Use a model
- Consider special cases
- Work backwards
- Use direct reasoning
- Use a formula
- Solve an equation
- Be ingenious

Polya's Third Principle: Carry Out the Plan This step is usually easier than devising the plan. In general, all you need is care and patience, given that you have the necessary skills. Persist with the plan that you have chosen. If it continues not to work, discard it and choose another. Don't be misled, this is how things are done, even by professionals.

Polya's Fourth Principle: Look Back Polya mentions that much can be gained by taking the time to reflect and look back at what you have done, what worked, and what didn't. Doing this will enable you to predict what strategy to use to solve future problems.

2 Pythagorean triples

A classical theorem of Pythgoras asserts that if a, b are the sides of a right triangle, and c is its hypotenuse, then $a^2 + b^2 = c^2$.

In general, a triple of integers (a, b, c) with $a^2 + b^2 = c^2$ is called a Pythagorean triple. For example, $(3, 4, 5)$ is a pythagorean triple. In this section we will deal with the following problem:

Problem 2.1. *Find all the Pythagorean triples.*

It is a simple exercise to show that if (a, b, c) is a pythagorean triple, then so does (ax, bx, cx) for all x. In particular it gives us infinitely many such triples. It is thus natural to restrict ourselves to those triple for which (a, b, c) have no common divisor. Such triples are called *primitive Pythagorean triples* (or PPT for short). For example: $(3, 4, 5)$ is a PPT while $(6, 8, 10)$ is a pythagorean triple which is not primitive.

Following the above discussion, it is clear that in order to be able to find all pythagorean triples, it is enough to find all the PPTs (WHY?).

Now, suppose that (a, b, c) is a PPT, and let's try to explore some properties of its coordinates. For example, is it possible that both a, b are even and c is odd? It is a trivial exercise to show that this is not possible (show it!).

Here we show the less trivial observation that it cannot be the case that both a, b are odd and c is even. Indeed, suppose that $a = 2x + 1$, $b = 2y + 1$, and $c = 2z$ for some x, y, z. Then,

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

translates to

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

which is an absurd. Hence, from now on we may assume that a is odd, b is even, and (a, b, c) is a PPT.

As a next step, observe that $a^2 + b^2 = c^2$ is equivalent to

$$a^2 = (c - b)(c + b).$$

Therefore, it makes sense to also investigate the numbers $c - b$ and $c + b$. For example, is it possible that these numbers have a common factor? suppose that x divides both numbers. Then, in particular we have that x divides $(c - b) + (c + b) = 2c$, $(c + b) - (c - b) = 2b$, and a^2. Since x must be odd (a is odd..) it means that x is a common factor of (a, b, c), which is a contradiction.

The above observation actually gives us a little bit more information! since $(c-b)(c+b) = a^2$, and since $c - b$ and $c + b$ have no common factors, it follows that both of them must be squares! (this observation will be made formal only in few lectures). Therefore, one can write

$$c - b = t^2 \text{ and } c + b = s^2$$

for some odd numbers $s, t \in \mathbb{N}$ (recall that c is odd and b is even and therefore both $c \pm b$ are odd).

Now, solving these equations, we get that

$$c = \frac{s^2 + t^2}{2} \text{ and } b = \frac{s^2 - t^2}{2}.$$

Moreover, by a simple calculation we get that $a = st$, and therefore, we showed that if (a, b, c) is a PPT, then there exist s, t odd such that

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

This gives us half way for proving the following theorem:

Theorem 2.2 (PPT theorem)**.** *The collection of triples* $(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$ *with* $s > t \geq 1$ *being odd numbers with no common factors give us* **all** *the PPTs.*

Proof. We've already shown that every PPT can be written in such a way for **some** $s > t \geq 1$ odd numbers with no common factors. It is thus enough to show that every such triple is indeed a PPT. To this end, observe that

$$(st)^2 + \left(\frac{s^2-t^2}{2}\right)^2 = \frac{s^4 + 2s^2t^2 + t^4}{4} = \left(\frac{s^2+t^2}{2}\right)^2$$

as desired. We also need to check that the triple $(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$ has no common factors, but for making this formal, we will have to wait few lectures. This (almost) completes the proof. □

The above theorem looks quite magical at first glance, and I'm not sure it actually sheds much light on why PPTs have so much structure. The proof we presented might look like a pure luck, but it is not really the case. In the next section we will show that there is a nice method which extends a bit more generally, and it also gives us much more intuition about the structure.

3 Pythagorean triples and the unit circle

Here we will show a different way to find all the possible Pythagorean triples. Observe that $a^2 + b^2 = c^2$ is equivalent (in case that $c \neq 0$) to

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Moreover, as the set of all $(x, y) \in \mathbb{R} \times \mathbb{R}$ for which $x^2 + y^2 = 1$ forms the unit circle, and since a pythagorean triple corresponds (after scaling by c) to a point of the form $(\frac{a}{c}, \frac{b}{c})$ on the unit circle, we are interested in finding all the *rational* points on the circle. One to do so is the following: let us fix some rational point on the unit circle, say $(-1, 0)$. Now, let $\ell_m(x)$ be the line passing through $(-1, 0)$ and with slope m. That is, $\ell(x) = m(x+1)$. Observe that for all $m \in \mathbb{R}$, this line has exactly two intersections with the circle (WHY?) and that for each point $p := (x, y)$ on the circle there exists a unique $m_p \in \mathbb{R}$ for which ℓ_{m_p} passes through p. Moreover, every rational point p on the circle corresponds to an $m_p \in \mathbb{Q}$ and every rational $m \in \mathbb{Q}$ corresponds to a rational point p_m on the circle (WHY?). Therefore, writing $y = m(x+1)$ with $m \in \mathbb{Q}$ we wish to solve

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

which gives us (after a small calculation) that

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

In particular, we proved that

Theorem 3.1. *Every point on the circle $x^2 + y^2 = 1$ with rational coordinates can be obtained from the formula*

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

where $m \in \mathbb{Q}$ (except for the point $(-1, 0)$ which is obtained by taking $m \to \infty$).

We can compare the formula we've just obtained to the formula from the previous section as follows: write $m = \frac{t}{s}$, and obtain that

$$\left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right) = \left(\frac{s^2 - t^2}{s^2 + t^2}, \frac{2st}{s^2 + t^2}\right)$$

which corresponds to the triple

$$(a, b, c) = (s^2 - t^2, 2st, s^2 + t^2).$$

Dividing the above by 2 we obtain the familiar formula for PPT.

4 Sum of higher powers and Fermat's last theorem

Fermat's last theorem asserts that the equation

$$a^n + b^n = c^n$$

has no non-trivial integer solutions for all $n \geq 3$.

This theorem was solved in 1994 by Andrew Wiles (it is highly recommended to watch the documentary about this problem! see for example `https://topdocumentaryfilms.com/fermats-last-theorem/`), 350 years after Fermat declared that he has a proof for it but "this margin is too small to contain"!

We won't give too much math content here. For a more detailed historical review please read Chapter 4 in the book [1].

5 Divisibility and the Greatest Common Divisor

Suppose that m, n are two given integers. We say that m *divides* n, and denote it by $m \mid n$, if and only if there exists some integer k for which $n = m \cdot k$. If m doesn't divide n then we write $m \nmid n$. A number that divides n is called a *divisor* of n. The *Greatest Common Divisor* (or GCD for short) of two numbers a, b, which is denoted by $\gcd(a, b)$, is an extremely important quantity in number theory, as we will see many times during our class.

Definition 5.1. *The* Greatest Common Divisor *of two numbers a, b (not both zero) is the largest integer that divides both a and b. It is denoted by* $\gcd(a, b)$. *If* $\gcd(a, b) = 1$ *then we say that a and b are* relatively prime.

In this section we deal with the problem of calculating the GCD of two given numbers efficiently, using the so called *Euclidean algorithm*.

Euclid's algorithm Euclid's algorithm (or the Euclidean algorithm) is a very efficient and ancient algorithm to find the *greatest common divisor* $\gcd(a, b)$ of two integers a and b. It is based on the following observations. First, $\gcd(a, b) = \gcd(b, a)$, and so we can assume that $a \geq b$. Secondly $\gcd(a, 0) = a$ by definition. Thirdly and most importantly, if

$$a = zb + c$$

where z is an integer then $\gcd(a, b) = gcd(b, c)$. Indeed any divisor of a and b will divide c, and conversely any divisor of b and c will divide a. We can compute c by taking the remainder after dividing a by b, i.e. c is a mod b. (We will discuss the mod operation in greater details in the next section, but at this point, we only need the definition of c as the remainder of dividing a by b.) But $c < b < a$ and thus we have made progress by reducing the numbers we have to compute their gcd of. And therefore, we can proceed and express b as:

$$b = yc + d,$$

(thus $d = b \bmod c$) and thus $\gcd(b, c) = \gcd(c, d)$. We continue until we express $\gcd(a, b)$ as $\gcd(g, 0) = g$, and at that point, we have found the gcd.

Example. Let $a = 365$ and $b = 211$. Then $c = 154$ and we have that $\gcd(365, 211) = \gcd(211, 154)$. Continuing, we get:

$$\begin{aligned}
\gcd(365, 211) &= \gcd(211, 154) \\
&= \gcd(154, 57) \\
&= \gcd(57, 40) \\
&= \gcd(40, 17) \\
&= \gcd(17, 6) \\
&= \gcd(6, 5) \\
&= \gcd(5, 1) \\
&= \gcd(1, 0) \\
&= 1.
\end{aligned}$$

The gcd of 365 and 211 is 1, which means that they are *relatively prime.*

We now state an easy consequence of Euclid's algorithm

Lemma 5.2. *For any positive integers, there exist integers s and t such that* $\gcd(a,b) = sa + tb$.

Indeed, Euclid's algorithm also allows to find such integers s and t. This clearly proves that no common divisor to a and b is greater than $\gcd(a,b)$ since any common divisor to a and b is also a divisor to $sa+tb$. To find s and t, we proceed bottom up. Suppose we have found u and v such that

$$\gcd(b,c) = ub + vc.$$

Then, knowing that $a = zb + c$ allows us to replace c by $a - zb$ and therefore get:

$$\gcd(a,b) = \gcd(b,c) = ub + v(a - zb) = va + (u - vz)b.$$

Thus, we have expressed the gcd as an integer combination of a and b, knowing it as an integer combination of b and c. Thus bottom up we can find s and t such that

$$\gcd(a,b) = sa + tb.$$

This procedure is often referred to as the *extended Euclidean algorithm.*

Example. Consider again the example with $a = 365$ and $b = 211$. We express their $\gcd(365, 211) = 1$ by going bottom up in the derivation above, and derive:

$$\begin{array}{rcll}
1 &=& 6 - 5 & \\
&=& 6 - (17 - 2 \cdot 6) & = \quad -17 + 3 \cdot 6 \\
&=& -17 + 3 \cdot (40 - 2 \cdot 17) & = \quad -7 \cdot 17 + 3 \cdot 40 \\
&=& 3 \cdot 40 - 7 \cdot (57 - 40) & = \quad 10 \cdot 40 - 7 \cdot 57 \\
&=& 10 \cdot (154 - 2 \cdot 57) - 7 \cdot 57 & = \quad 10 \cdot 154 - 27 \cdot 57 \\
&=& 10 \cdot 154 - 27 \cdot (211 - 154) & = \quad 37 \cdot 154 - 27 \cdot 211 \\
&=& 37 \cdot (365 - 211) - 27 \cdot 211 & = \quad 37 \cdot 365 - 64 \cdot 211
\end{array}$$

Exercise 5.3. *Show that* $\gcd(a,b)$ *is the minimal positive integer z for which the equation $ax + by = z$ has integer solutions.*

We want to investigate solutions to linear equations of the form $ax + by = c$ where a, b, c are given integers and (x, y) are integers. As we saw above, there exists a solution if and only if c is divisible by g. Can you find more solutions?

To get some intuition, recall that $ax + by = c$ is a linea equation, and therefore we are looking for the set of all integer points along this line (if there are any).

