Topic 3: Number Theory

Seppe Staelens

July 15, 2024

Introduction

In this topic, we revisit some very basic concepts which you have known of since primary school: divisibility and prime numbers. These concepts form the foundations of number theory, which is the study of the properties of numbers. We will however quickly discover new concepts, such as congruences and the Euler totient function. Most of the theory is assembled in one long build-up to its application in cryptography, in the form of the RSA algorithm.

1 Lecture 1: Number theory and modular arithmetic

1.1 Divisibility and congruences

You should be familiar with the concept of divisibility from primary school. A number a is **divisible** by a number b if there exists an integer c such that $a = bc$. You should also be familiar with the concept of the remainder of a division:

Lemma 1. *Let $a \in \mathbb{Z}, b \in \mathbb{Z}_0$. Then there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \quad \textit{and} \quad 0 \leq r < |b| \,. \tag{1}$$

*The number q is called the **quotient** of the division of a by b, and r is called the **remainder**.*

The remainder r is often denoted by $a \mod b$. We say that x is **congruent** to y modulo n if $x \mod n = y \mod n$, i.e. if they have the same remainder after division by n. This is often denoted as

$$x \equiv y \mod n \,.$$

Proposition 1. *Let $x, y \in \mathbb{Z}$ and $n \in \mathbb{N}_0$. Then the following equivalence holds:*

$$x \equiv y \mod n \quad \Leftrightarrow \exists k \in \mathbb{Z} : x = y + kn \,. \tag{2}$$

Proof. The proof is straightforward and left as an exercise. □

The following proposition is useful for calculations with congruences.

Proposition 2. *Let $x, x', y, y' \in \mathbb{Z}$ and $n \in \mathbb{N}_0$. Then the following equalities and equivalences hold:*

1. $(x + y) \mod n = (x \mod n + y \mod n) \mod n$.
2. $(x \cdot y) \mod n = (x \mod n \cdot y \mod n) \mod n$.
3. $x \equiv x' \mod n$ *and* $y \equiv y' \mod n \Rightarrow x + y \equiv x' + y' \mod n$.
4. $x \equiv x' \mod n$ *and* $y \equiv y' \mod n \Rightarrow xy \equiv x'y' \mod n$.

Proof. The proof is straightforward and left as an exercise. □

These rules are very useful when doing concrete calculations, as we can always reduce numbers to smaller values before doing the actual calculations.

Exercise 1. *Calculate* $12345^6 \mod 7$.

Exercise 2. *In primary school you may have learned a trick to check whether a number is divisble by 9, namely by checking whether the sum of its digits is divisible by 9. Can you explain this using congruences?*

1.1.1 Prime numbers

You should also be familiar with the concept of **prime numbers**.

Definition 1. *A number $p \in \mathbb{N}$ is called prime if it has exactly two divisors: 1 and p itself.*

Prime numbers are ubiquitous in number theory, and one could spend an entire summer school just on their properties and mysteries. Quite a number of applications become much more interesting when the numbers involved are prime, as will be the case for cryptography as well.

We mention the following two essential results.

Theorem 1. *Every number $n \in \mathbb{N}$ can be uniquely written as a product of prime numbers.*

We don't prove this one - it is not very complicated but a tiny bit too long for these notes. One has to prove existence and uniqueness, which can be proven for example by induction. The proof of the following theorem is shorter.

Theorem 2. *There are infinitely many prime numbers.*

Proof. We will prove this by contradiction. Suppose there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_r$. Consider the number $n = p_1 p_2 \cdots p_r + 1 > 1$. This number is not divisible by any of the prime numbers $p_1, p_2, \ldots, p_r$, as the remainder of the division by any of these numbers is 1. Therefore, n must have a prime factor p. This prime factor p cannot be any of the prime numbers $p_1, p_2, \ldots, p_r$, as we have just shown that n is not divisible by any of these numbers. Therefore, p is a new prime number, which is not in the list $p_1, p_2, \ldots, p_r$. This contradicts the assumption that there are only finitely many prime numbers. □

Another interesting concept in number theory is that of the **greatest common divisor** of two numbers.

Definition 2. *Let $a, b \in \mathbb{Z}$. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the largest number that divides both a and b.*

Definition 3. *Two numbers $a, b \in \mathbb{Z}$ are called **coprime** if $\gcd(a, b) = 1$.*

1.1.2 Some famous theorems

This section contains two theorems that turn out to be useful to understand the RSA algorithm later on. We will not prove them here, but they are not too difficult to prove, and proofs can be found on the internet.

