AN INTRODUCTION TO ARITHMETIC

XEVI GUITART

Abstract. This is an introduction to some topics of arithmetic. Most of the contents and examples are taken from the wonderful book *The magic of numbers* by Benedict Gross and Joe Harris, and from *Elementary Number Theory* by William Stein (this one freely available on his website).

Arithmetic is about the study of whole numbers. Recall that the set of natural numbers is

$$\mathbb{N} = \{1, 2, 3, 4 \dots\}$$

and the set of integer numbers is

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3 \dots\}.$$

1. Divisibility and primes

We begin with some basic notions.

Definition 1.1. Given $a, b \in \mathbb{Z}$ we say that a divides b if there exists $c \in \mathbb{Z}$ such that $b = ac$. It is usual to write $a \mid b$ for a divides b.

Example 1.2. $3 \mid 15$ and $4 \nmid 21$ (that is, 4 does not divide 21). Also, $-7 \mid 35$ and $-7 \mid -35$.

Exercise 1.3. Show that if a number a divides both x and y, then it divides $x + y$.

Definition 1.4. An integer $n > 1$ is prime if its only positive divisors are 1 and n.

For example, the list of the first prime numbers is

$$2, 3, 5, 7, 11, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \dots$$

The set of all prime numbers is among the most fascinating and studied objects in mathematics. There are many questions that one can make. For instance:

- How many primes are there?
- How can we find primes? Is there a formula giving all prime numbers?
- How are they distributed among the set of natural numbers? Are they very sparse? Is there a way to predict where the next prime is going to be?

But why are prime numbers important? Well, to begin with, in some sense they are the building blocks of integer numbers.

Theorem 1.5 (Fundamental Theorem of Arithmetic)**.** *Every natural number can be written as a product of primes, in a unique way up to order*

Example 1.6. $50 = 2 \cdot 5 \cdot 5 = 2 \cdot 5^2$, $130 = 2 \cdot 5 \cdot 13$, or $17 = 17$ is already prime.

Departament d'Àlgebra i Geometria, Universitat de Barcelona, Catalonia
E-mail address: xevi.guitart@gmail.com.

It is easy to see that every number can be written as a product of primes. Suppose n is such number. Then we can ask: Is it divisible by 2? Is it divisible by 3? Is it divisible by 4? And so on until we reach the number itself. If the answer is always "no", then n is prime. If at some point the answer is yes, this means that the number is a product of two smaller numbers, and we can apply the same process with these two numbers.

The part about uniqueness is a bit more tricky. For instance, we know that $130 = 2 \cdot 5 \cdot 13$. But would it be possible to express it as a product of some different primes? The answer is no, every expression of 130 as a product of primes cannot involve any prime other than $2, 5$ and 13; but we postpone the proof of this until a bit later on.

This gives a way to decide about divisibility. Suppose we are given two numbers a, and b. We factor them as $a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$ and $b = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$ (observe that we are using the same set of primes in both numbers; we can always do this if we allow the exponents to be 0). Then $a \mid b$ if $n_i \leq m_i$ for all exponents.

Exercise 1.7. Let a and b be positive integers. Prove that if $a^n \mid b^n$ then $a \mid b$.

1.1. **There are infinitely many primes.** This is was already known to the Greeks; it is due to Euclid.

Suppose that $p_1, \dots, p_n$ are prime numbers. We are going to show that there must exist a prime number not contained in the set $\{p_1, \dots, p_n\}$. This implies that there are in fact infinitely many prime numbers.

The idea is to form the number

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

This is clearly bigger than all the p_i's. If it is prime, then we are done. If it is not prime, it must be divisible by some prime. But this prime cannot be any p_i, because then p_i would divide 1. So there must be a prime not contained in that list.

Exercise 1.8. Find a sequence of 23 consecutive numbers which does not contain any prime number. Hint: consider the numbers $24! + 2$, $24! + 3$, $24! + 4$, etc.

Exercise 1.9. Show that for any $n > 1$ there exists a collection of n consecutive natural numbers not containing any prime number. (On the other hand, it is conjectured that there exist infinitely many pairs of prime numbers p such that $p + 2$ is also prime; the primes p and $p + 2$ are then called twin primes.)

