A GENTLE INTRODUCTION TO NUMBER THEORY AND CRYPTOGRAPHY

[NOTES FOR THE PROJECT GRAD 2009]

LUÍS FINOTTI

Contents

1. Important Sets

Before we start with the main topics, we need to review some notation:

Definition 1.1. (1) A *set* is just a collection of elements. We usually denote a set by enclosing its elements in braces "{ }". [So, $\{1, 2, 3, 4\}$ is a set whose elements are the numbers 1, 2, 3, and 4.] Sets don't need to have numbers as elements, but they likely will in this course. Note that the order that we write the elements of the set does not matter, all that matters is the content, i.e., what elements it has.

(2) An element of a set is said to *belong* to the set. We use the symbol "$\in$" for "belongs to" and "$\notin$" for "does not belong to", such as in:

$$1 \in \{0, 1, 2\} \qquad \text{and} \qquad 3 \notin \{0, 1, 2\}.$$

(3) We have that

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\},$$

denotes the set of *natural numbers*. [The *ellipsis* here means "continues in the same way".] **Careful:** Some authors exclude zero from the set of natural numbers. We will use instead

$$\mathbb{N}^* = \{1, 2, 3, 4, \ldots\},$$

and refer to $\mathbb{N}^*$ as the set of *positive integers*. [Note that zero is neither positive nor negative!]

(4) We define the set of *integers* as

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

(5) We define the set of *rationals* as

$$\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p \in \mathbb{Z} \text{ and } q \in \mathbb{N}^* \right\}.$$

[The colon " : " above reads as "such that". So, we read the set above as "the set of all [fractions] p/q such that p is in $\mathbb{Z}$ and q is in $\mathbb{N}^*$".] This set includes then all fractions of integers, such as $\frac{1}{2}$, $-\frac{3}{7}$, $\frac{7636524628}{8745834838388}$, etc. [Remember, *we can never divide by zero*!]

(6) The set of *real numbers*, which is studied in [pre]calculus is denoted by $\mathbb{R}$. It contains $\mathbb{Q}$ and all *irrational numbers* [which cannot be expressed as fractions of integers], such as $\sqrt{2}$, $\sqrt[17]{31}$, π, e, etc.

Loosely speaking, [classical] number theory, the subject of this course, is the study of integers. Sometimes, sets that are "similar" to the integers are also studied. But, for purists, the study of those sets are only relevant if it yields results or ideas of importance to the integers. It is then not very surprising that the rational numbers often show up in number theory, and it is also often considered to have its own interest in the field.

Although it would seem that the set of real numbers is not very relevant to the study of integers, it does show up often. Even more, the set of *complex numbers* [for those who have heard of them], which is usually denoted by $\mathbb{C}$, is quite important to number theory. [We will not deal with $\mathbb{C}$ in this course.]

Problems.

1.1) Decide if each statement below is true or false:

(a) $2 \in \mathbb{Q}$.

(b) $-2/3 \in \mathbb{Z}$.

(c) $\pi \in \mathbb{Q}$.

(d) $0 \in \mathbb{N}$.

(e) $0 \in \mathbb{N}^*$.

(f) $\sqrt{2} \in \mathbb{R}$.

(g) $\sqrt{2} + 1 \in \mathbb{Q}$.

(h) $\mathrm{e} \in \mathbb{Z}$.

(i) $-5 \in \mathbb{N}$.

(j) $5/4 \in \mathbb{Q}$.

2. Long Division

We will deal mostly with integers in this course, as it is the main object of study of number theory. We will need to know *long division* [also called *division algorithm*] of integers.

Example 2.1. Here is a quick example with 3812 divided by 15:

$$\begin{array}{r} 254 \\ 15\overline{)3812} \\ \underline{3000} \\ 812 \\ \underline{750} \\ 62 \\ \underline{60} \\ 2 \end{array}$$

In this example, we call 3812 the *dividend* and 15 the *divisor*. We also call 254 the *quotient* and 2 is the *remainder*. [Remember that we stop the division when the remainder becomes less than the divisor, in this case, less than 15.] This means that:

$$3812 = 15 \cdot 254 + 2.$$

[You should remember how to perform these long divisions! If you forgot, review and practice!]

In general if we divide a positive integer m by another positive integer n [so, n is *different from zero*, since, again, we can *never* divide by zero], we have that the quotient, say q, and remainder, say r, are such that

$$m = n \cdot q + r, \qquad \text{with } 0 \leq r < n. \tag{2.2}$$

We should observe also that the representation of formula (2.2) is unique! [The key factor is the restriction on the size of the remainder.] This means that if we have, for instance, $312 = 15 \cdot 20 + 12$, then, since $0 \leq 12 < 15$, this automatically means that the quotient of the division of 312 by 15 is 20 and the remainder is 12.

Example 2.3. Here is another example. If you know that:

$$377 = 12 \cdot 31 + 5,$$

then, since $0 \leq 5 < 12$, we know that the remainder of the division of 377 by 12 is 5. And, since $0 \leq 5 < 31$, we also have that the remainder of the division of 377 by 31 is 5. [So, 12 can be seen in the formula above as either the quotient or as the divisor.]

Now, what about if m, n, or both are negative? We can still perform the long division. Note that, as specified in equation (2.2), *the remainder is always either zero or positive*. On the other hand, the quotient might be negative.

Probably, the best way to see how it works is to show it with examples:

Examples 2.4. (1) *Division of* -3812 *by* 15*:* We perform the long division of the positive numbers [as done above]. If we multiply what we get [i.e., $3812 = 15 \cdot 254 + 2$] by negative one, we get:

$$\begin{aligned} -3812 &= -(15 \cdot 254) - 2 \\ &= 15 \cdot (-254) - 2, \end{aligned}$$

which is not yet what we want as we have now a "negative remainder". To fix that, we "borrow" 15 from the quotient, more precisely,

$$-3812 = 15 \cdot (-254 - 1) + (15 - 2),$$

i.e.,

$$-3812 = 15 \cdot (-255) + 13,$$

and so the new quotient and remainder are, respectively, -255 and 13. [Note that the quotient is negative, but the remainder is positive and less than 15.]

This is how it works in general. The new quotient is the negative of the old minus one, and the new remainder is the difference between the divisor [which is 15 in the above example] and the old remainder.

(2) *Division of* 3812 *by* -15*:* We, again, perform the long division of the positive numbers [as done above]. We then immediately get:

$$3812 = (-15) \cdot (-254) + 2,$$

and so the new quotient and remainder are, respectively, -254 and 2.

This is, again, how it works in general. The new quotient is the negative of the old one, and the new remainder equal to the old one.

(3) *Division of* -3812 *by* -15*:* We, yet again, perform the long division of the positive numbers [as done above]. We then get [borrowing from the quotient again]:

$$-3812 = (-15) \cdot (254 + 1) + (15 - 2),$$

i.e.,

$$-3812 = (-15) \cdot 255 + 13,$$

and so the new quotient and remainder are, respectively, 255 and 13.

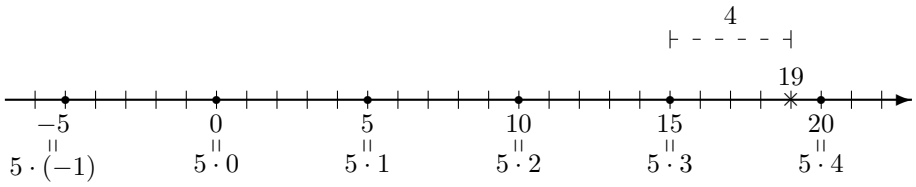
This is how it works in general. The new quotient is the old plus one, and the new remainder is the difference between the old divisor [which is 15 in the above example] and the old remainder.

[Note that we seldom try to divide by a negative number, but, as we have just seen, we can.]

In summary: if the quotient and remainder of m divided by n are, respectively, q and r, then:

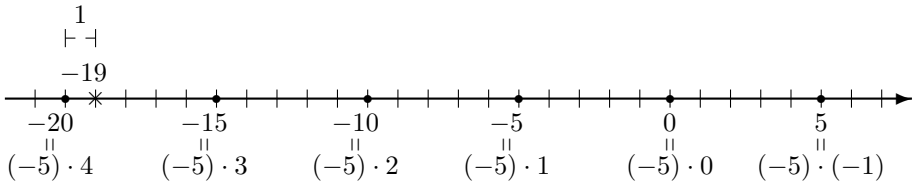
- the quotient and remainder of $-m$ divider by n [the most important case for us] are, respectively, $(-q-1)$ and $(n-r)$;
- the quotient and remainder of m divider by $-n$ are, respectively, $-q$ and r;
- the quotient and remainder of $-m$ divider by $-n$ are, respectively, $(q+1)$ and $(n-r)$.

One can also look at long division with a geometric point of view. For simplicity, I will use smaller and easier numbers. Say I want to divide 19 by 5. We mark all multiples of 5 [the divisor] in the real line [marked with circles in the picture below]. Then, we also mark 19 [the dividend] in the real line [marked with an "×" in the picture below].



Now, we look for the multiple of 5 that comes just *before* [to the left of] the dividend. In this case, the number just before 19 is $15 = 5 \cdot 3$. Then, 3 [taken from the "$5 \cdot 3$"] is the quotient, and the distance from this multiple of 5 on the left of 19 is the remainder. So, the quotient is 3 and the remainder is 4. Indeed, $19 = 5 \cdot 3 + 4$, as one can see from the picture.

It also works for negatives. Say I want to divide -19 by -5. We proceed in the exact same manner:



The multiple of -5 on the left of -19 is $-20 = (-5) \cdot 4$, and the distance to -19 is 1. Hence, the quotient is 4 and the remainder is 1, i.e., $-19 = -5 \cdot 4 + 1$.

Finally, you can also use a simple calculator to perform long division. [Calculators perform division *with decimals*.] To find the quotient and remainder of the division of m by n, here is what you do:

(1) Divide m by n in your calculator.
(2) You get a result which might not be an integer, i.e., it can have decimals. Discard the decimals [if you have any], and that is your quotient, say q.
(3) To find the remainder, we subtract $m - nq$ in your calculator.

Example 2.5. Here is an example: say you want find the quotient q and remainder r of 36459 when divided by 764. When you compute 36459/764, [with your calculator] you get 47.7212041884817. So, your quotient is $q = 47$. Now we compute $764 \cdot 47$, which is 35908, and subtract that from 36459, i.e., the remainder is $r = 36459 - 35908 = 551$.

We finish this section with some more terminology:

Definition 2.6. (1) Given two integers m and n, we define m *modulo* n [sometimes said "m *mod* n"] to be the remainder of the division of m by n. [So, as seen in the example above, 3812 modulo 15 is 2. Most scientific calculators have a "MOD" button for this operation.]

(2) We say that m divides n if n modulo m is zero, i.e., the long division has remainder zero, which is then called an *exact division*. [So, we have that $n = m \cdot q$, for some integer q.] In that case, we say that m is a *divisor* of n, or that n is a *multiple* of m.

(3) We write $n \mid m$ to say that "n divides m", and $n \nmid m$ to say that "n does not divide m". [So, for instance, we have $2 \mid 14$, but $2 \nmid 13$.]

Be careful: the symbol "|" is not the same as "/". We have that $n \mid m$ means "n *divides* m", while n/m means "n *divided* by m".

(4) An integer is called *even* if it is divisible by 2. [Hence, even numbers are those of the form $n = 2q$, where q is an integer.] They are $\{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \ldots\}$.

(5) An integer is called *odd* if it is *not* divisible by 2. [Hence, even numbers are those of the form $n = 2q + 1$, where q is an integer.] They are $\{\pm 1, \pm 3, \pm 5, \pm 7, \ldots\}$.

Problems.

2.1) Use long division to find the quotient and remainder of the following divisions:

(a) 431 divided by 7.

(b) 1263 divided by 349.

(c) 364 divided by 365.

(d) 7388 divided by 12.

2.2) In the following long divisions, identify the divisor, dividend, quotient, and remainder:

(a)
$$\begin{array}{r} 147 \\ 31\overline{)\,4567} \\ \underline{3100} \\ 1467 \\ \underline{1240} \\ 227 \\ \underline{217} \\ 10 \end{array}$$

(b) $423 = 42 \cdot 10 + 3$.

(c) $423 = 21 \cdot 20 + 3$.

2.3) Use the geometric method to find the quotient and remainder of the following:
(a) 11 divided by 3.
(b) -5 divided by 4.

2.4) Use a hand calculator to find the quotient and remainder of 64378723 when divided by 273.

3. A Useful Theorem and Some Semantics

We will soon state a *theorem*. It might be useful to say a few words on what a theorem is. A theorem is a statement [or proposition] whose validity can be deduced from its assumptions by logical steps. So, it is something that you can *deduce* [the key word here] from other facts. On the other hand, in mathematics often there is a *hierarchy* for theorems:

- The term *Theorem* is reserved for statements that have greater importance. You probably know a few: Pythagoras' Theorem, Fundamental Theorem of Arithmetic, Thale's Theorem, etc.
- When a theorem is useful to us, but is of limited universal importance, the term *Proposition* is used. It is basically a "minor theorem".
- A *Lemma* is a theorem whose main purpose is to help prove one or more statements [which can be either full Theorems or mere Propositions].
- Finally, a *Corollary* is a result, which can be of some relative importance, but is an immediate [or almost immediate] consequence of a previous Theorem or Proposition.

Note that we must always have a Proposition or Theorem, and never a Corollary, following a Lemma. In the same way, a Corollary always comes after a Proposition or a Theorem, but never after a Lemma.

So, here is a simple but useful theorem:

Theorem 3.1. *Let a, b, and d be integers, and suppose that $d \mid a$. Then d divides $(a+b)$ [and $(a-b)$] if, and only if, d divides b.*

[This might be too simple of a result to have the status of theorem. But, as you will see, we will derive many results from it, and so it has great importance to this text.]

First, we should say a few words about the "*if, and only if*" often used in mathematics: the above statement means that [with the assumption that $d \mid a$] if d divides b, then d must also divide $(a+b)$, *and*, conversely, if d divides $(a+b)$, then d must also divide b. Another way, equivalent to this one, to read this statement is: if $d \mid b$ [still assuming that $d \mid a$], then $d \mid (a+b)$, and if $d \nmid b$, then $d \nmid (a+b)$.

The language in math has to be very precise, and sometimes, in everyday conversation, we are not as careful. Here is an example. If someone says "if you don't eat your meat, [then] you cannot

have any pudding" [how can you have any pudding if you don't eat your meat?], often one assumes that this means that if you *do* eat your meat, you *will* be able to have pudding. [Wrong! Do it again!] But, in fact, it means only that you will not have pudding if you don't eat your meat, and it doesn't say absolutely *anything* about what happens if you do eat your meat! If the person saying "if don't eat your meat, [then] you cannot have any pudding" really means that you also *do* get to eat pudding if you eat your meat, then he/she should have said "you can have pudding if, and only if, you eat your meat".

Observe that if one says "you can have pudding if, and only if, you eat your meat", then, as in the interpretation of the statement of Theorem 3.1, this means that if you eat your meat, you get to eat the pudding. [This is the "if part" of the "if, and only if" statement above: you can eat pudding if you eat your meat]. So, eating your meat is a *sufficient* condition for you to eat your pudding [i.e., nothing else is needed]. It also means that you cannot eat pudding if you don't eat your meat. [This is the "only if part" of the "if, and only if": you can have pudding only if you eat your meat]. So, eating your meat is a *necessary* condition to eat pudding. [You cannot eat pudding if you don't eat your meat.] So, an equivalent statement to "you can have pudding if, and only if, you eat your meat" is "a *necessary and sufficient condition* for you to be allowed to eat pudding is that you eat your meat".

These "if, and only if" statements [or "necessary and sufficient conditions"] appear quite often in mathematics, and it is *crucial* that you have a perfect understanding of its meaning! In the same way, remember to not assume too much: "if" [by itself] does not mean the same as "if, and only if".

Also, a mathematician is a skeptic by nature. Although in high-school, and very often in college too, one accepts the validity of theorems on faith, we should try to see why they actually hold. A mathematician always want to see a *proof*, that is, a precise argument which leaves no doubt about the veracity of the theorem. We shall soon see a proof of the theorem above. Before that, let's check if the theorem works with a concrete example.

Example 3.2. Let $a = 10$, $b = 7$ and $d = 5$. So, these numbers satisfy the conditions asked by the theorem, namely, these numbers are all integers, and $5 \mid 10$ [corresponding to $d \mid a$]. Then, since all these are satisfied, the theorem says that, since $5 \nmid 7$, we have that $5 \nmid (10 + 7)$ [which is clearly true in this case]. Now, if we change b from 7 to 15, then we have that $5 \mid 15$, and the theorem then says that $5 \mid (10 + 15)$ [which is also clearly true in this case, since $25 = 5 \cdot 5$]. [Note that the differences also work, since $5 \nmid (10 - 7)$ and $5 \mid (10 - 15)$, since $-5 = 5 \cdot (-1)$].

Note that the above *is not a proof*! This is *a particular case* only, which shows that the theorem works when $a = 10$, b is either 7 or 15, and $d = 5$. This might be enough to convince you, but it doesn't really show that it works in general, or even for another case, like, say, $d = 63827382$, $a = 14935607388$, and $b = 487374833$. [Note that $a = 234 \cdot d$].

So, we now see an actual proof:

Proof of Theorem 3.1. Since $d \mid a$, we have that $a = dq$ [i.e., the remainder is zero]. Now, divide b by d, so that $b = dq' + r'$ with $0 \leq r < |d|$. [Here I am using the absolute value "| |", since d could be negative. But, if you want to think of only positive d, you can drop it.] So q' and r' are, respectively, the quotient and remainder of the division of b by d.

Then, we have that $a + b = (dq) + (dq' + r') = d(q + q') + r'$. So,

$$(a + b) = d(q + q') + r', \quad \text{with } 0 \leq r' < |d|\,,$$

and thus, by the uniqueness of the division algorithm [as in Example 2.3], the remainder of $(a + b)$, when divided by d is r', i.e., it is the same as the remainder of the division of b by d.

Now remembering the the division is exact if, and only if, the remainder is zero, we have that, if $d \mid (a + b)$, then $r' = 0$ and so $d \mid b$ [since r' is the remainder of the division of b by d]. Conversely, if $d \mid b$, then $r' = 0$, which means that $d \mid (a + b)$ [since r' is also the remainder of the division of $(a + b)$ by d].

The proof for $a - b$ is left as an exercise. □

[Note that we use the symbol "□" to mark the end of a proof. Sometimes the letters "QED" are also used. They stand for *"quod erat demonstrandum"*, which is Latin for "that which was to be demonstrated".]

It takes some time to get used to reading proofs. It takes even more time to get used to *writing* some yourself, but it is a *very* important part of mathematics. [Proofs are also quite important to computer scientists, especially those interested in *artificial intelligence*, and to philosophers! Also, many law schools like to admit math majors precisely because of their skills with proofs, which are basically *ironclad arguments*, which are crucial to [good] lawyers.] I recommend you work on this proof until you fully understand it. [Things should "click", it should make "perfect sense", you should slap your forehead and say "of course!"...]