Theorem 3. *(**Bézout-Bachet**) Let $a, b \in \mathbb{Z}$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*

Theorem 4. *(**Chinese Remainder Theorem**[1]) Let $n_1, n_2, \ldots, n_r \in \mathbb{N}_0$ be coprime. Then, $\forall a_1, a_2, \ldots, a_r \in \mathbb{Z}$, the system of congruences*

$$\begin{cases} x & \equiv a_1 \mod n_1\,, \\ x & \equiv a_2 \mod n_2\,, \\ & \vdots \\ x & \equiv a_r \mod n_r\,, \end{cases}$$

has a solution $x \in \mathbb{Z}$. Furthermore, all solutions are congruent modulo $n_1 n_2 \cdots n_r$, i.e. if a solution $x_0 \in \mathbb{Z}$ is known, all other solutions are of the form

$$x_0 + k n_1 n_2 \cdots n_r\,,$$

for $k \in \mathbb{Z}$.

Exercise 3. *Can you explain why the condition that the n_i are coprime is necessary for a solution to always exist? Find a counterexample where the n_i are not coprime.*

We do however prove the following corollary, which is a direct consequence of the Chinese Remainder Theorem.

Corollary 1. *Let $m, n \in \mathbb{N}_0$ be coprime. Then for all $x, x' \in \mathbb{Z}$ the following holds:*

$$x \equiv x' \mod mn \qquad \Leftrightarrow \qquad \begin{cases} x & \equiv x' \mod m\,, \\ x & \equiv x' \mod n\,. \end{cases} \tag{3}$$

Proof. The $\Rightarrow$ implication follows immediately when one writes $x = x' + kmn$ with $k \in \mathbb{Z}$.

The $\Leftarrow$ implication follows from the Chinese Remainder Theorem. Suppose $x \equiv x' \mod m$ and $x \equiv x' \mod n$. Denote $a = x \mod n$ and $b = x' \mod n$. Then both x, x' are solutions to the system of congruences

$$\begin{cases} y & \equiv a \mod m\,, \\ y & \equiv b \mod n\,. \end{cases}$$

By the Chinese Remainder Theorem, we know that there exists a $x_0 \in \{0, 1, \ldots, mn - 1\}$ such that $x = x_0 + kmn$ for $k \in \mathbb{Z}$ and $x' = x_0 + k'mn$ for $k' \in \mathbb{Z}$. From this, it immediately follows that $x \equiv x' \mod mn$. □

Exercise 4. *Show that $16 = 2^{1000} \mod 20$ using Cor. 1 and the rules for modular arithmetic.*

1.2 Modular arithmetic

At the start of the topic on algebra, we have discussed the concept of a group. Again, we will impose more structure on a group to obtain a new algebraic structure, called a ring.

Definition 4. *A **ring** is a set R with two binary operations $+$ and $\cdot$ such that:*

1. *$(R, +)$ is an abelian group.*
2. *The operation $\cdot$ is associative, i.e. $\forall x, y, z \in R : x \cdot (y \cdot z) = (x \cdot y) \cdot z$.*

[1] Problems of the kind that relate to the theorem date back as far as the third century, in the Chinese book on mathematics *Sunzi Suanjing* (Master Sun's Mathematical Manual).

3. *The operation $\cdot$ is distributive over $+$, i.e. $\forall x, y, z \in R : x \cdot (y+z) = x \cdot y + x \cdot z$ and $(x+y) \cdot z = x \cdot z + y \cdot z$.*

The ring is usually denoted as $(R, +, \cdot)$.

Note that the operation $\cdot$ does not need to be commutative. If it is, the ring is said to be **commutative**. Because $(R, +)$ is a group, there exists a neutral element 0 for the addition.

Exercise 5. *Prove that $\forall x \in R$, $0 \cdot x = 0$ and $x \cdot 0 = 0$.*

Exercise 6. *Suppose that $(R, \cdot)$ is also a group, and define the neutral element of the multiplication as 1. Prove that R consists of exactly 1 element, $0 = 1$. This is called the trivial ring.*

The most important examples are:

- The ring of the integers $\mathbb{Z}$.
- The rings $\mathbb{Z}_n$ for $n \in \mathbb{N}$. These are the sets $\{0, 1, \ldots, n-1\}$ with addition and multiplication modulo n.
- Square matrices of a fixed size $n \in \mathbb{N}$ with real or complex entries.

