Chapter 4

The Arithmetic of $\mathbb{Z}$

In this chapter, we start by introducing the concept of congruences; these are used in our proof (going back to Gauss[1]) that every integer has a unique prime factorization. We will also discuss the Euclidean Algorithm, a basic tool in computational number theory; we shall see later that the same method also works for polynomial rings $K[X]$ over fields K.

4.1 Divisibility

Just as subtraction was not defined for all pairs of natural numbers (in $\mathbb{N}$, we could have defined $m - n$ for $m, n \in \mathbb{N}$ with $m \geq n$), division is not defined for all pairs of nonzero integers. The theory of divisibility studies this observation in more detail. We say that an integer $b \in \mathbb{Z}$ divides $a \in \mathbb{Z}$ (and write $b \mid a$) if there exists an integer $q \in \mathbb{Z}$ such that $a = bq$.

Actually this definition makes sense in general domains (a commutative ring with 1 and without zero divisors), and even in monoids. A monoid is a set M on which a multiplication is defined (a map $M \times M \longrightarrow M$) such that

1. multiplication is commutative and associative;
2. M contains a neutral element ($1 \in M$);
3. M is cancellative: if $xy = xz$ for $x, y, z \in M$, then $x = y$.

Examples for monoids are the nonzero natural numbers, the nonzero integers, as well as e.g. the following sets:

1. $M = \{1, 3, 5, 7, \ldots\} = 2\mathbb{N} + 1$;
2. $M = \{1, 2, 4, 6, \ldots\} = 2\mathbb{N} \cup \{1\}$;
3. $M = \{1, 5, 9, 13, \ldots\} = 4\mathbb{N} + 1$

[1] Carl-Friedrich Gauss: 1777 (Braunschweig, Germany) – 1855 (Göttingen, Germany)

4. $M = \{1, 2, 4, 8, 16, \ldots\}$.

5. the nonzero elements in a domain R.

The main properties of the divisibility relation follow directly from the definition:

Proposition 4.1. *For all elements a, b, c of a monoid, we have*

1. $1 \mid a$ *and* $a \mid a$;

2. *if* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

The proofs are immediate. For showing the second claim, observe that we have $b = aq$ and $c = br$ for $q, r \in M$; but then $c = br = a(qr)$, hence $a \mid c$.

For domains, we have in addition a result involving the additive structure:

Proposition 4.2. *Let a, b, c be elements in some domain R. If $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$.*

Proof. These are formal consequences of the definition: We have $b = aq$ and $c = ar$ for $q, r \in R$; then $b \pm c = a(q \pm r)$ implies that $a \mid (b \pm c)$. □

Elements dividing 1 are called units; the units in $\mathbb{Z}$ are -1 and $+1$. First of all, they are units because they divide 1. Now assume that $r \in \mathbb{Z}$ is a unit; then there exists an element $s \in \mathbb{Z}$ with $rs = 1$. Clearly $r, s \neq 0$, hence $|r|, |s| \geq 1$. If $|r| > 1$, then $0 < |s| < 1$, but there are no integers strictly between 0 and 1.

Proposition 4.3. *The set $M^\times$ of units in some monoid forms a group.*

Proof. We have to check the axioms. First, $1 \in M^\times$ shows the existence of a neutral element. If u is a unit, then by definition there is some $v \in M$ such that $uv = 1$. But then $v = u^{-1}$ is also a unit, so inverses exist. Finally, if u and v are units, then $uu' = vv' = 1$ for some $u', v' \in M$, and then $(uv)(u'v') = 1$, hence uv is a unit.

Note that commutativity and associativity are inherited from M: if these axioms hold for all elements in M, then they surely will hold for all elements in $M^\times$. □

We now give two important definitions. Let M be a monoid; then a non-unit $p \in M$ is called

- irreducible if it only has trivial factorizations, i.e. if $p = ab$ for $a, b \in M$ implies that $a \in M^\times$ or $b \in M^\times$.

- prime if $p \mid ab$ for $a, b \in M$ implies that $p \mid a$ or $p \mid b$.