To help you understand, here is the proof being worked out with specific numbers: let, again, $a = 10$, $b = 7$, and $d = 5$. Let's follow the steps of the proof above. The long divisions by 5 give us $10 = 5 \cdot 2$ and $7 = 5 \cdot 1 + 2$. Then,

$$\begin{aligned} 17 &= 10 + 7 \\ &= (5 \cdot 2) + (5 \cdot 1 + 2) \\ &= (5 \cdot 2 + 5 \cdot 1) + 2 \\ &= 5 \cdot (2 + 1) + 2 \\ &= 5 \cdot 3 + 2. \end{aligned}$$

So, $17 = 5 \cdot 3 + 2$ [which we could have done directly, instead of following the proof, but the point is exactly to see the proof "in action"] and so, as in the proof, we see that the remainders of $(a+b) = 17$

and of $b = 7$ when divided by $d = 5$ are the same, in this case, both are 2. So, since this remainder is not zero, neither is divisible by $d = 5$.

If we, again, replace $b = 7$ by $b = 15$, we can see it all working again:

$$\begin{aligned} 25 &= 10 + 15 \\ &= (5 \cdot 2) + (5 \cdot 3) \\ &= 5 \cdot (2 + 3) \\ &= 5 \cdot 5. \end{aligned}$$

So, $25 = 5 \cdot 5$, and hence the remainder of 25 and 15 when divided by 5 are equal, and in this case 0, meaning that both 15 and $10 + 15$ are divisible by 5.

Finally, we have to be careful when applying a theorem. Look at this example: let $a = 3$, $b = 7$, and $d = 5$. Again $d \nmid b$ [since $5 \nmid 7$], and so it might *seem* that the theorem tells us that $d \nmid (a + b)$, but $5 \mid (3 + 7)$! So, what is wrong here? The problem is that for us to indeed be able to use the theorem, the conditions asked by the theorem *must* be satisfied. In this case, we need a, b, and d to be integers [which is true, since 3, 7, and 5 *are* integers] and we need $d \mid a$, which is *not* true here, since $5 \nmid 3$. So, we cannot apply the theorem to this case! Hence, before applying a theorem, make sure to check that all conditions are satisfied.

Before we end this section, let's state and prove another basic fact about divisibility:

Proposition 3.3. *Let a, b, and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. We have that $a \mid b$ means that $b = a \cdot q_1$ for some integer q_1, and $b \mid c$ means that $c = b \cdot q_2$ for some integer q_2. Combining these two equations, we have that $c = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$, and hence $a \mid c$. □

Problems.

3.1) Find if it is true or false [without computing!]:

(a) $3 \mid (3 \cdot 3262 + 2)$

(b) $7 \mid (14 \cdot 407 - 21)$

3.2) Suppose that $a, b, c, d \in \mathbb{Z}$, and that $d \mid a$, $d \mid b$, and $d \mid c$. Does d divide $a + b + c$? Try to justify your answer.

3.3) Suppose the following statement is true:

If the forecast says it will rain tomorrow, then it will rain tomorrow.

[I know this statement is not true in general. But, for the sake of this problem, let's believe it.] Assume further that the forecast either say "it will rain tomorrow" or "it will not rain tomorrow". [So, they don't talk about "chance of rain".]

(a) Suppose that it did not rain today. Can you tell if the forecast of yesterday said if it would rain or not?

(b) Suppose that it did rain today. Can you tell if the forecast of yesterday said if it would rain or not?

(c) Suppose that the forecast said that it will not rain tomorrow? Can we be sure whether or not it will rain tomorrow?

3.4) Prove the subtraction case of Theorem 3.1, i.e., suppose that $d \mid a$ and prove that then d divides $(a-b)$ if, and only if, d divides b. [**Hint:** Try to copy the steps of the proof we gave for the sum.]

4. Simple Divisibility Criteria

Here are a few divisibility criteria with which you might be familiar:

(1) A number is divisible by 2 [i.e., it is even] if, and only if, the last digit is even, i.e., the last digit is among 0, 2, 4, 6, and 8. **Example:** 87459734659374597534 is even since it ends in 4, and 3456329657454832901 is odd, since it ends in 1.

(2) A number is divisible by 3 if, and only if, the sum of its digits is divisible by 3. **Example:** 942 is divisible by 3, since $9+4+2=15$ is divisible by 3, and 725 is not divisible by 3 since $7+2+5=14$ is not divisible by 3. Note that if the number is too large, we can repeat the process until we get a number small enough to be easily decided if it is divisible by 3. For instance: 989797798979897988 is divisible by 3 if, and only if, $9+8+9+7+9+7+7+9+8+9+7+9+8+9+7+9+8+8=147$ is divisible by 3. To find out if 147 is divisible by 3, we add the digits again, getting $1+4+7=12$, and hence 989797798979897988 is divisible by 3. In fact, a slick application of Theorem 3.1 simplifies things even more: you don't have to add the digits 0 [of course!], 3, 6 or 9 of the number. So, to find if 989797798979897988 is divisible by 3, we just need to check that $8+7+7+7+8+7+8+7+8+8=75$ [so, I omitted all 9's in this sum] is divisible by 3. But since $7+5=12$, it indeed is [as we already knew].

(3) A number is divisible by 5 if, and only if, the last digit is either 5 or 0. **Example:** 8438746387835 is divisible by 5, since the last digit is 5, while 658374834873 is not, since the last digit is neither 0 nor 5.

(4) A number is divisible by 6 if, and only if, it is divisible by *both* 2 and 3. [This needs a little proof, but due to lack of time, we will skip it. The key factor here is that 2 and 3 are *relatively prime*, as defined in Definition 6.11!] So, we use the criteria for 2 and 3 above. **Example:** 443728198343 is not divisible by 6, since it is not divisible by 2 [since it ends with 3, an odd number]. 4378823782 is not divisible by 6, since it is not divisible by 3, as

$4+7+8+8+2+7+8+2=46$ [note we can skip the 3's] is not divisible by 3. On, the other hand, 93474628104 is divisible by 6, as it is divisible by 2 [since it ends in 4, an even number], and 3 [as $4+7+4+2+8+1+4=30$ is divisible by 3].

(5) A number is divisible by 9 if, and only if, the sum of its digits is divisible by 9. [Similar to the case of divisibility by 3.] **Example:** 342 is divisible by 9, since $3+4+2=9$ is divisible by 9, and 725 is not divisible by 9 since $7+2+5=14$ is not divisible by 9. Just as with 3, you can also repeat the process for large numbers.

(6) A number is divisible by 10 if, and only if, the last digit is zero. **Example:** 48383748320 is divisible by 10, but 9674629433425 is not.

If we let our mathematician's nature take over [and we should!], we will be compelled to find out *why* these criteria work. The truth is that they follow from our Theorem 3.1. But, I will fight my own instincts here and, instead of giving a formal proof, I will just give you a couple of examples that contain the heart of the proofs. These should be enough to convince you and give you an idea of how the actual proof goes.

Let's look at the case of divisibility by 2: consider the number $758x$, where x is the last digit [and so it's a number between 0 and 9]. We can write it then as $758x = 758 \cdot 10 + x$ [for instance, $7584 = 758 \cdot 10 + 4$]. So, we can write: $758x = 758 \cdot 5 \cdot 2 + x$. Then, clearly 2 divides $758 \cdot 5 \cdot 2$, and by Theorem 3.1 [with $a = 758 \cdot 5 \cdot 2 = 7580$, $b = x$, and $d = 2$] we have that 2 divides $758x$ if, and only if, $2 \mid x$ [as stated in the criterion]. The cases of divisibility by 5 and 10 are almost the same, since 5 and 10 also divide $758 \cdot 2 \cdot 5 = 758 \cdot 10$.

The case of 3 and 9 are also similar. Let's look at the number 8215. We can write it as $8215 = 8 \cdot 1000 + 2 \cdot 100 + 2 \cdot 10 + 5$. Now, here comes the trick: rewrite it again as $8215 = 8 \cdot (999+1) + 2 \cdot (99+1) + 1 \cdot (9+1) + 5$, and distribute and rearrange it to $8215 = (8 \cdot 999 + 2 \cdot 99 + 1 \cdot 9) + (8+2+1+5) = 3 \cdot (8 \cdot 333 + 2 \cdot 33 + 1 \cdot 3) + (8+2+1+5)$. So, $8215 = 3 \cdot (8 \cdot 333 + 2 \cdot 33 + 1 \cdot 3) + (8+2+1+5)$, and again by Theorem 3.1, since $3 \mid 3 \cdot (8 \cdot 333 + 2 \cdot 33 + 1 \cdot 3)$, we have that 3 divides 8215 if, and only if, it divides $8+2+1+5$, which is precisely the sum of the digits of 8215 [as stated in the criterion].

The case, of 9 is very similar. Just observe that $8215 = (8 \cdot 999 + 2 \cdot 99 + 1 \cdot 9) + (8+2+1+5) = 9 \cdot (8 \cdot 111 + 2 \cdot 11 + 1 \cdot 1) + (8+2+1+5)$, and use Theorem 3.1 again.

Problems.

4.1) Check if each of the numbers below are divisible by 2, 3, 5, 6, 9, and 10:

(a) 11470260960

(b) 2531680491

(c) 11843893499

(d) 360900365

4.2) Decide, without adding the numbers, if the statements are true or false:

(a) $3 \mid (3 \cdot 7483837283 + 94957291)$

(b) $5 \mid (743872835 + 90472638231)$

4.3) Can you guess a criterion for divisibility by 15?

5. GCD and LCM

We now review the concepts of *greatest common divisor*, which we shall abbreviate by *GCD*, and *least common multiple*, which we shall abbreviate by *LCM*. The names already tell us what they mean: the GCD of two integers a and b is the largest integer that divides a and b [at the same time], and the LCM is the smallest *positive* integer that is a multiple of a and of b [at the same time]. We shall denote them $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ respectively. Note that for all positive integers a and b, we have that $\gcd(a, b) \geq 1$ and $\operatorname{lcm}(a, b) \leq ab$. Moreover, since a divisor of a number is always *less than or equal to* the number itself, and a multiple of a number is always *greater than or equal to* the number itself, we can also conclude that $\gcd(a, b) \leq \min(a, b)$ [where $\min(a, b)$ is the *minimum* between a and b] and $\operatorname{lcm}(a, b) \geq \max(a, b)$ [where $\max(a, b)$ is the *maximum* between a and b]. In summary:

$$1 \leq \gcd(a, b) \leq \min(a, b) \qquad \text{and} \qquad \max(a, b) \leq \operatorname{lcm}(a, b) \leq ab.$$

Here are a few examples:

a	b	$\gcd(a, b)$	$\operatorname{lcm}(a, b)$
5	7	1	35
6	12	6	12
18	27	9	54
364	53	1	1908
12	144	12	144
270	924	6	41580

So, how does one compute the GCD and LCM? We will see soon a simple way using factorization of prime numbers, which is fine for small numbers, but not efficient enough for large numbers. One better way, at least to compute the GCD, is to use a succession of long divisions. This method is called the *Euclidean Algorithm*, since it had already appeared in Euclid's celebrated series of books *Elements* more than 2000 years ago. [The *Elements* is the book with the second largest number of editions published of all time, the Bible being the first. It was still used in schools in Europe as a text book in the recent past. The American publisher Dover still has it on print in the United States. The Elements collects most of the mathematical knowledge of its time [around 300 BC]. Note then that Euclid [the author] *collected* all the work, he did not, necessarily, do it all himself.] If you are unfamiliar with the word *algorithm*, it basically means a method that completely solves a [usually computational] problem.

So, let me show you how the *Euclidean Algorithm* works by showing it in action.

Example 5.1. Say we want to compute the GCD of 134 and 52. We first divide 134 by 52, obtaining:

$$134 = 52 \cdot 2 + 30$$

[i.e., quotient 2 and remainder 30.] Then, we take the dividend [i.e., 52] and divide it by the remainder [i.e., 30]:

$$52 = 30 \cdot 1 + 22.$$

And we repeat: take the new dividend [i.e., 30] and divide it by the new remainder [i.e., 22]:

$$30 = 22 \cdot 1 + 8.$$

And we repeat yet again:

$$22 = 8 \cdot 2 + 6.$$

And again:

$$8 = 6 \cdot 1 + 2.$$

If we repeat now, we get an exact division:

$$6 = 2 \cdot 3.$$

This means that the algorithm is over and the GCD of 2732 and 134 is the last non-zero remainder, i.e., 2. Here is the whole process:

$$\begin{aligned} 134 &= 52 \cdot 2 + 30 \\ 52 &= 30 \cdot 1 + 22 \\ 30 &= 22 \cdot 1 + 8 \\ 22 &= 8 \cdot 2 + 6 \\ 8 &= 6 \cdot 1 + \boxed{2} \longrightarrow \text{GCD} \\ 6 &= 2 \cdot 3 \end{aligned}$$

The general case is exactly the same. If you want to find $\gcd(a, b)$, where a and b are positive integers, you perform a series of long divisions:

$$\begin{aligned}
a &= b \cdot q_1 + r_1 \\
b &= r_1 \cdot q_2 + r_2 \\
r_1 &= r_2 \cdot q_3 + r_3 \\
r_2 &= r_3 \cdot q_4 + r_4 \\
&\vdots \\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} \cdot q_n + \boxed{r_n} \longrightarrow \text{GCD} \\
r_{n-1} &= r_n \cdot q_{n+1} \quad \text{[exact division]}
\end{aligned}$$

[So, basically you divide the previous dividend by the previous remainder, until we get a zero remainder. The last non-zero remainder is the GCD. But be careful to always take the *dividend* of the division *not the quotient*!] This process might seem long and tedious, but computers can perform it very quickly, and it's quite efficient.

One question that you may ask is if we indeed *always* get to the point where we get an exact division. If you think about it for a second, you will see that we must, since the remainders keep decreasing [since they are remainders, we have $b > r_1 > r_2 > \cdots$] and they are *positive integers*, at one point we must get to zero.

Another question, which is a bit harder to answer, is why this procedure indeed gives us the GCD. What is really behind this is Theorem 3.1. Let d denote the GCD of a and b. Then, of course, $d \mid a$ and $d \mid b$. If long division gives us $a = bq_1 + r_1$, clearly also $d \mid (b \cdot q_1)$ [in fact, d divides any multiple of b]. Since $r_1 = a - bq_1$, Theorem 3.1 gives us that $d \mid r_1$. In the same way, if $b = r_1q_2 + r_2$, we have that $r_2 = b - r_1q_2$. We have established that d divides b and r_1, and by Theorem 3.1 again, we have that d divides r_2. And, in the same way, d must divide r_3, r_4, etc., until r_n.

Now, going backwards, r_n divides r_{n-1} [from the last [exact] division]. Hence, r_n divides $r_{n-2} = r_{n-1} \cdot q_n + r_n$, yet again by Theorem 3.1. So, since r_n divides r_{n-1} and r_{n-2}, and we have $r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$, we have that r_n also divides r_{n-3}. Proceeding this way, we get finally that r_n divides a and b. So, r_n is a common divisor of a and b. Since d [remember $d = \gcd(a, b)$] divides r_n [as seen in the previous paragraph], we have that $r_n \geq d$. But since d is the *greatest* common divisor of a and b [and r_n is a common divisor of a and b], we have that $r_n \leq d$. Therefore, the only possibility is that $d = r_n$, i.e., the last non-zero remainder is indeed the GCD.

How about the LCM? How does one compute it efficiently? As with the GCD, factorization into primes works well for small numbers, or numbers that can be factored easily. But, if not, one can use the fact that

$$\operatorname{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}.$$

The proof of this will come in Section 7, but assuming for the moment that this formula holds, we can compute the LCM by first computing the GCD using the *Euclidean Algorithm* [which is fast!], and then divide the product of the numbers by this GCD. This is also a very efficient way of doing it.

One final note on the case of GCD and LCM of integers which might be negative: the signs do not matter. In other words, we have that

$$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$$

and

$$\operatorname{lcm}(a,b) = \operatorname{lcm}(-a,b) = \operatorname{lcm}(a,-b) = \operatorname{lcm}(-a,-b).$$

This is easy to see, as the divisors of a number and its negative are the same.

Problems.

5.1) Use the *Euclidean Algorithm* to compute the GCD of the following numbers:

(a) 300 and 222

(b) 1234 and 4321

5.2) Compute the LCM of 300 and 222.

6. The Extended Euclidean Algorithm

The computations performed in the *Euclidean Algorithm* can be used to prove the following result:

Theorem 6.1 (Bezout's Theorem or the Extended Euclidean Algorithm)**.** *Let a and b be integers, and $d = \gcd(a,b)$. Then, there are $x, y \in \mathbb{Z}$ such that $ax + by = d$.*

This Theorem is sometimes called [at least in France] *Bezout's Theorem*, but I haven't seen it referred to this way in America, so I will avoid calling it that, and refer to it simply as the *Extended Euclidean Algorithm*, or *EEA*. [Also, there is already another theorem in algebraic geometry often referred to as *Bezout's Theorem*.]

Let's illustrate the theorem with some examples:

$$\begin{aligned}
\gcd(5,7) = 1 \quad &\text{and} \quad 5\cdot(-4) + 7\cdot 3 = 1,\\
\gcd(6,12) = 6 \quad &\text{and} \quad 6\cdot 1 + 12\cdot 0 = 6,\\
\gcd(18,27) = 9 \quad &\text{and} \quad 18\cdot(-1) + 27\cdot 1 = 9,\\
\gcd(364,53) = 1 \quad &\text{and} \quad 364\cdot 15 + 53\cdot(-103) = 1,\\
\gcd(270,924) = 6 \quad &\text{and} \quad 270\cdot(-65) + 924\cdot 19 = 6.
\end{aligned}$$

Before we discuss the idea of the proof, let me make one observation: this is a "if" statement only, not an "if, and only if", which means that even though $5\cdot(-8) + 7\cdot 6 = 2$, the GCD of 5 and 7 is 1 [as seen above], not 2. So, be careful!

As mentioned before, the proof comes from the *Euclidean Algorithm*, and in fact gives the way to actually compute x and y [as in the statement].

Example 6.2. Let's use our example of the *Euclidean Algorithm* for 134 and 52 to illustrate the idea. The actual proof will be omitted, but hopefully one will be able to see that the idea works in general just from this particular example.