1.2. **The sieve of Eratostenes.** This is a method for enumerating all primes up to n. It is very simple. First of all, you write the list of numbers

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12, \dots$$

We can proceed as follows. Certainly 2 is prime. Then we cross out of the list the multiples of 2 because these will not be prime. The first number not crossed, namely 3, is then a prime. Then we cross out the multiples of 3. The first number not crossed must be prime; then we cross out the multiples of 5, and so on.

When do we stop crossing? Well, until we reach a prime which is greater or equal than $\sqrt{n}$. This is because of the following observation:

$$\text{if } n \text{ is not prime, then it must be divisible by some number } \leq \sqrt{n}. \tag{1.1}$$

This method for finding primes is called the sieve of Eratostenes. There are perhaps some more sophisticated ways of finding primes nowadays, but we do not have any formula that gives all the primes!

Exercise 1.10. Find the primes between 200 and 220.

Exercise 1.11. Prove the above claim (1.1).

1.3. **Integer division.** We need to recall a very helpful property of integers.

Theorem 1.12. *If $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exist unique integers q and r such that*

$$a = bq + r,$$

with $0 \leq r < |b|$.

You are probably familiar with the statement when a and b are positive, but the general case follows from this one.

Example 1.13. Let's divide 7 by 3:

$$7 = 3 \cdot 2 + 1;$$

and now -7 by 3:

$$-7 = 3 \cdot (-3) + 2.$$

Observe that we ask the residue to be always between 0 and $7 - 1 = 6$.

These are very simple examples, but there is an algorithm (that is, a method) for carrying out integer division, even for very large numbers. In fact, it is the algorithm that you learned at school.

1.4. **Greatest common divisor.**

Definition 1.14. The greatest common divisor of two numbers $a, b \in \mathbb{Z}$, denoted $\gcd(a, b)$, is the maximum number that divides both a and b.

Example 1.15. $\gcd(6, 9) = 3$

Now, how can we compute the gcd of a pair of numbers? You have probably learned at school one method, based on the prime factorization: write down the prime factorization of a and b, and choose the primes that are common, with exponent the minimum in which it appears in the two factorizations.

Example 1.16. To compute $\gcd(168, 140)$ we write $168 = 2^3 \cdot 3 \cdot 7$ and $140 = 2^2 \cdot 5 \cdot 7$, and then $\gcd(168, 140) = 2^2 \cdot 7 = 28$.

This method has a practical problem: it involves knowing the prime factorization of a number. It turns out, that if the number is huge (say several hundreds of digits) then this is a very hard problem, even using computers.

There is a much better method (algorithm) to compute gcd's. It is one of the greatest pieces of mathematics of all times, the Euclidean algorithm.

Let us begin with an example. Namely, $\gcd(168, 140)$. Let us divide these two numbers

$$168 = 140 + 28.$$

The key observation is that if $d \mid 168$ and $d \mid 140$, then d also divides 28. Conversely, if $d \mid 140$ and $d \mid 28$, it also divides 168. In particular, $\gcd(168, 140) = \gcd(140, 28)$. Thus we have reduced to compute the gcd of a couple of smaller numbers! Then we apply the same process. We divide 140 by 28 and we see that $140 = 28 \cdot 5$. Thus $\gcd(168, 140) = \gcd(140, 28) = 28$.

This method is called Euclid's algorithm[1].

Algorithm 1.17. To compute the gcd of a and b:

(1) Perform the integer division $a = bq + r$;
(2) If $r = 0$ we are done, and $\gcd(a, b) = b$;
(3) If $r \neq 0$, then replace the pair (a, b) by (b, r) and go back to step (1).

Example 1.18. Find $\gcd(532, 123)$. We divide:

$$532 = 4 \cdot 123 + 40, \tag{1.2}$$

so that $\gcd(532, 123) = \gcd(123, 40)$. We divide again:

$$123 = 3 \cdot 40 + 3 \tag{1.3}$$

so that our new pair is $(40, 3)$. Once again

$$40 = 13 \cdot 3 + 1 \tag{1.4}$$

so that $\gcd(40, 3) = \gcd(3, 1) = 1$. All in all, $\gcd(532, 123) = 1$.

We do it once again, but this time we write equations (1.2), (1.3), and (1.4) slightly different, emphasizing the sequence of residues:

$$40 = 532 - 4 \cdot 123 \tag{1.5}$$

$$3 = 123 - 3 \cdot 40 \tag{1.6}$$

$$1 = 40 - 13 \cdot 3 \tag{1.7}$$

We could perform one more division and get residue 0. Thus we see that the last non-zero residue is the gcd.