So from now on assume that c is divisible by g, and that some solution (x_0, y_0) is given. First of all, we want to show that we can find infinitely many solutions. Indeed, consider the pair $(x, y) = (x_0 + (b/g)n, y_0 - (a/g)n)$, where n is any integer. Clearly we have that

$$ax + by = ax_0 + bx_0 + (ab/d)n - (ab/d)n = c.$$

Next we want to convince ourselves that all solutions have this form. Indeed, let (x, y) be an arbitrary solution. Then in particular we have that

$$a(x - x_0) = -b(y - y_0),$$

and therefore

$$\frac{a}{g}(x - x_0) = -\frac{b}{g}(y - y_0).$$

Since $\frac{a}{g}$ and $\frac{b}{g}$ are relatively primes, it follows that

$$\frac{a}{g} \mid y - y_0.$$

In particular we have that $y - y_0 = \frac{a}{g}n$ for some integer n. Therefore, we have that

$$\frac{a}{g}(x - x_0) = -\frac{b}{g}\frac{a}{g}n,$$

which gives us

$$x - x_0 = -\frac{b}{g}n$$

as desired.

Exercise 5.4. *A farmer wishes to buy 100 animals and spend exactly* 100*. Cows are* 10*, sheep are* 3 *and pigs are* 0.50*. Is this possible?*

6 Factorization and the Fundamental theorem of arithmetic

A number $p \in \mathbb{N}$ is called a *prime* number if it only divisible by ± 1 and by itself. For example, $2, 3, 5, 7, 11$ are all primes. The numbers $4, 6, 9$ are not as they can be written as $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, and $9 = 3 \cdot 3$.

The following lemma about prime numbers is extremely important and also non-obvious:

Lemma 6.1. *Let p be any prime and suppose the $p \mid a \cdot b$, where $a, b \in \mathbb{Z}$. Then, $p \mid a$ or $p \mid b$.*

Proof. Suppose that $p \nmid a$, as otherwise there is nothing to prove. We will show that in this case we must have $p \mid b$. Since p is prime, it follows that $\gcd(p, a) = 1$ (WHY?). Therefore, there are $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Multiplying this expression by b we obtain

$$abx + pby = b.$$

Now, since $p \mid abx$ and $p \mid pby$, it follows that $p \mid b$. This completes the proof. □

Observe that the above proof can be easily generalized to prove the following:

Theorem 6.2 (Prime divisibility property)**.** *Let p be a prime number, and suppose that $p \mid a_1 \cdot a_2 \cdots a_r$. Then, $p \mid a_i$ for some $1 \leq i \leq r$.*

Proof. Exercise! □

The following theorem is the most fundamental theorem in Number Theory:

Theorem 6.3 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ can be written as a factor of (not necessarily distinct) primes*

$$n = p_1 \cdots p_r$$

in a unique way (up to the order of the factors).

Proof. Here we will only give a sketch of the proof and hopefully the completion will be obvious. Basically, the theorem follows from the following two assertions:

Assertion 1 The number n can be factored into prime factors in some way.

Assertion 2 There is a unique such factorization.

The idea is quite simple. For Assertion 1 we can just go by induction: $n = 2, 3, 4, 5$ are obvious. Suppose you know it for n and want to prove it for $n+1$. If $n+1$ is prime, then we can write $n+1 = n+1$. Otherwise, there exists some prime $p < n + 1$ such that $n + 1 = p \cdot m$, and $m < n + 1$. Now, by induction we can factorize m and we're done.

For the second assertion: Suppose $n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{\ell} q_j$, where all the p_i and q_j are primes. Fix some arbitrary prime p_i. Since it appears in the product, it must divide n. In particular we have that $p_i \mid \prod_{j=1}^{\ell} q_j$. Therefore, by our prime divisibility property we have that $p_i \mid q_j$ for some j. But, since q_j is also a prime, it must be the case that $p_i = q_j$. Dividing both expressions by p_i, we can continue by induction. □

Exercise 6.4. *Let $s > t \geq 1$ be two integers with $\gcd(s, t) = 1$. Show that the three number st, $\frac{s^2-t^2}{2}$, $\frac{s^2+t^2}{2}$ are pairwise relatively prime.*

Solution. Suppose that there exists some integer $x \geq 2$ dividing the three of them and we can assume that x is prime (WHY?). Now, $x \mid \frac{s^2-t^2}{2}$ and $x \mid \frac{s^2+t^2}{2}$, and therefore we have that

$$x \mid \frac{s^2+t^2}{2} + \frac{s^2-t^2}{2} = s^2,$$

and

$$x \mid \frac{s^2+t^2}{2} - \frac{s^2-t^2}{2} = t^2.$$

Since x is a prime, we have that $x \mid s$ and $x \mid t$ which contradicts the fact that $\gcd(s,t) = 1$.

7 Congruences

In this section we will discuss *congruences* and define *modular arithmetic*. Congruences give a convenient way to describe divisibility properties.

First let us give an easy definition: for integers a, b, m we say that a is *congruent* to b modulo m, and write $a \equiv b \pmod{m}$, if $a - b$ is a multiple of m. That is, if $a - b = xm$ for some integer $x \in \mathbb{Z}$. The number m is called the *modulus* of the congruence.

For any integer $n \in \mathbb{Z}$ there is a unique integer r in $\{0, 1, \ldots, m-1\}$ such that $n \equiv r \bmod m$. Then r is called the *residue* of n modulo m, and by slight abuse of notation we will refer to it as $n \bmod m$. One can find the residue of a number n by taking the remainder when dividing by m. Although we will often use them interchangeably, there is a slight difference between $a = n \bmod m$ and $a \equiv n \pmod{m}$; in the former case, a is the residue and thus between 0 and $m - 1$. In later notes, however, we typically simply write $a = n \pmod{m}$ and the interpretation is usually clear.

Congruences with the same modulus behave in many ways like ordinary equations. That is, if $a_1 \equiv b_1 \bmod m$ and $a_2 \equiv b_2 \bmod m$, then

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod m \text{ and } a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod m.$$

Indeed, let us check the former: we know that $a_1 = xm + b_1$ and $a_2 = ym + b_2$ for some integers $x, y \in \mathbb{Z}$. Therefore, we have that

$$a_1 + a_2 = (x + y)m + (b_1 + b_2),$$

so $(a_1 + a_2) - (b_1 + b_2)$ is divisible by m. You can prove the other cases in a similar fashion (do it!).

Warning! It is not always possible to divide congruences! that is, if $ab \equiv ac \bmod m$, it does not necessarily imply that $a \equiv c \bmod m$, even if both $a, c \neq 0 \bmod m$. Indeed, suppose that $m = 8$, and observe that for $a = 4, b = 2, c = 4$ we have

$$ab \equiv ac \bmod 8 = 0 \bmod 8.$$

Congruences with unknowns can be solved in the same way that equations are solved. For example, suppose we wish to solve

$$x + 10 \equiv 3 \bmod 12.$$

Then we clearly have that

$$x \equiv -7 \bmod 12.$$

It is an easy observation that $-7 \bmod 12 \equiv 5 \bmod 12$ (WHY?), so we can use either of them.

Note that some congruences have no solutions. For example, $x^2 = 3 \mod 10$ has no solutions (one can simply check all the residues).

In general, there is a deeper theory behind this "modular arithmetic" which is not explained in the text book, but I feel obliged to explain.

Let us define binary operations $\oplus, \otimes$ on the set $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ as follows. For $a, b \in \mathbb{Z}_m$ we define $a \oplus b$ to be the residue of $(a + b)$ modulo m. Similarly, we define $a \otimes b$ to be the residue of $(a \times b)$ modulo m (so one can think about these operations as "addition modulo m" and "multiplication modulo m", respectively).

Example. In $\mathbb{Z}_5$, one has $3 \oplus 4 = 2$ and $3 \otimes 4 = 2$.

For $a \in \mathbb{Z}_m$, we denote $\ominus a$ the residue of $-a$ modulo m. Here are a few very easy facts that you are invited to check. If $a \in \mathbb{Z}_m$ and $d = \ominus a$ then

$$a \oplus 0 = 0 \oplus a = a,$$

and

$$a \oplus d = d \oplus a = 0.$$

Moreover, for all $a, b, c \in \mathbb{Z}_m$,

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

The above relation are precisely the conditions showing that $(\mathbb{Z}_m, \oplus)$ is a *group*. It is not a class about group theory so we won't talk much about groups in general, but it is important (in my opinion) at least to know that we are talking about some special cases of more general algebraic structures.

If we consider the operation $\otimes$ (instead of $\oplus$), the role of 0 for $\oplus$ is now played by 1 since $a \otimes 1 = 1 \otimes a = a$. 1 is the multiplicative identity, in the same way as 0 was the additive identity. However 0 never has a multiplicative inverse (in the same way as $\ominus a$ is playing the role of the additive inverse); the *multiplicative inverse* of an element a is defined as an element b such that $b \otimes a = 1$. Even if we exclude 0 and consider $\mathbb{Z}_m - \{0\}$, we will see that some nonzero elements may not have a multiplicative inverses. However, when m is a prime number, $(\mathbb{Z}_m - \{0\}, \otimes)$ is a group (or in other words: each element has a multiplicative inverse).

Let us go back to congruences, and our first task is to solve congruences of the form

$$ax \equiv c \bmod m.$$

Observe that some congruences of this type have no solutions. For example, if we wish to solve

$$8x \equiv 21 \bmod 248,$$

then we need to find integer solutions to $8x - 21 = 248y$ which we clearly don't have (WHY?).

In general, we know that $ax + my = c$ has integer solutions if and only if $\gcd(a, m) \mid c$. Moreover, we derived a formula to obtain all these solutions based on a private solution (which can be found by the Euclidean algorithm).

Let us explain once again how to solve it: let $g := \gcd(a, m)$ and we wish to solve $ax \equiv c \bmod m$, where $g \mid c$. First, we can find a solution to

$$as + mt = g.$$

Then, we can multiply both parts by c/g to obtain

$$a \cdot (sc/g) + m \cdot (tc/g) = c,$$

as desired.

This means that

$$x = \frac{sc}{g} \bmod m \text{ and } y = \frac{tc}{g} \bmod m$$

is a solution to the congruence. Are there any other solutions?

Suppose that (x_1, y_1) is another solution. Then in particular we have that

$$ax \equiv ax_1 \bmod m$$

and therefore m divides $a(x - x_1)$. Since $\gcd(a, m) = g$, and since $a/g, m/g$ are relatively prime, we obtain that m/g divides $x - x_1$. In particular, we have that $x_1 = x + n \cdot \frac{m}{g}$ for some $n \in \mathbb{Z}$.

Now, since any two solutions that differ by a factor of m are considered the same modulu m, there are exactly g different solutions. Namely, $n = 0, \ldots, g - 1$.

To summarize our findings, let us state Theorem 8.1 from Chapter 8 in the book.

Theorem 7.1. *Let a, c, and m be integers with $m \geq 1$, and let $g = \gcd(a, m)$.*

1. *If $g \nmid c$ then the congruence $ax = c \bmod m$ has no solutions.*
2. *If $g \mid c$ then the congruence $ax = c \bmod m$ has exactly g distinct solutions in $\mathbb{Z}_m$. To find all solutions we dirst need to find one solution (s, t) to the lineae equation $as + mt = c$ (for example, by the Euclidean algorithm). Then, $x = s + k \cdot \frac{m}{g}$ is a solution to the congruence for every $k = 0, \ldots, g-1$.*

Next, let us show that if m is a prime then every element in $\mathbb{Z}_m^*$ has a multiplicative inverse. Indeed, let $a \in \mathbb{Z}_m^*$, since $a \neq 0 \bmod m$, and since m is prime, we know that $\gcd(a, m) = 1$. In particular, there are $x, y \in \mathbb{Z}$ such that $ax + my = 1$. This is equivalent to saying that $ax \equiv 1 \bmod m$. Let $r \in \mathbb{Z}_m$ be the unique residue with $x \equiv r \bmod m$, we obtain that $ar = 1 \bmod m$ as desired.

Exercise 7.2. *Let $m \in \mathbb{N}$, and let $a \in \mathbb{Z}_m^*$. Show that if a has a multiplicative inverse, then it is unique.*

In general, we can show that for all a, m with $\gcd(a, m) = 1$, the congruence $ax = c \bmod m$ has exactly one solution for all $c \in [m]$. In particular we have that a is invertible mod m. On the other hand, if $\gcd(a, m) \neq 1$, then it can easily be shown that a is not invertible mod m.