Remember we had:

$$\begin{aligned}
134 &= 52\cdot 2 + 30\\
52 &= 30\cdot 1 + 22\\
30 &= 22\cdot 1 + 8\\
22 &= 8\cdot 2 + 6\\
8 &= 6\cdot 1 + \boxed{2} \longrightarrow \text{GCD}\\
6 &= 2\cdot 3
\end{aligned}$$

The idea is to write each remainder of the successive long divisions of the algorithm as a sum of products of 134 and 52. So, the first long division gives us $134 = 52\cdot 2 + 30$. We solve for 30, obtaining:

$$30 = 134 + 52\cdot(-2). \tag{6.3}$$

[Note that we *never* multiply out the 134's and 52's.] Now, we solve the second equation for the remainder again [22 in this case], and then replace 30 by what we've got in the previous step [i.e.,

equation (6.3)]:

$$\begin{aligned} 22 &= 52 - 30 \cdot 1 \\ &= 52 - (134 + 52 \cdot (-2)) \\ &= 134 \cdot (-1) + 52 \cdot 3. \end{aligned}$$

So, we have:

$$22 = 134 \cdot (-1) + 52 \cdot 3. \tag{6.4}$$

Now, we again solve for the next remainder [i.e. 8], and now replace 22 by what we just found [i.e., equation (6.4)] and 30 again by what we've got in equation (6.3):

$$\begin{aligned} 8 &= 30 - 22 \\ &= (134 + 52 \cdot (-2)) - (134 \cdot (-1) + 52 \cdot 3) \\ &= 134 \cdot 2 + 52 \cdot (-5). \end{aligned}$$

So,

$$8 = 134 \cdot 2 + 52 \cdot (-5) \tag{6.5}$$

Proceeding as before [using equations (6.4) and (6.5)] we get

$$\begin{aligned} 6 &= 22 - 8 \cdot 2 \\ &= (-134 + 52 \cdot 3) - (134 \cdot 2 - 52 \cdot 5) \cdot 2 \\ &= 134 \cdot (-5) + 52 \cdot 13, \end{aligned}$$

i.e.,

$$6 = 134 \cdot (-5) + 52 \cdot 13, \tag{6.6}$$

and finally, with the next equation [using equations (6.5) and (6.6)], we get

$$\begin{aligned} 2 &= 8 - 6 \\ &= (134 \cdot 2 + 52 \cdot (-5)) - (134 \cdot (-5) + 52 \cdot 13) \\ &= 7 \cdot 134 + 52 \cdot (-18), \end{aligned}$$

giving us what we were looking for:

$$2 = 7 \cdot 134 + 52 \cdot (-18).$$

[since $\gcd(134, 52) = 2$].

The EEA gives us many nice results. We will now show a few of its applications.

Corollary 6.7. *Let a and b be integers. Then, $\gcd(a, b) = 1$ if, and only if, there are integers x and y such that $ax + by = 1$.*

We had just noted that the EEA is not an "if, and only if" statement, but the corollary above tells us that it is *when the GCD is* 1 [and *only* then]. So, if we have, for instance,

$$432 \cdot 84 + 131 \cdot (-277) = 1,$$

we know that $\gcd(432, 131) = 1$.

Proof of Corollary 6.7. If $\gcd(a, b) = 1$, then the EEA already gives us the existence of x and y as in the statement.

Now, suppose that there are x and y such that $ax + by = 1$. [We must show that $\gcd(a, b) = 1$.] Suppose that d is positive integer that divides a and b. Then, it clearly divides ax and by also. Then, by Theorem 3.1, we have that $d \mid (ax + by) = 1$. Since the only positive divisor of 1 is 1 itself, we have that the only possibility for d is 1. Hence, the GCD of a and b is 1 [as it is the *only* common divisor]. □

Here is another corollary:

Corollary 6.8. *If a and b are integers and $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$. [Note that a/d and b/d are integers!]*

Proof. By the EEA, there are integers x and y such that

$$ax + by = d.$$

Dividing this equation by d, we have:

$$\left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y = 1.$$

Hence, by Corollary 6.7, we have that $\gcd(a/d, b/d) = 1$. □

Here is yet another consequence of the EEA:

Proposition 6.9. *Let a and b be positive integers and $d = \gcd(a, b)$. If n divides a and b, then n divides d.*

Proof. By EEA, we can write $ax + by = d$, for some integers x and y. Then, since n divides a and b, it divides ax and by, and hence it divides $d = ax + by$. □

One last observation about GCD is that we can naturally define it for any number of integers [rather than just a pair]. For instance, $\gcd(a, b, c)$ is just the largest common divisor of all three integers a, b, and c. Now, how do we compute this GCD? We first compute the GCD of a and b, say $d_1 = \gcd(a, b)$, and then we compute $\gcd(d_1, c)$. That is the GCD of a, b, and c. So, in summary, we have

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c).$$

Indeed, let's denote by d the $\gcd(a, b, c)$, by d_1 the $\gcd(a, b)$, and by e the $\gcd(d_1, c)$. [We want to show that $e = d$.] Since d divides a, b [and c], by Proposition 6.9, we have that $d \mid d_1$. Since d also divides c, we have that d is a common divisor of d_1 and c, and hence $d \leq e$ [as e is the *greatest* common divisor of d_1 and c].

Now, since $e \mid d_1$ and $d_1 \mid a$, by Proposition 3.3, we have that e must also divide a. In the same way, e must also divide b. Therefore e is a common divisor of a, b, and c, and hence $e \leq d$ [as d is the *greatest* common divisor of a and b].

Thus, since we have just seen that $d \leq e$ and $e \leq d$, the only possibility is that $e = d$, i.e., $\gcd(\gcd(a, b), c) = \gcd(a, b, c)$.

This generalizes in the following way:

Proposition 6.10. *Let $a_1, a_2, \ldots, a_n$ be integers. Then,*

$$\gcd(a_1, a_2, \ldots, a_n) = \gcd(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n).$$

Finally, here is some more terminology:

Definition 6.11. If a and b are integers such that $\gcd(a, b) = 1$, then we say that a and b are *relatively prime*. More generally, if $\gcd(a_1, a_2, \ldots, a_n) = 1$, we say that $a_1, a_2, \ldots, a_n$ are *relatively prime*.

Problems.

6.1) Use the EEA to find integers x and y such that:

(a) $17 \cdot x + 22 \cdot y = 1$;

(b) $300 \cdot x + 222 \cdot y = 6$. [**Hint:** You have already computed the GCD of 300 and 222 in the previous section. If you still have the calculations, you can use it instead of repeating it all here.]

6.2) Compute the GCD of 81, 36 and 45.

7. Prime Numbers

Prime numbers are one of the most important concepts in mathematics, and one of the main interests of number theory. [More on both later.] Let's start by giving a precise definition:

Definition 7.1. A *positive* integer is called *prime* if it has *exactly* two positive divisors: 1 and the number itself. [Note that 1 is *not* prime, since it has only one divisor. But 2 is a prime.] Also, a positive integer that is not 1 nor prime is called *composite*.

A word, again, about semantics. If we had defined that a prime is a number with two positive divisors, without quantifying with the word "exactly", we would have that, for instance, $6 = 2 \cdot 3$ would also be prime, as it has indeed two divisors. [For instance, 2 and 3 are two divisors.] It has,

in fact, four positive divisors in total, namely 1, 2, 3, and 6, but if it has four, in particular it also has two. Again, we see the need of being precise, as sometimes in day-to-day conversations, the "exactly" might be left out when we actually mean it.

Here are all primes less than 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Note that, for instance, 32 is not prime, since 16 divides 32 [as $32 = 16 \cdot 2$].

Here is another defining property of prime numbers:

Theorem 7.2. *An integer $p > 1$ is prime if, and only if, whenever $p = a \cdot b$, with $a, b \in \mathbb{N}$, then either $a = 1$ [and $b = p$], or $b = 1$ [and $a = p$].*

So, for instance, since $43763 = 107 \cdot 409$, the theorem says that 43763 is not prime. On the other hand, if you look at 7, and $7 = a \cdot b$, we can see that the only way $a \cdot b = 7$ is if either $a = 1$ and $b = 7$, or $a = 7$ and $b = 1$.

The actual proof is easy enough to see it here.

Proof. Suppose that p is prime and $p = a \cdot b$. Then, both a and b are clearly divisors of p. Since p is prime, then the only divisors are 1 and p. Hence, a and b can be either 1 or p.

Now, suppose that p is not prime. Then, it has a divisor not equal to 1 and p, say a. Then, $p = ab$. Since $a \neq 1, p$, we have that $b \neq 1, p$. □

So, how does one check if a number is prime? How "difficult" is it? The answer depends on whether or not you are interested in *efficiency*. It is quite easy to find if small numbers are prime. [We shall see a way below.] But, even with modern computers, deciding whether or not a number is prime can be *very* difficult [i.e., it can take a long, *long* time.] These days, the most powerful supercomputer in the world [in Oak Ridge??] would take many years to verify that a prime number with a few million digits is in fact prime. [If you are too naive in *how* you program this computer to do it, it would take millions and millions of years!] Of course, sometimes even with millions, or even billions of digits, it can be easy. For instance, if the last digit is even, it is not prime [as it is divisible by 2].

The most natural way to determine if a number is prime is to test its divisors. If we find a divisor different from 1 and the number itself, then the number is not prime. Otherwise, it is.

Example 7.3. Let's check if 149 is prime. We check whether or not 2, 3, 4, 5, etc., divide 149. But, when do we stop trying? Of course, if we find a divisor different from 1 and 149 we immediately stop and conclude that 149 is not prime. What if we don't find a divisor? Of course, we don't need to check that any number above 149 divides it, since a divisor is always less than the number itself. Hence, the process is *finite*: you perform at most 149 divisions.

But, we can still improve it. It is not necessary to go all to way to 148! What happens if we get to 13 and we haven't found any divisor besides 1? Then, any divisor of 149 that is not 1 has to be larger then 13. If it is not prime, by Theorem 7.2, we have $149 = a \cdot b$, with a and b both greater than 1. Then, since both a and b are divisor of 149, they need to be greater than or equal to 13 [since we've

checked that no number smaller than 13 divides 149], we would have then, $149 = a \cdot b \geq 13 \cdot 13 = 169$. So, this would mean that $149 \geq 169$, which is absurd. So, this cannot happen, in other words, we cannot write 149 as a product of two numbers different from 1 and 149, and thus 149 must be prime [by Theorem 7.2 again]. [This is called a *proof by contradiction*: if we make an assumption that leads to a contradiction, i.e., something that cannot be true, then this assumption must be false.]

So, in general, when deciding if n is prime, we keep trying dividing by 2, 3, 4, etc., until either we find a divisor different from 1 and n [and the number is *not* prime], or until we reach the first number d for which $d^2 > n$. In this latter case, as with $n = 149$ and $d = 13$, we can conclude that n is prime.

Back to the case of 149, we would have to try to see if one of $2, 3, \ldots, 12$ is a divisor of 149. The criteria from the previous section gives us that 149 is not divisible by 2 nor 3. The next step is to see of it would be divisible by 4. But do we need to really check 4? Note that if $4 \mid n$, then $2 \mid n$ by Proposition 3.3. So, we don't have to try 4 [as we already know that $2 \nmid 149$], and in the same way, neither 6, nor 8, nor 10, nor 12, i.e., no multiples of 2. In the same way, we don't need to try multiples of 3 either, which excludes 6, 9, and 12. This leaves 5, 7, 11. For 5 we can check easily that $5 \nmid 149$, since the last digit is neither 5 nor 0. The other two we check by long division. We have that $149 = 7 \cdot 21 + 2$ and $149 = 11 \cdot 13 + 6$, so $7 \nmid 149$ and $11 \nmid 149$, and we can conclude the 149 is prime.

Note that in the end, the numbers by which we had to really try to divide 149 were 2, 3, 5, 7, and 11, all primes! In fact, Proposition 3.3 tells us that it suffices to check divisibility by other primes only, saving us some divisions. But note that this method has one catch: if the number you are checking is large, you might run out of known primes. For example, say you want to check if 10007 is prime. You try 2, 3, 5, 7, 11, 13, 17, and all of them fail to divide 10007. So, now you need to check the next prime after 17. You might not know whether or not 19 is prime. [Clearly 18 is not, since it is divisible by 2.] So, you might need to check if 19 is prime itself! Well, this is quick, and you can see that 19 is prime [since neither 2, nor 3 divide 19]. But then, comes the next odd number, namely 21, and you might need to check if it is prime again. Well, again, this is quick, but if your number is really large, it might turn out to be way too much work to keep doing this. In fact, at that point, it might be easier to just divide by the next odd number, even if you don't know if the number is prime, since this division might be quicker then checking primality.

So, finally, we give the general method:

General Method: To find if a positive integer $n > 1$ is prime, we successively try to divide by 2 and odd numbers $3, 5, 7, 9, 11, \ldots$, *in order*. If you know that an odd number is not prime, you may skip it. If you don't know whether or not the next odd number is prime, you can check if it seems it would be quicker than just dividing by it. This process continues until either:

- 2 or one of those odd numbers [or primes] divide n, in which case we can stop and conclude that n is *not* prime;

- or until try to divide by an odd number [or prime] whose square is greater than n, in which case we can stop and conclude that n *is* prime.

Here is one of the most basic, and yet important, properties of natural numbers, which shows the importance of primes.

Theorem 7.4 (Fundamental Theorem of Arithmetic)**.** *Any integer $n > 1$ can be written as a product*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k},$$

where $p_1, p_2, \ldots, p_k$ are all primes with $p_1 < p_2 < \cdots < p_k$, and $r_1, r_2, \ldots, r_k$ are positive integers. Moreover, this factorization is unique*, and it's called the* prime factorization *of n.*

Let's illustrate this important theorem with a few examples:

n	prime factorization
12	$2^2 \cdot 3$
71	71
105	$3 \cdot 5 \cdot 7$
144	$2^4 \cdot 3^2$
2513	$7 \cdot 359$
327112	$2^2 \cdot 31 \cdot 1319$
76434751	76434751

[Note that 71 and 76434751 are prime!]

The statement about uniqueness says that we cannot factor the same number as two different products of primes. We can change the order, like $12 = 2^2 \cdot 3 = 3 \cdot 2^2 = 2 \cdot 3 \cdot 2$, but nothing else. [But, since we asked in the statement that the primes are in increasing order, we exclude any possible change in the order of the primes, and hence have uniqueness.]

The *Fundamental Theorem of Arithmetic* shows us that prime numbers are the "building blocks" of all natural numbers. Since, natural numbers can be seen as the most basic elements of algebra, on which almost all else is built, prime numbers are then of great importance.

If you've seen the science fiction movie *"Contact"* [from 1997, based on a novel by the astronomer Carl Sagan, directed by R. Zemeckis, staring Jodie Foster], or read the book, aliens try to communicate with other life forms by sending pulses in prime numbers. The rational behind the author's idea is that any civilization who has any understanding of mathematics, a prerequisite for technology, must know of prime numbers. The important aspect here is that mathematics is *universal*. It is the same anywhere! To quote Galileo Galilei:

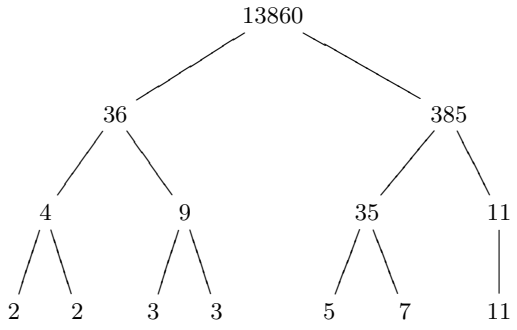
"Mathematics is the language with which God has written the universe."

A hypothetical technologically capable alien civilization might have discovered a different set of theorems than us, but the basics have to be the same, and prime numbers are at the very core of mathematics.

Back to the technical aspects, you might be asking how does one prove the *Fundamental Theorem of Arithmetic*. We will again avoid giving a formal proof, but give the general idea. First, one can observe that if $a = bc$, where a, b, and c are positive integers, with $b, c \neq 1$, then we have that b and c are both [strictly] less than a. [To be completely formal, we'd need to prove this statement. But let's just assume this to save some time.] Now, take a number n. If it is prime, then it has the trivial prime factorization $n = n$. If is not, by Theorem 7.2, we have that $n = ab$, with $a, b \neq 1$. Then, we look at a and b, and check if they are prime or not. If both are prime, then $n = ab$ is its prime factorization. Suppose that a is not prime. We repeat the argument for a: we can write it as $a = cd$. And we repeat with c and d if necessary. Since the numbers keep decreasing [we have $c < a < n$], this process must stop eventually, i.e., we must reach a prime number. We have to continue now with the other "branches".

Well, I admit that that was *sketchy* at best. So, let's look at a specific example.

Example 7.5. Let $n = 13860$. It is not prime, since, for instance, $13860 = 36 \cdot 385$. We now repeat for 36 and 385. Also, 36 is not prime, since $36 = 4 \cdot 9$, etc. Here is a picture of the process:



So, we finish a branch when we get a prime number. The above process then gives us $13860 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$.

I should observe here that I omitted the statement about uniqueness here. The proof of uniqueness relies on the following theorem, which also characterizes primes numbers:

Theorem 7.6. *If p is a prime integer and $p \mid (a \cdot b)$, then either $p \mid a$ or $p \mid b$.*

We need to make another observation on semantics here. In mathematics, unlike how we often do in our day-to-day, the term "or" is *non-exclusive*. So, in the theorem above, it *could* happen that p divides *both* a and b. [So, one possibility does not exclude the other.] If we wanted to exclude the

other, we would have to phrase it accordingly. For instance, we would say "if p is a prime integer and $p \mid (a \cdot b)$, then either $p \mid a$ and $p \nmid b$, or $p \mid b$ and $p \nmid a$".

Note also that the statement is clearly false if we don't ask for the primality of p. For instance, $6 \mid 2 \cdot 3$, but $6 \nmid 2$ and $6 \nmid 3$. It works for primes since they are "indivisible": if p is a part of $a \cdot b$, it must be itself either a part of a or a part of b, unlike 6, of which part goes with 2 and part goes with 3.

Proof of Theorem 7.6. If $p \mid a$, there is nothing to be done, as the statement is immediately true. So, assume that $p \nmid a$. Hence, since p is prime [i.e., 1 and p are the only divisors of p] and $p \nmid a$, we have that $\gcd(a, p) = 1$. By the EEA [i.e., Theorem 6.1], we have that there are $x, y \in \mathbb{Z}$ such that

$$ax + py = 1.$$

Multiplying by b we have that

$$(ab)x + p(yb) = b.$$

Now, since by assumption $p \mid ab$, we also have that $p \mid (ab)x$. Since clearly also $p \mid p(by)$, we have that $p \mid ((ab)x + p(by)) = b$.

So, if $p \nmid a$ [as we've assumed here], we must have that $p \mid b$. □

This theorem can be easily extended for a product with more terms, by repeating the same argument.

Corollary 7.7. *Let p be a prime. If $p \mid a_1 \cdot a_2 \cdots a_n$, then $p \mid a_i$ for some i in $\{1, 2, \ldots, n\}$.*

This helps us prove uniqueness in the following way: suppose that the number n has two factorizations into primes, say $n = p_1^{r_1} \cdots p_k^{r_k}$ and $n = q_1^{s_1} \cdots q_l^{s_l}$. Then clearly $p_1 \mid n$ [from the first factorization]. By Corollary 7.7, then p_1 divides some q_i. But since p_1 and q_i are primes, they must be equal. What we can do then is divide n by p_1, and repeat the argument. Eventually we get that each p_i is equal to a q_j and the factorizations are the same. [Again, for sake of time and simplicity, this is just a very rough sketch of the proof.]

The *Fundamental Theorem of Arithmetic* is quite useful, even though computationally speaking, it can be quite hard to use it, i.e., it might take a very long time to factor a very large integer. [As we shall see later, this difficulty in factorization is the heart of the *RSA cryptosystem*.]

