# Lecture notes of Algebra. Week 2

## 4. The extended Euclidean algorithm in the integers

**4.1. The extended Euclidean algorithm.** The calculations done in the Euclidean algorithm on integers $a$ and $b$ can be read backwards and allow one to express their greatest common divisor $d = (a, b)$ *as linear combination of* $a$ *and* $b$ *(with integer coefficients),* meaning finding integers $x$ and $y$ such that $d = ax + by$. The fact that this is always possible is an important fact known as *Bézout's Lemma.*

LEMMA 7 (Bézout's Lemma). *Let* $a, b \in \mathbb{Z}$*, and let* $d = (a, b)$ *be their greatest common divisor. Then there exist* $x, y \in \mathbb{Z}$ *such that*

$$ax + by = d.$$

EXAMPLE. Recall the calculations of a previous example, where we applied the Euclidean algorithm to 391 and 299 to find $(391, 299) = 23$.

$$391 = 299 \cdot 1 + 92$$

$$299 = 92 \cdot 3 + 23$$

$$92 = 23 \cdot 4.$$

Working backwards through the above calculations we find

$$\begin{aligned} \mathbf{23} &= \mathbf{299} - \mathbf{92} \cdot 3 \\ &= \mathbf{299} - (\mathbf{391} - \mathbf{299} \cdot 1) \cdot 3 = -\mathbf{391} \cdot 3 + \mathbf{299} \cdot 4. \end{aligned}$$

Hence $d = (391, 299) = 391x + 299y$ with $x = -3$ and $y = 4$. In the calculation I have set the remainders in boldface in order to better distinguish them from the various coefficients involved. (It is not necessary to do so if one is tidy, but if you find it helpful in writing by hand you may them underline them, for example.)

Here is what we have done. We have started by writing the GCD 23 as a linear combination of the previous two remainders 299 and 92, using the division where 23 appears as the remainder. Then we have considered the smaller of those two remainders, which is 92, and using the previous division, where 92 appeared as the remainder, we have replaced it with a combination of 391 and 299. Now after simplification the GCD 23 has been expressed as linear combination of the remainders 391 and 299. We are done in this case, but in general we may continue, at each step getting rid of the lower of the two remainders in terms of which the GCD is expressed, at the expense of a the previous (larger) reminder, until we have expressed $d$ as a combination of $a$ and $b$.

It may be convenient (depending on preference) to arrange the calculations for the extended part of the algorithm next to the main part, but going up from the bottom, as

follows,

$$\begin{aligned}
391 &= 299 \cdot 1 + 92 && = \mathbf{299} - (\mathbf{391} - \mathbf{299} \cdot 1) \cdot 3 = -\mathbf{391} \cdot 3 + \mathbf{299} \cdot 4 \\
299 &= 92 \cdot 3 + 23 && \mathbf{23} = \mathbf{299} - \mathbf{92} \cdot 3 \\
92 &= 23 \cdot 4
\end{aligned}$$

In this way each line at the right-hand side uses exactly the result of the division to the left of it, and an extra calculation is done continuing on the same line.

Reading the calculations of the Euclidean algorithm backwards as in the example is sometimes called the *extended Euclidean algorithm* (which really includes the original part of the algorithm). Writing out the procedure in a formal general way (rather than just for specific numbers as in the example) actually provides a proof of Bézout's lemma. This would be an example of a *constructive proof,* as opposed to a *non-constructive proof* which merely proves the existence of $x$ and $y$ without actually giving a procedure (that is, an *algorithm*) for computing them.[1]

EXAMPLE. Compute the GCD $d$ of 83 and 53, and then express it in the form $d = 83x + 53y$ for some integers $x$ and $y$ (that is, find a solution in the integers of the equation $83x + 53y = d$). Here is the Euclidean algorithm, which shows $d = (83, 53) = 1$, and the extended part to the right of it:

$$\begin{aligned}
83 &= 53 \cdot 1 + 30 && = -\mathbf{53} \cdot 13 + (\mathbf{83} - \mathbf{53} \cdot 1) \cdot 23 = \mathbf{83} \cdot 23 - \mathbf{53} \cdot 36 \\
53 &= 30 \cdot 1 + 23 && = \mathbf{30} \cdot 10 - (\mathbf{53} - \mathbf{30} \cdot 1) \cdot 13 = -\mathbf{53} \cdot 13 + \mathbf{30} \cdot 23 \\
30 &= 23 \cdot 1 + 7 && = -\mathbf{23} \cdot 3 + (\mathbf{30} - \mathbf{23} \cdot 1) \cdot 10 = \mathbf{30} \cdot 10 - \mathbf{23} \cdot 13 \\
23 &= 7 \cdot 3 + 2 && = \mathbf{7} - (\mathbf{23} - \mathbf{7} \cdot 3) \cdot 3 = -\mathbf{23} \cdot 3 + \mathbf{7} \cdot 10 \\
7 &= 2 \cdot 3 + 1 && \mathbf{1} = \mathbf{7} - \mathbf{2} \cdot 3
\end{aligned}$$