We can also ask ourselves about the number of solutions to polynomial equations over $\mathbb{Z}_m$. Recall that over the reals, each linear equation of the form $ax = c$ has a unique solutions (unless $a = 0$, which is the only non-invertible element in $\mathbb{R}$). Moreover, we know that for a polynomial of degree d, $P(x)$, the equation $P(x) = c$ can have at most d solutions. This follows from the fact that $\mathbb{R}$ is a *field*. It is not hard to show that $\mathbb{Z}_m$ is a field if and only if m is a prime (try to do it, we won't do it in class). Therefore, we have the following

Theorem 7.3 (Polynomial roots mod p)**.** *Suppose p is a prime and $P(x)$ is a polynomial of degree exactly $d \geq 1$ with integer coefficients such that the leading coefficient is not divisible by p. Then, the congruence $P(x) = 0 \bmod p$ has at most d distinct solutions.*

8 Congruences, powers, and Fermat's Little Theorem

Suppose that we want to compute $13^{270} \bmod 131$. Do you see a simple way to do it?

Let us state a simple and extremely useful theorem:

Theorem 8.1. *Fermat's Little Theorem Let p be a prime, and let a be any integer with $a \neq 0 \bmod p$. Then, $a^{p-1} \equiv 1 \bmod p$.*

Proof. There are many proofs for this theorem. Here we will give a direct one, but in general, it is not hard to show that for every group G and every element $a \in G$, we have that $a^{|G|} = e_G$, where e_G is the identity element of G.

First, observe that $a, 2a, \ldots, (p-1)a$ correspond to all the non-zero distinct residues $\bmod p$. Indeed, if $sa \equiv ta \bmod p$, then $(s-t)a \equiv 0 \mod p$, which yields $p \mid a$, contradiction.

So we know that modulo p we have that

$$\{a, 2a, \ldots, (p-1)a\} = \{1, 2, \ldots, p-1\}.$$

In particular, we have that

$$a^{p-1}(p-1)! = (p-1)! \bmod p,$$

and since $(p-1)! \neq 0 \bmod p$, it must be invertible modulo p so we can multiply by its inverse and obtain the desired. □

Complete the example.

Exercise 8.2. *Try to find a formula for $(p-1)! \mod p$ for any prime p. Hint: distinguish the cases $p = 2$ and $p > 2$.*

Exercise 8.3. *Try to do the same for general numbers. That is, find a formula to compute $(m-1)! \bmod m$. Do you see how to distinguish the cases m is a prime or not?*

9 Congruences, Powers, and Euler's formula

In the previous section we proved that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$. This formula is certianly not true if we replace p by some composite number m (find example!). So, the question we are interested at is whether there exists some power x, depending on m, for which $a^x \equiv 1 \bmod m$. First observe that if $\gcd(a, m) \neq 1$, then this is impossible! Indeed, suppose that $a^k \equiv 1 \bmod m$ for some $k \geq 1$. Therefore, it follows that $\gcd(a, m)$ divides $a^k - my = 1$ for some integer y, but this is clearly an absurd.

Next, we will restrict our attentions only to these residues $a \in \mathbb{Z}_m$ for which $\gcd(a, m) = 1$. Let $\mathbb{Z}_m^*$ be the set of all these residues. It is not hard to show that $\mathbb{Z}_m^*$ is a multiplicative group (for our discussion, just convince yourselves that if $a, b \in \mathbb{Z}_m^*$ then we also have that $ab \in \mathbb{Z}_m^*$). Let us define the following function, known as *Euler's phi function*, as follows:

$$\phi(m) = |\mathbb{Z}_m^*| = |\{a \in \mathbb{Z}_m \mid \ \gcd(a, m) = 1\}| .$$

Note that if p is prime, then we clearly have that $\phi(p) = p - 1 = p(1 - \frac{1}{p})$. It is not hard to show that $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.

In general, we will see later that the function is *multiplicative* in the sense that if $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a) \cdot \phi(b)$. In particular it gives that:

Lemma 9.1. *Euler's product formula For every n we have that*

$$\phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p}).$$

Do you see how to prove this lemma "by hands"?

The main goal of this chapter is to prove the following theorem, known as Euler's formula:

Theorem 9.2 (Euler's formula)**.** *For all $m \in \mathbb{N}$ and $a \in \mathbb{Z}_m^*$ we have that*

$$a^{\phi(m)} \equiv 1 \bmod m.$$

Note that this theorem extends Fermat's little theorem to all values of m. In particular, if m is a prime, then since $\phi(m) = m - 1$, Fermat's little theorem just follows.

Proof. We can prove it either by using group theory (the structure $(\mathbb{Z}_m^*, \times)$ is a group, and it is known that for every finite group G and every element $a \in G$ we have that $a^{|G|} = e$, where e is the identity element of the group). Since we don't assume background in group theory, we will give a direct proof here:

Let $\mathbb{Z}_m^* = \{b_1, \ldots, b_t\}$, where $t = \phi(m)$, be all the distinct elements of $\mathbb{Z}_m^*$. As we have already convinced ourselves, for every $a, b \in \mathbb{Z}_m^*$, we have that $a \cdot b \in \mathbb{Z}_m^*$. In particular we have that $\{ab_1, \ldots, ab_t\} = \{b_1, \ldots, b_t\}$ (WHY?). Therefore, we have that

$$a^{\phi(m)} \cdot \prod b_i = \prod b_i \bmod m.$$

Since $\prod b_i \in \mathbb{Z}_m^*$, it has a multiplicative inverse, and therefore we conclude that

$$a^{\phi(m)} \equiv 1 \bmod m.$$

This completes the proof. □

10 Public Key Cryptosystems

In this section we will talk about a topic that I originally planned to do at the end of the course. The reason is that it is a good time to pause, review all the material that we learnt, and motivate some topics that we need to learn in order to complete the arguments.

The topic is about one of the main applications of Number Theory in our everyday life: Cryptography.

Our goal is to construct *secret codes*. A sender would like to encrypt his message to protect its content while the message is in transit. The receiver would like to easily decode the received message.

Question 10.1. *Can you think about unbreakable codes? Can you list their disadvantages?*

The traditional way of creating secret codes is that both the sender and the receiver share a secret, called a key. The sender scrambles the message in a complicated way that depends on the key. The receiver then uses the key to unscramble the message. If these codes are constructed properly (something which is surprisingly hard to do), it seems virtually impossible for somebody without the key to decode the message, even if they have many examples of pairs of messages and their encodings to work from in trying to deduce the key.

For example, imagine that I'm having coffee with a friend and I want to be able to send him private messages which I'm not interested anyone else to read. I can generate a random matrix A and tell him its inverse (finding an inverse of a matrix is computationally not very hard). Whenever I want to send him some message x (think about x as a string of numbers), then I simply send him the value $y := Ax$. Therefore, unless x is an eigenvector (very unlikely to have...), the message is "well mixed". Regarding my friend, in order to read my message, he needs to multiply y by A^{-1} and then he recovers A. Can someone break this code? it is very unlikely that you can guess which matrix A I chose, and basically you gain no information from the messages y which theoretically you can see (imagine that I post the vector y in facebook).

The drawback of this method is ensuring that every pair of people who need to communicate secretly have a shared secret key (that is, I cannot just post the matrix A online because then everyone can find its inverse very easily!). Distributing and managing these keys is very difficult and it makes it hard for secret communication over the internet. For example, suppose you want to send your credit card securely to a store you have never before heard of, how can you do that?

Here we will learn a better way to do it. In general, if you think about it a bit, we don't really need unbreakable codes. We need "efficient" codes (whatever it means), which are "very hard" to break (let's say, if it takes around 10,000 years to break it using a home computer). These are the basic needs in modern cryptography.

A "good" coding scheme have the following properties:

1. encoding is easy to perform;
2. decoding is extremely difficult (for protection against eavesdroppers);
3. decoding is easy if you are in possession of some secret "key".

In 1976 Diffie and Hellman came up with a scheme for handling such communications, called a *public key cryptosystem*. It is based on the assumption that there is a wide class of functions that are relatively easy to compute but extraordinarily difficult to invert unless you possess a secret (and here Number Theory comes into the play).

According to this scheme, each communicator or recipient, say Bob or B, publishes in a well defined place (a kind of telephone directory) a description of his function, f_B from this class; this is Bob's *public key*. Bob knows also the inverse of f_B, this is his *private key*. The assumption is that this inverse is extremely difficult to compute if one does not know some private information.

Suppose now that someone, say Alice or A, would like to send a message m to B. She looks up Bob's public key and sends $m' = f_B(m)$. Since Bob knows his own private key, he can recover $m = f_B^{-1}(m')$. The problem here is that Bob has no guarantee that Alice sent the message. Maybe someone else claiming to be Alice sent it. So, instead, suppose that Alice sends the message $m' = f_B(f_A^{-1}(m))$ to Bob. Notice that Alice needs to know Bob's public key (which she can find in the diretory) and also her own private key, which is known only to her. Having received this message, Bob can look up Alice's public key and recover m by computing $m = f_A(f_B^{-1}(m'))$; again, for this purpose, knowledge of Bob's private key and Alice's public key is sufficient. Anyone else would have to solve the said-to-be-extraordinarily-difficult task of inverting the action of one or another of these functions on some message in order to read the message or alter it in any way at all. This is the basic setup for a public-key cryptosystem. One can also use it for digital signatures. If Alice wants to show to anyone that she wrote message m, she can publish or send $m' = f_A^{-1}(m)$, and anyone can test it came from Alice by computing $f_A(m')$.

In what follows, we will talk about the so-called RSA public key cryptosystem. It was invented by Ron **R**ivest, Adi **S**hamir and Len **A**dleman in 1977. Their scheme is based on the fact that it is easy to multiply two large numbers together, but it appears to be very hard to factor a large number. The record so far for factoring has been to factor a 768-bit number (i.e., 232 digits) given in an RSA challenge, and this took the equivalent of 20,000 years of computing on a single-core machine... The task of factoring a 1024-bit number appears to be 1,000 harder with the current algorithms.

10.1 The RSA code

For this code, choose two very large prime numbers (say with several hundred digits), p and q, and form the product $N = pq$. Choose a number $z < N$ such that z is relatively prime to $(p-1)(q-1) = N - p - q + 1$. Knowing p and q (or $(p-1)(q-1)$) we can find the multiplicative inverse y to z modulo $(p-1)(q-1)$ by the extended Euclidean algorithm. The pair (N, z) constitutes the public key, and (N, y) constitutes the private key.

If we want to encode a message, we first view it as a number in base N. Every digit is a number between 0 and $N-1$ and we will encode each digit $0 \leq m < N$ separately. The sender computes $s = m^z \bmod N$ and transmits s. Upon receiving s, the receiver, who knows the private key, computes $s^y \bmod N$. The claim is that this is precisely m, i.e. $m = s^y \bmod N$.

If one could factor N into $N = pq$ then one can easily compute y from z (by the extended Euclid algorithm) and therefore break this public-key cryptosystem. However, as we said previously, factoring large numbers appears to be very challenging.

Why does this scheme work? Let $x = s^y$; we want to show that $m = x \bmod N$. We have that

$$x = s^y = m^{yz} \pmod{N},$$

and since z and y are multiplicative inverses modulo $(p-1)(q-1)$, we get that

$$x = m^{1+k(p-1)(q-1)} = mm^{k(p-1)(q-1)} \pmod{N}.$$

We want to prove that this is equal to $m \bmod N$. We will first show that $x \equiv m \pmod{p}$ and $x \equiv m \pmod{q}$, and then we wish to conclude that $x \equiv m \bmod pq$ (this will be a simple observation from a

theorem called "the Chinese Remainder Theorem" that we will earn soon). To show that $x \equiv m \pmod{p}$, we need to consider two cases. First, if m is a multiple of p, then x is also a multiple of p, and so $x \equiv m \equiv 0 \pmod{p}$. Otherwise, if m is not a multiple of p then it must be relatively prime to p (since p is prime): $\gcd(m, p) = 1$. Thus we can apply Fermat's Little Theorem, which tells us that $m^{p-1} \equiv 1 \pmod{p}$, and thus

$$m^{k(p-1)(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}.$$

Multiplying by m, we indeed obtain $x \equiv m \pmod{p}$.

Similarly, we will show that the same conclusion holds for q. Therefore, we can conclude (for now, informally) that $x \equiv m \bmod N$, which concludes the correctness of RSA.

What do we need to do in order to use RSA?

- Find large primes.
- Calculate the inverse of z (and also finding some z with $\gcd(z, (p-1)(q-1)) = 1$).
- Compute $m^z \bmod N$ (or $s^y \bmod N$) when z is very large.

We are already familiar with parts of the above list, but we still need to learn some new ingredients.