So, how does one compute the prime factorization of a [small] number? Basically, you can just keep trying to divide it by all primes, as shown in the following example.

Example 7.8. Let's try to factor 504.

- We start with 2. We have that 2 divides 504, and we get $504 = 2 \cdot 252$. Now, we see if 2 divides 252. It does, and it gives $252 = 2 \cdot 126$. We now try to see if 2 divides 126. It, again, does, and we get $126 = 2 \cdot 63$. Now we would see if 2 divides 63, but it does not. [So, 2 divided 504 three times, giving us the factor 2^3.]

- So, we go to the next prime, namely 3. Does 3 divide 63? Yes, giving us $63 = 3 \cdot 21$. We now try to see if 3 divides 21. It does, and we get $21 = 3 \cdot 7$. Next, we try to see if 3 divides 7, and it does not. [So, 3 divides 504 twice, and hence we have a factor of 3^2.]
- Next we would check 5 [the next prime]. Clearly 5 does not divide 7, and hence 504 has no factor of 5.
- The next prime is 7 itself, and of course, 7 divides 7, as $7 = 7 \cdot 1$. Since we got to 1, we are done, as no prime divides 1. [Then, since 7 divided only once, we get only one factor of 7 in 504.]

So, we get $504 = 2^3 \cdot 3^2 \cdot 7$. We can do it like the picture below:

504	2
252	2
126	2
63	3
21	3
7	7
1	

[So, we divide the numbers on the left by the primes on the right, putting the result below on the left, and trying then another prime. We finish when we get to 1. Then we see we have three 2's, two 3's, and one 7, giving us $504 = 2^3 \cdot 3^2 \cdot 7$.]

Problems.

7.1) Which of the following numbers are prime:
(a) 111 (c) 367
(b) 259 (d) 541

7.2) Suppose a, b, and d are positive integers such that $d \mid a \cdot b$, but $d \nmid a$ and $d \nmid b$. Can d be prime? Justify.

7.3) Give the prime factorization of the following numbers:
(a) 90 (c) 875
(b) 231 (d) 1573

8. GCD and LCM Again

We now revisit the GCD and LCM, from the point of view of prime factorization. We first observe that if a and b are integers, we can write:

$$a = p_1^{r_1} \cdots p_k^{r_k} \qquad \textit{and} \qquad b = p_1^{s_1} \cdots p_k^{s_k},$$

where the p_i's are *distinct* primes [and we can even assume that $p_1 < p_2 < \cdots < p_k$ if we want to, but it's not necessary], and with $r_i, s_i \in \mathbb{N}$. So, this is similar to the prime factorizations of a and b,

but not quite, since some of the r_i's or s_j's might be *zero*. On the other hand, this allows us to use *the same primes for two different numbers*.

Maybe this is better understood with an example.

Example 8.1. The prime factorizations of 140 and 6776 are:

$$140 = 2^2 \cdot 5 \cdot 7 \qquad \text{and} \qquad 6776 = 2^3 \cdot 7 \cdot 11^2.$$

The factorization using the same primes [as above] is then:

$$140 = 2^2 \cdot 5 \cdot 7 \cdot 11^0 \qquad \text{and} \qquad 6776 = 2^3 \cdot 5^0 \cdot 7 \cdot 11^2.$$

[Remember that for any number $a \neq 0$, we have that $a^0 = 1$.] The advantage again is that we have the same primes showing up in both factorizations, even if with exponent zero.

With that observation we state the following proposition:

Proposition 8.2. *Let a and b be positive integers with*

$$a = p_1^{r_1} \cdots p_k^{r_k} \qquad \textit{and} \qquad b = p_1^{s_1} \cdots p_k^{s_k},$$

where the p_i's are distinct primes and with $r_i, s_i \in \mathbb{N}$ [just as above]. Then, $a \mid b$ if, and only if, $r_i \leq s_i$ for all i in $\{1, 2, \cdots, k\}$.

Sketch of the Proof. If $a \mid b$, then, since $p_1^{r_1} \mid a$ and $a \mid b$, we have that $p_1^{r_1} \mid b$ [by Proposition 3.3]. So, p_1 must divide b at least r_1 times, and hence $s_1 \geq r_1$ [so that I have "enough p_1's" in b to divide by $p_1^{r_1}$].

The converse is easy, since we have that if $s_i \geq r_i$, we have that $s_i - r_i \geq 0$, and so

$$b = a \cdot (p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}).$$

[Note that it's crucial that $s_i - r_i \geq 0$ in order to have that $(p_1^{s_1-r_1} \cdots p_k^{s_k-r_k})$ is an *integer*. □

This proposition gives us a new way to compute the GCD and LCM, stated in the theorem below:

Theorem 8.3. *Let a and b be positive integers with*

$$a = p_1^{r_1} \cdots p_k^{r_k} \qquad \textit{and} \qquad b = p_1^{s_1} \cdots p_k^{s_k},$$

where the p_i's are distinct primes and with $r_i, s_i \in \mathbb{N}$ [just as above]. Then,

$$\gcd(a, b) = p_1^{\min(r_1, s_1)} \cdots p_k^{\min(r_k, s_k)} \qquad \textit{and} \qquad \operatorname{lcm}(a, b) = p_1^{\max(r_1, s_1)} \cdots p_k^{\max(r_k, s_k)}.$$

Proof. If $d \mid a$ and b, we must have, by Proposition 8.2, that

$$d = p_1^{t_1} \cdots p_k^{t_k},$$

with $t_i \leq r_i$ [for $d \mid a$], and $t_i \leq s_i$ [for $d \mid b$] for all i's. Hence, $t_i \leq \min(r_i, s_i)$, and so the most that d can be [which gives us the *greatest* common divisor] is attained when all t_i's are equal to $\min(r_i, s_i)$, giving us the first part of the theorem.

For the second part, if m is a common multiple of a and b, we have that $a \mid m$ and $b \mid m$. This tells us that [again by Proposition 8.2]

$$m = p_1^{t_1} \cdots p_k^{t_k} \cdot p_{k+1}^{t_{k+1}} \cdots p_l^{t_l}.$$

[Note that we had to add some extra primes in here, namely $p_{k+1}, \ldots, p_l$, that may appear in m but not in a or b.] Then, for i in $\{1, \ldots, k\}$, we must have that $t_i \geq s_i$ [since $a \mid m$], and $t_i \geq s_i$ [since $b \mid m$], and thus, $t_i \geq \max(r_i, s_i)$. Hence, the least that m can be [which gives us the *least* common multiple] is attained when $t_i = \max(r_i, s_i)$ for i in $\{1, \ldots, k\}$, and $t_i = 0$ for i in $\{(k+1), \ldots, l\}$. $\square$

Example 8.4. So, with 140 and 6776 as in Example 8.1 above, we have:

$$\begin{aligned} \gcd(140, 6776) &= 2^{\min(2,3)} \cdot 5^{\min(1,0)} \cdot 7^{\min(1,1)} \cdot 11^{\min(0,2)} \\ &= 2^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \\ &= 28, \end{aligned}$$

and

$$\begin{aligned} \operatorname{lcm}(140, 6776) &= 2^{\max(2,3)} \cdot 5^{\max(1,0)} \cdot 7^{\max(1,1)} \cdot 11^{\max(0,2)} \\ &= 2^3 \cdot 5^1 \cdot 7^1 \cdot 11^2 \\ &= 33880. \end{aligned}$$

Theorem 8.3 gives us the following result [which has been mentioned previously]:

Proposition 8.5. *If a and b are positive integers, then*

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b.$$

We can see that it works with all examples of GCD and LCM we have already computed. As an easy one, note that $\gcd(5, 7) = 1$, $\operatorname{lcm}(5, 7) = 35$, and $1 \cdot 35 = 5 \cdot 7$.

The idea of the proof is that if

$$a = p_1^{r_1} \cdots p_k^{r_k} \qquad \textit{and} \qquad b = p_1^{s_1} \cdots p_k^{s_k},$$

where the p_i's are distinct primes and with $r_i, s_i \in \mathbb{N}$, then if $r_1 \leq s_1$, then the GCD has the factor $p_1^{r_1}$ while the LCM has the factor $p_1^{s_1}$. If not, i.e., if $r_1 > s_1$, we have the other way around, i.e., the LCM now has $p_1^{r_1}$ and the GCD has $p_1^{s_1}$. But in either case, when we multiply the GCD and LCM, we get $p_1^{r_1+s_1}$, the same power of p_1 that we get when multiplying a and b. The same is true for all other primes p_i's, and one can then see why the proposition holds.

Example 8.6. Here is a numerical example [using the factorizations of 140 and 6776 shown above]:

$$\begin{aligned}\gcd(140,6776)\cdot\operatorname{lcm}(140,6776) &= (2^2\cdot 5^0\cdot 7^1\cdot 11^0)\cdot(2^3\cdot 5^1\cdot 7^1\cdot 11^2)\\ &= 2^{2+3}\cdot 5^{0+1}\cdot 7^{1+1}\cdot 11^{0+2}\\ &= (2^2\cdot 5^1\cdot 7^1\cdot 11^0)\cdot(2^3\cdot 5^0\cdot 7^1\cdot 11^2)\\ &= 140\cdot 6776.\end{aligned}$$

An immediate consequence is the following:

Corollary 8.7. *If a and b are relatively prime positive integers, then* $\operatorname{lcm}(a,b)=ab$.

We also can prove now an analogue of Proposition 6.9 [which deals with GCD] for the LCM:

Proposition 8.8. *Let a and b positive integers and $m=\operatorname{lcm}(a,b)$. If n is a multiple of a and b, then n is a multiple of m.*

Proof. As in the second part of the proof of Theorem 8.3 if we write

$$a=p_1^{r_1}\cdots p_k^{r_k}\qquad \textit{and}\qquad b=p_1^{s_1}\cdots p_k^{s_k},$$

where the p_i's are distinct primes and with $r_i,s_i\in\mathbb{N}$, then, since n is multiple of a and b, it is of the form

$$n=p_1^{t_1}\cdots p_k^{t_k}\cdot p_{k+1}^{t_{k+1}}\cdots p_l^{t_l},$$

with $t_i\geq\max(r_i,s_i)$ for i in $\{1,\ldots,k\}$. Then, by Proposition 8.2, we see that $m\mid n$. □

Problems.

8.1) Compute the GCD and LCM of the following numbers by means of the prime factorization:

(a) 81 and 90

(b) $2^2\cdot 3\cdot 11^3$ and $2\cdot 3^3\cdot 5\cdot 11$

8.2) Check if it is true or false:

(a) $(2^2\cdot 5^{11}\cdot 13^6)\mid(2^3\cdot 3\cdot 5^{11}\cdot 13^5)$

(b) $(2\cdot 5\cdot 11\cdot 17)\mid(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19)$

(c) $(5^2\cdot 11^3)\mid(2\cdot 5^2\cdot 7^{11}\cdot 11^5)$

8.3) If a and b are integers such that $\gcd(a,b)=6$ and $\operatorname{lcm}(a,b)=18$, then what is $a\cdot b$?

8.4) If a and b are positive integers with $\gcd(a,b)=12$, can $\operatorname{lcm}(a,b)=30$? Justify your answer.

9. Some Problems in Number Theory

So what is number theory? As we mentioned before, classical number theory studies properties of integers. On the other hand, modern number theory deals with many ramifications of this initial

idea. And even in questions about integers, sometimes the tools necessary to solve the problems are quite sophisticated, and although the statements might be accessible to a "layperson", the proofs are far beyond the reach of non-specialists. [A typical example is *Fermat's Last Theorem* stated below.]

Number theory has always fascinated [and eluded] mathematicians and amateurs. Today still it has great importance and there is a great deal of research being done on its many beautiful problems. In fact, according to Gauss:

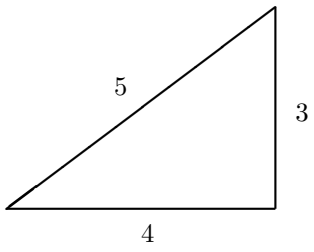
> *"Mathematics is the queen of the sciences and number theory is the queen of mathematics."*

[Gauss is certainly one of the greatest mathematicians who ever lived. If you study math long enough, you will hear his name many, many times. He is so important that his picture appears on the ten [German] mark bill.] Also, Kronecker, another great German mathematician, said:

> *"Number theorists are like lotus-eaters – having tasted this food, they can never give it up."*

To give you a better idea of the kind of questions of interest to number theorists, we will now state some theorems and some *conjectures* [i.e., statements which are believed to be true, but no one has found a proof yet]. Most of these theorems have very complex proofs, which are far beyond the scope of this course, and therefore will be omitted.

Let's start with an observation about the *Pythagoras' Theorem*. In geometry we have the well-known 3-4-5 right triangle:



By Pythagoras, this is a right triangle since

$$3^2 + 4^2 = 5^2.$$

In general we have that the equation of *Pythagoras' Theorem*, namely $x^2+y^2 = z^2$, have non-integral solutions, as we often have non-exact square roots: $1^2 + 1^2 = (\sqrt{2})^2$, $3^2 + 5^2 = (\sqrt{34})^2$, etc. As number theorists, we are interested in *integral solutions* only, i.e., we want to find x, y, and z *all integers*, such that $x^2 + y^2 = z^2$, as with $x = 3$, $y = 4$, and $z = 5$ above. So, can we find other solutions? Are there infinitely many, or just a few? Can we find *all* solutions?

Some of the answers are not too hard. For instance, observe that for any integer n that you pick, we have $(3n)^2 + (4n)^2 = (5n)^2$. It seems like cheating, but we were able to use one solution to produce infinitely many others! But the question now is whether or not there are integral solutions which are not like those above.

It turns out that there are. For instance $x = 5$, $y = 12$, $z = 13$. [Note that there is no number n such that $5 = 3n$, $12 = 4n$, and $13 = 5n$ at the same time.] The answer to this problem is known, and although the proof is very clever, it's not difficult at all. But, since its proof is unrelated to the mains goals of this text, we shall omit it.

To state the complete answer, first observe that we don't care about solutions that contain zero(s), since they are trivial. Moreover, because of the squares, signs can be changed still yielding solutions. So, we really want to look for solutions in $\mathbb{N}^*$.

Also, note that, just as with the 3-4-5 solution, taking multiples of any solution gives us infinitely many others. Conversely, suppose that $x^2 + y^2 = z^2$, with $x, y, z \in \mathbb{N}^*$, and let $d = \gcd(x, y, z)$. Then, we have that $\gcd(x/d, y/d, z/d) = 1$ [similarly to Corollary 6.8] and $(x/d)^2 + (y/d)^2 = (z/d)^2$ [by dividing the original equation by d^2]. Thus, the solution (x, y, z) is just a multiple of the solution $(x/d, y/d, z/d)$.

This shows us that all solutions involving positive integers can be obtained as multiples of solutions that are *relatively prime*.

Here is the theorem:

Theorem 9.1. *If*

$$x = st, \qquad y = \frac{s^2 - t^2}{2}, \qquad z = \frac{s^2 + t^2}{2}$$

with $1 \leq t < s$, and both s and t relatively prime odd integers, then $x^2 + y^2 = z^2$, and in this case, x, y, and z are also relatively prime. Moreover, every solution of $x^2 + y^2 = z^2$, with $x, y, z \in \mathbb{N}^*$ is a multiple of a solution as above.

So, for instance, $x = 3$, $y = 4$, and $z = 5$ is obtained by taking $s = 3$ and $t = 1$, and $x = 5$, $y = 12$, and $z = 13$ is obtained by taking $s = 5$ and $t = 1$.

Now, one might ask about higher powers in the same equation. In other words, does the equation

$$x^3 + y^3 = z^3$$

have an *integral* solution with $x, y, z \neq 0$. [It clearly has *real* solutions, like, $x = y = 1$, and $z = \sqrt[3]{2}$.] How about $x^4 + y^4 = z^4$? And, in general, how about $x^n + y^n = z^n$, for some integer $n \geq 3$? If there are integral solutions, can we find them all again?

In 1637, Pierre Fermat, a French amateur mathematician, asked that same question while reading [Bachet's translation of] Diophantus's *Arithmetica*, an ancient Greek text from the 3rd century. [Don't let Fermat's *amateur* status deceive you. He was a truly great mathematician.] He [seemed to have] found that the answer was no, i.e., he stated:

Theorem 9.2 (Fermat's Last Theorem)**.** *For any integer $n \geq 3$, the equation $x^n + y^n = z^n$ has no integral solution unless at least one among x, y, and z, is zero.*

He then wrote at the margin of the *Arithmetica*:

> *"I have discovered a truly remarkable proof which this margin is too small to contain."*

Many among the greatest mathematicians tried to find a proof of this fact, but failed. It is now widely believed that Fermat's claimed proof was incorrect, although it is impossible to be sure.

Fermat's Last Theorem therefore became a great challenge to mathematicians. Many special cases were proved for specific values of n, but the full statement was proved only in 1995 by the A. Wiles, a British mathematician in Princeton, 357 years after Fermat's claim. [Wiles first claimed it in 1993, but there was a gap in his proof. He and his student, R. Taylor, fixed the gap in 1995, completing the proof.]

This was likely the most celebrated proof in mathematics to date. It brought the attention of the whole media [which is usually not very interested in developments in mathematics], receiving worldwide newspaper coverage, generating various popularizations in books, and even a BBC Horizon program, which aired in the United States as a PBS NOVA special entitled *"The Proof"*.

Also in 1995, *"The Simpsons"* aired "Treehouse of Horror VI", a special Halloween episode, containing a segment called "Homer 3D" [in which Homer goes to the *third* dimension]. This segment, made with computer graphics, is a spoof on science fiction movies, and floating in the "third dimension" are formulas, like the famous Einstein's formula "$E = m \cdot c^2$", or Euler's "$\mathrm{e}^{2\pi \mathrm{i}} = -1$", among many others. One of then, is the following:

$$782^{12} + 1841^{12} = 1922^{12},$$

[check `http://www.youtube.com/watch?v=3uQwjgZ0kQM`] which would be an integral solution to $x^{12} + y^{12} = z^{12}$, contradicting *Fermat's Last Theorem*. Of course, this formula is not really correct. We have that the left-hand-side is

$$151586472050497548095196587112190091065 7,$$

while the right-hand-side is

$$254121025931480141081927864964365156761 6.$$

On the other hand, I've read that if you try this in an old [or cheap] calculator with low precision, since these number are so large, the results will appear to be the same. [I haven't tried it, though.] In any event, this seems to have been just a "tribute" to this much celebrated problem.

The proof of *Fermat's Last Theorem* took not only many years, but also the effort of many great mathematicians, who paved the way for Wiles's final and crucial step. The proof is quite deep and complex, involving, despite the simplicity of the theorem's statement, quite advanced mathematics.

In fact, the truth of the matter is that more important than whether or not there is a solution for the equation $x^n + y^n = z^n$, is that all the mathematics generated to solve this problem could be used to solve many other problems.