Being prime is a stronger property than being irreducible:

Proposition 4.4. *Primes are irreducible.*

Proof. Let p be prime. We want to show it's irreducible, so assume that $p = ab$; we have to prove that a or b is a unit. Now clearly $p \mid ab$, and since p is prime, we have $p \mid a$ or $p \mid b$. Assume without loss of generality that $p \mid a$. Then $a = pc$ for some $c \in M$, hence $p = ab = pbc$, and since M is cancellative we deduce that $1 = bc$. Thus b is a unit, and this concludes the proof. □

It is not true at all that irreducibles are always prime. It is basically in order to have lots of examples that we have dealt with monoids here. Consider e.g. the monoid $M = \{1, 2, 4, 6, \ldots\}$; here 2 is irreducible since clearly $2 = 1 \cdot 2 = 2 \cdot 1$ are the only factorizations of 2. On the other hand, 2 is not prime: we have $2 \mid 6 \cdot 6$ since $36 = 2 \cdot 18$, but $2 \nmid 6$ because 6 is not divisible by 2 in M.

Now we claim

Proposition 4.5. *There are infinitely many primes in $\mathbb{Z}$.*

Proof. We give a proof by contradiction. Assume that there are only finitely many primes, namly $p_1 = 2, \ldots, p_r$, and consider the integer $N = p_1 \cdots p_r + 1$. Then $N > 1$, hence it is divisible by a prime p. This prime p is not in our list: if we had $p = p_i$, then $p \mid N$ and $p \mid N - 1 = p_1 \cdots p_i \cdots p_r$, hence p divides $1 = N - (N - 1)$: contradiction, because p is a prime, hence can't be a unit by definition. □

This is a really nice proof; unfortunately, it is not completely correct. In order to see what is missing, consider the monoid $M = \{1, 5, 9, 13, \ldots\}$. We can imitate the proof above as follows: assume that $p_1 = 5, \ldots, p_r$ is the list of all primes in M (the number 5 is indeed prime, as is easily shown: if $5 \mid ab$ for $a, b \in M$, then $5 \mid ab$ in $\mathbb{Z}$, hence we may assume that $5 \mid a$ in $\mathbb{Z}$. But this means $a = 5c$, and we see that c must have the form $4n + 1$ just like 5 and a: thus $5 \mid a$ in M). Then we form $N = p_1 \cdots p_r + 4 \in M$; clearly $N > 1$, so it must be divisible by some prime p, and as above we see that $p \neq p_j$ for $1 \leq j \leq r$.

What's wrong with this proof? Let us start with the list of primes consisting only of 5. Then $N = 5 + 4 = 9$. And although $N > 1$, N does not contain any prime factor because it is irreducible, but not prime! In fact, we have $9 \mid 21 \cdot 21 = 9 \cdot 49$, but $9 \nmid 21$.

Thus what is missing in our proof is the following:

Proposition 4.6. *Every integer $n > 1$ has a factorization into irreducible elements.*

Proof. This is clear if $N = 2$; now do induction on N and assume the claim is true for all $N < n$. If n is irreducible, everything is fine; if not, then $n = ab$, and by induction assumption both a and b are products of irreducibles, hence so is n. □

The proof of Prop. 4.5 shows that there are infinitely many irreducibles in $\mathbb{Z}$: this is because every $N > 1$ in $\mathbb{Z}$ (or in $M = 4\mathbb{N} + 1$) is divisible by an irreducible element.

The claim that there exist infinitely many primes in $\mathbb{Z}$ will be complete once we have proved that irreducibles are prime in $\mathbb{Z}$. We will do this using congruences, which we will discuss next.

4.2 Congruences

Congruences are a very clever notation invented by Gauss (and published in 1801 in his "Disquisitiones Arithmeticae") to denote the residue of a number a upon division by a nonzero integer m. More precisely, he wrote $a \equiv b \bmod m$ if $m \mid (a - b)$. for elements $a, b, m \in \mathbb{Z}$.

Examples.

- $10 \equiv 3 \bmod 7$;
- $10 \equiv 0 \bmod 5$;
- $5 \equiv 2 \equiv -1 \bmod 3$.