11 Euler's Phi function and the Chinese remainder theorem

Recall that in the previous section we proved Euler's theorem which asserts that

$$a^{\phi(m)} \equiv 1 \bmod m,$$

for all $a \in \mathbb{Z}_m^*$. This theorem won't be useful unless we can find an efficient way to calculate $\phi(m)$. We already gave a hint for how a formula for $\phi(m)$ should look like, and here we will prove it.

Theorem 11.1. *If* $\gcd(m,n) = 1$ *then* $\phi(mn) = \phi(m) \cdot \phi(n)$.

Proof. We will show that

$$|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*|$$

by define a bijection between these sets. Let us define:

$$f(a) = (b,c) \text{ where } b \equiv a \bmod m \text{ and } c \equiv a \bmod n.$$

First, observe that this is well defined, as we must have that b is in $\mathbb{Z}_m^*$ and $c \in \mathbb{Z}_n^*$. Indeed, if $\gcd(b,m) = g > 1$, then since $a = b + ym$, we obtain that $\gcd(a,m) \geq g > 1$ and hence $\gcd(a,mn) > 1$, contradiction. Similarly, we can prove that $c \in \mathbb{Z}_n^*$.

Second, we show that f is one-to-one. Suppose that $f(a) = f(a') = (b,c)$ for some $a, a' \in \mathbb{Z}_{mn}^*$, and we wish to show that $a = a'$. Note that $f(a) = f(a')$ implies that

$$m \mid a - a' \text{ and } n \mid a - a'.$$

Since $\gcd(m,n) = 1$, it follows that $mn \mid a - a'$, and therefore we have that $a \equiv a' \bmod mn$.

Lastly, we wish to show that f is onto. Indeed, let $(b,c) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, and we wish to show that there exists an $a \in \mathbb{Z}_{mn}^*$ for which $f(a) = (b,c)$. Since $\gcd(m,n) = 1$, there exists an integer solution (x,y) to $mx + ny = 1$. Define, $a = cmx + bny$ (or more formally, the residue of the above a modulo mn). OBserve that

$$a = c(1 - ny) + bny \equiv c \bmod n \text{ and } a = cmx + b(1 - mx) \equiv b \bmod n.$$

Therefore, in order to complete the proof, it is enough to show that $a \in \mathbb{Z}_{mn}^*$. Suppose that $a \notin \mathbb{Z}_{mn}^*$. Then we have $\gcd(a,mn) = g > 1$. Let p be some prime dividing g. Since $\gcd(m,n) = 1$ and $p \mid mn$ we have that $p \mid m$ or $p \mid n$. Suppose that $p \mid m$ (the case $p \mid n$ is similar) and observe that since $a = b + mz$ for some integer z, it follows that $p \mid b$. But then we have that $\gcd(b,m) \geq p > 1$, contradiction to the fact that $b \in \mathbb{Z}_m^*$. This completes the proof.

□

A similar proof strategy as in the above theorem can help us to prove the so-called "Chinese remainder theorem". This theorem was discovered by the Chinese mathematician Sun Tzu in the 4-th century AD and written in his book the Sun Tzu Suan Ching. It says the following. If a and b are relatively prime then there is a bijection between the possible remainders modab and the pairs of possible remainders mod$a$ and mod$b$. In other words, the two numbers (the remainder of x upon dividing by a and the remainder of x upon dividing by b) uniquely determines the number x upon dividing by ab, and vice versa. Let's look at an example. Let $a = 7$ and $b = 13$, then $ab = 91$. Any arbitrary remainder, say 73 mod 91, is equivalent to the pair $(3,8) = (73 \bmod 7, 73 \bmod 13)$. No other remainder mod 91 leads to the pair $(3,8)$.

Theorem 11.2 (Chinese Remainder Theorem)**.** *Suppose that m, n are relatively prime. Then, the system of equations*

$$x = a \mod m$$
$$x = b \mod n$$

has a unique solution for $x \in \mathbb{Z}_{mn}$.

Proof. We will see two proofs.

Proof 1: same like previous proof.

Proof 2: Let $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Since $\gcd(m, n) = 1$ we have that $m \in Z_n^*$ and $n \in \mathbb{Z}_m^*$. Therefore, one can find a multiplicative inverse m' for m mod n, and a multiplicative inverse n' for n mod m. Let

$$x = ann' + bmm' \mod mn.$$

Clearly we have that x is a solution to the above congruent. □

This theorem implies that we can represent elements in $\mathbb{Z}_{mn}$ by pairs in $\mathbb{Z}_m \times \mathbb{Z}_n$. Moreover, this correspondence goes even further: suppose that $a, a' \in \mathbb{Z}_{mn}$ and $(b, c), (b', c')$ are the corresponding pairs, respectively. Then, a moment's thought reveals that $a+a'$ corresponds to $(b+b', c+c')$, and aa' corresponds to (bb', cc') (convince yourself!).

Now let us play a little bit with the remainder pairs representations. For example, let's try to find the solutions of the equation $x^2 = 1$ mod ab where a and b are relatively prime. Since the remainder 1 mod ab is represented by the remainder pair $(1, 1)$ (where the pair represents the values modulo a and b), it is easy to see that this equation has four solutions: the remainder pairs $(1, 1), (-1, 1), (1, -1), (-1, -1)$. (Here, $(-1, 1)$ is a convenient notation for $(a - 1, 1)$.) Try to convince yourself that there are no other solutions.

Exercise 11.3. *Find all solutions to $x^2 = 1 \mod 15$.*

Here we will give an extension of the Chinese Remainder Theorem for more variables:

Theorem 11.4. *Let $m_1, \ldots, m_r$ be pairwise relatively primes integers (that is, $\gcd(m_i, m_j) = 1$ for all $i \neq j$). Then, for all $a_1, \ldots a_r$, the system of r congruences*

$$x = a_1 \mod m_1$$
$$x = a_2 \mod m_2$$
$$\vdots$$
$$x = a_r \mod m_r$$

has a unique solution modulo $M = m_1 \cdot m_2 \cdots m_r$.

Exercise 11.5. *Solve the following problem which is the first recorded instance of the Chinese Remainder Theorem (by Sun Tzu Suan Ching): "We have number of things, but we do not know exactly how many. If we count them by threes, we have two leftovers. If we count them by fives, we have three leftovers. If we count them by sevens, we have two left overs. How many things are there?"*

12 Prime Numbers

The fact that primes are basic building blocks in arithmetic is a sufficient reason to study their properties, and in this section we will mention some interesting such properties.

Let us start with one of the oldest results in Number Theory which appeared in Euclid's book "Elemenets" more than 2000 years ago!

Theorem 12.1. *There are infinitely many primes.*

We will now give two proofs for this theorem (many other proofs exist!), each contain some interesting and useful ideas.

First proof (Euclid). Suppose that there are only finitely many primes $p_1, \ldots, p_r$, and we wish to show that there must exists a prime number q which is not in this list. This will give us a contradiction.

Indeed, let us consider the number

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

Since $N > p_i$ for all i it follows that if N is a prime then we are done. Therefore, assume that N is not a prime and let q be any prime number dividing N. We show that $q \neq p_i$ for all i. Indeed, assume otherwise, then since $q \mid N$ and $q \mid p_1 \cdots p_r$, we have that $q \mid 1$ which is impossible. □

Second proof. Let $\pi(x) = |\{1 \leq p \leq x \mid \ p \text{ is a prime}\}|$. That is, $\pi(x)$ is the number of all prime numbers between 1 and x. Our goal is to show that $\pi(x) \to \infty$ as $x \to \infty$. In fact, we will show the stronger statement that $\log x \leq \pi(x) + 1$, which also gives us some clue about the "density" of primes.

Recall from calculus that for all $n \in \mathbb{N}$ and $n \leq x < n + 1$ we have

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Moreover, we can upper bound the above sum by

$$S := \sum_{\substack{m \text{ has only prime} \\ \text{divisors smaller than } x}} \frac{1}{m}.$$

Since every m like in the above sum can be factorized to primes smaller than x in a unique way, letting $\mathbb{P} := \{p_1, \ldots, p_r, \ldots\}$ be an enumeration of all primes in an increasing order, we see that

$$S = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right).$$

As the inner sum is a geometric series we have that

$$\log x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\frac{1}{1 - \frac{1}{p}} \right) = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Finally, as we trivially have that $p_k \geq k+1$ for all k, we conclude that

$$\frac{p_k}{p_k - 1} \leq \frac{k+1}{k},$$

which gives us that

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

This completes the proof. □

Next we will prove that infinitely many primes are congruent to 3 mod 4.

Theorem 12.2. *Infinitely many primes are congruent to* 3 mod 4.

Proof. The proof strategy is similar to the proof of Euclid that there are infinitely many primes. Indeed, let us assume towards a contradiction that there are finitely many such primes. Let $3, p_1, p_2, \ldots, p_r$ be an enumeration of all such primes, and let us define the integer

$$N = 4p_1p_2 \cdots p_r + 3.$$

Observe that $N \equiv 3 \bmod 4$, and that $N > p_i$ for all i (and also $N > 3$). Now, if N is prime, then we are done because it is not in our list. Otherwise, there must be some prime $q \equiv 3 \bmod 4$ for which $q > 3$ and $q \mid N$ (WHY?). Observe that if q appears in our list, then $q \mid N - 4p_1p_2 \cdots p_r = 3$, which is impossible. This completes the proof. □

The above theorem is a special case of a famous theorem in Number Theory which we won't prove in our class (it involves some complex analysis). It is highly recommended to the curious reader to google it and read its proof!

Theorem 12.3 (Dirichlet's Theorem)**.** *For every $a, m \in \mathbb{N}$ for which $\gcd(a, m) = 1$, infinitely many primes are congruent to $a \bmod m$.*

Indeed, our previous theorem is a special case if we take $a = 3$ and $m = 4$.

To conclude this section, we will prove a nice theorem using both Chinese Remainder Theorem and the fact that there are infinitely many primes. Before stating the theorem, we need some definition. Consider the infinite grid $\mathbb{Z}^2$. For each point $p := (a, b) \in \mathbb{Z}^2$, draw a line segment ℓ_p from the origin to (a, b). If this line passes through another grid point but $(0, 0)$ and (a, b) then we say that (a, b) is *invisible from the origin*. Otherwise, we say that (a, b) is *visible from the origin*.

Theorem 12.4. *For every $n \in \mathbb{N}$, there exists a point $(a, b) \in \mathbb{Z}^2$ for which all the points $(a + k, b + \ell)$, with $1 \leq k, \ell \leq n$ are invisible from the origin.*

Proof. The crucial part of the proof is the simple observation that (a, b) is invisible from the origin if and only if $\gcd(a, b) > 1$ (prove it!). Therefore, we wish to show that for every $n \in \mathbb{N}$, one can find a point $(a, b) \in \mathbb{Z}^2$ such that for all $1 \leq k, \ell \leq n$ we have $\gcd(a + k, b_\ell) > 1$.

To this end, let us take n^2 distinct primes p_{ij}, $1 \leq i, j \leq n$. The existence of such primes follows from the fact that there are infinitely many primes.

Now, define, for each $1 \leq i \leq n$, the integer $R_i = \prod_{j=1}^{n} p_{ij}$, and for each $1 \leq j \leq n$, the integer $C_j = \prod_{i=1}^{n} p_{ij}$. It is useful to think about the chosen primes in a matrix form, where each ijth entry equals p_{ij}. In this notation, R_i is just the product of all primes in row i and C_j is the product of all primes in column j.

Observe that $\gcd(R_i, R_j) = 1$ and $\gcd(C_i, C_j) = 1$ for all $i \neq j$, and that $\gcd(R_i, C_j) = p_{ij} > 1$ for all i, j.