Remark 1.19. This is a very efficient algorithm. With the help of a computer we can compute gcd's of hughe numbers, easily of hundreds of digits. Indeed, every time you divide a by b you get a residue between 0 and $b - 1$; on average, you expect it to be around $b/2$. This suggests that at every step the size of the numbers involves gets divided by a factor of 2. Thus if, for instance, we begin with numbers of size roughly 1.000.000, which is close to 2^{20}, Euclid's algorithm should finish in roughly 20 steps.

Exercise 1.20. Let a, m, and n be positive integers with $m \neq n$. Compute $\gcd(a^{2^m} + 1, a^{2^n} + 1)$.

1.5. Combinations.

Definition 1.21. Given two numbers $a, b \in \mathbb{Z}$, a sum of a multiple of a and a multiple of b is a combination of a and b. That is to say, the combinations of a and b are the numbers of the form

$$x \cdot a + y \cdot b, \quad \text{for some } x, y \in \mathbb{Z}.$$

Let $d = \gcd(a, b)$. Clearly if n is a combination of a and b then $d \mid n$. So all combinations of a and b are multiples of d. It turns out that d itself is a combination of a and b. That is to say, we can always write $\gcd(a, b)$ as a combination of a and b. The reason is...Euclid's algorithm!

[1] for us an algorithm is just a sequence of instructions that can be followed to perform a specific calculation, that must finish on any valid imput

We have seen that $\gcd(532, 123) = 1$, so we would like to write 1 as a combination of 532 and 123. How do we do that? Well, let's look again at the equalities (1.5) throught (1.7). The last one tells us how to write 1 as a combination of 40 and 13:

$$1 = 1 \cdot 40 - 13 \cdot 3;$$

but then, (1.6) tells us how to write 3 as a combination of 40 and 123; plugging this into the above equality we get:

$$1 = 1 \cdot 40 - 13 \cdot (123 - 3 \cdot 40) = -13 \cdot 123 + 40 \cdot 40.$$

Finaly, (1.5) tells us how to write 40 as a combination of 123 and 532:

$$1 = -13 \cdot 123 + 40 \cdot 40 = -13 \cdot 123 + 40(532 - 4 \cdot 123) = -173 \cdot 123 + 40 \cdot 532$$

Theorem 1.22. *The combinations of a and b are exactly the multiples of $\gcd(a, b)$. Moreover, we can effectively compute the combination by means of Euclid's algorithm.*

Exercise 1.23. Let a, b, c, and n be integers. Prove that:

(1) If $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$ then $ab \mid n$.
(2) If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

Exercise 1.24. Show that if we can write 1 as a combination of a and b, then we can also write 1 as a combination of a^m and b^n for all $m, n \geq 1$.

1.6. **Solving linear equations.** We can rephrase what we just saw in the language of solving equations. Suppose that a, b, n are integer numbers and you want to solve the equation

$$ax + by = n;$$

that is, you want to find all integers x and y that satisfy the above equality. There are two steps to solve this problem: the first one is to decide whether the equation has solutions or not. The second one is to find them all, in case there are any.

From what we have seen, here's a method:

(1) Run Euclid's algorithm to compute $d = \gcd(a, b)$.
(2) If $d \nmid n$, the equation has no solutions at all.
(3) If $d \mid n$, say $n = cd$, then run Euclid's algorithm to find $x_0, y_0 \in \mathbb{Z}$ with

$$ax_0 + by_0 = d$$

(4) Multiply the above equality by c, to get a solution of the original equation:

$$acx_0 + bcy_0 = n;$$

This is one solution, but there are more. Observe that $a \cdot \frac{b}{d} - b \cdot \frac{a}{d} = 0$, so if you add this equation (or any multiple $a \cdot \frac{kb}{d} - b \cdot \frac{ka}{d} = 0$) you get another solution

$$a(cx0 + \frac{kb}{d}) + b(cy_0 - \frac{ka}{d}) = n.$$

Actually, by varying k you get all the solutions.

Exercise 1.25. For each of the following equations determine whether there is a solution in integer numbers. If so, find one.

$$24x + 106y = 2$$
$$24x + 106y = 3$$
$$24x + 106y = 4.$$

1.7. **Primes, again.** We will use the Euclidean algorithm to prove the following very important property about primes.