So we find $1 = 83 \cdot 23 + 53 \cdot (-36)$. Note that, of $x$ and $y$, one had necessarily to be negative and one positive, if we want the result to be 1. However, which of them will be positive and which negative we do not know until we do Euclid's algorithm, as it depends on the parity of the number of steps.

REMARK. One may show that the solution $x, y$ of $ax + by = d$ which is produced by the extended Euclidean algorithm always satisfies $|x| \leq |b/d|$ and $|y| \leq |a/d|$.

[1]Many such non-constructive proof exist in mathematics, and are often shorter and more elegant than corresponding constructive ones. Obviously constructive proofs have an important practical advantage. But for certain theorems only non-constructive proofs are known.

**4.2. (Optional) A variant of the extended Euclidean algorithm.** We now present a variant of the extended Euclidean algorithm, which is perhaps easier to describe formally, and involves doing some calculations on the side while executing the Euclidean algorithm, rather than working back from the end once the algorithm is finished.[2] We start with writing

$$\begin{aligned} a &= a \cdot 1 + b \cdot 0 \\ b &= a \cdot 0 + b \cdot 1 \end{aligned}$$

We divide as in the Euclidean algorithm, $a = bq_1 + r_1$, with $0 \leq r_1 < b$, and then extend the table as follows:

$$\begin{aligned} a &= a \cdot 1 + b \cdot 0 \\ b &= a \cdot 0 + b \cdot 1 \\ r_1 &= a \cdot 1 + b \cdot (-q_1) \end{aligned}$$

We divide again: $b = r_1q_2 + r_2$, with $0 \leq r_2 < r_1$. Hence $r_2 = b - r_1q_2$. We use the last two rows of the above table to express $r_2$ in terms of $a$ and $b$:

$$\begin{aligned} a &= a \cdot 1 + b \cdot 0 \\ b &= a \cdot 0 + b \cdot 1 \\ r_1 &= a \cdot 1 + b \cdot (-q_1) \\ r_2 &= a \cdot u_2 + b \cdot v_2 \end{aligned}$$

Here $u_2 = -q_2$ and $v_2 = 1 + q_1q_2$. But these exact expressions for $u_2$ and $v_2$ are not important, the important fact is that they exist, and they can be found by taking a suitable linear combination of the previous two lines of the table. Eventually one of the remainders will be the GCD $d$ of $a$ and $b$, the table will read

$$\begin{aligned} a &= a \cdot 1 + b \cdot 0 \\ b &= a \cdot 0 + b \cdot 1 \\ r_1 &= a \cdot 1 + b \cdot (-q_1) \\ r_2 &= a \cdot u_2 + b \cdot v_2 \\ &\vdots \\ d &= a \cdot u + b \cdot v \end{aligned}$$

and we will have found the desired linear combination.

[2]This version has practical advantages over the other, which are more apparent when the number of steps of the algorithm is large. For example, when implemented on a computer (or, especially, a smartcard with limited memory) this variant requires very little memory compared to the other, as only two consecutive steps of the calculation need to be kept in the memory at a given time (as opposed to memorising all the calculations done in the Euclidean algorithm in order to read them backwards at the end).

For example, take $a = 24$ and $b = 14$. The successive divisions are

$$\begin{aligned} \mathbf{24} &= \mathbf{14} \cdot 1 + \mathbf{10} \\ \mathbf{14} &= \mathbf{10} \cdot 1 + \mathbf{4} \\ \mathbf{10} &= \mathbf{4} \cdot 2 + \mathbf{2} \\ \mathbf{4} &= \mathbf{2} \cdot 1 + 0 \end{aligned}$$

This shows that the GCD is 2. (We have set remainders in boldface font for clarity.) Now we compute, as explained earlier,

$$\begin{aligned} \mathbf{24} &= \mathbf{24} \cdot 1 + \mathbf{14} \cdot 0 \\ \mathbf{14} &= \mathbf{24} \cdot 0 + \mathbf{14} \cdot 1 \\ \mathbf{10} &= \mathbf{24} \cdot 1 + \mathbf{14} \cdot (-1) \\ \mathbf{4} &= \mathbf{24} \cdot (-1) + \mathbf{14} \cdot 2 \\ \mathbf{2} &= \mathbf{24} \cdot 3 + \mathbf{14} \cdot (-5) \end{aligned}$$