It is possible for a neutral element for the multiplication to exist, usually denoted by 1. However, usually $(R, \cdot)$ will not be a group for the above reason.

Definition 5. *If there exists a $1 \in R$ such that $\forall x \in R : 1 \cdot x = x \cdot 1 = x$, then R is called a **ring with unity** 1.*

Exercise 7. *Given what we learned about group homomorphisms / isomorphisms, can you define a ring homomorphism / isomorphism yourself?*

1.2.1 Optional: unit groups

This section will not be treated in class, but can serve as additional material for interested / advanced students. Some proofs further in the text are labelled saying that they rely on the concepts in this section.

Suppose now that we have a ring R with unity 1. Any element $u \in R$ for which there exists and *inverse element* $v \in R$ such that $u \cdot v = v \cdot u = 1$ is called a **unit**.

Definition 6. *The set of all units in R is called the **unit group** of R, denoted $R^\times$.*

Exercise 8. *Prove that the unit group of a ring is a group under the operation $\cdot$.*

The following two theorems are useful to understand the proofs later on. Their proofs are not included but can be found in introductory textbooks, and are good exercises for the reader.

Theorem 5. *Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings with unity. Then $(R \times S)^\times = R^\times \times S^\times$.*

Theorem 6. *Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings with unity. If $f : R \to S$ is a ring isomorphism that maps the unity of R to the unity of S, then f maps the unit group of R to the unit group of S. This means that the unit groups are isomorphic.*

The following theorem focuses on the unit group of $\mathbb{Z}_n$, central to the proofs later on.

Theorem 7. *Let $n \in \mathbb{N}$. Then $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$.*

Proof. Suppose x is a unit in $\mathbb{Z}_n$, i.e. there exists a $y \in \mathbb{Z}_n$ such that $xy = 1 \mod n$. This means that there exists a $k \in \mathbb{Z}$ such that $xy = 1 + kn$. This however implies that any common divisor of x and n is also a divisor of 1, and therefore $\gcd(x, n) = 1$.

Conversely, suppose $\gcd(x, n) = 1$. Then by Thm. 3 there exist $k, y \in \mathbb{Z}$ such that $kx + ny = 1$. This means that $kx = 1 \mod n$, and therefore x is a unit in $\mathbb{Z}_n$. □

1.2.2 The Euler totient function

Definition 7. *The Euler totient function $\phi : \mathbb{N} \to \mathbb{N}$ is defined as the number of positive integers less than n that are coprime to n.*

The proof of the following theorem requires concepts from the optional section 1.2.1.

Theorem 8. *Take $m, n \in \mathbb{N}_0$ with $\gcd(m, n) = 1$. Then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. It is left as an exercise to prove that

$$\theta : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n : x \mapsto (x \mod m, x \mod n) \tag{4}$$

is a ring isomorphism (check that it is well-defined, bijective using Thm. 4). Theorems 5 and 6 then imply that $\mathbb{Z}_{mn}^\times$ and $\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ are isomorphic, as θ maps the unity of $\mathbb{Z}_{mn}$ to the unity of $\mathbb{Z}_m \times \mathbb{Z}_n$.

Note now that $\forall n \in \mathbb{N} : \phi(n) = \#\left(\mathbb{Z}_n^\times\right)$ because of Thm. 7. The theorem now follows as

$$\phi(mn) = \#\left(\mathbb{Z}_{mn}^\times\right) = \#\left(\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times\right) = \#\mathbb{Z}_m^\times \cdot \#\mathbb{Z}_n^\times = \phi(m)\phi(n)\,. \tag{5}$$

□

This is a very useful theorem, as it allows us to calculate $\phi(n)$ for any n by factorizing n into its prime factors. Indeed, suppose

$$n = p_1^{e_1} \cdots p_r^{e_r}\,,$$

then

$$\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r})\,,$$

simply because prime numbers are by definition coprime.

The following lemma gives us the last piece of the puzzle to fully calculate $\phi(n)$.

Lemma 2. *For any prime number p and any $e \in \mathbb{N}_0$, we have*

$$\phi(p^e) = (p-1)\,p^{e-1}\,.$$

Proof. We count the number of elements in $\{1, 2, \ldots, p^e\}$ that are coprime to p^e. The only numbers that are not coprime to p^e are the multiples of p, i.e.

$$p, 2p, 3p, \ldots, p^{e-1}p\,.$$

There are p^{e-1} such multiples, so there are $p^e - p^{e-1} = (p-1)p^{e-1}$ numbers that are coprime to p^e. □

The following theorem summarizes the above.