By the Chinese remainder theorem we can find $a \in \mathbb{Z}$ such that $a \equiv -i \bmod R_i$ for all i, and $b \in \mathbb{Z}$ such that $b \equiv -j \bmod C_j$ for all j. Fix such a, b and consider the point $(a, b) \in \mathbb{Z}^2$. Observe that for all $1 \leq k, \ell \leq n$ we have that

$$(a + k, b + \ell) \equiv (0 \bmod R_k, 0 \bmod C_\ell),$$

and therefore we have that $\gcd(a + k, b + \ell) \geq p_{k\ell} > 1$. This completes the proof. □

13 Counting primes

A natural question is about the *density* of primes up to some given number x. That is, let $\pi(x)$ be the number of primes $p \leq x$, we wish to study the asymptotic behavior of $\pi(x)$. One of the corner stones of Number Theory is the following theorem:

Theorem 13.1 (The Prime Numbers Theorem)**.** *We have that*

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

In other words, the above theorem says that for every $\epsilon > 0$, there exists x_0 such that for all $x \geq x_0$ we have

$$\frac{(1-\epsilon)x}{\ln x} \leq \pi(x) \leq \frac{(1+\epsilon)x}{\ln x}.$$

The proof of the above theorem is quite involved, so here we will prove the following weaker statement which will suffice for our applications:

Theorem 13.2. *There exists $0 < C_1 < C_2$ such that for all x we have that*

$$\frac{C_1 x}{\log x} \leq \pi(x) \leq \frac{C_2 x}{\log x}.$$

We will split the proof of the above theorem into two parts: one for the upper bound and the other part for the lower bound.

For the upper bound, we will need the following simple but yet impressive result due to Erdős:

Lemma 13.3. *For all $n \in \mathbb{N}$ we have that $\prod_{\substack{p\leq n \\ p \text{ is prime}}} p \leq 4^{n-1}$.*

Proof. Let $P(n) = \prod_{\substack{p\leq n \\ p \text{ is prime}}} p \leq 4^{n-1}$, and we prove the lemma by induction on n. For $n = 2$ we have $2 \leq P(2) = 4^{2-1} = 4$. Now, suppose that statement is true for n and we want to prove it for $n+1$. Observe that if $n+1$ is even, then we trivially have $P(n+1) = P(n) \leq 4^{n-1} < 4^{(n+1)-1}$. Therefore, it is enough to prove it for and odd number $n+1$. Since $n+1$ is odd, we can find some integer m for which $n+1 = 2m+1$. Now, observe that

$$P(2m+1) = P(m+1) \cdot \prod_{\substack{m+1<p\leq 2m+1 \\ p \text{ is prime}}} p. \tag{1}$$

The crucial part of the proof is the following claim:

Claim 13.4. *For all $m \in \mathbb{N}$ we have that*

$$\prod_{\substack{m+1<p\leq 2m+1 \\ p \text{ is prime}}} p \leq \binom{2m+1}{m}.$$

Proof. Recall that $\binom{2m+1}{m} = \frac{(2m+1)!}{(m+1)!m!}$ and is an integer. Moreover, since all primes $m+1 < p \leq 2m+1$ appear in the numerator and non of them appears in the denominator, we conclude that

$$\text{the number } \left(\prod_{\substack{m+1<p\leq 2m+1 \\ p \text{ is prime}}} p \right) \text{ divides } \binom{2m+1}{m}$$

and this completes the proof of the claim. □

Next, observe that since $\binom{2m+1}{m} = \binom{2m+1}{m+1}$, and since $\sum_k \binom{2m+1}{k} = 2^{2m+1}$, it follows that

$$\binom{2m+1}{m} \leq 2^{2m} = 4^m.$$

Plugging everything into (1) and using the induction hypothesis, we obtain that

$$P(2m+1) \leq 4^m \cdot 4^m = 4^{2m}$$

as desired. This completes the proof. □

Now we are ready to prove the upper bound in Theorem 13.2.

Proof. From Lemma 13.3 we know that

$$\prod_{p\leq x} p \leq 4^x.$$

Moreover, if we fix any $t > 0$, then we can easily see that

$$t^{\pi(x)-\pi(t)} \leq \prod_{p\leq x} p \leq 4^x.$$

Now, using the trivial bound $\pi(t) \leq t$, we obtain that

$$t^{\pi(x)-t} \leq 4^x,$$

which by talking logs gives us

$$(\pi(x) - t) \log t \leq x \log 4,$$

which is equivalent to

$$\pi(x) \leq \frac{x \log 4}{\log t} + t.$$

Observe that the above inequality holds for all $t > 0$ and since we are interested on upper bounding $\pi(x)$ we are interested in minimizing the right hand side (this can be done by differentiating this expression as a function of t). For our purpose, we can just observe that if we choose $t = Cx/\log x$ for some large enough constant C, the we get the desired bound. □

For the lower bound we also need some short preparation. First, let us prove the following simple theorem by Legendre:

Theorem 13.5 (Legendre's)**.** *For every $n \in \mathbb{N}$ and every prime number p, the largest power of p that divides $n!$ is exactly*

$$\sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Proof. Indeed, there are exactly $\left\lfloor \frac{n}{p} \right\rfloor$ numbers appearing in $n!$ which are divisible by p, there are exactly $\left\lfloor \frac{n}{p^2} \right\rfloor$ numbers appearing in $n!$ which are divisible by p^2, etc. □

We will also need the following simple estimate on the largest power of primes dividing $\binom{2n}{n}$.

Lemma 13.6. *The number $\binom{2n}{n}$ contains the prime factor p exactly*

$$r := \sum_{k\geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right),$$

that is, r is the largest integer for which $p^r \mid \binom{2n}{n}$.

Moreover, we have that

$$\sum_{k\geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \max\left\{ r \mid p^r \leq 2n \right\}.$$

Proof. The first assertion of the lemma follows immediately from Legendre's theorem (13.5) and the fact that $\binom{2n}{n!\cdot n!}$.

For the second assertion, observe that each summand is either 0 or 1. Indeed,

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2 \cdot \left(\frac{n}{p^k} - 1 \right) = 2,$$

and since it must be integer we obtain that it should be either 0 or 1. Next, observe that if $p^k > 2n$ then the corresponding summands are 0 and therefore p^k does not divide $\binom{2n}{n}$ in case that $p^k > 2n$. This completes the proof. □

Now we are ready to prove the lower bound in the weak version of the prime number theorem.

Proof. Recall from any introductory class that $\frac{4^n}{2n} \leq \binom{2n}{n}$ (this can be proved by a simple induction. In fact, for large values of n we have, from Stirling's approximation that $\binom{2n}{n} \approx \frac{4^n}{\sqrt{\pi n}}$ which is a much better estimate). On the other hand, we want to upper bound $\binom{2n}{n}$ by writing its prime factorization. To this end we will use Lemma 13.6 and observe that for every $p \leq \sqrt{2n}$ we have that the largest power r for which $p^r \mid \binom{2n}{n}$ must satisfy $p^r \leq 2n$. Moreover, every prime $p > \sqrt{2n}$ can divide $\binom{2n}{n}$ with power at most 1. Recall the definition of $\pi(n)$, we obtain that

$$\begin{aligned} \frac{4^n}{2n} \leq \binom{2n}{n} &\leq \prod_{\substack{p\leq\sqrt{2n} \\ p \text{ is prime}}} 2n \cdot \prod_{\substack{\sqrt{2n}<p\leq 2n \\ p \text{ is prime}}} p \\ &\leq (2n)^{\pi(n)}. \end{aligned}$$

In particular, we see that for the above inequality to be true for all values of n we must have

$$\pi(n) \geq \frac{cn}{\log n}$$

as otherwise the right hand side is smaller than exponential in n. This completes the proof. □

With not too much effort we can prove another nice and famous result, known as Bertrand's postulate:

Theorem 13.7 (Bertrand's postulate)**.** *For every integer $n \in \mathbb{N}$, there must exist at least one prime $n < p \leq 2n$.*

Proof. We will only sketch the proof here. The interested reader is encouraged to complete the details be herself/himself.

First, observe that all the numbers $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$ are all primes and each is smaller than twice the previous. Therefore, Bertrand's postulate holds for $n < 4000$. Therefore, it is enough to prove the theorem for $n \geq 4000$.

The key part of the proof is the following simple observation:

Observation 13.8. *No prime $\frac{2n}{3} < p \leq n$ divides $\binom{2n}{n}$.*

Proof. Indeed, since for each such prime we have that $3p > 2n$, it follows that the only product of p that appear in the denominator of $\frac{(2n)!}{n!n!}$ are p and $2p$, and that there are no large powers of p. Moreover, since $p \leq n$, we have two appearances of p in the denominator, one from each of the $n!$s. Therefor, all the appearances of p vanish. □

Next, we will use a similar estimate like in the proof of the lower bound for the weak version of the prime number theorem and write:

$$\begin{aligned}\frac{4^n}{2n} \leq \binom{2n}{n} &\leq \prod_{\substack{p \leq \sqrt{2n} \\ p \text{ is prime}}} 2n \cdot \prod_{\substack{\sqrt{2n} < p \leq 2n/3 \\ p \text{ is prime}}} p \cdot \prod_{\substack{n < p \leq 2n \\ p \text{ is prime}}} p \\ &\leq (2n)^{\sqrt{2n}} \cdot \prod_{\substack{p \leq 2n/3 \\ p \text{ is prime}}} p \cdot \prod_{\substack{n < p \leq 2n \\ p \text{ is prime}}} p.\end{aligned}$$

If we assume that there are no primes between n and $2n$, then the last factor is 1, and by Lemma 13.3 we obtain that

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{n}} 4^{2n/3},$$

which is clearly false for all $n < 4000$ (show it!). This completes the proof. □

Exercise 13.9. *Try to prove using the same method as above, that in fact there are at least $\frac{cn}{\log n}$ many primes in the interval $[n, 2n]$ (assuming that n is large enough).*

Let us conclude this section with a list of few interesting open problems that involve prime numbers:

Conjecture 13.10 (Goldbach's Conjecture)**.** *Every even integer $n \geq 4$ can be written as a sum of two primes.*

Conjecture 13.11 (The Twin Primes Conjecture)**.** *There are infinitely many pairs $(p, p+2)$ where both elements are primes.*

Conjecture 13.12 (The $N^2 + 1$ conjecture)**.** *There are infinitely many primes of the form $N^2 + 1$.*

14 Review exercises

1. Prove the following:
   (a) For all $m \in \mathbb{N}$ we have $\gcd(m, m+1) = 1$.
   (b) Suppose that $m, n \in \mathbb{N}$ are such that $\gcd(m, n) = 1$. Show that $\gcd(m+n, m-n)$ can be either 1 or 2.
   (c) Show that for all $m \in \mathbb{N}$ we have that $\gcd(3m+2, 5m+3) = 1$.
   (d) Show that if $\gcd(m, n) = 1$ then $\gcd(2m+n, 2n+m)$ is either 1 or 3.
   (e) Compute $g := \gcd(12345, 67890)$ and find an integer solution to $12345x + 67890y = g$.
   (f) Compute $g := \gcd(54321, 9876)$ and find an integer solution to $54321x + 9876y = g$.
   (g) Is 45867723 a prime? (Hint: think about a divisibility criteria that we learnt in class).
2. Prove the following:
   (a) Show that for all $n \in \mathbb{N}$ we have that $(n-1)^3 + 1$ is divisible by n.
   (b) Prove that $m^3 + 1$ can never be a prime unless $m = 1$.
   (c) Prove that $m^2 - 1$ is divisible by 8 for all odd integers m.
3. Prove the following:
   (a) Prove that $N := n! + 1$ must have a prime divisor larger than n and explain how to show, best on what you proved, there are infinitely many primes.
   (b) Show that for all $a \geq 5$ we have that $a, a+2, a+4$ cannot be all primes.
4. Solve the following:
   (a) Find all the solutions to $x^2 = 4 \pmod{143}$ (explain why there are no other solutions than the ones you found).
   (b) Suppose that $n \in \mathbb{N}$ is such that $\phi(n) = 36$. List all the primes that might possibly divide n.
   (c) Find all integers n for which $\phi(n) = 36$.
5. Solve the following:
   (a) Compute $\phi(3750)$.
   (b) Find a number $1 \leq a \leq 5000$ which is not divisible by 7 and for which $a = 7^{3003} \bmod 3750$.
6. Solve the following:
   (a) Either find all integer solutions or prove that there are no integer solutions for the equation $21x + 7y = 147$.
   (b) A grocer orders apples and bananas at a total cost of 8.4 USD. If the apples cost 25 cents each and the bananas 5 cents each, how many of each type of fruit did he order?
7. Prove the following:

(a) Let a be an integer such that $13 \nmid a$, $7 \nmid a$. Show that $a^{12} \equiv 1 \pmod{91}$.

(b) Let n be a positive integer such that $2^n \equiv 1 \pmod{91}$, show that $12|n$.

8. Solve the following:

(a) Find a positive integer x such that $x \equiv 5 \pmod{24}$, $x \equiv 17 \pmod{18}$.

(b) Does there exist an integer x such that $x \equiv 20 \pmod{24}$, $x \equiv 16 \pmod{18}$?