## 5. Some consequences of Bézout's lemma

**5.1. Some basic properties of the GCD.** The important case when two integers $a$ and $b$ have GCD equal to 1 has a special name: such $a$ and $b$ are called *coprime,* or *relatively prime.* (Do not confuse this with the notion of a *prime.*)

The following four lemmas express important properties of the GCD. For convenience we will refer to them collectively as *the Arithmetical Lemmas.* Lemma B is the most used (and Lemmas C and D are direct consequences of it).

Lemma 8 (Arithmetical Lemma A). *For two integers $a$ and $b$, the following properties are equivalent:*

(1) *$a$ and $b$ are coprime;*
(2) *there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Proof. That (1) implies (2) is simply Bézout's lemma.

The converse is easier: the greatest common divisor $d$ of $a$ and $b$ divides both $ax$ and $by$, hence it divides their sum 1, and consequently $d = 1$ (or $-1$, but we have seen that it makes no difference when taking GCD's). □

However, beware that if $ax + by = d$ for certain integers, and $d > 1$, then we can only conclude that the greatest common divisor $(a, b)$ divides $d$, but not that $(a, b) = d$.

Lemma 9 (Arithmetical Lemma B). *Suppose $(a, b) = 1$. If $a$ divides the product $b \cdot c$, then $a$ divides $c$.*

Proof. According to Bézout's lemma, there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = 1.$$

Multiplying both sides by $c$ we find

$$a(xc) + (bc)y = c.$$

Because $a$ divides each of the products at the left-hand side, it divides their sum as well, which is $c$. □

LEMMA 10 (Arithmetical Lemma C). *Let $a$ and $b$ be integers, not both zero. Then*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

PROOF. According to Bézout's lemma, there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = (a, b).$$

After dividing by $(a, b) \neq 0$ we find

$$\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = 1,$$

and hence $\dfrac{a}{(a,b)}$ and $\dfrac{b}{(a,b)}$ are coprime. □

Lemma C is relevant to simplifying fractions 'in one go': instead of several steps like $42/60 = 21/30 = 7/10$, because $(42, 60) = 6$ Lemma C tells us that $\dfrac{42/6}{60/6} = \dfrac{7}{10}$ cannot be further simplified. Hence simplifying a fraction can always be done in a single step (and the Euclidean algorithm provides the factor to simplify).

LEMMA 11 (Arithmetical Lemma D). *Let $a$ and $b$ integers, not both zero. If $a \mid b \cdot c$, then*

$$\frac{a}{(a,b)} \mid c.$$

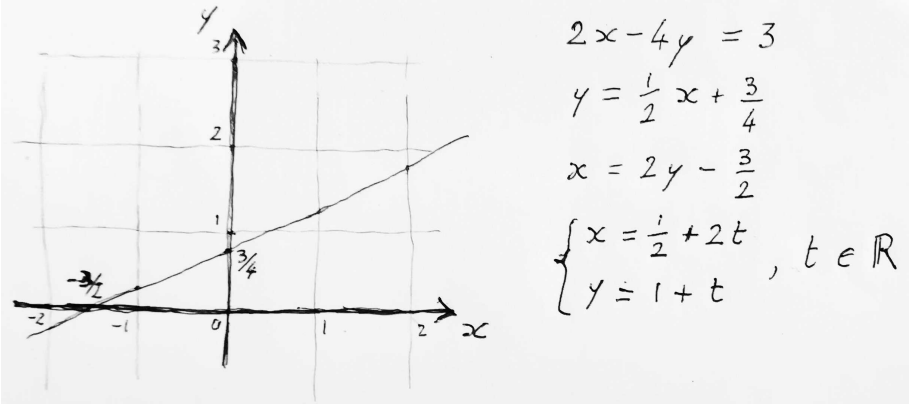
PROOF. By assumption there exists $x$ such that $ax = bc$. Dividing both sides by $(a, b)$ (which is not zero) we get

$$\frac{a}{(a,b)} \cdot x = \frac{b}{(a,b)} \cdot c.$$

According to Arithmetical Lemma C, the integers $\dfrac{a}{(a,b)}$ and $\dfrac{b}{(a,b)}$ are coprime, and hence Arithmetical Lemma B applies. □

**5.2. Solving $ax + by = c$ in $\mathbb{Z}$.** Consider the equation $ax + by = c$, where $a, b, c$ are integers. We want to solve the equation *in the integers*. By *solving* we mean finding *all* solutions (which may include saying that there are none, in certain cases), that is, all pairs of integers $x, y$ such that $ax + by = c$, where $a, b, c$ are any given integers.