Theorem 1.26. *If a prime p divides a product of integer numbers ab, then either p divides a or p divides b*

Indeed, suppose that $p \nmid a$. Then, since p is a prime we have that $\gcd(a,p) = 1$. Therefore, we can write

$$1 = xa + yp \quad \text{for some } x, y \in \mathbb{Z}.$$

Multiplying by b we get

$$b = xab + ypb \quad \text{for some } x, y \in \mathbb{Z}.$$

from which we see that p divides b.

This property is what allows us to proof uniqueness in the prime decomposition of integers. Indeed, suppose that an integer n can be written in two different ways as $n = p_1 \cdot \cdot p_2 \cdots$ and $n = q_1 \cdot q_2 \cdots$. Then p_1 divides $q_1 \cdot q_2 \cdots$, so it must divide one of the q_i's; since the q_i's are primes, we must have $p_1 = q_i$ for some i; then we can eliminate p_1 from both factorizations and apply the same argument.

1.8. **Relatively prime numbers and Euler's Phi function.**

Definition 1.27. We say that two numbers m and n are relatively prime if $\gcd(m, n) = 1$.

Equivalently, m and n are relatively prime if 1 can be written as a combination of m and n. Or, also equivalently, if every integer number is a combination of m and n.

In this section we are interested in the following problem: given a number n, how many numbers between 0 and $n - 1$ are relatively prime to n? We will denote by $\phi(n)$ this quantity.

Example 1.28. $\phi(6) = 2$; indeed, we look at the numbers $0, 1, 2, 3, 4, 5$ and we see that only two of them are relatively prime to 6.

For prime numbers this is a very simple quantity to compute:

Exercise 1.29. Show that if p is prime then $\phi(p) = p - 1$.

For composite numbers there is also a nice formula.

Theorem 1.30. *Suppose that the prime numbers dividing n are $p_1, p_2, \ldots, p_r$. Then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

Proof. Let's just do the case where $n = pq$ is the product of 2 primes. In fact, let us just do the case where $n = 3 \cdot 5$. One uses a modified sieve. We write

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14$$

and we cross out the multiples of 3; this leaves crosses 1/3 of the numbers, so it leaves $15(1-1/3)$ of the numbers. Then we cross out the multiples of 5, and this crosses 1/5 of the numbers living $15(1-1/3)(1-1/5)$.

The general case is done similarly, although one needs to pay attention to independence. The number of numbers crossed off in the first step is n/p, in the second is n/q, and in both steps is n/pq (this is because p and q are relatively prime, so the multiples of p and q are precisely the multiples of pq). Then the total remaining is

$$n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

□

2. Modular Arithmetic

Let's begin with some motivation. Suppose that we are interested in computing the integer solutions to the following equation

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

Well, it turns out that it does not have any integer solution. That is to say, there does not exist any $x, y \in \mathbb{Z}$ such that $x^2 + x = 2y^2 + 1$. Here is one argument for this. Suppose that such x, y existed. Then x is either even or odd. If x was even, then $x^2 + x$ would also be even and it cannot be equal to $2y^2 + 1$, which is odd. Similarly, if x was odd then $x^2 + x$ would also be even.

So thinking classifying the numbers between odd and even is very helpful. But it has limitations, for instance we can not apply the same reasoning to $x^2 + 3x = 3y^2 - 1$. This section is about a generalization of the concept of even and odd. We can think of even numbers as those that when divided by 2 leave residue 0; and odd numbers are those that leave residue 1. Thus even numbers leave all the same residue when divided by 2 (they leave residue 0), and odd numbers leave the same residue when divided by 2 (they leave residue 0).

2.1. **Addition, substraction, multiplication.**

Definition 2.1. Let n be a number. We say that two numbers a and b are congruent modulo n, written $a \equiv b \pmod{n}$, if $a - b$ is divisible by n. In other words, if they leave the same residue when divided by n.

Example 2.2. $5 \equiv 2 \pmod{3}$, $17 \equiv 5 \pmod{12}$.

Every number is congruent $\pmod{n}$ to one and only one of the numbers $0, 1, 2, \ldots, n-1$. For instance, if we are working modulo 7, then 221 is going to be congruent to exactly one of the numbers $0, 1, 2, 3, 4, 5, 6$. To find out which, we do integer division: $221 = 31 \cdot 7 + 4$; since the residue is 4, then $221 \equiv 4 \pmod{7}$.