Another interesting theorem in number theory is the following, due to Lagrange:

Theorem 9.3 (Lagrange)**.** *Every positive integer is a sum of four squares, but not every integer is a sum of three squares.*

It is easy to see that not all integers are a sum of three squares. For instance, 7 is not. Indeed, if $7 = x_1^2 + x_2^2 + x_3^2$, with $x_1, x_2, x_3 \in \mathbb{N}$, then clearly $x_i \leq 2$. So, we can try all possibilities, and check that no such sum exist. [But note that $7 = 2^2 + 1^2 + 1^2 + 1^2$.]

The real problem is to show that *all* integers are indeed sum of four squares. Here is some random examples:

$$31 = 5^2 + 2^2 + 1^2 + 1^2$$
$$54 = 7^2 + 2^2 + 1^2 + 0^2$$
$$101 = 10^2 + 1^2 + 0^2 + 0^2$$
$$1012 = 31^2 + 7^2 + 1^2 + 1^2$$
$$3647 = 59^2 + 11^2 + 6^2 + 3^2$$
$$223729 = 473^2 + 0^2 + 0^2 + 0^2$$
$$765743 = 875^2 + 10^2 + 3^2 + 3^2$$
$$19293842 = 4392^2 + 64^2 + 9^2 + 1^2$$

[Note that we allow zeros!] Observe also that the representation is not necessarily unique. For instance, $4 = 2^2 + 0^2 + 0^2 + 0^2 = 1^2 + 1^2 + 1^2 + 1^2$.

The proof is quite ingenious, and not too complex, but beyond the scope of this course.

Another "hot topic" in number theory is, of course, prime numbers, as they are the building blocks of integers. As we shall see, prime numbers are more elusive than they might appear. Even determining if a large number is prime, with all of the computer power we have today, can be quite difficult. There are, though, much more efficient ways than the naive one described previously in Section 7, which involve some very clever ideas. Also, some *probabilistic methods*, which can tell within a small margin of error if a number is prime, are even faster, but still, *primality testing* is a quite difficult problem, and people keep working on it to find better algorithms.

Also, it's worth mentioning that there is no efficient enough way to *generate* primes known today, which is also something that many have sought.

So, let's start with something easy:

Theorem 9.4. *There are infinitely many primes.*

Proof. Suppose that $p_1, p_2, \ldots, p_n$ are *all* prime numbers, and let $n = p_1 \cdot p_2 \cdots p_n + 1$ By the *Fundamental Theorem of Arithmetic*, we have that n is divisible by some prime, i.e., some p_i. But $p_i \mid p_1 \cdots p_n$, while $p_i \nmid 1$. Thus, by Theorem 3.1, we have that p_i cannot divided n. So, this cannot happen, i.e., there has to be infinitely many primes. □

The proof above appears already in Euclid's *Elements*. Another proof, more complicated, but groundbreaking and pregnant with new possibilities, was given by Euler in 1737. It was one of the first examples of the use of calculus tools in an arithmetic question. [Today we call this area of number theory studied with "calculus" *analytic number theory*.] In fact, this proof led Riemann to make a conjecture in 1859, which is still unproven and known today as *Riemann Hypothesis*. Even the statement of this conjecture is too complex for this text, but it suffices to say that it tells us, among other things, something about how primes are distributed among the integers. To give you an idea of the importance of this problem, the *Clay Mathematics Institute* offered a prize of one million dollars to whoever solves it first. [The *Riemann Hypothesis* is one of the seven *Millennium Prize Problems*, which are believed to be among the most important problems for this new millennium. Only one of them apparently has been solved. This problem is called the "Poincaré Conjecture" and a possible proof was given by the Russian mathematician G. Perelman. Although it seems to be a valid proof, it is still, by the time of this writing being investigated. Each one of these seven problems carry a million dollar prize. Number theory has a second problem among those, called the *Birch and Swinnerton-Dyer Conjecture*, whose statement is also beyond the scope of this introductory text. For more details on all these problems, visit `http://www.claymath.org/millennium/`. They have videos of talks given at The University of Texas at Austin that discuss each one of these problems. [And you can even spot yours truly in the audience.]]

The *Riemann Hypothesis* is also mentioned in the 2001 movie *"A Beautiful Mind"*, based on the biography of the mathematician [gone schizophrenic] John Nash, written by S. Nasar. The movie was directed by Ron Howard, and starred Russel Crowe, as Nash, and Jennifer Connelly. [*Spoiler alert:* Nash could not prove it.]

So, this *Riemann Hypothesis* tells us something about how primes numbers are distributed. Let's see what else is known about this. First we can look at the *density of primes*, i.e., give an integer n, we look at the proportion of primes among all integers between 1 and n. The usual notation is:

$$\pi(x) = \text{number of primes less than or equal to } x.$$

So, we want to look at the proportion $\pi(n)/n$. Here is a table:

x	10	25	50	100	500	1000	10000	100000
$\pi(x)$	4	9	15	25	95	168	1229	9592
$\pi(x)/x$	0.400	0.360	0.300	0.250	0.190	0.168	0.123	0.096

As you can see, the primes become less and less frequent as we consider longer stretches: among the first ten positive integers, 40% of them are prime, and if we consider the first ten thousand positive integers, only 9.6% of them are prime. In fact, one can be much more precise:

Theorem 9.5 (Prime Number Theorem)**.** *For large values of x, the number of primes less than or equal to x is* approximately $x/\ln(x)$.

If you are not too familiar with *natural logs* [even though you should be!], don't worry too much about it now. The point is that we have a precise way to see how this density of primes behaves for very large x.

Both Gauss and Legendre independently conjectured this statement [great minds think alike] around 1800, but the proof only came in 1896, when Hadamard and Poussin also independently found proofs [*ditto*]. This proof, again, involves calculus.

So, primes become more rare if we restrict ourselves to larger numbers. In fact we have the following easy proposition:

Proposition 9.6. *Given any positive integer N [which can be as large as you want], there are N* consecutive *integers, say $\{k, k+1, k+2, \ldots, k+(N-1)\}$, with no primes among them.*

Proof. Let $p_1, p_2, \ldots, p_r$ be *all* primes that are less than or equal to $N+1$ [for whatever N was chosen], and take $k = p_1 \cdot p_2 \cdots p_r + 2$. Let's look at $k+i$, for some i in $\{0, 1, 2, \ldots, (N-1)\}$. We have that $i+2$ is in $\{2, 3, 4, \ldots, (N+1)\}$, and so, whatever i is, we have that $i+2$ is divisible by one of the primes p_j, for some j in $\{1, 2, \ldots, r\}$. Now,

$$k + i = p_1 \cdots p_r + (i+2).$$

Since p_j also clearly divides $p_1 \cdots p_r$, Theorem 3.1 tells us that $p_j \mid (k+i)$. Since clearly $1 < p_j < (k+i)$, we have that $k+i$ cannot be prime. □

So, we have gaps as large as you might want, with no primes in it. Notice, though, that to get a large gap following the proof of the proposition above, we have to go *really* far down the real line. For instance, to get ten consecutive composite numbers [i.e., non-primes], we have to start at 212, to get fifty consecutive composite numbers, we need to start at 614889782588491412. The number at which we would have to start to get a thousand consecutive integers that are composite has 416 *digits*!

So, it seems that if we go far enough, some primes become very far apart. On the other hand, one might try to find if we also get primes that are very close together. Note that the only pair of primes that are consecutive are 2 and 3, as if p and $p+1$ are both primes, one of then must even, and the only even prime is 2. Hence, if p is not 2, the closest that the next prime can be is $p+2$. If indeed p and $p+2$ are prime, we call them *twin primes*. Early on, we have many twin primes: 3 and 5, 5 and 7, 11 and 13, 17 and 19, etc. [So, there are four pairs of twin primes between 2 and 20.] But, as we go farther, they seem to get more rare. For instance, between 20 to 100, there are

also only four pairs of twin primes: 29 and 31, 41 and 43, 59 and 61, and 71, 73. Between 1 and 100 there are 35 pairs of twin primes, while between 1000 and 2000 there are only 26. So, it seems that they become rarer, but we still always seem to find a pair of twin primes, not matter how far down the real line we go. This is in fact a known conjecture:

Conjecture 9.7 (Twin Primes Conjecture)**.** *There are infinitely many primes p such that $p+2$ is also prime.*

Note that this means that given any positive integer N [which can be as large as you want], there exists a prime $p > N$ such that $p+2$ is also prime. [Hence, p and $p+2$ are twin primes larger than N.]

This conjecture, likely due to its simple statement [and evasive proof], is mentioned in the 1996 movie *"The Mirror Has Two Faces"*, directed and starred by Barbra Streisand [sic!], and also starring Jeff Bridges, who plays a math professor from Columbia University. [He actually mentions it on their first date! I don't recommend talking about math on a first date unless you are dating a mathematician.]

As mentioned before, the term "conjecture" is only used when the statement is believed to be true. [Otherwise, one should call it an "open question", or "open problem".] So, as you can imagined, this conjecture has been widely tested with the use of the most powerful computers. For instance, we know that the humongous numbers

$$242206083 \cdot 2^{38880} - 1 \quad \text{and} \quad 242206083 \cdot 2^{38880} + 1$$

are twin primes. [Just a quick detour. You might not realize how large these numbers actually are, as powers can be deceiving. But, just to give you an idea, if you pile 2^{63} quarters, the tower will go far beyond the bounds of the solar system, the top being over *one light-year* away from the bottom. [That's over 5.8 million [times one] million miles!] These number are much larger. They have 1177 *digits*, while 2^{63} has only 19 digits!]

So, it seems [if the conjecture is indeed true] that we have primes that are very far apart and, at the same time, primes that are very close together when we deal with very large numbers.

Here is yet another conjecture concerning prime numbers:

Conjecture 9.8 (Goldbach Conjecture)**.** *Every even number greater than two is a sum of two primes.*

The question was posed by Goldbach to Euler in 1742, and there is still no proof, although there is plenty of evidence. Here are the first few numbers:

$$\begin{array}{llll} 4 = 2+2, & 6 = 3+3, & 8 = 3+5, & 10 = 3+7, \\ 12 = 5+7, & 14 = 7+7 & 16 = 5+11, & 18 = 5+13, \\ 20 = 3+17, & 22 = 11+11, & 24 = 5+19, & 26 = 13+13 \\ 28 = 5+23, & 30 = 7+23, & 32 = 3+29, & 34 = 5+29. \end{array}$$

It also works for very large numbers:

$$\begin{aligned} 1000000 &= 17 + 999983, \\ 758436384732 &= 23 + 758436384709, \\ 217837643716218 &= 67 + 217837643716151, \\ 329873854787429387236 &= 3 + 329873854787429387233. \end{aligned}$$

We end this section with a final result on prime numbers:

Theorem 9.9 (Dirichlet's Theorem of Primes in Arithmetic Progressions)**.** *If a and m are relatively prime positive integers, then there are* infinitely *many primes in the set*

$$\{a, a+m, a+2m, a+3m, a+4m, \ldots\}.$$

[A note on terminology: an *arithmetic progression* is a sequence

$$a, a+m, a+2m, a+3m, \ldots,$$

i.e., a sequence that changes by always adding a same amount.]

First observe that the hypothesis that a and m are relatively prime is crucial. If not, say that d is a common divisor greater than one, then, by Theorem 3.1, we have that $d \mid (a + k \cdot m)$ for all integers k, and hence there can be only one prime in the progression, namely a itself [and in that case we must have $a = d$, i.e., a a prime divisor of m].

Here are a few examples. The sequence

$$2, 35, 68, 101, 134 \ldots$$

is an arithmetic progression, namely, we have

$$2, 2+33, 2+2\cdot 33, 2+3\cdot 33+24\cdot 33, \ldots.$$

So, with notation of the theorem, we have that $a = 2$ and $m = 33$. Since $\gcd(2, 33) = 1$, by the theorem, we have infinitely many primes in the sequence.

On the other hand, if we consider the sequence,

$$7, 28, 49, 70, 91, 112, \ldots$$

we have an arithmetic progression with [using again the notation from the theorem] $a = 7$ and $m = 21$. Now, we have $\gcd(7, 21) = 7$. So, the theorem does not say anything, but as we've observed above, this means that all terms in this sequence are divisible by this GCD. So, there is only one prime in this sequence, namely 7.

Finally, the sequence

$$6, 21, 36, 51, 66, 81, \ldots$$

has [using again the notation from the theorem] $a = 6$ and $m = 15$. Now, we have $\gcd(6, 15) = 3$, and hence all terms in the sequence are divisible by 3. Since 3 itself is not in the sequence, there is no prime in the sequence.

I hope this section gave you a little taste of number theory. [Although I must say that it is a bit of an *artificial* flavor, as the real flavor is in the proofs!]

Problems.

9.1) How many solutions with $x, y, z \in \mathbb{N}^*$ does $x^2 + y^2 = z^2$ have? How about $x^5 + y^5 = z^5$?

9.2) Can every positive integer be written as a sum of three squares? How about four squares? How about five?

9.3) Write the following numbers as the sum of four squares:
(a) 81
(b) 12
(c) 53
(d) 105

9.4) Is there a prime larger than one million?

9.5) State the *Twin Primes Conjecture*.

9.6) Write the following even numbers are as sum of two primes:
(a) 36
(b) 50

9.7) How many primes do we have in the following arithmetic progressions:
(a) $4, 10, 16, 22, 28, 34, \ldots$
(b) $22, 25, 28, 31, 34, 37, \ldots$
(c) $3, 18, 33, 48, 63, 78, \ldots$

10. So, What's Number Theory Good For?

You might be wondering at this point, why should you care whether or not a positive integer can be written as the sum of four squares? Let me answer it with another question: why should you care if someone can run one hundred meters in less than ten seconds? Or why should you care if someone can throw a ball through a hoop from three meters away? The point is, like sports, mathematics is humanity pushing its limits, but its intellectual, rather than physical limits.

Well, someone might complain that sports might be pointless [why should any one try to throw a ball through a hoop?], but they are fun to watch. Well, math is a lot of fun to watch! But, as with sports, where you have to understand the rules to fully enjoy it, the same is true for mathematics. The difference is that the rules are much more complicated. But, you can take my word that if you do understand them, it can be a lot of fun to read a nice proof. [Like, for instance, Lagrange's proof that every positive integers is the sum of four squares.] When you see someone come up with a really brilliant idea, it is like seeing your team hit a home run! In the same way it can be exhilarating to watch some one run one hundred meters in less than ten seconds, which would seem *impossible* [have you ever tried it?!], it is just as breathtaking to see that someone could solve a problem that appeared to be too difficult to ever be solved! [And imagine how much more thrilling it would be if that someone is you!]

And if you don't like sports, think that math is like art. It might not have any concrete usefulness, but it has *beauty*. When you read a well written poem or a look at a well painted canvas, it touches you. Math also has beauty. It is hard to explain, just as it is hard to explain why or how a poem or painting can touch you, but believe me, it does, and it can send shivers down your spine.

Now, you might ask what is so special about mathematics? Aren't all sciences like that too? Well, certainly other sciences have beauty and challenge your intellect. But the difference is that they all depend on "external factors". They depend on measurements, labs, quality of materials and equipment, etc. Mathematics does not depend on anything but itself. It is all in the *realm of ideas* [it is all in your head, but in a good way], and does not have any *need* to relate to the real world! [Although it certainly can.] So, to keep the analogy with sports, you might think of other sciences as car races: you need skills, but you also need a good car.

In fact, mathematics is closer to philosophy than it is to any [experimental] science. Some might even say that mathematics is a branch of philosophy [gone wild]. The famous Greek philosopher Plato hung over the entry to his school the words *"Let no one unversed in geometry enter"*. [At Plato's time, geometry was the most regarded form of mathematics.]

Of course, math in general, has many applications. In fact, it's everywhere, and all other sciences use and depend on it. The point I am trying to make is that there is more to math than its applications. As teachers we are often pressured to emphasize these applications, but I think it would be a disservice to the students if we would not help them realize that math is so much more than its applications, and that there is nothing wrong with pure and abstract mathematics, even if

you are pragmatic. Studying math, even abstract math, is the best way to improve your problem solving skills. And don't think that if you work on math you will only be good at math. This is the same as saying that if you lift [gym] weights you are only going to be able to lift [gym] weights! In fact, in my own experience [and of some to whom I've spoken], when you become more proficient in math, you change the way you think about *everything*. You analyze matters in a more methodical way, you become more precise in your thinking, and you start to question more. To give you an idea, some countries under dictatorship have diminished the roll of mathematics in schools to prevent the development of critical thinking. [All the propaganda in the world is not enough if the citizens are capable of critical thinking!]

So, mathematics has many applications, but does number theory in particular have applications? Let me start with an evasive answer. The truth is that we never know when something might someday become applicable. For instance, Einstein's *Theory of Relativity* heavily relies on Riemann's theory of *curved spaces*. Until Einstein realized the need for this new kind of geometry in physics, this theory of curved spaces was considered totally abstract! In fact, Einstein was extremely fortunate to have found the math that he needed for this own theory already done for him, mostly in the [until then purely abstract] works of Riemann. [The physicists working in *string theory* [the new "hot topic" in physics] were not as lucky, and much of the mathematics that they need still have to be developed.]

But, back to applications of number theory, here is a quote from the British number theorist G. H. Hardy:

> *"The Theory of Numbers has always been regarded as one of the most obviously useless branches of Pure Mathematics."*

But, he goes on to explain the term "useless":

> *"A science is said to be useful if its development tends to accentuate the existing inequalities in the distribution of wealth, or more directly promotes the destruction of human life. [...] I have never done anything 'useful'. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world..."*

So, Hardy was proud of the fact that number theory was not applicable, as it seems that all that mankind can use for good, it also can use for harm. But, alas, he was wrong. [As observed above, what might seem "useless" today, might become "useful" tomorrow.] Number theory has applications today, most notably cryptography and coding theory.

We should clarify what those terms mean. *Cryptography* is the practice and study of hiding information, i.e., codifying a message to preserve its content from unwanted eyes. These are widely used today on the Internet: when you send your credit card number, you don't want anyone besides

the merchant to be able to read it. So, cryptography is used to encode it, and [supposedly] only the merchant can decode it.

We will deal with a particular *cryptosystem* [i.e., a particular way to encode and decode messages in the context of cryptography] in Section 13.

But be careful that in math the term *coding theory* should be distinguished from cryptography. Coding theory studies ways to preserve messages [likely sent through less than ideal channels] from interference not due to malicious attacks, but due to *noise*. Maybe it would be clearer with an example: a mission in space has to communicate with earth. The message sent is subject to interference due to radiation and electromagnetic waves in space, which may corrupt parts of the message. Coding theory tries to encode this message in such a way that when earth receives the corrupted message, it is still able to read it clearly. Coding theory is widely used in communications [such as cell phones] and digital data storage [like CDs].

We will not discuss coding theory here, but if you are wondering how can one correctly read a corrupted message, here is an idea: send the message three times. Unless you are very unlucky, different pieces of each copy will be corrupted by interference. When reading, you look at the three messages, which should be equal. If there is one message which is not equal to the other two, this one is corrupted, but the other two allow you to know which was the correct message.