The rules for divisibility can now be transferred painlessly to congruences: first we observe

Proposition 4.7. *Congruence between integers is an equivalence relation.*

Proof. Recall that a relation is called an equivalence relation if it is reflexive, symmetric and transitive. In our case, we have to show that the relation $\equiv$ has the following properties:

- reflexivity: $a \equiv a \bmod m$;
- symmetry: $a \equiv b \bmod m$ implies $b \equiv a \bmod m$;
- transitivity: $a \equiv b \bmod m$ and $b \equiv c \bmod m$ imply $a \equiv c \bmod m$

for $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z} \setminus \{0\}$.

The proofs are straightforward. In fact, $a \equiv a \bmod m$ means $m \mid (a-a)$, and every integer $m \neq 0$ divides 0. Similarly, $a \equiv b \bmod m$ is equivalent to $m \mid (a-b)$; but this implies $m \mid (b - a)$, hence $b \equiv a \bmod m$. Finally, if $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $m \mid (b - a)$ and $m \mid (c - b)$, hence m divides the sum $c - a = (c - b) + (b - a)$, and we find $a \equiv c \bmod m$ as claimed. □

Since $\equiv$ defines an equivalence relation, it makes sense to talk about equivalence classes. The equivalence class $[a]$ (or $[a]_m$ if we want to express the dependence on the modulus m) of an integer a consists of all integers $b \in \mathbb{Z}$ such that $b \equiv a \bmod m$; in particular, every residue class contains infinitely

many integers. In the special case $m = 3$, for example, we have

$$\begin{aligned}
[0] &= \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \\
[1] &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \\
[2] &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}, \\
[3] &= \{\ldots, -3, 0, 3, 6, 9, \ldots\} = [0],
\end{aligned}$$

etc. Note that $[0] = [3] = [6] = \ldots$ (in fact, $[0] = [a]$ for any $a \in [0]$), and similarly $[1] = [4] = \ldots$. In general, we have $[a] = [a']$ if and only if $a \equiv a' \bmod m$, that is, if and only if $m \mid (a - a')$.

In the case $m = 3$, there were exactly 3 different residue classes modulo 3, namely [0], [1], and [2] (or, say, [0], [1], and $[-1]$ since $[-1] = [2]$). This holds in general:

Lemma 4.8. *For any integer $m > 1$, there are exactly m different residue classes modulo m, namely $[0]$, $[1]$, $[2]$, $\ldots$, $[m-1]$.*

Proof. We first show that these classes are pairwise distinct. To this end, assume that $[a] = [b]$ for $0 \leq a, b < m$; this implies $b \in [a]$, hence $a \equiv b \bmod m$ or $m \mid (b - a)$: but since $|b - a| < m$, this can only happen if $a = b$.

Next, there are no other residue classes: given any class $[a]$, we write $a = mq + r$ with $0 \leq r < m$ (the division algorithm at work again), and then $[a] = [r]$ is one of the classes listed above. □

The set $\{0, 1, 2, \ldots, m-1\}$ is often called a complete set of representatives modulo m for this reason. Sometimes we write $r + m\mathbb{Z}$ instead of $[r]$.

The one thing that makes congruences *really* useful is the fact that we can define a ring structure on the set of residue classes. This is fundamental, so let us do this in detail.

The elements of our ring $\mathbb{Z}/m\mathbb{Z}$ will be the residue classes $[0]$, $[1]$, $\ldots$, $[m-1]$ modulo m. We have to define an addition and a multiplication and then verify the ring axioms.

• Addition $\oplus$: Given two classes $[a]$ and $[b]$, we put $[a] \oplus [b] = [a + b]$. We have to check that this is well defined: assume that $[a] = [a']$ and $[b] = [b']$; then we have to show that $[a + b] = [a' + b']$. But this is easy: we have $a - a' \in m\mathbb{Z}$, say $a - a' = mA$, and similarly $b - b' = mB$. But then $(a + b) - (a' + b') = m(A + B) \in m\mathbb{Z}$, hence $[a + b] = [a' + b']$.

The neutral element is the residue class $[0] = m\mathbb{Z}$, and the inverse element of $[a]$ is $[-a]$, or, if you prefer, $[m - a]$. In fact, we have $[a] \oplus [0] = [a + 0] = [a]$ and $[a] \oplus [-a] = [a + (-a)] = [0]$. The law of associativity and the commutativity are inherited from the corresponding properties of integers: since e.g. $(a + b) + c = a + (b + c)$, we have $([a] \oplus [b]) \oplus [c] = [a] \oplus ([b] \oplus [c])$.