Proposition 2.3. *The congruence class* $\pmod{n}$ *of a sum or product of numbers is determined by the congruence classes* $\pmod{n}$ *of the numbers added or multiplied.*

Proof. Call a and b these numbers. Then we can write $a = xn + k$ and $b = yn + l$, with k and l between 0 and $n-1$. Then $a + b = k + l + n(x+y)$. Similarly for the product. □

Exercise 2.4. Take a pair of numbers congruent to 3 and 5 $\mod 7$. What is their sum congruent to $\pmod{7}$? And their product?

Now we can see that the equation $x^2 + 3x = 3y^2 - 1$ does not have any integer solution. Indeed, if we look it modulo 3 the left hand side is congruent to either 0 or 1 and the right hand side is -1.

Exercise 2.5. Compute the following in modular arithmetic:

(1) $639 \cdot 437 \pmod 7$,
(2) $224 \cdot 376 \pmod{17}$,
(3) $632^2 \pmod{633}$.

Exercise 2.6. Show that a number $n \in \mathbb{Z}$ is divisible by 3 if and only if the sum of the digits of n is divisible by 3.

Exercise 2.7. (Wilson's Theorem) Prove that if $p > 1$ is prime then $(p-1)! \equiv -1 \pmod p$. (Hint: prove first that $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$.) In fact, Wilson's theorem also says the converse: if $(p-1)! \equiv -1 \pmod p$ then p is prime. You can try to prove it as well.

2.2. **Division.** What does it mean to divide in arithmetic $\pmod n$? For example, can we make sense of something like 2/3 in arithmetic $\pmod{10}$? We can think of this as 2 times the inverse of 3. But then, what is the inverse of $3 \pmod{10}$?

Definition 2.8. Let $a \in \mathbb{Z}$. The inverse of $a \pmod n$ is a number $b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod n$.

For example, the inverse of $3 \pmod{10}$ is 7, because $3 \cdot 7 = 21 \equiv 1 \pmod{10}$. We warn you that inverses do not always exist.

Exercise 2.9. Check that the inverse of $3 \pmod 6$ does not exist.

In general, the inverse of $a \pmod n$ exists when $\gcd(a, n) = 1$. The proof, as well as the method for computing the inverse is given to us by the great Euclidean algorithm.

Theorem 2.10. *If* $\gcd(a, n) = 1$ *then* a *has an inverse* $\pmod n$. *(We will denote by* a^{-1} *this inverse.)*

Proof. By the euclidean algorithm there exist $x, y \in \mathbb{Z}$ such that

$$a \cdot x + n \cdot y = 1.$$

The above equality is saying, precisely, that $a^{-1} = x$. □

Example 2.11. Compute the inverse of $8 \pmod{11}$. If we run Euclid's algorithm to 8 and 11 we find that

$$\begin{aligned} 3 &= 11 - 1 \cdot 8; \\ 2 &= 8 - 2 \cdot 3; \\ 1 &= 3 - 1 \cdot 2; \end{aligned}$$

If we run it backwards we find that

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= 3 \cdot 3 - 1 \cdot 8 \\ &= 3 \cdot (11 - 1 \cdot 8) - 1 \cdot 8 \\ &= -4 \cdot 8 + 3 \cdot 11. \end{aligned}$$

All in all, $1 = -4 \cdot 8 + 3 \cdot 11$ or, what is the same

$$-4 \cdot 8 = 1 - 3 \cdot 11;$$

this tells us that $8^{-1} \equiv -4 \equiv 7 \pmod{11}$. We can also check that $7 \cdot 8 = 56 \equiv 1 \pmod{11}$.

Corollary 2.12. *If* $\gcd(a, n) = 1$ *then the equation* $ax \equiv b \pmod{n}$ *has a solution, which is unique* $\pmod{n}$*.*

Lemma 2.13. *If R is a complete set of residues* $\pmod{n}$ *and* $a \in \mathbb{Z}$ *with* $\gcd(a, n) = 1$*, then*

$$\{ax \mid x \in R\}$$

is also a complete set of representatives $\pmod{n}$*.*

Proof. If $ax \equiv ax' \pmod{n}$ then multiplying by $a^{-1} \pmod{n}$ we see that $x \equiv x' \pmod{n}$. □

Example 2.14. Let us work $\pmod 6$, and let us take $a = 5$. A complete set of residues $\pmod 6$ is

$$R = \{0, 1, 2, 3, 4, 5\}.$$

Then, if we multiply the above numbers by 5 we get

$$\{0, 5, 10, 15, 20, 25\};$$

If we reduce them $\pmod 6$ we get

$$\{0, 5, 4, 2, 1\}$$

which is a reordered version of the system we started with.