Note that only two copies would not have been enough: in that case if you see two different messages, you don't know which one is the correct. So, this method works, but requires three times more information to be sent! The main idea of coding theory is to be able to detect and correct errors while minimizing the amount of extra data that has to be sent.

11. Integers Modulo n

In this section we introduce a new set of numbers. We can perform operations like addition and multiplication in a similar manner as we do with our familiar real numbers or integers.

Definition 11.1. Given a positive integer n we define the set of *integers modulo* n, which we shall denote by $\mathbb{Z}/n\mathbb{Z}$, to be the set with n elements

$$\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

[The bars over the numbers are introduce to make a distinction between the usual integer, say $2 \in \mathbb{Z}$, and the elements in $\mathbb{Z}/n\mathbb{Z}$, such as $\overline{2} \in \mathbb{Z}/n\mathbb{Z}$.]

We refer to $\bar{k}$ as the *class of* k in $\mathbb{Z}/n\mathbb{Z}$. Also, we call n [from $\mathbb{Z}/n\mathbb{Z}$] the *modulus*.

We can perform sum, products, and differences in this set in following manner: perform the operation as if the elements were integers [i.e., forget about the "bar" for a second], and compute the remainder of the resulting integer when divided by n [i.e., the modulus]. The result of the operation is then the class of this remainder in $\mathbb{Z}/n\mathbb{Z}$. [In fact, one can think of $\mathbb{Z}/n\mathbb{Z}$ as the set of possible *remainders* from a division by n. Even the notation, $\mathbb{Z}/n\mathbb{Z}$ was designed to indicate the "divided by n".]

The set $\mathbb{Z}/n\mathbb{Z}$ can be quite helpful in answering questions about divisibility and remainders when dividing by n, and hence the term "*modulo n*" in its name. We will not deal with this aspect here, though, as our actual goal is to use $\mathbb{Z}/n\mathbb{Z}$ in cryptography.

The definition of $\mathbb{Z}/n\mathbb{Z}$ is better understood with an example.

Example 11.2. Let's take $n = 5$. Then,

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Then, what is $\overline{2} \cdot \overline{4}$? We compute the operation as if with usual integers: $2 \cdot 4 = 8$. Then, we take the result [i.e., 8 in this case] and compute the remainder of its division by 5 [as we are in $\mathbb{Z}/5\mathbb{Z}$]: $8 = 1 \cdot 5 + 3$. Since the remainder is 3, we have $\overline{2} \cdot \overline{4} = \overline{3}$.

Here are other computations in $\mathbb{Z}/5\mathbb{Z}$ [verify them yourself!]:

$$\overline{2} + \overline{3} = \overline{0}$$
$$\overline{2} - \overline{3} = \overline{4}$$
$$\overline{2} \cdot \overline{3} = \overline{1}$$

Note that we have to be very careful here about *where* the operations are occurring, as for instance $\overline{2} \cdot \overline{4} = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ [as seen above], but $\overline{2} \cdot \overline{4} = \overline{1}$ in $\mathbb{Z}/7\mathbb{Z}$ [as now we divide by 7 instead of 5]. This is one of the shortcomings of this "bar notation", as it does not indicate to which set exactly the elements belong. But this is standard notation, and notation could become a bit too heavy if we were to specify the modulus with it. We just have to be careful to clarify in which set we are working.

There is another way see this set with its operations: we can say that $\overline{a} = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$ if the remainders of a and b when divided by the modulus n are equal. [Remember, the set $\mathbb{Z}/n\mathbb{Z}$ deals with remainders when dividing by n, and hence it makes sense that numbers with same remainder are to be considered equal in this set.] So, in $\mathbb{Z}/5\mathbb{Z}$ we would have:

$$\cdots = \overline{-15} = \overline{-10} = \overline{-5} = \overline{0} = \overline{5} = \overline{10} = \overline{15} = \cdots$$
$$\cdots = \overline{-14} = \overline{-9} = \overline{-4} = \overline{1} = \overline{6} = \overline{11} = \overline{16} = \cdots$$
$$\cdots = \overline{-13} = \overline{-8} = \overline{-3} = \overline{2} = \overline{7} = \overline{12} = \overline{17} = \cdots$$
$$\cdots = \overline{-12} = \overline{-7} = \overline{-2} = \overline{3} = \overline{8} = \overline{13} = \overline{18} = \cdots$$
$$\cdots = \overline{-11} = \overline{-6} = \overline{-1} = \overline{4} = \overline{9} = \overline{14} = \overline{19} = \cdots$$

So, we are *not* introducing new elements to $\mathbb{Z}/5\mathbb{Z}$ [it still has only 5 elements], we are only introducing new ways to write the same elements. [This is similar to what happens in $\mathbb{Q}$, where $1/2$ and $2/4$ are two representations of the same number.]

In the same way, for a general modulus n, we would have:

$$\begin{gathered}
\cdots = \overline{-3n} = \overline{-2n} = \overline{-n} = \overline{0} = \overline{n} = \overline{2n} = \overline{3n} = \cdots \\
\cdots = \overline{-3n+1} = \overline{-2n+1} = \overline{-n+1} = \overline{1} = \overline{n+1} = \overline{2n+1} = \overline{3n+1} = \cdots \\
\cdots = \overline{-3n+2} = \overline{-2n+2} = \overline{-n+2} = \overline{2} = \overline{n+2} = \overline{2n+2} = \overline{3n+2} = \cdots \\
\vdots \\
\cdots = \overline{-3n+k} = \overline{-2n+k} = \overline{-n+k} = \overline{k} = \overline{n+k} = \overline{2n+k} = \overline{3n+k} = \cdots \\
\vdots \\
\cdots = \overline{-2n-1} = \overline{-n-1} = \overline{-1} = \overline{n-1} = \overline{2n-1} = \overline{3n-1} = \overline{4n-1} = \cdots
\end{gathered}$$

The benefit of this new representation of the elements of $\mathbb{Z}/n\mathbb{Z}$ is that we can then perform these operations by simply observing that if $0 \leq a, b \leq (n-1)$, then:

$$\begin{aligned}
\overline{a} + \overline{b} &= \overline{a+b} \\
\overline{a} - \overline{b} &= \overline{a-b} \\
\overline{a} \cdot \overline{b} &= \overline{a \cdot b}
\end{aligned}$$

For example, we can write in $\mathbb{Z}/5\mathbb{Z}$ that $\overline{2} \cdot \overline{4} = \overline{8}$, and this is the same result we obtained before, as $\overline{8} = \overline{3}$.

The only thing is that we want to represent the results with *smaller numbers*. For instance, in $\mathbb{Z}/6\mathbb{Z}$ we have $\overline{4} \cdot 5$ is then $\overline{4 \cdot 5} = \overline{20}$. But we don't want to deal with $\overline{20}$, as $\overline{20} = \overline{2}$ in $\mathbb{Z}/6\mathbb{Z}$ [as the remainder of 20 when divided by 6 is 2]. So, we want to say that the result is $\overline{2}$, and not $\overline{20}$ [even though they are equal]. In the end we are doing the same as above, as we have to take the result and compute its remainder when divided by the modulus.

It should be clear now that this gives the same operation as we initially defined. There is only one catch: initially we only had n elements, namely $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. But now we can put bars over all integers. We had before $\overline{2} \cdot \overline{4} = \overline{2 \cdot 4} = \overline{8} = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ [as seen above]. But we have, for instance, $\overline{2} = \overline{7}$ and $\overline{4} = \overline{-1}$. So, one can ask if we can use those when performing the computations, i.e., can we write [in $\mathbb{Z}/5\mathbb{Z}$] $\overline{2} \cdot \overline{4} = \overline{7} \cdot \overline{-1} = \overline{-7}$? In this case it does seem to work, as $\overline{-7} = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$. In fact, this works in general:

Proposition 11.3. *In $\mathbb{Z}/n\mathbb{Z}$, we always have*

$$\begin{aligned}
\overline{a} + \overline{b} &= \overline{a+b} \\
\overline{a} - \overline{b} &= \overline{a-b} \\
\overline{a} \cdot \overline{b} &= \overline{a \cdot b},
\end{aligned}$$

even if a or b are not in $\{0, 1, 2, \ldots, (n-1)\}$.

Before we prove this proposition, we need the following lemma, which gives a new way to see if $\overline{a} = \overline{b}$.

Lemma 11.4. *We have $\overline{a} = \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$ if, and only if, n divides $a - b$.*

Proof. With the division algorithm, write $a = q_1 n + r_1$ and $b = q_2 n + r_2$, where $r_1, r_2 \in \{0, 1, \ldots, (n-1)\}$. Suppose also that $r_1 \geq r_2$. If not, we can switch the places of a and b. Then, $(a - b) = (q_1 n + r_1) + (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2)$. Since $r_1 \geq r_2$ [and hence $r_1 - r_2 \geq 0$], and $r_1, r_2 \in \{0, 1, \ldots, (n-1)\}$, we have that $r_1 - r_2 \in \{0, 1, \ldots, (n-1)\}$. Hence, by the uniqueness in the division algorithm [as in Example 2.3], the remainder of the division of $a - b$ by n is $(r_1 - r_2)$. Hence, n divides $a - b$ if, and only if $r_1 - r_2 = 0$, i.e., $r_1 = r_2$. By definition, $r_1 = r_2$ is the same as to say $\overline{a} = \overline{b}$. □

Proof of Proposition 11.3. Remember that to perform the operation as we defined, we need to find numbers $a', b' \in \{0, 1, \ldots, (n-1)\}$ such that $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ [as we have only defined how to add, subtract, and multiply with $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$]. To do that we just compute a and b modulo n, i.e., find the remainders of a and b when divided by n. Thus, we have

$$a = q_1 n + a', \qquad b = q_2 n + b', \qquad a', b' \in \{0, 1, \ldots, (n-1)\}.$$

Then, by definition,

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a' + b'} \\ \overline{a} - \overline{b} &= \overline{a' - b'} \\ \overline{a} \cdot \overline{b} &= \overline{a' \cdot b'}. \end{aligned}$$

We then need to show that $\overline{a + b} = \overline{a' + b'}$, $\overline{a - b} = \overline{a' - b'}$, and $\overline{a \cdot b} = \overline{a' \cdot b'}$. To do this, we use the lemma above:

$$\begin{aligned} (a + b) - (a' + b') &= (q_1 n + a' + q_2 n + b') - (a' + b') \\ &= (q_1 - q_2)n. \end{aligned}$$

Hence, n divides $(a+b)-(a'+b')$, and therefore the lemma tells us that $\overline{a + b} = \overline{a' + b'}$. The case of differences follows from the same steps, and so we leave it as a [very simple] exercise for the reader. Now, for products:

$$\begin{aligned} (a \cdot b) - (a' \cdot b') &= (q_1 n + a') \cdot (q_2 n + b') - (a' \cdot b') \\ &= q_1 q_2 n^2 + b' q_1 n + a' q_2 n + a' \cdot b' - a' \cdot b' \\ &= (q_1 q_2 n + b' q_1 + a' q_2)n. \end{aligned}$$

Hence, n divides $(a \cdot b) - (a' \cdot b')$, and therefore the lemma tells us that $\overline{a \cdot b} = \overline{a' \cdot b'}$. □

Problems.

11.1) Mark true or false:

(a) $\overline{3} = \overline{-11}$ in $\mathbb{Z}/7\mathbb{Z}$.

(b) $\overline{3} = \overline{-11}$ in $\mathbb{Z}/8\mathbb{Z}$.

(c) $\overline{21821} = \overline{9303}$ in $\mathbb{Z}/3\mathbb{Z}$.

(d) $\overline{43847833} = \overline{8437898}$ in $\mathbb{Z}/5\mathbb{Z}$.

11.2) Compute:

(a) $\overline{7} + \overline{8}$ in $\mathbb{Z}/9\mathbb{Z}$.

(b) $\overline{7} \cdot \overline{8}$ in $\mathbb{Z}/11\mathbb{Z}$.

(c) $\overline{24} \cdot \overline{13}$ in $\mathbb{Z}/5\mathbb{Z}$.

(d) $\overline{369303} \cdot \overline{172647183}$ in $\mathbb{Z}/3\mathbb{Z}$.

(e) $(\overline{2} + \overline{5}) \cdot \overline{7}^{\,2}$ in $\mathbb{Z}/8\mathbb{Z}$.

(f) $(\overline{31} - \overline{44}) \cdot (\overline{33} + \overline{-13})$ in $\mathbb{Z}/7\mathbb{Z}$.

12. Exponents and Divisions in $\mathbb{Z}/n\mathbb{Z}$

Definition 12.1. We define exponentiation of elements of $\mathbb{Z}/n\mathbb{Z}$ by nonnegative integers in the usual way: given $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ and r a nonnegative integer we define:

$$\overline{a}^{\,0} = \overline{1},$$

$$\overline{a}^{\,1} = \overline{a},$$

$$\overline{a}^{r} = \underbrace{\overline{a} \cdot \overline{a} \cdots \overline{a}}_{r \text{ factors}} \quad [\text{if } r > 1].$$

The problem of division is a bit harder, as in general we cannot divide two integers [if we also want to get an integer as a result]. The same is true for $\mathbb{Z}/n\mathbb{Z}$. But the idea of division is the same: $\overline{b}$ divides $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ if there is $\overline{k}$ in $\mathbb{Z}/n\mathbb{Z}$ such that $\overline{a} = \overline{bk}$. So, $\overline{2}$ divides $\overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ [as weird as this might sound], since $\overline{3} = \overline{2} \cdot \overline{4}$ [as seen in Example 11.2]. On the other hand, $\overline{2}$ does not divide $\overline{3}$ in $\mathbb{Z}/6\mathbb{Z}$, as

$$\overline{2} \cdot \overline{0} = \overline{0}$$

$$\overline{2} \cdot \overline{1} = \overline{2}$$

$$\overline{2} \cdot \overline{2} = \overline{4}$$

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$

$$\overline{2} \cdot \overline{4} = \overline{8} = \overline{2}$$

$$\overline{2} \cdot \overline{5} = \overline{10} = \overline{4}$$

So, there is no $\overline{k} \in \mathbb{Z}/6\mathbb{Z}$ such that $\overline{2} \cdot \overline{k} = \overline{3}$.

So, one might ask now when does $\overline{k}$ divide $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$.

Definition 12.2. A divisor of $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ is called a *unit* of $\mathbb{Z}/n\mathbb{Z}$. We denote the set of units in $\mathbb{Z}/n\mathbb{Z}$ by $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

The following proposition tells us exactly what are the units of $\mathbb{Z}/n\mathbb{Z}$.

Proposition 12.3. *An element $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ is a unit if, and only if,* $\gcd(k,n) = 1$. *In other words,*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \ : \ \gcd(k,n) = 1\}.$$

Proof. Saying that $\overline{k}$ is a unit is the same [by definition] as saying that $\overline{k}$ a divisor of $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$. On the other hand, that is equivalent to saying that there is $\overline{x}$ in $\mathbb{Z}/n\mathbb{Z}$ such that $\overline{1} = \overline{k} \cdot \overline{x}$. This says that $\overline{k} \cdot \overline{x} = \overline{xk} = \overline{1}$. By Lemma 11.4, this is the same as to say that n divides $1 - xk$, i.e., there is an integer y such that $1 - xk = yn$, or $1 = xy + yn$. By Corollary 6.7, this last condition is the same as to say that $\gcd(k,n) = 1$. □

Note that if $\overline{k}$ divides $\overline{1}$, then it divides $\overline{a}$ for all $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$: if $\overline{1} = \overline{x} \cdot \overline{k}$, then $\overline{a} \cdot \overline{1} = \overline{a} \cdot \overline{x} \cdot \overline{k}$, and hence $\overline{a} = \overline{a \cdot 1} = \overline{a \cdot x} \cdot \overline{k}$.

Also, if $\overline{x} \cdot \overline{k} = \overline{1}$ [in $\mathbb{Z}/n\mathbb{Z}$], we can write $\overline{x} = \overline{k}^{-1}$, and thus define negative exponents to elements of $(\mathbb{Z}/n\mathbb{Z})^\times$: with $\overline{k}$ and $\overline{x}$ as above [which implies that $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$], and if r is a nonnegative integer, we define $\overline{k}^{-r} = \overline{x}^r$. [We will not need negative exponents here, though.]

Definition 12.4. Given a positive integer n, define the *Euler phi function* of n, denoted by $\varphi(n)$, as the number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$. ["Phi" is the name of the Greek letter φ.]

Example 12.5. Let's find $(\mathbb{Z}/5\mathbb{Z})^\times$ and $\varphi(5)$. To find $(\mathbb{Z}/5\mathbb{Z})^\times$, we just have to find all elements in $\{0,1,2,3,4\}$ which are relatively prime to 5. Since 5 is prime, this is an easy task, and we can easily see that $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, and hence $\varphi(5) = 4$.

In fact, we have in general that for all primes p that $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$, as the the only [positive] divisors of p are 1 and p [since p is prime], no positive number less that p can have a common divisor with p greater than 1. Hence, we also have $\varphi(p) = p - 1$.

Example 12.6. Let's find $(\mathbb{Z}/12\mathbb{Z})^\times$ and $\varphi(12)$. Again, to find $(\mathbb{Z}/12\mathbb{Z})^\times$, we just have to find all elements in $\{0,1,2,\ldots,11\}$ which are relatively prime to 12. Here we just check:

$$\begin{array}{lll} \gcd(0,12) = 12, & \gcd(1,12) = 1, & \gcd(2,12) = 2, \\ \gcd(3,12) = 3, & \gcd(4,12) = 4, & \gcd(5,12) = 1, \\ \gcd(6,12) = 6, & \gcd(7,12) = 1, & \gcd(8,12) = 4, \\ \gcd(9,12) = 3, & \gcd(10,12) = 2, & \gcd(11,12) = 1. \end{array}$$

Hence, $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, and $\varphi(12) = 4$.

We now state a couple of simple results about $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 12.7. *Let n be a positive integer.*

(1) *If $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. [I.e., the product of two units of $\mathbb{Z}/n\mathbb{Z}$ is also a unit.]*

(2) *Let $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. We then have that $\overline{k} \cdot \overline{a} = \overline{k} \cdot \overline{b}$ if, and only if, $\overline{a} = \overline{b}$. [I.e., we can "cancel units".]*

Before proving the proposition, we should make a quick remark about its second item: it is not necessary true that $\overline{k} \cdot \overline{a} = \overline{k} \cdot \overline{b}$ implies that $\overline{a} = \overline{b}$ [i.e., we can cancel $\overline{k}$] when $\overline{k}$ is not a unit! For example, in $\mathbb{Z}/4\mathbb{Z}$, we have that $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$, and also $\overline{2} \cdot \overline{0} = \overline{0}$. So, we have $\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0}$, but $\overline{2} \neq \overline{0}$ [as 4 does not divide $2 = 2 - 0$], i.e., we *cannot* cancel the $\overline{2}$ [in $\mathbb{Z}/4\mathbb{Z}$]. [Observe that $\overline{2}$ is not a unit of $\mathbb{Z}/4\mathbb{Z}$, as $\gcd(2, 4) = 2 \neq 1$.]