Theorem 9. *For any $n \in \mathbb{N}_0$, given its prime factorization $n = p_1^{e_1} \cdots p_r^{e_r}$, we have that*

$$\phi(n) = (p_1 - 1)\,p_1^{e_1-1} \cdots (p_r - 1)\,p_r^{e_r-1}\,. \tag{6}$$

So, the Euler totient function of any natural number can be calculated once its prime factors are known.

We state the following theorem without proof, as it requires more knowledge of groups and rings.

Theorem 10. ***(Euler's congruence)*** *Let $a \in \mathbb{Z}, n \in \mathbb{N}_0$ be coprime. Then*

$$a^{\phi(n)} \equiv 1 \mod n\,. \tag{7}$$

Corollary 2. *Let $a \in \mathbb{Z}, n \in \mathbb{N}_0$ be coprime. Then $\forall e \in \mathbb{N}_0$*

$$a^e \equiv a^{e \mod \phi(n)} \mod n\,. \tag{8}$$

Proof. The proof follows from Thm. 10 and the properties of modular arithmetic. □

2 Lecture 2: Cryptography

Cryptography is concerned with creating algorithms to encode and decipher messages and information. It is impossible to overstate the importance of cryptography in everyday life: it is used in banking, online shopping, secure messaging and so much more.

Basic cryptographic methods have been around for thousands of years, but the field has evolved rapidly in the last century with the advent of computers. A famous example of an old method is the Caesar cipher, where each letter in the message is shifted by a fixed number of positions in the alphabet. More general permutations of the alphabet can be used as well of course, making the algorithm even more obscure. Methods like these ones are examples of **private key cryptography**, where the same key is used to encode and decode the message. The succes of the method relies on the secrecy of the algorithm and the key.

This is however not the most secure method of encryption, as the key must be shared between the sender and the receiver, but remain unknown to anyone else. To this end, modern algorithms often rely on a **public key system**, where the key used to encode the message is different from the key used to decode it. This means that a malevolent third party does not gain any advantage from knowing the encoding key, as it needs the decoding key as well to actually read the message.

2.1 RSA algorithm

One of the most famous public key algorithms is the **RSA algorithm**, named after its inventors Rivest, Shamir and Adleman. The RSA algorithm hinges on the fact that it is *complicated* to find solutions to equations of the form

$$x^e \equiv c \mod n\,. \tag{9}$$

Exercise 9. *Try to solve for* $e = 7, c = 5, n = 143$.

Answer: $x = 125$.

Note that complicated here means that is computationally very intensive - with enough time and computing power, solutions to these equations can be found by brute-forcing all possible values of x.

In cryptography, one often talks about Alice and Bob, who want to communicate securely without the inference of a third party, Eve. For Alice and Bob to communicate securely by means of RSA, a couple steps are required, which are summarised below. The mathematical justification for these steps follows after.

First of all, Bob will choose two numbers for his public key, e and n. These two numbers have to satisfy a couple of conditions:

1. (ideally) n is the product of two large prime numbers, p and q.
2. The number e is coprime to $\phi(n)$, where ϕ is the Euler totient function.

Additionally, Bob will create a private key, d, which satisfies the equation

$$de \equiv 1 \mod \phi(n)\,. \tag{10}$$

Bob now publishes his public key, (e, n), and keeps his private key d secret.

When Alice wants to send a message to Bob, she will encode the message as a number M, e.g. by replacing letters by their number in the alphabet, or for more complicated messages by using ASCII. Alice splits her encoded message M in chunks M_i such that $M_i < n$, and encrypts them as $C_i = M_i^e \mod n$. She then sends the encrypted messages C_i to Bob.

For Eve to try and decipher these messages, she needs to solve the equation $x^e \equiv C_i \mod n$ for x, which is *complicated* as we mentioned before. For Bob, however, decoding is easier by means of his private key d. Indeed, as we explain the algroithm in more detail below, Bob recovers the original messages as

$$M_i \equiv C_i^d \mod n\,, \tag{11}$$

allowing him to read the messages Alice sent him.