EXAMPLE. The equation $2x - 4y = -3$ has infinitely many solutions in the real numbers. In fact, the equation describes a straight line in the plane in Cartesian coordinates, and the solutions of the equation correspond to the points on the line.




Hence all solutions can be described depending on a single arbitrary real parameter, for example as all pairs $(x, y) = (t, \frac{1}{2}t + \frac{3}{4})$ with $t \in \mathbb{R}$, or as all $(x, y) = (s, -2s - \frac{3}{2})$ with $s \in \mathbb{R}$ (or in other ways as well, different *parametrisations* of the line). However, for none of these solutions both $x$ and $y$ take integer values, and so the equation $2x - 4y = -3$ has no solution in the integers. For example, because the left-hand side can only be an even number if $x$ and $y$ are integers, while the right-hand side $-3$ is odd.

More generally, if an integer $d$ divides both $a$ and $b$, and the equation $ax + by = c$ has at least one solution $(x_0, y_0)$ in the integers, then $d$ must also divide $c = ax_0 + by_0$. Consequently, if we find a common divisor $d$ of $a$ and $b$ which does not divide $c$ as well, then we know that $ax + by = c$ cannot have any integer solution. But we need not check all common divisors $d$ of $a$ and $b$, as checking if their GCD $d = (a, b)$ divides $c$ takes care of them all at once.

Therefore, a *necessary* condition for the equation $ax + by = c$ to have integer solutions is that $(a, b)$ divides $c$. But that is actually also a *sufficient* condition. This is because according to Bézout's lemma we have $a' + by' = (a, b)$ for certain integers $x_1$ and $y_1$ (which we can find through the extended Euclidean algorithm), and then $(x_0, y_0) = \left(x_1 \frac{c}{(a,b)}, y_1 \frac{c}{(a,b)}\right)$ is a solution of $ax + by = c$.

EXAMPLE. Suppose we need to solve $83x + 53y = -2$ in the integers. In a previous example we found by the extended Euclidean algorithm that 83 and 53 are coprime, and that their GCD 1 can be written as $1 = 83 \cdot 23 + 53 \cdot (-36)$. Multiplying both sides by $-2$ we see that one solution of $83x + 53y = -2$ is given by $x_0 = 23 \cdot (-2) = -46$ and $y_0 = -36 \cdot (-2) = 72$.

At this point we may assume that $a$ and $b$ are not both zero, otherwise the equation becomes $0 = c$, which is easy to discuss (no solutions if $c \neq 0$, and any arbitrary integer values of $x$ and $y$ are solutions if $c = 0$). The discussion so far makes sense even when

$a = b = 0$, but what we are going to do now would not. The cases where just one of $a$ or $b$ is zero would be easy to discuss separately, but there is no need to do that as the following discussion will take care of those cases as well.

We have already seen that in order for $ax + by = c$ to have integer solutions we need that $(a, b)$ divides $c$. Because $a$ and $b$ are not both zero, $(a, b) \neq 0$, and so we may divide both sides of the equation by $(a, b)$ and obtain the equivalent equation $a'x+b'y = c'$, where $a' = a/(a, b)$, $b' = b/(a, b)$, and $c' = c/(a, b)$. Now $(a', b') = 1$ according to Arithmetical Lemma C.

It remains to see how to solve $a'x + b'y = c'$, but for simplicity let us switch notation and just call $a, b, c$ the new coefficients. So we want to solve the equation $ax + by = c$, with $(a, b) = 1$. We already know how to find one integer solution, so a pair of integers $x_0$ and $y_0$ satisfying $ax_0 + by_0 = c$. If $k$ is any integer, then $x_0 - kb$ and $y + ka$ give another solution, simply because

$$a(x_0 - kb) + b(y_0 + ka) = ax_0 + by_0 = c.$$

Now we show that every solution $x, y$ has that form. If $x$ and $y$ form an arbitrary solution, that means $ax + by = c$. Subtracting this equation from $ax_0 + by_0 = c$ side by side and rearranging we find $a(x_0 - x) = b(y - y_0)$. Hence $b$ divides $a(x_0 - x)$, but we have assumed that $(b, a) = 1$, and so $b$ divides $x_0 - x$ according to Arithmetical Lemma B. Hence $x_0 - x = kb$ for some $k \in \mathbb{Z}$. Substituting this into $a(x_0 - x) = b(y - y_0)$ and dividing by $b$ we find $y - y_0 = ka$. (This works only if $b \neq 0$; but if $b = 0$ then $a = \pm 1$ because $(a, b) = 1$, and then the conclusions remain correct, namely $x = x_0$ and $y = k \in \mathbb{Z}$ arbitrary in this case.) Hence $x = x_0 - kb$ and $y = y_0 + ka$ as we wanted. In conclusion, we have shown that under the condition $(a, b) = 1$ all integer solutions of $ax + by = c$ are given by the formulas