15 Mersenne Primes

Mersenne primes are primes that can be written as $a^n - 1$ for some $a \in \mathbb{Z}$. For example, $2^2 - 1 = 3$ and $2^3 - 1 = 7$ are Mersenne primes.

It is relatively easy to see that if $a^n - 1$ then we must have that $a = 2$ (can you see why?). Now, let us try to investigate which power $n \in \mathbb{N}$ can potentially make $2^n - 1$ being prime.

For example, suppose that n is even. Then, since $2 \equiv -1 \bmod 3$, we have that $2^n \equiv 1 \bmod 3$ and therefore $2^n - 1$ is divisible by 3 (and therefore it cannot be a prime unless it equals 3). In general, if n is divisible by k, then we can easily show that $2^k - 1$ divides $2^n - 1$ as follows:

$$2^n - 1 = 2^{km} - 1 = (2^k - 1)(1 + 2^k + 2^{2k} + 2^{3k} + \ldots + 2^{k(m-1)}).$$

In particular we obtain the following simple proposition:

Proposition 15.1. *If $a^n - 1$ is a prime, then $a = 2$ and n must be a prime.*

We can now rewrite the definition and say that a Mersenne prime is a prime of the form $2^p - 1$, where p is some prime. It is easy to show that not all number of the form $2^p - 1$ are primes (do it!). There is a lot of work on finding arbitrary large Mersenne primes and quite large ones are known, but the following question is still open:

Question 15.2. *Are there infinitely many Mersenne primes?*

16 Mersenne Primes and Perfect Numbers

The ancient Greeks observed that the number 6 has the very nice property that if you add up all its proper divisors then you obtain 6 (indeed, we have that $1+2+3=6$). The Greeks called such numbers *perfect numbers*. For example, we also have that $28 = 1+2+4+7+14$ is a perfect number. The Greeks knew a method to find some perfect numbers and interestingly their method is related to Mersenne primes.

Theorem 16.1 (Euclid's Perfect Number Formula)**.** *If $2^p - 1$ is prime, then $2^{p-1}(2^p-1)$ is perfect,*

Proof. Let $q = 2^p - 1$, and we need to check that $2^{p-1}q$ is perfect. Note that its proper divisors are

$$1, 2, 2^2, \ldots, 2^{p-1}, q, 2q, 2^2q, \ldots, 2^{p-2}q.$$

Now, lets sum them up and obtain:

$$(1+2+\ldots+2^{p-1}) + q + (1+2+\ldots+2^{p-2}) = \frac{2^p-1}{2-1} + q + \frac{(2^{p-1}-1}{2-1} = 2^{p-1}q.$$

(the last inequality follows from the fact that $2^p - 1 = q$). This completes the proof. □

The next question to ask is whether Euclid's formula gives all the perfect numbers. Around 2000 years after Euclid, Euler showed that Euclid's formula gives all the even perfect numbers:

Theorem 16.2 (Euler's Perfect Number Theorem)**.** *If n is an even perfect number, then it must look like*

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

where $2^p - 1$ is a Mersenne prime.

Before proving this theorem we need to introduce a convenient function. Let $\sigma(n)$ be the sum of all the divisors of n. For example $\sigma(2) = 1+2 = 3$, $\sigma(4) = 1+2+4 = 7$, etc. An important example is when $n = p^k$ with p being a prime. In this case we have

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

We will now show that σ is a *multiplicative function*:

Theorem 16.3. *For every $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ we have $\sigma(mn) = \sigma(m)\sigma(n)$.*

Proof. Let m, n be coprimes. Then, we know that each divisor d of mn can be written uniquely as $d = d_1 d_2$, where $d_1 \mid m$ and $d_2 \mid n$. Therefore, we have that

$$\begin{aligned}\sigma(mn) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} d_1 d_2 \\ &= (\sum_{d_1 \mid m} d_1)(\sum_{d_2 \mid n} d_2) = \sigma(m) \cdot \sigma(n).\end{aligned}$$

This completes the proof. □

How is the σ function related to perfect numbers? observe that a number n is perfect if and only if $\sigma(n) = 2n$. Now we are ready to prove Euler's perfect number theorem:

Proof. Suppose that n is an even perfect number. In particular, it means that we can write $n = 2^k m$, with $k \geq 1$ and m being odd. Next, we write

$$\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Since n is perfect we obtain

$$2n = 2^{k+1}m = (2^{k+1} - 1)\sigma(m).$$

The number $2^{k+1} - 1$ is odd, so we have that $\sigma(m) = c \cdot 2^{k+1}$ for some $c \in \mathbb{N}$. Therefore, by dividing the above expression by 2^{k+1} we obtain

$$m = (2^{k+1} - 1)c, \text{ and } \sigma(m) = 2^{k+1}c.$$

Next, since m is divisible by $1, c, m$ (do you see why $c \neq m$? to see it we use the fact that our original number n is even!), we have, as long as $c \neq 1$, that

$$\sigma(m) \geq 1 + c + m.$$

On the other hand, we have that

$$\sigma(m) = 2^{k+1}c = (2^{k+1} - 1)c + c = m + c < 1 + c + m,$$

and this gives a contradiction. Therefore, we must have $c = 1$, so $m = 2^{k+1} - 1$ and $\sigma(m) = 2^{k+1} = m + 1$. It is now easy to show that the only numbers m for which $\sigma(m) = m + 1$ are prime numbers, and since $m = 2^{k+1} - 1$ it follows that it must be a Mersenne prime. This completes the proof. □

Note that Euler's theorem doesn't give any clue on odd perfect numbers, and therefore one can ask if such numbers exist? Unfortunately, no one knows the answer!

17 Primality testing and Carmichael numbers

Recall that in order to generate a public key for RSA we need to be able to generate large primes. From the prime number theorem we know that around the number n, when n is large, approximately $\frac{1}{\ln n}$ proportion of numbers are prime.

To generate a large prime, we can then generate a random number with the appropriate number of digits or bits, and check if it is prime. If it is, we are done, else we increment it (and can skip numbers that are obviously not primes, like even ones), and try again until we find a prime number. From the prime number theorem, we know that approximately, we will need to perform a number of trials proportional to the number of digits (or bits) of n (which is proportional to $\log n$).

We therefore need to be able to efficiently check if a number is prime. This is known as *primality testing*. We could try whether it is divisible by any of the small primes, say all primes up to 30. This would detect a good fraction of the composite numbers, but clearly not all of them. Checking all possible factors up to the square root of the number n is *extremely* slow if n is large (as this would be exponential in the number of digits of n), and we are interested in numbers with hundreds of digits.

One approach is based on Fermat's little theorem, and is called the *Fermat primality test*.

17.1 Fermat primality test

Suppose we are given a large number n, and we want to determine if it's prime.

Let a be any positive number less than n; then by Fermat's Little Theorem, if n is indeed prime, then since $\gcd(a, n) = 1$ we have that

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

If n is not prime, on the other hand, this doesn't have to be true (though it might happen, depending on the specific a and n we choose). So here is a test: choose a large number of randomly chosen values $a_1, a_2, \ldots, a_N$, all positive and less than n, and calculate $a_i^{n-1} \pmod{n}$ for each. This we can do very quickly by repeated squaring, as we saw in the discussion. If we obtain a value other than 1 for *some* a, then n is not prime; that a acts as a certificate ("proof") that n is not prime. We call such an a a *Fermat witness* for n being composite. On the other hand, if $a^{n-1} \equiv 1 \pmod{n}$ (and n is composite) then we instead call a a "Fermat liar" for n.

Let's define precisely our primality test as follows:

Fermat primality test for an integer n

1. Pick $a \in \{1, 2, 3, \ldots, n-1\}$ uniformly at random.
2. Calculate (efficiently via repeated squaring) the value $a^{n-1} \bmod n$. If this is not 1, output "not prime"; otherwise output "maybe prime".

We can repeat this test many times; if it outputs "not prime" at least once, we can be sure that it is indeed not prime; if it returns "maybe prime" each time, then perhaps we can conclude that n is very likely to be prime?

This turns out to be almost, but not quite, true. There are certain special composite numbers, called *Carmichael numbers*, that do a very good job of fooling this test.

Definition 17.1. *A positive integer n is a* Carmichael number *if it is composite and $a^{n-1} \equiv 1 \pmod{n}$ for all a relatively prime to n.*

If we apply Fermat's test to a Carmichael number, then the only way it can spot that it's not prime is if the a chosen happens to share a common factor with n. If the factors of n are all large, then there are few such numbers (compared to n) and we're very unlikely to pick one of them.

It's not obvious that these numbers exist, but they do, and there are infinitely many of them; the smallest is $561 = 3 \cdot 11 \cdot 17$. Since $3 - 1 = 2$, $11 - 1 = 10$ and $17 - 1 = 16$ all divide 560 (this explains why 561 is a Carmichael number), we have that $a^{560} = 1$ modulo 3, 11 and 17 whenever a is not divisible by 3, 11 or 17. Thus, by applying the Chinese remainder theorem we get $a^{560} = 1 \pmod{3 \cdot 11 \cdot 17}$. Carmichael numbers are very rare however (only 22 values less than 10,000, and they are much rarer than primes), and if you pick a large random n, you'd have to be very unlucky to pick a Carmichael number.

In order to understand why Carmichael numbers are rare, it is recommended to prove the following theorem as an exercise (or just look at [1], Page 135, Theorem 19.1):

Theorem 17.2 (Korselt's Criterion for Carmichael Numbers)**.** *Let n be a composite number. Then, n is a Carmichael number if and only if it is odd and every prime p dividing n satisfies the following two conditions:*

1. *p^2 does not divide n, and*
2. *$p - 1$ divides $n - 1$.*

What we will prove now is that the Fermat test *does* work on all numbers except for Carmichael numbers.

Theorem 17.3. *If $n > 2$ is composite and not a Carmichael number, then the probability that the Fermat test works is at least $1/2$.*

Proof. Let

$$L = \{b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \bmod n\},$$

i.e., the set of Fermat liars for n. Let $W = \mathbb{Z}_n^* \setminus L$, the set of Fermat witnesses that are relatively prime to n. Since n is not a Carmichael number, W is nonempty. (Note that all elements of $\mathbb{Z}_n \setminus \mathbb{Z}_n^*$ are also Fermat witnesses.)

We will show that $|L| \leq |W|$, from which the theorem follows. Since then the probability we pick $a \in L$ is not more than $1/2$; and so the probability of choosing a Fermat witness is at least $1/2$.

The plan is to find a one-to-one map f from L to W, which immediately gives us that $|L| \leq |W|$. The map is very simple: pick an arbitrary $a \in W$ (recall it's nonempty), and define

$$f(b) = ab \bmod n \qquad \forall b \in L.$$

First, let's see that it is a map from L to W, and not merely a map from L to $\mathbb{Z}_n$. For any $b \in L$,

$$f(b)^{n-1} = a^{n-1}b^{n-1} \equiv a^{n-1} \not\equiv 1 \pmod{n}.$$

So indeed $f(b) \in W$. It's also clearly one-to-one: if $f(b) = f(b')$, then multiplying by a^{-1} gives $b = b'$.

This concludes the proof. □

We can conclude that the probability that if we run the Fermat test K times on a number n that is composite and not a Carmichael number, the probability that the Fermat test outputs "maybe prime" on all tries is at most 2^{-K}; by choosing K large enough, we can make the error probability tiny.

In order to overcome the problem of dealing with Carmichael numbers, we will learn another primality testing.

17.2 The Miller-Rabin test

Consider the equation

$$x^2 \equiv 1 \pmod{n},$$

where $n > 2$ and odd. There are two very obvious solutions to this: $x \equiv 1$ and $x \equiv -1$. Are there other solutions? Recall that if n is prime then these are the only solutions; this fact we won't prove. It's also true (and we had something like that in our midterm) that if n is not a prime or power of a prime (but still odd), then there are at least 4 solutions - 2 extra solutions besides 1 and -1 (prove it!).

This gives us an extra tool for primality testing: if we find a solution to $x^2 = 1 \pmod{n}$ that is not 1 or -1, then we know that n is not prime. By the way, one might wonder what happens when you have a prime power as the theorem cannot distinguish between a prime and a prime power. However, a prime power is not a Carmichael number, and the more basic Fermat test works already for prime powers.