2.1.1 Mathematical details

Let's start from the perspective of Bob, who wants to set up his public and private keys. The first thing he has to consider is the number n. This number will partially determine e and d satisfying $\gcd(e, \phi(n)) = 1$ and $de \equiv 1 \mod \phi(n)$. Importantly, he wants d to remain secret, and therefore it needs to be hard to calculate d. He can do this by making $\phi(n)$ hard to calculate, i.e. by making it hard to factorize n in primes.

It is known that factorizing large numbers is computationally expensive, and therefore calculating $\phi(n)$ is complicated for large numbers. However, Bob needs to know $\phi(n)$ himself! Checking whether a number is prime, however, is much easier. Therefore, Bob should construct a number n bottom-up, by fixing its prime factorization.

Exercise 10. *Should Bob fix a prime factorization with many prime numbers? What should the relative size of the prime numbers be? Keep Thm. 4 in mind.*

Answer: If the prime factorization contains many different primes, it will be easier to find solution to the equation $x^e \equiv c \mod n$ for large n by using Thm. 4. Furthermore, it is easier to find prime factors if multiple exist: if n has k prime factors, at least one of them is smaller than $n^{1/k}$. A brute force approach that looks for small prime factors will quickly find these.

So, ideally Bob picks two large prime numbers p and q, in practice often having about 300 digits, and sets $n = pq$.

Exercise 11. *What is $\phi(pq)$ if p and q are prime numbers?*

Answer: $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Exercise 12. *Even though p, q should be of similar order of magnitude, they should still have a sufficiently large difference between them. Why is this?*

Answer: If p and q are too close to each other, it is easier to find the prime factorization of n by brute force. One can start looking around $\sqrt{n}$ for prime factors, and if p and q are close to each other, this search will be much quicker.

So, to summarize, Bob has chosen two large prime numbers p, q and set $n = pq$. He can now pick any number e coprime to $\phi(n)$ to form his public key. There exist numbers $d, k \in \mathbb{Z}$ such that $de + k\phi(n) = 1$, i.e. $de \equiv 1 \mod \phi(n)$. Euclid's algorithm can be used to find these numbers.

Exercise 13. *Why is this the case? Which theorem did we use?*

Answer: We used Thm. 3. The numbers e and $\phi(n)$ are coprime, and therefore there exist $d, k \in \mathbb{Z}$ such that $de + k\phi(n) = 1$.

Now it's Alice's turn to send a message to Bob. She encodes her message as a number M, and splits it in chunks M_i such that $M_i < n$. We take any such chunk M_i, and calculate

$$C_i = M_i^e \mod n\,.$$

This is straightforward to calculate, as the numbers e, n are known to Alice. The claim is now that Bob recovers the original messages as

$$M_i = C_i^d \mod n\,.$$

Exercise 14. *Assume M_i and n are coprime. Why can the original message be recovered like this? Which theorem did we use?*

Answer: We used Thm. 10. If M_i and n are coprime, then $M_i^{\phi(n)} \equiv 1 \mod n$. Therefore, $M_i^{de} \equiv M_i \mod n$.

Exercise 15. *Does the result still hold if M_i and n are not coprime? Suppose $p|M_i$, and use Cor. 1.*

Answer: Without loss of generality we can assume that $p|M_i$. Then q cannot be a divisor of M_i, as that would imply n is a divisor of M_i. Using Cor. 1, we can write $M_i = 0 \mod p$ and $M_i = M_i \mod q$. However, since $\phi(n) = \phi(p)\phi(q)$ and since M_i and q are coprime, we have that $M_i^{de} \equiv M_i \mod q$, as $de \equiv 1 \mod \phi(q)$. Since $p \mid M_i$, we also have $M_i^{de} \equiv M_i \mod p$. Therefore, $M_i^{de} \equiv M_i \mod n$ by Cor. 1.

Exercise 16. *Why did we use that $M_i < n$?*

Answer: If $M_i \geq n$, we would not recover the original messages mod n.

3 References

These notes are based on my own knowledge of these basic mathematical concepts, and the writing has been accelerated by the use of *Github copilot* and its implementation in VSCode. Inspiration has been taken from the course notes (particularly in Chapters 1 and 3) for *"Algebraische Structuren"* (Algebraic Structures), used in the first year of the Bachelor of Mathematics at the KU Leuven, at the time taught by Prof. Raf Cluckers - also the author of the lecture notes. The part on cryptography is largely taken from these notes as well.