$$x = x_0 - kb, \qquad y = y_0 + ka, \qquad \text{for } k \in \mathbb{Z}.$$

Example. We want to find all integer solutions of the equation $54x + 21y = 15$. We start with the extended Euclidean algorithm on 54 and 21.

$$\begin{aligned} & & 54 &= 54 \cdot 1 + 21 \cdot 0 \\ & & 21 &= 54 \cdot 0 + 21 \cdot 1 \\ 54 &= 21 \cdot 3 - 9 & 9 &= 54 \cdot (-1) + 21 \cdot 3 \\ 21 &= 9 \cdot 2 + 3 & 3 &= 54 \cdot 2 + 21 \cdot (-5) \end{aligned}$$

The first part of the Euclidean algorithm tells us that $(54, 21) = 3$, and because that divides 15 the equation has solutions in the integers (otherwise we could have stopped right there).

The extended part of the Euclidean algorithm tells us that $54 \cdot 2 + 21 \cdot (-5) = 3$, and so it gives us a solution of the equation $54x + 21y = 3$, which is different from the one we are interested in. But multiplying both sides by 5 we find $54 \cdot 10 + 21 \cdot (-25) = 15$, and so $x_0 = 10$ and $y_0 = -25$ form a solution of our equation $54x + 21y = 15$.

Now, one sees immediately $x = 10 - 21k$ and $y = -25 + 10k$ certainly are other solutions of $54x + 21y = 15$, for any integer $k$, but these formulas would not give us *all* integer solutions. The problem is that $(54, 21) = 3 \neq 1$, so this would be a wrong way to proceed.

The correct way is replacing $54x + 21y = 15$ with the equation $18x + 7y = 5$ (obtained by dividing by 3), which is equivalent to the other and so has the same solutions. Now 18 and 7 are coprime, and so our theory tells us that the formulas $x = 10 - 7k$ and $y = -25 + 2k$ do give us all solutions of $18x + 7y = 5$ as $k$ varies over the integers, and so also the solutions of our original equation $54x + 21y = 15$, which is equivalent.

Remark (Optional). There is an interesting variation, useful in some applications, which is solving the equation $ax + by = c$ in the *nonnegative* integers. Let $a, b$ be coprime positive integers. Then for each integer $c \geq (a-1)(b-1)$ there exist integers $x, y \geq 0$ such that $ax + by = c$.

We omit the proof of this fact (which is not difficult), but for practice we show that the stated hypothesis on $c$ is *best possible,* because $ax + by = ab - a - b$ has no solution with integers $x, y \geq 0$. In fact, rewriting the equation in the form $a(x+1) + b(y+1) = ab$, because $(a, b) = 1$ we have that $b \mid x + 1$ and $a \mid y + 1$. But if $x, y \geq 0$ then $x + 1$ and $y + 1$ are positive multiples of $b$ and $a$, hence $x + 1 \geq b$ and $y + 1 \geq a$. But then $a(x + 1) + b(y + 1) \geq 2ab > ab$, a contradiction.

As an example, every integer which is at least $(4-1)(3-1) = 6$ can be written as $4x + 3y$ with $x, y$ nonnegative integers:

$$6 = 4 \cdot 0 + 3 \cdot 2$$

$$7 = 4 \cdot 1 + 3 \cdot 1$$

$$8 = 4 \cdot 2 + 3 \cdot 0$$

$$9 = 4 \cdot 0 + 3 \cdot 3$$

$$10 = 4 \cdot 1 + 3 \cdot 2$$

$$11 = 4 \cdot 2 + 3 \cdot 1$$

$$12 = 4 \cdot 3 + 3 \cdot 0 = 4 \cdot 0 + 3 \cdot 4$$

$$13 = 4 \cdot 1 + 3 \cdot 3$$

$$14 = 4 \cdot 2 + 3 \cdot 2$$

$$15 = 4 \cdot 3 + 3 \cdot 1 = 4 \cdot 0 + 3 \cdot 5$$

and so on. However, $6-1=5$ cannot be written like that, as one of the coefficients needs to be negative: $5 = 4 \cdot 2 - 3 \cdot 1$.