Here is the Miller-Rabin test (we will assume that n is odd, otherwise it is trivially not prime):

Pick a uniformly at random from $\{1, 2, \ldots, n-1\}$ Write $n - 1 = t2^s$, where t is odd; s will be positive, since $n - 1$ is even Calculate $a^t \bmod n$ (we've seen how to do this fast) Repeatedly square to obtain the sequence

$$a^t, a^{2t}, a^{2^2 t}, \ldots, a^{2^s t} = a^{n-1} \quad \text{all modulo } n.$$

If the last term in this sequence, $a^{n-1} \bmod n$, is not equal to 1, then return that n is composite If for some $i < s$, $a^{2^i} t \neq 1, -1 \pmod{n}$ but $a^{2^{i+1} t} = 1 \pmod{n}$, then return that n is composite Otherwise return that n is "probably prime".

Note that if n is indeed prime, our test will always return "probably prime". If n is composite, it may or may not detect this. But:

Theorem 17.4. *For any odd composite number n, the probability that the Miller-Rabin test returns "probably prime" when n is composite is at most* $1/4$.

This means that by repeating the test N times, each time with a new random choice of a, we can reduce the probability of making a mistake to less than $1/2^N$. For N large, this is really negligible.

For a proof of the above theorem and some interesting discussion about the Miller-Rabin test, you can look at the following **paper** and the references therein.

There is also a (much more complicated) *deterministic* primality test, due to Agrawal, Kayal and Saxena.

18 Squares modulo p

We've already learnt how to solve linear congruences. It is natural to study congruences of higher degree as well. Here we will study a special case of this problem, by considering congruences of the form $x^2 \equiv a \bmod p$. The theory we develop here illustrates many of the ideas we learnt earlier, and also has some interesting applications.

For convenience, let us define $(\mathbb{Z}_n^*)^2$ to be the set of all *quadratic residues* modulo n. That is, $(\mathbb{Z}_n^*)^2 = \{x^2 \mid x \in \mathbb{Z}_n^*\}$. Clearly, this set is not empty as we always have $1 \in (\mathbb{Z}_n^*)^2$. The numbers in $\mathbb{Z}_n^* \setminus (\mathbb{Z}_n^*)^2$ are called *quadratic non-residues* modulo n.

Let us start with the following simple theorem:

Theorem 18.1. *Let n be any positive integer, and let $a, b \in \mathbb{Z}_n^*$. Then,*

1. *If $a \in (\mathbb{Z}_n^*)^2$ then $a^{-1} \in (\mathbb{Z}_n)^2$.*
2. *If $a, b \in (\mathbb{Z}_n^*)^2$ then $ab \in (\mathbb{Z}_n^*)^2$.*
3. *If $a \in (\mathbb{Z}_n^*)^2$ and $b \notin (\mathbb{Z}_n^*)^2$ then $ab \notin (\mathbb{Z}_n^*)^2$.*

Proof. Observe that if $a = x^2$ for some $x \in Z_n^*$, then clearly $a^{-1} = (x^{-1})^2$. This proves 1.

For 2. observe that if $a = x^2$ and $b = y^2$, then $ab = (xy)^2$.

Finally, to prove 3. let $a \in (\mathbb{Z}_n^*)^2$ and $b \notin (\mathbb{Z}_n^*)^2$, and assume that $ab \in (\mathbb{Z}_n^*)^2$. Then, by 1. we have that $a^{-1} \in (\mathbb{Z}_n^*)^2$, and by 2. we have that $a^{-1} \cdot (ab) = b \in (\mathbb{Z}_n^*)^2$, which is a contradiction. This completes the proof. □

Next we discuss the case where $n = p$ is some odd prime. As we've already seen (or at least stated...), the polynomial $x^2 - a$ has at most 2 roots modulo p (do you see how to prove this specific case?). Moreover, it follows that $x^2 \equiv y^2 \bmod p$ if and only if $x = \pm y$. Observe that $-y = p - y$, and since p is odd we obtain that $y \neq -y$ for all $y \in Z_p^*$. Apparently, this observation is enough to prove the following simple theorem:

Theorem 18.2. *Let p be an odd prime. Then there are exactly $(p-1)/2$ quadratic residues modulo p and exactly $(p-1)/2$ quadratic non-residues modulo p.*

Proof. By the above observations we have that

$$(\mathbb{Z}_n^*)^2 = \{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}.$$

(do you see why?). Therefore, in order to complete the proof, it is enough to show that all these elements are distinct. To this end, let $1 \leq a \leq b \leq \left(\frac{p-1}{2}\right)^2$ be two residues for which $a^2 = b^2 \bmod p$. We wish to show that $a = b$. Indeed, we have that $b^2 - a^2 = (b-a)(b+a) = 0 \bmod p$, and therefore

$$p \mid b + a \text{ or } p \mid b - a.$$

Since $0 < b + a \leq p - 1$, the former cannot hold. Therefore, we must have $p \mid b - a$. But, since $|b - a| < (p-1)/2$, we must have that $|b - a| = 0$, and therefore $a = b$. This completes the proof. □

Our next theorem gives us an extremely important characterization of quadratic residues mod p.

Theorem 18.3 (Euler's criterion)**.** *Let p be an odd prime and let $a \in \mathbb{Z}_p^*$.*

1. $a^{(p-1)/2} = \pm 1 \bmod p$.
2. *If $a \in (\mathbb{Z}_p^*)^2$, then $a^{(p-1)/2} = 1$.*
3. *If $a \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$, then $a^{(p-1)/2} = -1 \bmod p$.*

Proof. For 1., let $b = a^{(p-1)/2}$, and observe, by Euler's theorem, that $b^2 = a^{p-1} = 1 \bmod p$. Therefore, since p is prime we have that $b = \pm 1$.

For 2., let $a = b^2$ for some $b \in \mathbb{Z}_p^*$. Then, $a^{(p-1)/2} = b^{p-1}$, which again, by Euler's theorem, is equivalent to 1 modulo p.

For 3. we need to work a little bit harder. Let $a \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$, and consider the product

$$\prod_{x \in \mathbb{Z}_p^*} x = (p-1)!.$$

By Wilson's theorem (that we've seen) we know that $(p-1)! \equiv -1 \bmod n$. On the other hand, we want to show that this product also equals $a^{(p-1)/2} \bmod p$. This will clearly complete the proof. To this end, let us pair up elements of $\mathbb{Z}_p^*$ together into pairs of the form (x, y) for which $xy = a \bmod p$. Observe that indeed, for every element $x \in \mathbb{Z}_p^*$ there exists some $y \in \mathbb{Z}_p^*$ for which $xy = a \bmod p$ (simply take $y = x^{-1}a$), and that all these pairs are disjoint. Moreover, it cannot be that for some pair (x, y) we have that $x = y$ as otherwise we would have $a = x^2 \in (Z_p^*)^2$, which is false. All in all, we have managed to find $\frac{p-1}{2}$ such pairs, and they cover the entire set $\mathbb{Z}_p^*$. This means that $(p-1)! = a^{(p-1)/2} \bmod p$. This completes the proof. □

As a simple corollary we also obtain the following:

Corollary 18.4. *Let $a, b \in Z_p^*$ be two quadratic non-residues. Then ab is a quadratic residue.*

Proof. By Euler's criterion we have that $a^{(p-1)/2} = b^{(p-1)/2} = -1 \bmod p$. Therefore, we have that $(ab)^{(p-1)/2} = 1 \bmod p$, which again, by Euler's criterion means that ab is a quadratic residue. This completes the proof. □

As an another immediate corollary we obtain:

Corollary 18.5 (Quadratic Reciprocity (part 1))**.** *Let p be an odd prime.*

- *If $p \equiv 1 \bmod 4$, then (-1) is a quadratic residue.*
- *If $p \equiv 3 \bmod 4$, then (-1) is a quadratic non-residue.*

Proof. Do it! □

To summarize our findings, let QR stand for quadratic residue, and NR for quadratic non-residue, then we have:

$$QR \times QR = QR,\ QR \times NR = NR,\ NR \times NR = QR.$$

Note that QR behaves like $+1$ and NR behaves like a (-1) in the above expression. This leads us to define, for all $a \in \mathbb{Z}_p^*$, the following useful notation which is known as Legendre's symbol:

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

With this notation in hands, we can restate the above multiplication rule as follows:

Theorem 18.6 (Quadratic Residue Multiplication Rule)**.** *Let p be an odd prime. Then*

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

Example 18.7. *Suppose we want to check whether 75 is a square modulo 97. We can write:*

$$\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{3}{97}\right).$$

Now, we can observe that $10^2 = 100 = 3 \bmod 97$, and therefore 3 is a QR. All in all we obtain that $\left(\frac{75}{97}\right) = 1$.

Next, as a simple application of the Quadratic Reciprocity (part 1) we can easily prove the following theorem:

Theorem 18.8. *There are infinitely many primes of the form $p \equiv 1 \bmod 4$.*

Proof. Suppose that we are given a list of primes $p_1, \ldots, p_r$, all are congruent to 1 modulo 4. We are going to find another such prime which is not in our list. Consider the number

$$N = (2p_1 \cdots p_r)^2 + 1.$$

Clearly, we have that $N \equiv 1 \bmod 4$. Moreover, N can be factored as product of some primes (non of them is from our list!)

$$N = q_1 \cdots q_t.$$

We will show that all of the q_is are of the form 1 mod 4, and this will complete the proof. Observe that N is odd, so all the q_i are odd. Moreover, since each q_i divides N we have that

$$(2p_1 \cdots p_r)^2 + 1 = 0 \bmod q_i \text{ for all } i.$$

That is, taking $x = (2p_1 \cdots p_r)^2$ we have that

$$x^2 \equiv -1 \bmod q_i \text{ for all } i,$$

so in particular we have that -1 is a quadratic residue for all the q_i. This means that $q_i \equiv 1 \bmod 4$ for all i. This completes the proof. □

Our next challenge is to understand the behavior of $\left(\frac{2}{p}\right)$. Let p be any odd prime, and define $P = \frac{p-1}{2}$. We start with the even numbers $2, 4, 6, \ldots, p-1$: multiplying them together and factoring 2 from each, we obtain

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^P \cdot P!.$$

Next, take each of these numbers and write it as its negative expression if needed, to get only values in $[-P, P]$. Comparing the two products we obtain that

$$2^P \cdot P! = (-1)^{\text{number of minus signs}} \cdot P! \bmod p.$$

Therefore, by cancelling the factor $P!$ in both sides, we obtain the fundamental formula:

$$2^{(p-1)/2} = (-1)^{\text{number of minus signs}}.$$

Using this formula we can easily prove the following:

Theorem 18.9 (Quadratic reciprocity (part 2))**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \mod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \mod 8 \end{cases}$$

Proof. There are four cases to study, we will only deal with one of them (the others are quite similar and are being left as an exercise).

The only case that we consider is $p \equiv 1 \bmod 8$. That is, $p = 8k+1$ for some $k \in \mathbb{Z}$. Consider the fundamental formula and lets try to understand how many minus signs we have. Observe that $P = \frac{p-1}{2} = 4k$. Now, considering all the even numbers $2, 4, 6, \ldots, p-1$, it is clear that the first $2k$ numbers are at most P and the other $2k$ numbers are larger than P. Therefore, we have exactly $2k$ minus signs and we have

$$2^{(p-1)/2} = 1.$$

Therefore, by Euler's criterion we obtain that 2 is a quadratic residue. □

In general, the Law of quadratic reciprocity is the following statement, that we will probably won't have time to prove in class (we proved the first two statements which are the easiest ones):

Theorem 18.10 (Law of quadratic reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}.$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}.$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4. \end{cases}$$

The Law of quadratic reciprocity is not just a beautiful theorem, but it also serves as a practical tool for determining whether a number is a quadratic residue in a relatively simple way. The power of this law is that it enables us to flip the Legendre's symbol $\left(\frac{q}{p}\right)$ and replace it by $\pm\left(\frac{p}{q}\right)$. Then we can reduce p modulo q and repeat the process with smaller entries, until we eventually arrive at Legendre symbols that we can compute.

Example 18.11. *Suppose we wish to compute* $\left(\frac{14}{137}\right)$. *We can do the following:*

$$\begin{aligned}\left(\frac{14}{137}\right) &= \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) \text{ multiplicative rule}\\ &= \left(\frac{7}{137}\right) \text{ since } 137 \equiv 1 \bmod 8\\ &= \left(\frac{137}{7}\right) \text{ quadratic reciprocity and } 137 \equiv 1 \bmod 4\\ &= \left(\frac{4}{7}\right)\\ &= 1 \text{ since } 4 = 2^2 \text{ is a square.}\end{aligned}$$

It is also useful to observe that the third part of the Law of Quadratic Reciprocity can equivalently stated as follows:

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

In particular it says that the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ have the same values if and only if either $p \equiv 1 \bmod 4$ or $q \equiv \bmod 4$.