Proof of Proposition 12.7. Suppose that $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then, by definition, both are divisors of $\overline{1}$. So, there are $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{x} \cdot \overline{a} = \overline{xa} = \overline{1}$ and $\overline{y} \cdot \overline{b} = \overline{yb} = \overline{1}$. Then, $\overline{xy} \cdot \overline{ab} = \overline{xa} \cdot \overline{yb} = \overline{1} \cdot \overline{1} = \overline{1}$. Then, $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since, $\overline{a} \cdot \overline{b} = \overline{ab}$, we have that $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, proving item 1.

Now suppose that $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. Since $\overline{k}$ is a unit, there is $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\overline{xa} = 1$. If $\overline{k} \cdot \overline{a} = \overline{k} \cdot \overline{b}$, then $\overline{x} \cdot \overline{k} \cdot \overline{a} = \overline{x} \cdot \overline{k} \cdot \overline{b}$, and so $\overline{1} \cdot \overline{a} = \overline{1} \cdot \overline{b}$, and thus $\overline{a} = \overline{b}$.

Note that the converse, i.e., if $\overline{a} = \overline{b}$, then $\overline{k} \cdot \overline{a} = \overline{k} \cdot \overline{b}$ is true even if $\overline{k}$ is not a unit. [In fact, we just used that above, when we multiplied an equation by $\overline{x}$.] □

Here is a beautiful theorem due to Euler which allows us to compute powers of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ more efficiently.

Theorem 12.8 (Euler)**.** *If $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{k}^{\varphi(n)} = \overline{1}$.*

Proof. [This is likely the most ingenious proof on these notes!] Let's write, to make the notation simpler, $m = \varphi(n)$. Then, $(\mathbb{Z}/n\mathbb{Z})^\times$ has m elements [by definition of φ], and we can label them as:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m\}.$$

Multiplying all these elements by $\overline{k}$, we have:

$$\overline{k} \cdot (\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \cdot \overline{a}_1, \overline{k} \cdot \overline{a}_2, \ldots, \overline{k} \cdot \overline{a}_m\}.$$

What can we say about this set $\overline{k} \cdot (\mathbb{Z}/n\mathbb{Z})^\times$? First, by Proposition 12.7(1), we have that all $\overline{k} \cdot \overline{a}_i$ are units. Second, by Proposition 12.7(2), if $\overline{a}_i \neq \overline{a}_j$, then $\overline{k} \cdot \overline{a}_i \neq \overline{k} \cdot \overline{a}_j$ [for if $\overline{k} \cdot \overline{a}_i = \overline{k} \cdot \overline{a}_j$, we could cancel $\overline{k}$ obtaining $\overline{a}_i = \overline{a}_j$].

Hence, all elements $\overline{k} \cdot \overline{a}_i$'s are distinct, which means that $\overline{k} \cdot (\mathbb{Z}/n\mathbb{Z})^\times$ has m elements [which is the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$] and it is contained in $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore we have that $\overline{k} \cdot (\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, and $\{\overline{k} \cdot \overline{a}_1, \overline{k} \cdot \overline{a}_2, \ldots, \overline{k} \cdot \overline{a}_m\}$ is just a reordering of $\{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m\}$. [See Example 12.9 below for a concrete example.]

So, if we multiply all elements of $(\mathbb{Z}/n\mathbb{Z})^\times$, we get some element of $\mathbb{Z}/n\mathbb{Z}$, say $\overline{b}$:

$$\overline{a}_1 \cdot \overline{a}_2 \cdots \overline{a}_m = \overline{b}.$$

What happens if we multiply all elements of $\overline{k} \cdot (\mathbb{Z}/n\mathbb{Z})^\times$? On the one hand, we are multiplying exactly the same elements in a different order, so we get $\overline{b}$ again. On the other hand, if we collect all the $\overline{k}$'s, we get:

$$(\overline{k} \cdot \overline{a}_1) \cdot (\overline{k} \cdot \overline{a}_2) \cdots (\overline{k} \cdot \overline{a}_m) = \overline{k}^m \cdot (\overline{a}_1 \cdot \overline{a}_2 \cdots \overline{a}_m) = \overline{k}^m \cdot \overline{b}.$$

Since the same product results in $\overline{b}$ and in $\overline{k}^m \cdot \overline{b}$, these must equal, i.e., $\overline{k}^m \cdot \overline{b} = \overline{b}$. But, since $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ [which follows from Proposition 12.7(1), as $\overline{b}$ is a product of units], we can cancel $\overline{b}$ [by Proposition 12.7(2)] to obtain $\overline{k}^m = \overline{1}$, which is what we needed to prove. □

Example 12.9. Here we look how the proof above works in a particular example. Take, for instance, $n = 5$ and $\overline{k} = \overline{3}$. Then,

$$\begin{aligned}\overline{3} \cdot (\mathbb{Z}/5\mathbb{Z})^\times &= \{\overline{3} \cdot \overline{1}, \overline{3} \cdot \overline{2}, \overline{3} \cdot \overline{3}, \overline{3} \cdot \overline{4}\} \\ &= \{\overline{3}, \overline{1}, \overline{4}, \overline{2}\},\end{aligned}$$

so, it is indeed just a reordering of $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Now, let's find the product of all terms in $(\mathbb{Z}/5\mathbb{Z})^\times$:

$$\begin{aligned}\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} &= \overline{1} \cdot \overline{2} \cdot \overline{-2} \cdot \overline{-1} \\ &= \overline{4} = \overline{-1}.\end{aligned}$$

So, since we are just changing the order, we have:

$$\begin{aligned}(\overline{3} \cdot \overline{1}) \cdot (\overline{3} \cdot \overline{2}) \cdot (\overline{3} \cdot \overline{3}) \cdot (\overline{3} \cdot \overline{4}) &= \overline{3} \cdot \overline{1} \cdot \overline{4} \cdot \overline{2} \\ &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \\ &= \overline{-1},\end{aligned}$$

while when collecting the $\overline{3}$'s together we obtain

$$\begin{aligned}(\overline{3} \cdot \overline{1}) \cdot (\overline{3} \cdot \overline{2}) \cdot (\overline{3} \cdot \overline{3}) \cdot (\overline{3} \cdot \overline{4}) &= \overline{3}^4 (\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4}) \\ &= \overline{3}^4 \cdot \overline{-1}.\end{aligned}$$

But since those represent exactly the same product, only performed in different orders [which do not matter anyway], we must have $\overline{3}^4 \cdot \overline{-1} = \overline{-1}$, and thus $\overline{3}^4 = \overline{1}$ [by canceling the $\overline{-1}$].

[Of course, we did not have to work this hard to check that $\overline{3}^4 = \overline{1}$, we could just check it, as $\overline{3}^4 = \overline{3^4} = \overline{81} = \overline{1}$. The point here is really to illustrate how the proof works.]

In the example above we saw that

$$\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} = \overline{-1} \qquad \text{in } \mathbb{Z}/5\mathbb{Z}.$$

This is in fact true for all *primes*, i.e., if p is a prime, then we have

$$\overline{1} \cdot \overline{2} \cdots \overline{p-2} \cdot \overline{p-1} = \overline{-1} \qquad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

This result is called *Wilson's Theorem*. Its proof is not difficult, but since it is not important to our application in cryptography, we shall omit it.

Now, observe that *Euler's Theorem* gives us a quick way to compute powers in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example 12.10. Let's compute $\overline{5}^{1001}$ in $\mathbb{Z}/12\mathbb{Z}$. If we were to compute 5^{1001}, it would take a lot of time [we have to perform a thousand products!] and the resulting number [before computing the remainder when divided by 12] would be *huge*! [It has 700 digits!] So, we do it in a smarter way.

Since $\gcd(5,12)=1$, we have that $\overline{5}\in(\mathbb{Z}/12\mathbb{Z})^\times$. As we have seen in Example 12.6, we have that $\varphi(12)=4$, and therefore *Euler's Theorem* tells us that $\overline{5}^4=\overline{1}$.

Now, we have that the division algorithm gives us that $1001=250\cdot 4+1$. Therefore,

$$\begin{aligned}
\overline{5}^{1001} &= \overline{5}^{250\cdot 4+1} \\
&= \overline{5}^{250\cdot 4}\cdot\overline{5}^{1} && [\text{as } a^{x+y}=a^x\cdot a^y] \\
&= (\overline{5}^4)^{250}\cdot\overline{5} && [\text{as } a^{x\cdot y}=(a^x)^y] \\
&= \overline{1}^{250}\cdot\overline{5} && [\text{as } \overline{5}^4=\overline{1}] \\
&= \overline{5}.
\end{aligned}$$

The example above contains the idea of the proof of the following:

Corollary 12.11. *Let $\overline{k}\in(\mathbb{Z}/n\mathbb{Z})^\times$ and m be an integer. If the remainder of m when divided by $\varphi(n)$ is r, then $\overline{k}^m=\overline{k}^r$.*

[We called it a corollary as it is an almost immediate consequence of Euler's Theorem above.]

We need one more result before applying these concepts to cryptography.

Proposition 12.12. *Let p and q be two* distinct *primes. Then, $\varphi(p\cdot q)=(p-1)\cdot(q-1)$ [where φ is the Euler phi function].*

Proof. We need to count how many elements in $\{1,2,3,\dots,pq\}$ are relatively prime to pq. Since this set has pq elements, we can also how many are *not* relatively prime to it, and subtract this number from pq [the total number of elements in the set]. [This is the same as if you want to see how many people are married in a group of say, 5 people. If you find out the exactly 2 people are *not* married, then we must have $5-2=3$ people married.]

If k is not relatively prime to pq, it must have a common divisor greater than one. But, since p and q are primes, the only divisors of pq which are greater than one are p, q, and pq itself. Hence, if k is *not* relatively prime to pq, then it is divisible by either p or q [or both].

So, let's take out the multiples of p from $\{1,2,3,\dots,pq\}$. How many of those do we have? Well, it should be clear that they are $\{p,2p,3p,\dots,qp\}$, and thus we have q of those. Now, in the same way, we have that the multiples of q in that set are $\{q,2q,3q,\dots,pq\}$, and we have p of those. By the remarks in the previous paragraph, taking out both multiples of p and q leaves only the terms which are relatively prime to pq.

So, at first one might think that the number of elements of $\{1,2,\dots,pg\}$ which are relatively prime to pq [which is the $\varphi(pq)$ which we are looking for] is $pg-q-p$ [i.e., the total number, minus multiples of p, minus multiples of p]. But there is a catch! If there are elements that are multiples

of both p and q, we are "taking it out twice": once when we take out multiples of p and again when we take out multiple of q. [See Example 12.13 below to see how it goes in a concrete example.] But, since p and q are *distinct* [by assumption], we have that the first element which is divisible by both p and q is pq [since both p and q should appear in the decomposition of this number as products of primes], and hence this is the only one that we took out twice [while we should have taken out only once]. To compensate for this, we have to only take out $(p-1)$ instead of p multiples of q [as pq has been taken out already], giving

$$\varphi(pq) = pq - q - (p-1) = (p-1)(q-1),$$

as we needed to prove. □

Let's again illustrate how this prove works with a concrete example:

Example 12.13. Let's compute $\varphi(15)$. Now, $15 = 3 \cdot 5$, and 3 and 5 are primes. Let's cross out number in the list

1,	2,	3,	4,	5,
6,	7,	8,	9,	10,
11,	12,	13,	14,	15,

which are not relatively prime to 15. These must be multiples of 3 or multiples of 5. Let's cross out the multiples of 5 first:

1,	2,	3,	4,	~~5~~,
6,	7,	8,	9,	~~10~~,
11,	12,	13,	14,	~~15~~.

This leaves $15 = 3 = 12$ elements left. Now, let's cross out multiples of 3:

1,	2,	~~3~~,	4,	~~5~~,
~~6~~,	7,	8,	~~9~~,	~~10~~,
11,	~~12~~,	13,	14,	~~15~~.

This seems to take out another 5 elements, but 15 was already out [it's the only one crossed twice], so we actually subtract only 4. So, $\varphi(15) = 15 - 3 - 4 = 8 = (3-1) \cdot (5-1)$.

There is a general formula for $\varphi(n)$ that can be used when we know how n factors as product of primes. If $n = p_1^{r_1} \cdots p_k^{r_k}$, then

$$\varphi(n) = \varphi(p_1^{r_1} \cdots p_k^{r_k}) = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_k - 1)p_k^{r_k - 1}. \tag{12.14}$$

But remember that, as we mentioned before, it's sometimes difficult to factor a [very large] number. Again, since we won't need this general formula, but only the particular case of Proposition 12.12, we won't prove it here.

Problems.

12.1) Find $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n = 13, 18, 36$.

12.2) Compute $\varphi(n)$ for $n = 36, 131, 1457$. [**Hint:** 131 is prime and $1457 = 31 \cdot 47$.]

12.3) Compute:

(a) $\overline{6}^{1000}$ in $\mathbb{Z}/7\mathbb{Z}$.

(b) $\overline{31}^{12}$ in $\mathbb{Z}/36\mathbb{Z}$.

(c) $\overline{3}^{4}$ in $\mathbb{Z}/12\mathbb{Z}$.

(d) $\overline{7}^{4632726732}$ in $\mathbb{Z}/11\mathbb{Z}$.

13. The RSA Cryptosystem

We've already briefly mentioned what cryptography means in section 9. Again, the idea is to send a secret messages in a secure way: a person who can somehow obtain this message should not be able to read it unless he possesses some extra information, usually called the *decoding key*, on how to decode it.

One can think of many ways to do this, and it's been done since ancient times. One of the most natural ways is the *Caesar Cipher*: you just permute the letter in some random way. Say, replace `A` by `T`, `B` by `S`, `C` by `K`, etc. [There is no pattern in my example. You just have to be careful to not replace two different letters by the same one.] This is flawed, as one can break with some statistical analysis of the message: if the message is long enough [or if someone obtains enough messages] one can look for the letter the appears the largest number of times. Since the letter that shows up more often in English is `E`, one could guess that this letter is `E`. And, since one can find what are the most common letters, one can start to break this code. The ones who have seen the 1983 movie *"A Christmas Story"*, written by Jean Shepherd and directed by Bob Clark, might remember that the main character, Ralph, uses a decoder pin from the *Orphan Annie's Secret Society* to decode secret messages from its radio show. That was a Caesar's Cipher and the pin just gave the correct replacement of the letters.

There are other ways of doing it. One might, for instance, use a *Block Cipher*, where you replace say, a set of two letters instead of a single letter. For instance, replace `AA` by `RT`, `AB` by `XI`, `AC` by `YQ`, etc. [Again, there is no patter here.] This makes it much harder, but still one can try statistical analysis. Moreover, it becomes much more difficult to encode and decode messages. [The conversion table has $26^2 = 676$ entries instead of 26.]

And, of course, there are many other ways. But let's think of one particular problem: sending your credit card over the Internet. It's widely known that the Internet is not safe, as communications can be intercepted. So, you need some strong method to keep your credit card number secure. Suppose

that the merchant actually has a such a method. He needs to tell you how to encode your message so that you can send your number safely. The problem with many methods, including the two mentioned above, is that if one knows how to encode, then he/she also knows how to decode it. So, if you intercepted some other customer's encoded credit card number to this merchant, you'd be able to decode it. Well, it might not be too difficult, depending on the method, for the merchant to come up with a different encoding system for each customer, and this might seem to solve the problem. But there is another catch! Remember that the merchant needs to tell you how to encode. How is he going to do that? He cannot send you encoded, as the two of you haven't agreed on a method yet, and if some one is reading your communications, this person might get both the encoding method, which gives the decoding method also, and your encoded credit card number. Hence, he will have access to your correct credit card number.

The way to fix this would be to have an encoding method, or *encoding key*, that does not give away the decoding method, or decoding key. Then, the merchant could tell the whole world how to send him credit card numbers, by making the encoding key available to all, but still only he would be able to decode the information, by keeping the decoding key secret. This is called *Public Key Cryptography*.

We shall now describe one such method: the RSA Cryptosystem. The name RSA comes from the last names of the people who first described it in 1977: Ron Rivest, Adi Shamir, and Leonard Adleman. [Apparently, another mathematician, named Clifford Cocks, found this method in 1973, but it was classified by the British government, and hence it was not known. In fact this was only announced in 1997.]

We will describe the basic method now.

(1) The merchant chooses two very large primes, say p and q. [See some comments below about some restrictions that should be made this choice.] Then, compute the product and call it n. [I.e., $n = pq$.] The number n will be made public, but p and q must remain secret!
(2) The merchant now computes also $\varphi(n)$. By Proposition 12.12, this number is simply $(p-1)(q-1)$. Then, he choose some integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n))$. [See some comments on some restrictions on this choice below.] If p and q are chosen well, it's quite likely that random guesses of e will automatically satisfy $\gcd(e, \varphi(n)) = 1$.
(3) When checking that $\gcd(e, \varphi(n)) = 1$, the merchant uses the EEA to find $x, y \in \mathbb{Z}$ such that $xe + y\varphi(n) = 1$. Let d be the remainder of the division of x by $\varphi(n)$.
(4) The merchant makes available the numbers e and n [while, p, q, $\varphi(n)$, x, and d are all kept secret!], and tells his customer that to send their credit card number, say m, they should send him the result of $\overline{m}^{\,e}$ in $\mathbb{Z}/n\mathbb{Z}$. Here it is necessary that the number m is less than n. [We will discuss how we can deal with larger numbers below.]
(5) The merchant receives the result, i.e., the encoded credit card number, say $\overline{r}$. [So, $\overline{r} = \overline{m}^{\,e}$, but he cannot see $\overline{m}$, only $\overline{r}$. The number m is what he needs to find.] To get m, he

computes $\overline{r}^{\,d}$, as $\overline{m} = \overline{r}^{\,d}$. Since $1 \leq m < n$, if we know $\overline{m}$, we know m. [Since d is secret, no one knows how to decode $\overline{r}$.]

Why does this work? In other words, why $\overline{r}^{\,d} = \overline{m}$? We have:

$$\overline{r}^{\,d} = (\overline{m}^{\,e})^d = \overline{m}^{\,de} \qquad [\text{as } \overline{r} = \overline{m}^{\,e} \text{ and } (a^x)^y = a^{x\cdot y}].$$

But also, the remainder of de when divided by $\varphi(n)$ is 1: first, we can write [by the division algorithm] $x = k\varphi(n) + d$. Now, replacing x by this formula in the equation from item 3 above, we obtain

$$1 = (k\varphi(n) + d)e + y\varphi(n) = (k + y)\varphi(n) + de.$$

So, $de = (-k - y)\varphi(n) + 1$, and thus, by the uniqueness in the division algorithm, we must have that the remainder of de when divided by $\varphi(n)$ is indeed 1. Thus, by Corollary 12.11, we have that $\overline{m}^{\,de} = \overline{m}^{\,1} = \overline{m}$. Hence, $\overline{r}^{\,d} = \overline{m}$.