## 6. Unique factorisation in the integers

### 6.1. Primes, and unique factorisation.

DEFINITION 12. An integer $a > 1$ is *composite* if it can be written as $a = bc$, where $b$ and $c$ are positive integers larger than 1 (or, equivalently, $b$ and $c$ are smaller than $a$; or, equivalently again, where $1 < b < a$); it is *prime* if it is not composite. Equivalently, an integer $a > 1$ is a prime if it has no divisors different from 1 and itself.

We have deliberately excluded 1 from both definitions: it is neither a prime nor a composite. (For several reasons this is much more convenient than including it within the set of primes.) Note that two different primes are certainly coprime (as their only positive common factor is 1), but two integers can be coprime without being primes, for example $6 = 2 \cdot 3$ and $35 = 5 \cdot 7$. This is the reason for the term *coprime*: having no prime factors in common.

LEMMA 13. *Let $p$ be a prime (integer), and let $a, b$ be integers. If $p$ divides the product $ab$, then $p$ divides either $a$ or $b$.*

PROOF. Suppose that $p$ does not divide $a$. Then $(p, a)$, which divides $p$, is not $p$, and so it can only be 1. Then Arithmetical Lemma B applies, and hence $p$ divides $b$, as desired. □

THEOREM 14 (Fundamental Theorem of Arithmetic). *Every integer larger than* 1 *factorises into a product of primes, and in a unique way.*

(OPTIONAL) SKETCH OF PROOF. A proper proof requires induction, but the idea of the proof of existence is easy enough to explain informally. If our number $n$ is not prime, we may factorise it as $n = ab$, with $a$ and $b$ integers smaller than $n$. If $a$ and $b$ are primes then we are done. Otherwise we may factorise at least one of them, and so on. This process cannot go on forever, because otherwise we would keep producing smaller and smaller positive integers, and so it must eventually stop, and we are left with a factorisation of $n$ as a product of primes.

A proof of uniqueness uses Lemma 13, and goes roughly as follows. Suppose that $n$ can be written in two ways as a product of primes, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

where the $p_i$ and the $q_j$ are (positive) primes, possibly with repetitions. (Note that we initially we do not even know if the two factorisations involve the same number of

prime factors.) In particular, $p_1$ divides $q_1 q_2 \cdots q_t$, but according to Lemma 13 (possibly repeated a number of times) it follows that $p_1$ divides at least one of the factors $q_j$. Possibly after renumbering them, say that $p_1$ divides $q_1$. But $q_1$ being a prime itself, its only positive divisors are 1 and $q_1$. Because $p_1 \neq 1$ we have $p_1 = q_1$. Hence

$$n/p_1 = p_2 \cdots p_s = q_2 \cdots q_t,$$

and we may repeat the same argument on those two factorisations (which have fewer prime factors than the original ones). Eventually (details omitted) we reach the desired conclusion that the two factorisations are the same. □

We have only worked with positive integers in this subsection, but we might as well have allowed any nonzero integers. However, the definition of composite in Definition 12, for an integer $a \neq, 0, \pm 1$, should be modified into the existence of some factorisation $a = bc$, where neither $a$ nor $b$ is $\pm 1$ (that is, a *proper* factorisation). Here $\pm 1$ play a special role because they are the *invertible* integers: those integers $x$ for which $1/x$ is also an integer (called the *inverse* of $x$, although this is traditionally called the *reciprocal* of $x$). Then $-2$,$-3$,$-5$,... are also primes, but they are essentially the same as $2, 3, 5, \ldots$, respectively, because they can be obtained from the latter through multiplication by an invertible integer (that is, $-1$). With this extended meaning, uniqueness of factorisation still holds up to changing sign to some factors (that is, multiplying them by $-1$), as in $6 = 2 \cdot 3 = (-2) \cdot (-3)$, or $-6 = 2 \cdot (-3) = (-2) \cdot 3$.

### 6.2. The least common multiple.

Definition 15 (Least common multiple). Let $a, b \in \mathbb{Z}$. An integer $m$ is a *least common multiple (lcm)* of $a$ and $b$ if

(1) $a$ and $b$ divide $m$, and
(2) if $c$ is any integer divisible by both $a$ and $b$, then $m$ divides $c$.

A least common multiple of $a$ and $b$ is sometimes denoted by $[a, b]$ (or $\operatorname{lcm}(a, b)$).

As for the greatest common divisor, this definition easily shows that, if the least common multiple of two integers exists, then it is unique up to a sign. (This is because, again, if we have two least common multiples then each of them divides the other.) However, to prove that the lowest common multiple exists (and also to compute it) we may now rely on what we already know about the greatest common divisor, as follows.