Example 18.12. *Let us characterize those primes* p *modulo which* 5 *is a quadratic residue. Since* $5 \equiv 1 \bmod 4$, *the law of quadratic reciprocity tells us that*

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Now, among the numbers $\pm 1, \pm 2$, *the quadratic residues modulo* 5 *are* ± 1. *It follows that* 5 *is a quadratic residue modulo* p *if and only if* $p \equiv \pm 1 \bmod 5$. *This example obviously generalizes, replacing* 5 *by any prime* $q \equiv 1 \bmod 4$, *and replacing the above congruences modulo* 5 *by appropriate congruences modulo* q.

Observe that the hard part in computing the Legendre symbols is not the use of quadratic reciprocity but is the part of factorizing the numbers that appear in the symbol. Apparently, there is a way to do it without factorizing any number. For this, we need to extend the Legendre symbol to arbitrary odd numbers, that is to define $\left(\frac{a}{b}\right)$ for all odd a, b. This symbol is called the Jacobi symbol and is defined as follows:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right),$$

where $b = p_1 p_2 \cdots p_r$ is its prime factorization. With this notation in hands, we can state (and prove) the following theorem:

Theorem 18.13 (Generalized Law of Quadratic Reciprocity)**.** *Let a, b be positive odd number. Then*

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \bmod 4 \\ -1 & \text{if } b \equiv 3 \bmod 4. \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \bmod 8. \end{cases}$$

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \bmod 4 \text{ or } b \equiv 1 \bmod 4 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv 3 \bmod 4. \end{cases}$$

Note that if you use the above theorem then you are only allowed to flip $\left(\frac{a}{b}\right)$ whenever both a, b are positive odd numbers. If at least one of them is even, then we need to first factor off a power of $\left(\frac{2}{b}\right)$ out of it, and if at least one of them is negative, then we need to first factor off the $\left(\frac{-1}{b}\right)$ terms.

Example 18.14. *Calculate*

$$\left(\frac{37603}{48611}\right) = -\left(\frac{48611}{37603}\right) = -\left(\frac{11008}{37603}\right) = -\left(\frac{2^8 \cdot 43}{37603}\right) = -\left(\frac{43}{37603}\right)$$
$$= \left(\frac{37603}{43}\right) = \left(\frac{21}{43}\right) = \left(\frac{43}{21}\right) = \left(\frac{1}{21}\right) = 1.$$

Unfortunately, even though we've just proved that $x^2 \equiv 37604 \bmod 48611$ has a solution, we have no clue how to find it except of going through brute force. However, there are more advanced methods that actually solve this congruence. For certain special cases of primes, it is possible to write explicit solutions as is shown in the next exercises:

Exercise 18.15. *Suppose that $p \equiv 3 \bmod 4$ is a prime, and suppose that a is a quadratic residue mod p. Show that $x = a^{(p+1)/4}$ is a solution to the congruence $x^2 \equiv a \bmod p$.*

Exercise 18.16. *Suppose that $p \equiv 5 \bmod 8$ is a prime, and suppose that a is a quadratic residue mod p. Show that one of the values*

$$x = a^{(p+3)/8} \text{ or } x = 2a \cdot (4a)^{(p-5)/8}$$

is a solution to the congruence $x^2 \equiv a \bmod p$.

Let us now prove one part of Theorem 18.13. The other parts are left as an exercise:

Proof. We are given an odd integer b and we wish to compute $\left(\frac{-1}{b}\right)$. Let us factorize b as

$$b = p_1 \cdots p_r q_1 \cdots q_s,$$

where the p_is are primes congruent to 1 mod 4 and the q_is are 3 mod 4. Observe that

$$b = \begin{cases} 1 \bmod 4 & \text{if } s \text{ is even} \\ 3 \bmod 4 & \text{if } s \text{ is odd.} \end{cases}.$$

From this, and from the definition of the Jacobi symbol we can deduce the desired. □

18.1 Vinogradov's trick

In this section we will discuss a nice trick by Vinogradov's to upper bound the size of the least quadratic non-residue modulo some prime $n \equiv 1 \bmod 4$. In what follows we will restrict our attention to the case where $n = 1 \mod 4$ is a prime (and hence $\left(\frac{-1}{n}\right) = 1$). The problem that we are interested at is: How large is the least quadratic non-residue? Let $m(n)$ be the smallest $0 \leq a \leq n-1$ for which $\left(\frac{a}{n}\right) = -1$, and our goal will be the bound $m(n)$ from above.

The following Lemma shows that if one can get some "discrepancy" bound for short intervals, then $m(n)$ is bounded polynomially by the length of the interval:

Lemma 18.17. *Let $\chi(n) = \left(\frac{n}{p}\right)$ be the Legendre's symbol modulo p and let $\varepsilon > 0$. Suppose that $\sum_{n \leq x} \chi(n) = o(x)$ for some x. Then, the list quadratic non-residue is at most $y := x^{1/\sqrt{e}+\varepsilon}$.*

Proof. Recall that $\chi(n)$ is multiplicative and therefore, if $\chi(n) = -1$, then there exists some prime q dividing n and with $\chi(p) = -1$. If we assume that the smallest quadratic non-residue is at least y, then in particular it means that $\chi(q) = 1$ for all primes $1 \leq q < y$. Therefore, we can write

$$\begin{aligned} o(x) = \sum_{1 \leq n \leq x} \chi(n) &= \sum_{1 \leq n \leq x} 1 - 2 \sum_{\substack{1 \leq n \leq x \\ \chi(n) = -1}} 1 \\ &\geq \lfloor x \rfloor - 2 \sum_{\substack{y \leq q \leq x \\ \chi(q) = -1}} \frac{x}{q} \\ &\geq x - 1 - 2x \sum_{y \leq q \leq x} \frac{1}{q} \end{aligned}$$

and the last expressions equals, by Merten's theorem, to

$$x - 1 - 2x \left(\log\log x - \log\log y + \delta\right).$$

Now, observe that by our choice of y, we have that

$$\log\log x - \log\log y + \delta = -\log\left(e^{-1/2} + \varepsilon\right) + \delta < \frac{1}{2},$$

and this implies that there exists some constant $C > 0$ for which the RHS of the above display is at least Cx. This contradicts the assumption that the sum is $o(x)$. □

19 Review problems

1. Solve the following:

   (a) Show that if $\gcd(a,b)=1$ then $a^{\phi(b)}+b^{\phi(a)}\equiv 1 \bmod ab$.

   (b) Prove that if p is a prime congruent 1 mod 4 then

   $$\sum r = \frac{p(p-1)}{4} ,$$

   where the summation is over all quadratic residues r with $1 \leqslant r \leqslant p-1$.(Hint: Start from pairing r with $p-r$.)

2. Alice submits an encrypted bid to an auction so that other bidders cannot see her bid. Suppose that the auction service provides a public key (n,z) for an RSA. Assume that bids are encoded simply as integers between 0 and n prior to encryption and that Alice's bid is a multiple of 10. Now, suppose that you have an access to Alice's encrypted massage (that is, you know $a^z \bmod n$), and explain how can you submit an encryption of a bid that exceeds Alice's bid by 10%, without knowing her actual bid.

3. Show that for all $n \in \mathbb{N}$ there exists some $x \in \mathbb{N}$ such that each of the numbers $x, x+1, \ldots, x+n-1$ is divisible by some square of a prime.

4. Solve the following:

   (a) Let p be any prime other than 2 or 5. Show that p divides infinitely many of the numbers 9, 99, 999, etc.

   (b) Use the Prime Number Theorem to show that there exists some constant $C>0$ such that for all $n \in \mathbb{N}$, the nth prime p is at most $Cn\log n$.

5. This problem shows that there are infinitely many primes congruent to 1 modulo 3. We want to prove by contradiction and first assume that $p_1, p_2, \cdots, p_r$ are all such primes.

   (a) Let $A=(2p_1p_2\cdots p_r)^2+3$, show that there is a prime q such that $3 \nmid q$, $q|A$, and $q \equiv 3 \pmod 4$.

   (b) For the same q as in (a), show that $-3q=1$.

   (c) Use Quadratic Reciprocity to show that $q3=1$.

   (d) Find a contradiction to our assumption at the beginning.

6. Let p be any prime and $a \in \mathbb{Z}_p^*$. Let r be the minimal integer for which $a^r \equiv 1 \bmod p$ (explain why such an r exists!), and let $A_r := \{a, a^2, \ldots, a^r\}$.

   (a) Show that all the elements in A_r are distinct.

   (b) Show that for every integer k, each number in A_r appears exactly k times in the sequence a^t, $1 \leq t \leq kr$.

   (c) Show that for each prime which is not 2 or 5, there exist infinitely many numbers of the form $3, 33, 333, 3333$, etc. which are divisible by p

7. Show that for all odd integers n we have that n divides $1^n + 2^n + \ldots + (n-1)^n$.

8. Complete the steps of the Rabin-Miller primality test for the number $n = 115921$. You may use a calculator.

   (a) Write $n-1$ in the form $2^k q$ where q is odd. Then write q as a sum of powers of 2.

   (b) Use successive squaring to find $2^q \mod n$.

   (c) Compute the list $(2^q, 2^{2q}, \cdots, 2^{2^{k-1}q}) \mod n$. What is the conclusion?

9. Show that for even integers n, n does not divide $1^n + 2^n + \ldots + (n-1)^n$.

   Solution: Since n is even we can write $n = 2^s m$, where m is odd. Now, observe that for all $1 \leq k \leq n-1$, if k is even then $2^s \mid k^n$, and that if k is odd, then by Euler's we have that $k^{2^{s-1}} \equiv 1 \bmod 2^s$. This gives us that $1^n + 2^n + \ldots + (n-1)^n \equiv \frac{n}{2} \bmod 2^s$. In particular, if we assume that n divides $1^n + 2^n + \ldots + (n-1)^n$, then we obtain that $n/2 \equiv 0 \bmod 2^s$ which is clearly a contradiction.

10. Let p, q be distinct primes and let $n = pq$. Suppose that you know n and $\phi(n)$ (but you don't know the values of p, q), show how can you easily factorize n.

11. Show that for all $n \in \mathbb{N}$ there exists some $x \in \mathbb{N}$ such that each of the numbers $x, x+1, \ldots, x+n-1$ is divisible by a product of at least 10 distinct primes.

12. Show that for every integer n we have that $n^2 \mid (n+1)^n - 1$.

13. Let n be an odd square free positive integer. Show that there is an integer a such that $\gcd(a, n) = 1$ and $\left(\frac{a}{n}\right) = -1$

14. Determine whether each of the following numbers is a Carmichael number. You may use a calculator.

   (a) 29341

   (b) 89243

   (c) 105545

15. Determine, by congruence conditions, the set of primes p such that

$$\left(\frac{10}{p}\right) = 1.$$

16. Let the residue classes $1, 2, ..., p-1$ modulo an odd prime p be divided into two nonempty sets S_1 and S_2 such that the product of two elements of the same set is in S_1, whereas the product of an element of S_1 and an element of S_2 is in S_2. Prove that S_1 consists of the quadratic residues and S_2 consists of the quadratic non-residues modulo p.

17. Solve the following:

   (a) Show that if p is a prime congruent to 3 mod 4 and if $q = 2p+1$ is a prime then $2^p \equiv 1 \bmod q$. Deduce that $2^{251} - 1$ is not a Mersenne prime.

(b) Use the Prime Number Theorem to show that for all $\varepsilon > 0$ and a sufficiently large $n \in \mathbb{N}$, there is at least one prime in the interval $[n, n + \varepsilon n]$.

18. Determine whether each of the following congruences has a solution.

    (a) $x^2 \equiv 115 \pmod{277}$.

    (b) $x^2 \equiv 65 \pmod{664}$. (Hint: Use Chinese Remainder Theorem.)

19. Let $P_{6k+5} = \{p \mid p \text{ is prime and } p \equiv 5 \pmod{6}\}$. Show that $|P_{6k+5}| = \infty$ without using Dirichlet's Theorem.

References

[1] J. H. Silverman, A friendly introduction to number theory, fourth edition