2.3. **Powers.** Given a number $a \in \mathbb{Z}$ and $k \in \mathbb{N}$ then we may be interested in computing $a^k \pmod{n}$. This is nothing really new because it's just a multiplied by itself k times. For example to compute $11^4 \pmod 3$ we can do

$$11^4 = 14641 \equiv 1 \pmod 3. \tag{2.1}$$

That is, we compute 11^4 as an integer and then reduce $\pmod{11}$. But this might become very costly if the numbers are big. Suppose that we want to compute $13^{3456422} \pmod{100}$. The number $13^{3456422}$ is enormous (it has millions of digits!), but in this chapter we will learn some techniques that will allow us to compute $13^{3456422} \pmod{100}$, by hand! In particular, we will never know what the number $13^{3456422}$ is, but we can easily compute its last, say, two digits.

To begin with, let's go back to (2.1). An easy observation is that instead of raising 11 to the 4 and then reducing $\pmod 3$, we can do it the other way around: reduce 11 $\pmod 3$ and then raise the result to the power 4 (and reduce again). Namely, $11 \equiv -1 \pmod 3$, and then $11^4 \equiv (-1)^4 = 1 \pmod 3$. We get the result without having to compute 11^4 as an integer. This is the first trick, the most elementary one.

The second one is to use a theorem of Fermat, and its generalization due to Euler.

Theorem 2.15 (Fermat)**.** *If* $a \in \mathbb{Z}$ *and* $p \nmid a$ *then* $a^{p-1} \equiv 1 \pmod{p}$*.*

Example 2.16. Take $a = 2$ and $p = 5$; Then $2^4 = 16 \equiv 1 \pmod 5$. This is helpful in computing powers. For instance, suppose that we want to compute $3^{22} \pmod 5$. Then

$$3^{22} = 3^{2+4\cdot 5} = 3^2 \cdot (3^4)^5 \equiv 3^2 \equiv 9 \equiv 4 \pmod 5.$$

Theorem 2.17 (Euler)**.** *If* $a, n \in \mathbb{Z}$ *and* $\gcd(a, n) = 1$*, then* $a^{\phi(n)} \equiv 1 \pmod{n}$*.*

Proof. Let R be a set of representatives of the invertible elements $\pmod{n}$:

$$R = \{x\colon 1 \leq x \leq n \text{ and } \gcd(x,n) = 1\}.$$

We know that it has cardinal $\phi(n)$. Then, as in Lemma 2.13 we have that $\{ax \mid x \in R\}$ is also a complete set of representatives of invertible elements $\pmod{n}$. Therefore

$$\prod_{x\in R} ax \equiv \prod_{x\in R} x \pmod{n}.$$

Since the $x \in R$ are invertible, we can cancel them out and we get that

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

□

Exercise 2.18. Compute the last two digits of 3^{45}

We have seen that in order to compute $a^k \pmod{n}$, we can always reduce to exponents k which are $\leq \phi(n)$. Still, $\phi(n)$ can be pretty big, specially in the applications to cryptography that we will see in the next chapter. So the naive approach of multiplying $a \pmod{n}$ by itself k times might be very slow. Here is a better way to do it. Let us begin with an example. Suppose that we want to compute, say, $3^{16} \pmod{23}$. The naive method would be to multiply $3\cdots 3$ 16 times. This means, 15 multiplications. Here's a better way to do it: We first compute $3^2 \equiv 9 \pmod{23}$; then we square this: $3^4 \equiv 9^2 \equiv 12 \pmod{23}$; then we square this again: $3^8 \equiv 12^2 \equiv 6 \pmod{23}$; finally we square again: $3^{16} \equiv 6^2 \equiv 13 \pmod{23}$. So that's just four multiplications, instead of 16.