Let $c$ be any common multiple of $a$ and $b$. Hence $c = b \cdot x$ for some integer $x$. Because $a \mid b \cdot x$, Arithmetical Lemma D implies $\frac{a}{(a,b)} \mid x$, and so $x = \frac{a}{(a,b)} \cdot y$ for some integer $y$. Therefore,

$$c = b \cdot x = b \cdot \frac{a}{(a,b)} \cdot y = \frac{ab}{(a,b)} \cdot y.$$

Hence every common multiple of $a$ and $b$ is also a multiple of $m = ab/(a,b)$. Moreover, $m$ itself is a multiple of $a$ and $b$, because

$$m = \frac{ab}{(a,b)} = a \cdot \frac{b}{(a,b)} = b \cdot \frac{a}{(a,b)},$$

and the two fractions are integers. Hence $m$ is a least common multiple of $a$ and $b$ according to Definition 15. We have discovered the following:

THEOREM 16. $(a,b) \cdot [a,b] = a \cdot b$.

However, you actually already knew this from school, because of the following way of computing GCD and lcm (whose correctness follows from the theorem on unique factorisation):

THEOREM 17.
- *The GCD of two integers is the product of all their* common *prime factors, each taken with the* lower *exponent.*
- *The lcm of two integers is the product of all their prime factors,* common or not*, each taken with the* higher *exponent.*

If this is the formulation you knew from school, note that you may remove the distinction between *common* factors and *common or not* simply by writing both factorisations of $a$ and $b$ using the same prime factors, but possibly with exponent zero.

EXAMPLE. We compute GCD and lcm of

$$a = 12 = 2^2 \cdot 3^1 \cdot 5^0, \qquad b = 45 = 2^0 \cdot 3^2 \cdot 5^1,$$

where we have included $5^0$ and $2^0$ in their factorisations in order to use the same set of primes. Taking each prime factor with the lower exponent we get

$$(12,45) = 2^0 3^1 5^0 = 3,$$

and taking each prime factor with the higher exponent we get

$$[12,45] = 2^2 3^2 5^1 = 180.$$

If you look at both GCD and lcm, you see that altogether we have taken all powers of 2, 3, and 5, which appear in the factorisations of 12 and 45, just in a different order. Consequently, we have

$$(24,45) \cdot [24,45] = 2^0 3^1 5^0 \cdot 2^2 3^2 5^1 = 2^2 3^1 5^0 \cdot 2^0 3^2 5^1 = 12 \cdot 45,$$

as predicted by Theorem 16.

REMARK. The parentheses and square brackets notation used to denote GCD and lcm can be extended to more than two integers. Theorem 17 easily extends by replacing *lower* and *higher* exponent with *lowest* and *highest* exponent. However, the product of $(a,b,c)$

and $[a, b, c]$ does not equal the product $abc$ of three integers. The correct generalisation of Theorem 16 to the case of three integers is

$$[a, b, c] = abc \cdot \frac{(a, b, c)}{(a, b) \cdot (a, c) \cdot (b, c)}.$$

**6.3. (Optional) Computational complexity.** The school method for finding the GCD of two integers $a$ and $b$ (say both positive) starts with factorising $a$ and $b$ into products of prime factors. When $a$ and $b$ are large this is not a good idea, as we informally explain now.

The simplest method for factorising an integer $a$ (called *method of trial divisions*) is dividing it by $2, 3, 4, 5, \ldots$. (One may restrict oneself to dividing by the prime numbers $2, 3, 5, 7, \ldots$, but this is not a huge saving; more on this later.) One can stop at $\lfloor \sqrt{a} \rfloor$. In fact, if $a$ is not a prime, and hence $a = bc$, with $0 < b, c < a$, then we may assume $b \leq c$, hence $b^2 \leq bc = a$, and so $b \leq \sqrt{a}$. If we have not find a factor of $a$ after dividing it by $2, 3, \ldots \lfloor \sqrt{a} \rfloor$ (that is, none of the divisions gave zero remainder), then we must conclude that $a$ is a prime.

Therefore, in order to find a proper factor of $a$ in case it is composite the method of trial divisions requires at most $\lfloor \sqrt{a} \rfloor - 1$ divisions, in the worst case. (And in case $a$ was prime, which we would usually not know in advance, the method produces a (long) proof that $a$ is prime only after exactly $\lfloor \sqrt{a} \rfloor - 1$ divisions.) Here the $-1$ makes an insignificant difference when $a$ is large, and so does taking the integral part of $\sqrt{a}$. Therefore, we may say that the method of trial divisions requires at most *about* $\sqrt{a}$ divisions, in the worst case, to factorise $a$.