We need to make an observation here: we've used Corollary 12.11 above, and this would require m to be relatively prime to $n = pq$, so we would need that neither p nor q divides m. The actual probability of either happening in practice is relatively small, but in fact this computation also *does* work in those cases, as still $\overline{m}^{de} = \overline{m}$ when $\overline{m}$ is not a unit, even thought it does not follow directly from the corollary anymore. [The key fact here is that n is a product of two distinct primes.] The proof that it still works is in fact simple, but we shall omit it here to not stretch the discussion too much.

Let's see an example:

Example 13.1. We will use small primes just to keep the numbers easy. Let's pretend we are the merchant here. We choose, say, $p = 23$ and $q = 37$. Then, we compute n, which is $n = 23 \cdot 37 = 851$ and $\varphi(n) = 22 \cdot 36 = 792$.

Now, we need to choose e. We can try $e = 7$. Then, the EEA gives us that the GCD is 1 and:

$$1 = (-113) \cdot 7 + 1 \cdot 792$$

So, since the GCD is 1, the choice works and we have $x = -113$. We then find d as the remainder of the division of -113 by $\varphi(n)$ [i.e., by 792 in this case], and so $d = 679$.

Say that some one now wants to send us a secret number, say 311. The person needs to compute $\overline{311}^{\,7}$ in $\mathbb{Z}/851\mathbb{Z}$. The result is $\overline{775}$. So, the person sends us that.

When we receive the $\overline{775}$, we compute the d-th power, i.e., $\overline{775}^{\,679}$, obtaining $\overline{311}$, and so we know that the number sent was 311.

Of course the primes used in the example are *way* too small for real application in encryption. The security of this system is based on the difficulty on factoring n. Indeed, if one factors n, i.e., finds the primes p and q such that $n = pq$, then one can compute $\varphi(n)$, and then compute d. With such small numbers a computer can factor in less than a hundredth of a second! But, observe that even with such small numbers, we had to compute $\overline{775}^{\,679}$ in $\mathbb{Z}/851\mathbb{Z}$. [Note that since $1 < 679 < \varphi(n) = 792$,

Corollary 12.11 does not help with this computation.] The naive way of doing this would be to compute 678 products. Using a method called *Successive Squares Exponentiation*, one can compute that power with only 19 [or less] products! If there were no fast way to compute exponents, this method would be too time consuming to actually be used in real life.

One should also observe that many of the other computations in this process, such as division algorithm and extended Euclidean algorithm, are fast [when using a computer], even with huge numbers.

The part of the process that take the longest is finding the primes p and q. Even though primality testing is *much* faster than factorization, it might take a few minutes, perhaps even hours, depending on the size of the numbers with which you are dealing. Usually probabilistic algorithms are used, which can give numbers that are *likely* prime, with a probability over 99.99% or more if you need, quite quickly [in relative terms].

Here are some important considerations on the choices made in this method. If any of these are not satisfied, there are some specific methods for someone to find the private key.

(1) The primes p and q should be generated in a random manner, so that they don't become predictable.
(2) In order to make the factoring of $n = pq$ take long enough for the key to be secure, the primes p and q should be greater than 2^{1024}, and some suggest that they should be greater than 2^{2048}. [The sizes can be smaller if you change your keys frequently, as it would take, at the very least, a few months to factor n if the primes are larger than 2^{1024}.] For truly high security, it is suggested to use primes larger than 2^{4096}. [Note that 2^{4096} has 1233 digits!]
(3) The primes p and q should not be [relatively] close to each other. For instance, if $p < q$, then you need that $q - p > 2\sqrt[4]{pq}$, and you'd probably want it much larger than that.
(4) Neither $(p-1)$ nor $(q-1)$ should have only small primes in their prime factorization.
(5) The private key d should not be small. At the very least it should be larger than $\sqrt[4]{n}/3$.
(6) It's suggested to add some *padding* to the message. In a text message this can be done by adding some white spaces or phrase like "The message starts here." and "The message ends here." The point is to not let the number to be sent be too small. Therefore, anything that adds something to the message that does not interfere with the reading can be added. [We talk about how to deal with texts rather than numbers below.]
(7) With padding, there is no known problem with taking e small, but apparently people are reluctant to do so, and $e = 65537$ is a common choice.

One other thing we should observe: as stated we need that the number to be sent, say m, should be less than n. What if we need to send a number larger than n? One just break it into pieces. One can always write m as

$$m = m_0 + m_1 \cdot n + m_2 \cdot n^2 + \cdots + m_k \cdot n^k, \quad \text{with } 0 \leq m_0, m_1, \ldots, m_k < n \tag{13.2}$$

[for some k large enough], where each m_i is an integer in $\{0, 1, 2, \ldots, (n-1)\}$, in a *unique way*. The method of doing this is simple enough: m_0 is the remainder of m when divided by n, m_1 is the remainder of $(m - m_0)/n$ [which is an integer] when divided by n, m_2 is the remainder of $(m - m_0 - m_1 \cdot n)/n^2$ [which is an integer] when divided by n, m_3 is the remainder of $(m - m_0 - m_1 \cdot n - m_2 \cdot n^2)/n^3$ [which is an integer] when divided by n, and so on until we obtain a difference

$$m - (m_0 + m_1 \cdot n + m_2 \cdot n^2 + \cdots + m_k \cdot n^k)$$

which is zero. [This is to put m on *base* n.]

Example 13.3. We will use the same data as Example 13.1, except that now someone wants to send us the number $m = 1745291$. First, as $1745291 > 851$, it needs to be broken as described above:

$$1745291 = 741 + 348 \cdot 851 + 2 \cdot 851^2.$$

So, $m_0 = 741$, $m_1 = 348$, and $m_3 = 2$. So, the person should send the three values [in $\mathbb{Z}/851\mathbb{Z}$] $\overline{741}^{\,7} = \overline{408}$, $\overline{348}^{\,7} = \overline{738}$, and $\overline{2}^{\,7} = \overline{128}$, in that order. [Note that some padding should be used in practice to avoid small numbers like the $\overline{2}$ above.] We can then decode each piece with the private key and put them together again to obtain the original number.

Now, how does one send texts instead of number? One can use the *American Standard Code for Information Interchange* (ASCII) to replace characters with numbers. This particular method represents 256 different characters, including letters [lower and upper case], numbers, brackets, punctuation, and other symbols, by numbers from 0 to 255. [See `http://www.asciitable.com/`, for instance.] For instance, the ASCII code for `A` is 65, for `B` is 66, and so on. Then, let's say you have a text with k characters, with ASCII codes $m_1, m_2, \ldots, m_k$ respectively. To convert this to a single number, we use Formula (13.2) again, with $n = 256$ [the number of different ASCII values], i.e., we use the number m defined by:

$$m = m_0 + m_1 \cdot 256 + m_2 \cdot 256^2 + \cdots + m_k \cdot 256^k.$$

When decoding, we receive m and break it as above, then finding the m_i's, which we can then translate to characters using the ASCII table.

Example 13.4. Let's do a simple example now using the data of Example 13.1, but say some wants to send us the text `YES`. The ASCII codes for the letters are 89, 69, and 83 respectively. So, this text leads to the number

$$m = 89 + 69 \cdot 256 + 83 \cdot 256^2 = 5457241.$$

Since $m > 851 = n$, this has to be broken in parts as in the previous example:

$$5457241 = 629 + 455 \cdot 851 + 7 \cdot 851^2.$$

Then, the person should send us the three values $\overline{629}^{\,7} = \overline{518}$, $\overline{455}^{\,7} = \overline{788}$, and $\overline{7}^{\,7} = \overline{626}$.

Example 13.5. Let's see an example on decoding, again with $n = 851$, $e = 7$, and $d = 679$. Suppose we receive 686, 737, 84, and 1 in this order. We first find the number using the private key: $\overline{686}^{679} = \overline{405}$, $\overline{737}^{679} = \overline{599}$, $\overline{84}^{679} = \overline{824}$, and $\overline{1}^{679} = \overline{1}$ [which in real applications should have been avoided with the use of some padding]. So, the *number* sent was:

$$m = 405 + 599 \cdot 851 + 824 \cdot 851^2 + 1 \cdot 851^3 = 1213546829$$

Now, let's recover the text using the ASCII code. We have that

$$1213546829 = m = 77 + 65 \cdot 256 + 85 \cdot 256^2 + 72 \cdot 256^3.$$

So, the message is a four letter word with codes 77, 65, 85, and 72. These are the ASCII codes for the letters `M`, `A`, `T`, and `H`, and thus the text sent was `MATH`.

We finish this text with a few remarks on the security of the RSA cryptosystem. As we have already pointed out, it depends exclusively on the difficulty in factoring numbers which are products of two very large primes. But why is this problem difficult? Well, the truth is that we think it is difficult because no one could find a quick way of doing it so far [which does not mean that there isn't one]. Thus, perhaps some one will come up with a new and smart way of doing it tomorrow, and this method will not be secure anymore. [By the way, this RSA method *is* used in the real world. This is not just something theoretical!] Although it seems that this would be unlikely, it could happen. So, there is no real guarantee it this method will be safe in the future.

On the other hand, it is likely [although not certain] that only a professional mathematician could come up with a better way to factor these numbers. It would be a true accomplishment, and hence this person, likely being an academic, would welcome all the praise and recognition that would come from it. Thus, this result would be immediately made public [as maybe someone will do it before you if you wait], at which point every one who uses the RSA method should move to another one. [There are many different public key cryptosystems whose security would not be compromised by a fast factorization algorithm.] So, attaching the security of a cryptosystem to a famous math problem has two advantages: solving this problem [and hence breaking the code] should be *truly difficult* [or some would have done it] and you will *know* when the method is not secure anymore.

14. Solutions

1.1) (a): T, (b): F, (c): F, (d): T, (e): F, (f): T, (g): F, (h): F, (i): F, (j): T.

2.1) (a): quotient: 61; remainder: 4.
(b): quotient: 3; remainder: 216.
(c): quotient: 0; remainder: 364.
(d): quotient: 615; remainder: 8.

2.2) (a): dividend: 4567; divisor: 31; quotient: 115; remainder: 2.
(b): dividend: 423; divisor: 42; quotient: 10; remainder: 3, or dividend: 423; divisor: 10; quotient: 42; remainder: 3.

(c): dividend: 423; divisor: 21; quotient: 20; remainder: 3, or dividend: 423; divisor: 20; quotient: 21; remainder: 3.

2.3) (a): quotient: 3; remainder: 2.

(b): quotient: -2; remainder: 3.

2.4) quotient: 235819; remainder: 136.

3.1) (a): False. We use Theorem 3.1 and observe that $3 \mid (3 \cdot 3262)$ and $3 \nmid 2$. So, $3 \nmid (3 \cdot 3262 + 2)$.

(b): True. We use Theorem 3.1 again and observe that $7 \mid (14 \cdot 407)$ [since $7 \mid 14$ and $14 \mid (14 \cdot 407)$, we can conclude that $7 \mid (14 \cdot 407)$] and $7 \mid 21$. So, $7 \nmid (14 \cdot 407 - 21)$.

3.2) Yes! By Theorem 3.1, we have that $d \mid (a + b)$, since $d \mid a$ and $d \mid b$. Now, we have that $d \mid (a + b)$ and $d \mid c$, and we apply the same theorem again, obtaining that $d \mid ((a + b) + c) = (a + b + c)$.

3.3) (a): Yes! They said it would not rain, for if they said it would, by the above statement, it would have rained.

(b): No! The statement does not say what happens if they say it will not rain. In that case, it might rain or not. So, they might have said it would rain or they might have said it wouldn't.

(c): No! The statement does not say anything about what happens if the forecast says it will not rain.

4.1) (a): 2: yes; 3: yes; 5: yes; 6: yes; 9: yes; 10: yes.

(b): 2: no; 3: yes; 5: no; 6: no; 9: no; 10: no.

(c): 2: no; 3: no; 5: no; 6: no; 9: no; 10: no.

(d): 2: no; 3: no; 5: yes; 6: no; 9: no; 10: no.

4.2) (a) Since $3 \mid (3 \cdot 7483837283)$ and, using the criterion for divisibility by 3 we can see that $3 \nmid 94957291$, by Theorem 3.1, we have that $3 \nmid (3 \cdot 7483837283 + 94957291)$.

(b) Since $5 \mid 743872835$ [since it ends with 5] but $5 \nmid 90472638231$ [since it does not end with 0 or 5], Theorem 3.1 tell us that $5 \nmid (743872835 + 90472638231)$.

4.3) We have that a number is divisible by 15 if, and only if, it is divisible by both 3 and 5.

5.1) (a): 6. (b): 1.

5.2) 11100.

6.1) (a): $x = -9$ and $y = 7$.

(b): $x = 20$ and $y = -27$.

6.2) 9.

7.1) (a): No, as $3 \mid 111$. (b): No, as $7 \mid 259$. (c): Yes, it is prime. (d): Yes, it is prime.

7.2) No, as by Theorem 7.6, if it were prime, then either $d \mid a$ or $d \mid b$.

7.3) (a): $90 = 2 \cdot 3^2 \cdot 5$. (b): $231 = 3 \cdot 7 \cdot 11$. (c): $875 = 5^3 \cdot 7$. (d): $1573 = 11^2 \cdot 13$.

8.1) (a) $\gcd(81, 90) = 3^2 = 9$, and $\text{lcm}(81, 90) = 2 \cdot 3^4 \cdot 5 = 810$. (b): the GCD is $2 \cdot 3 \cdot 11$ and the LCM is $2^2 \cdot 3^3 \cdot 5 \cdot 11^3$.

8.2) (a); False. (b): True. (c): True.

8.3) $a \cdot b = 6 \cdot 18 = 108$.

8.4) No, since the GCD must divide the LCM [as, for instance, the GCD divides a, and a divides the LCM], and $12 \nmid 30$.

9.1) By Theorem 9.1, there are infinitely many solutions in the case $x^2 + y^2 = z^2$. By *Fermat's Last Theorem*, there is no solution $x, y, z \in \mathbb{N}^*$ for $x^5 + y^5 = z^5$, since the only solutions involve zero [and $0 \notin \mathbb{N}^*$].

9.2) 7 cannot be written as a sum of three integers. But Theorem 9.3 tells us that all positive integers can be indeed written as sum of four integers. Then, all positive integers can also be written as sum of five integers, as we can take one them to be zero.

9.3) (a) $81 = 9^2 + 0^2 + 0^2 + 0^2$. (b) $12 = 3^3 + 1^2 + 1^2 + 1^2$. (c) $53 = 7^2 + 2^2 + 0^2 + 0^2$. (d) $105 = 10^2 + 2^2 + 1^2 + 0^2$.

9.4) Yes, since there are infinitely many primes, there must be a prime larger than a million [otherwise there would be at most a million primes].

9.5) You could just copy the statement from Conjecture 9.7. [The point is to make sure you remember these statements.] It is: *"There are infinitely many primes p such that $p + 2$ is also prime."*

9.6) (a): $36 = 5 + 31$. (b): $50 = 3 + 47$.

9.7) (a) Since all the numbers are even, and none of them is 2, there is no prime in the sequence.

(b) We use Theorem 9.9: since $\gcd(22, 3) = 1$, we have that there are infinitely many primes in this sequence.

(c) We have that 3 is prime, and since all numbers are multiples of 3, there is only one prime in the sequence.

11.1) (a): True, as $3 - (-11) = 14$ is divisible by 7. [We are using Lemma 11.4 here.]

(b): False, as $8 \nmid 14 = 3 - (-11)$.

(c): False. There are many ways to do it, but here is a smart one: observe that $3 \mid 9303$ [use, for instance the criterion from Section 4, or just observe that $9303 = 3 \cdot 3101$]. Then, $\overline{9303} = \overline{0}$. Also, $3 \nmid 21821$ [use the criterion from Section 4 again] and thus $\overline{21821} \neq \overline{0} = \overline{9303}$.

(d) True. We reduce the numbers to actual remainders, as the remainder of the division by 5 is easy. We have that $\overline{43847833} = \overline{4384783 \cdot 2 \cdot 5 + 3} = \overline{3}$, and $\overline{8437898} = \overline{843789 \cdot 2 \cdot 5 + 8} = \overline{8} = \overline{3}$. So, they are equal as both are $\overline{3}$.

11.2) (a) $\overline{7} + \overline{8} = \overline{15} = \overline{6}$.

(b) $\overline{7} \cdot \overline{8} = \overline{56} = \overline{1}$.

(c) $\overline{24} \cdot \overline{13} = \overline{-1} \cdot \overline{3} = \overline{-3} = \overline{2}$.

(d) Using the criterion from Section 4 again, we see that $\overline{369303} = \overline{0}$, and so $\overline{369303} \cdot \overline{172647183} = \overline{0} \cdot \overline{172647183} = \overline{0}$.

(e) $(\overline{2} + \overline{5}) \cdot \overline{7}^2 = \overline{7} \cdot \overline{7}^2 = \overline{7}^3 = \overline{-1}^3 = \overline{(-1)^3} = \overline{-1} = \overline{7}$.

(f) $(\overline{31} - \overline{44}) \cdot (\overline{33} + \overline{-13}) = (\overline{3} - \overline{2}) \cdot (\overline{5} + \overline{1}) = \overline{1} \cdot \overline{6} = \overline{6}$.

12.1) For $n = 13$ we can use the comments of Example 12.5 [as 13 is prime], and so

$$(\mathbb{Z}/13\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \ldots, \overline{10}\}.$$

For $n = 18 = 2 \cdot 3^2$, we need to exclude the multiples of 2 and 3. Hence, we get

$$(\mathbb{Z}/18\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}.$$

For $n = 36 = 2^2 \cdot 3^2$, we also need to exclude the multiples of 2 and 3. Hence, we get

$$(\mathbb{Z}/36\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, , \overline{35}\}.$$

12.2) For $n = 36$ we can use the previous problems and obtain $\varphi(36) = 12$.

Since 131 is prime, the comments in Example 12.5 tells us that $\varphi(131) = 131 - 1 = 130$.

Since 31 and 47 are primes, Proposition 12.12 tells us that $\varphi(1457) = \varphi(31 \cdot 47) = 30 \cdot 46 = 1380$.

12.3) (a) We can use Corollary 12.11, or just observe that $\overline{6}^{1000} = \overline{-1}^{1000} = \overline{(-1)^{1000}} = \overline{1}$.

(b) As we have seen in Problem 12.2, $\varphi(36) = 12$. Then, since $\gcd(31, 36) = 1$, by *Euler's Theorem* [i.e, Theorem 12.8], we have $\overline{31}^{12} = \overline{1}$.

(c) Note that although $\varphi(12) = 4$ [as seen in Example 12.6], we *cannot* use Euler's Theorem here, as $\gcd(3, 12) = 3 \neq 1$. Indeed, $\overline{3}^4 \neq \overline{1}$ in this case. We just really compute it $\overline{3}^4 = \overline{81} = \overline{9}$.

(d) We use Corollary 12.11, as $\gcd(7, 11) = 1$. We have that $\varphi(11) = 10$, and hence, the remainder of 4632726732 when divided by 10 is 2. [This is easy, as $4632726732 = 463272673 \cdot 10 + 2$.] So, $\overline{7}^{4632726732} = \overline{7}^2 = \overline{49} = \overline{5}$.

Index