Now, what's so special about the exponent 16? Well, in fact that $16 = 2^4$. What if we wanted to raise to the power, say 19? Then we realize that $19 = 2^4 + 2 + 1$ and we can compute 2^{19} as follows:

1. Compute 3^2 (1 multiplication)
2. Compute $3^{2^2} = 3^2 \cdot 3^2$ (one multiplication)
3. Compute $3^{2^3} = 3^{2^2} \cdot 3^{2^2}$ (one multiplication)
4. Compute $3^{2^4} = 3^{2^3} \cdot 3^{2^3}$ (one multiplication)
5. Finally, compute $3^{19} = 3^{2^4+2+1} = 3^{2^4} \cdot 3^2 \cdot 3$ (two multiplications)

What we just did for the exponent 19 can be done for any exponent n, by considering its binary expression. That is, we just need to compute the digits of n in base 2:

$$n = n_r \cdot 2^{2^r} + n_{r-1} \cdot 2^{2^{r-1}} + \cdots n_2 \cdot 2^{2^2} + n_1 \cdot 2 + n_0.$$

In order to find the binary expression of n, first of all we need to find the highest power of 2 that divides n, say $2^m \mid n$ and $2^{m+1} \nmid n$. This tells us that $n_m = 1$ and it is the first non-zero bit. Then we subtract it from n, i.e., we compute $n - 2^m$ and we repeat the process. For example, 2^0 is the highest power of 2 dividing 19. Then $n_0 = 1$; now $19 - 1 = 18$ and 2^1 is the highest power of 2 that divides it, so $n_1 = 1$; then $18 - 2 = 16$ and 2^4 is the highest power dividing it so that $n_4 = 1$; and we are done because $16 - 2^4 = 0$. That is, $19 = 10011$ i binary.

Exercise 2.19. Find the last two digits of 7^{91}, by computing $7^{91} \pmod{100}$.

3. An application to Cryptography

Cryptography is about secure communication in the presence of adversaries. That is, it provides mechanisms for interchanging a message without a third party being able to understand it. Before the 20th century this was mainly important for military applications; for example, if the officers wanted to send a message to the troops without the enemy being able to understand in case it was intercepted. In the second half of the 20th century, with the explosion of digital communication this has found way more applications to our everyday life. For example, every time that you buy online your browser encrypts your credit card number before sending it.

So the setting is that party A wants to send a secret message to party B and we know that party C (the adversary) is listening. So he can read the message. Our aim is that only B is able to understand it.

3.1. **Private key cryptography.** The traditional method to solve this problem is to use what is known as *private key cryptography.* The easiest example of this is to shift every letter of the alphabet certain number of positions. For example, we can do the following substitution: $a \to d$; $b \to e$; $c \to f$; and so on. That is, we shift every letter 3 positions to the left.

Example 3.1. To ciphered message for "attack" would be "dwwdn".

Another way to think about it is the following: replace every letter by a number modulo 26 (suppose there are 26 letters in the alphabet): $a \to 0$; $b \to 1$, and so on. To cipher a message, translate the letters to numbers and add 3 (mod 26). To decipher the coded message you need to undo the ciphering. In this case, subtract 3. In this case the key is 3. This system has two drawbacks:

(1) It can be easily broken, by using frequency analysis: not all letters are equally common in English. For instance, e is the most common. So if you read a long enough message, it is very likely that the letter that appears the most corresponds to e. This knowledge gives you the key, and you can decode the rest of the message.
(2) Alice and Bob need to meet beforehand for arranging the key, in such a way that only they (and nobody else) know it. This is why it is called private key.

The first drawback can be overcome (to some extent). For example, there is a generalization of the method that we just saw which is known as the Vigenère cipher. It is also a substitution code, but the same letter gets substituted by different letters according to the position. We are going to do it by an example.

Example 3.2. Suppose that we want to cipher "BARKING UP THE WRONG TREE". Translated to numbers this is

$$01\ \ 00\ \ 17\ \ 10\ \ 08\ \ 13\ \ 06\ \ 20\ \ 15\ \ 19\ \ 07\ \ 04\ \ 22\ \ 17\ \ 14\ \ 13\ \ 06\ \ 19\ \ 17\ \ 04\ \ 04$$