There is a theory of *computational complexity,* which studies, roughly speaking, how many operations are required (which can be then translated into how long a computer takes to perform them) to complete a certain algorithm. There are a lot more details to this, and variations. For example, we may be interested in how long an algorithm takes to complete *on average* rather than in the worst possible case. Also, for the sake of simplicity, above we just counted the number of divisions required to factorise $a$, without considering that some single divisions may take longer than others to be done (depending on the sizes of the numbers involved).

We now show that the Euclidean algorithm takes much fewer operations to complete than factorising integers of similar size. In fact, in the general step we divide

$$r_j = r_{j+1} q_{j+2} + r_{j+2},$$

and hence $r_j > r_{j+1} > r_{j+2}$. But because $q_{j+2} \geq 1$ we have

$$r_j = r_{j+1} q_{j+2} + r_{j+2} \geq r_{j+1} + r_{j+2} > 2 r_{j+2}.$$

Hence, although the remainder may not change much in two consecutive divisions, every two divisions it decreases at least by a factor two:

$$r_{j+2} < \frac{1}{2}\, r_j.$$

Hence if we start with $r_{-1} = a > r_0 = b > 0$, and the last nonzero remainder is $r_{2k}$ or $r_{2k+1}$, then

$$1 \leq r_{2k} < \frac{r_0}{2^k} = \frac{b}{2^k},$$

whence $2^k < b$, which means $k < \log_2(b)$. Hence the total number of divisions required, which is either $2k+1$ or $2k+2$, is no more than $2k+2 < 2\log_2(b)+2$. Because $\log_2(b) = \log_2(10)\log_{10}(b)$, and $\log_2(10) = \ln(10)/\ln(2)$ equals about $3.32\cdots$, we conclude that the total number of divisions required for the Euclidean algorithm on $a > b$ is, roughly, less than $7\log_{10}(b)$, that is, again roughly, seven times the number of decimal digits of $b$.

If, for example, $b$ is about $10^{200}$, the Euclidean algorithm requires less than about $7 \cdot 200 = 1400$ divisions with remainder. These can be done in a split second by a modern computer. Attempting to factorise $b$ by trial divisions, however, may require up to $\sqrt{b} = 10^{100}$ divisions with remainder. This is a huge number, with about 100 digits. For example, if a computer were able to perform one trillion, that is, $10^{12}$, divisions with remainder in a second, it would take $10^{100}/10^{12} = 10^{88}$ seconds to finish. (For comparison, the fastest desktop personal computers in 2015 can process about 200 000 MIPS, that is, only one fifth of a trillion *instructions* per second; and of course each of our trial divisions would require many such instructions.) To gauge how long $10^{88}$ seconds is, consider that in a year there are $60 * 60 * 24 * 365$ seconds, which is about $3 \cdot 10^7$ seconds. Hence $10^{88}$ seconds is around $3 \cdot 10^{80}$ years. For comparison, note that the estimated age of the universe is only 13.8 billion years, that is, $13.8 \cdot 10^9$ years!

One may object that, in the method of trial divisions, instead of dividing by the integers $2, 3, 4, 5, \ldots$, it would be enough to divide by the prime numbers $2, 3, 5, 7, 11, 13, 17, \ldots$. Although this seems to make a significant time saving at the beginning (for example, dividing only by 2 and the *odd* integers $3, 5, 7, 9, 11, \ldots$, which certainly include all the remaining primes, already saves about half the time), this saving becomes less and less important as the numbers increase. This is because the prime numbers are certainly sparse, but still *relatively many,* so to say, among the positive integers. In fact, not only there are infinitely many primes, but we have

THEOREM 18 (The prime number theorem). *The function*

$$\pi(n) := \sharp\{p\text{: } p \text{ is a prime and } p \leq n\},$$

*which counts the number of primes $p$ not exceeding $n$, satisfies*

$$\pi(n) \sim \frac{n}{\log n},$$

*meaning that the ratio of the two sides tends to the limit* 1 *as* $n$ *tends to infinity.*

For example, of the integers with less than 100 decimal digits (that is, integers less than $10^{100}$), about one in 230 is a prime (because $\ln(10^{100}) = 100 \cdot \ln(10)$ is about $230.258\cdots$). Hence if we were to try factorise a number $b$, as in the previous example, hence of size around $10^{200}$, by only doing trial divisions by the primes less than $\sqrt{b}$, we would save a meager factor 230 in the huge required time.