The key is going to be a word, for example "iniesta", which translates into 08 13 08 04 18 19 00. Then we do the following

$$\begin{array}{ccccccccccccccccccccc} 01 & 00 & 17 & 10 & 08 & 13 & 06 & 20 & 15 & 19 & 07 & 04 & 22 & 17 & 14 & 13 & 06 & 19 & 17 & 04 & 04 \\ 08 & 13 & 08 & 04 & 18 & 19 & 00 & 08 & 13 & 08 & 04 & 18 & 19 & 00 & 08 & 13 & 08 & 04 & 18 & 19 & 00 \end{array}$$

and we sum modulo 26:

$$09\ \ 13\ \ 25\ \ 14\ \ 00\ \ 06\ \ 06\ \ 02\ \ 02\ \ 01\ \ 11\ \ 22\ \ 00\ \ 14\ \ 23\ \ 11\ \ 23\ \ 04$$

which back to letters is "JNZOAGGCCBLWAOXLXE". Observe that this makes it difficult the frequency analysis because, for instance, the several E's are converted in different letters, according to their position in the message.

3.2. **Public key cryptography: RSA.** Suppose that Alice wants to send a message to Bob. Here is how RSA works. First of all, Bob:

- Chooses two random and very large prime numbers p and q.
- Then he computes, very easily, $n = pq$ and $\phi(n) = (p-1)(q-1)$.
- He chooses a random integer e such that $\gcd(e, \phi(n)) = 1$.
- Bob makes public n and e. This is the public key, everybody knows it.
- Bob computes $d \in \mathbb{Z}$ such that $ed \equiv 1 \pmod{\phi(n)}$ (using Euclid's algorithm!). This is the private key, he keeps it to himself.

The messages are going to be integers $\pmod{n}$. So if Alice wants to send a message to Bob, she translates his message, in some way, into a sequence of integers modulo n. Suppose that m is one such integer modulo n forming the message.

- Alice computes $m^e \pmod{n}$ and this is the encrypted message that she sends to Bob.

Now Bob can recover m from m^e by computing $(m^e)^d$. Indeed, observe that

$$(m^e)^d = m^{1+k\phi(n)} = m \cdot (m^{\phi(n)})^k \equiv 1 \pmod{n}.$$

Now the key point is that in order to decipher we need d. But d is the inverse of e modulo $\phi(n)$. Everybody knows n and e, so you might think: OK, what prevents the adversaries to compute $\phi(n)$, which in the end is just $(p-1)(q-1)$, and then compute the inverse of $e \pmod{\phi(n)}$. Well, this method works...in theory! Observe that for computing $\phi(n)$ one needs to know p and q. But what is public is just n. So one would need to factor n, and this is very time consuming if p and q are large. So in practice, it is impossible.

4. Problems

These problems are extracted from Niven&Zukerman's *Introduction to the theory of numbers.*

1. What is the largest number of consecutive square-free positive integers? And of consecutive cube-free positive integers?
2. If x and y are odd, prove that $x^2 + y^2$ cannot be a perfect square.
3. Two primes are called *twin primes* if they differ by two. For example 3 and 5 are twin primes. Also the pairs 5 and 7, 11 and 13, 17 and 19,...Show that 5 is the only prime belonging to two such pairs.

   (It is a very famous conjecture in number theory that there are infinitely many twin primes. But we do not know yet whether this is true or not.)
4. Prove that any positive integer of the form $4k+3$ has a prime factor of the same form; similarly for $6k+5$.
5. Prove that there are infinitely many primes of the form $4k+3$; similarly[2] for $6k+5$.
6. Prove that no polynomial $f(x)$ of degree $n > 1$ with integral coefficients can represent a prime for every positive integer x.
7. Show that if p is prime, then $\binom{p}{k} \equiv 0 \pmod{p}$ for all $0 < k < p$.
8. Show that for any prime p, if $a^p \equiv b^p \pmod{p}$ then $a^p \equiv b^p \pmod{p^2}$.
9. If p is a prime other than 2 and 5, prove that p divides infinitely many of the integers 9, 99, 999, 9999,...
10. What is the last digit (in the usual base 10) of the number 3^{400}?

[2] These results can be stated as follows: the arithmetic progressions $4k+3$ (these are the numbers 3,7,11,15,19,...) and $6k+5$ (the numbers 5,11,17,23,29,...) contain infinitely many primes. Dirichlet's Theorem on arithmetic progressions says that if $(k,n) = 1$ then the arithmetic progression $k, k+n, k+2n, k+3n, \ldots$ contains infinitely many primes. The proof is not elementary though, and it uses complex analytic tools.