• Multiplication $\odot$: of course we put $[a] \odot [b] = [ab]$. The verification that this is well defined is left as an exercise. The neutral element is the class $[1]$.

• Distributive Law: Again, $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ follows from the corresponding properties of integers.

Theorem 4.9. *The residue classes* $[0]$, $[1]$, $\ldots$, $[m-1]$ *modulo* m *form a ring* $\mathbb{Z}/m\mathbb{Z}$ *with respect to addition* $\oplus$ *and multiplication* $\odot$.

Now that we have introduced the rings that we will study for some time to come, we simplify the notation by writing $+$ and $\cdot$ instead of $\oplus$ and $\odot$. Moreover, we will drop our references to classes and deal only with the integers representing them; in order to make clear that we are dealing with residue classes, we write $\equiv$ instead of $=$ and add a "mod m" at the end. What this means in practice is that we identify $\mathbb{Z}/m\mathbb{Z}$ with the set of integers $\{0, 1, \ldots, m-1\}$.

Applications: ISBN (International Standard Book Number)

From the 1970s onward books are assigned an ISBN consisting of four parts: the first block specifies the country (or rather the language of the country), the second block gives information about the publishing company, the third about the book within that company, and the last digit is a check digit that is computed as follows: multiply the digits of the ISBN by 1, 2, 3, $\ldots$, 10, starting on the left; the check digit is the integers ≤ 10 for which the sum of these product is $\equiv 0 \bmod 11$. The check 'digit' X stands for 10.

Example: compute the check digit of the ISBN 0-387-94225-?. We find $1\cdot 0+2\cdot 3+3\cdot 8+4\cdot 7+5\cdot 9+6\cdot 4+7\cdot 2+8\cdot 2+9\cdot 5+10? \equiv 4+10? \bmod 11$, and since $10 \equiv -1 \bmod 11$, this gives $4-? \equiv 0 \bmod 11$, so $? = 4$, and the complete ISBN is 0-387-94225-4.

It is easy to see that if you type in an ISBN and make a single error, then the check digit will catch it; thus the ISBN is an example of a 1-error detecting code.

4.3 Unique Factorization in $\mathbb{Z}$

Before we can prove that irreducibles are prime, we need

Proposition 4.10. *If* p *is irreducible, then* $\mathbb{Z}/p\mathbb{Z}$ *is a field.*

Let us do some work first. For any rational number $x \in \mathbb{Q}$, define the ceiling $\lceil x \rceil$ of x to be the smallest integer $\geq x$; by definition we have

$$x \leq \lceil x \rceil < x + 1.$$

Put $x = \frac{p}{a}$ for $a > 0$ and multiply through by a; then $p \leq a\lceil \frac{p}{a} \rceil < p + a$, or, after subtracting p, $0 \leq a\lceil \frac{p}{a} \rceil - p < a$.

Proof of Prop. 4.10. We have to show that if $[a] \neq [0]$, i.e., if $0 < a < p$, then there exists a residue class $[b]$ such that $[ab] = [1]$.

This is trivial if $a = 1$, so assume $a > 1$ and put $r_1 = \lceil p/a \rceil$; then $0 \leq ar_1 - p < a$. If we had $ar_1 - p = 0$, then the fact that p is irreducible implies $a = 1$ or $a = p$, contradicting our assumption. Thus $0 < ar_1 - p < a$.

If $a_1 = ar_1 - p = 1$, then $b = r_1$ is the inverse of a: in fact, reducing $ar_1 - p = 1$ modulo p gives $ar_1 \equiv 1 \bmod p$, i.e., $[a][r_1] = [1]$.

If $a_1 > 1$, then put $r_2 = \lceil p/a_1 \rceil$ and repeat the above argument. If $a_1 r_2 - p = 1$, then $[a][r_1 r_2] = [1]$, and $b = r_1 r_2$ is the desired inverse of a; if not repeat this step. Since a_i decreases by at least 1 in each step, the process must eventually terminate: if $a_n = 1$, then we have the following equations:

$$\begin{aligned} 0 < a_1 &= ar_1 - p < a, \\ 0 < a_2 &= a_1 r_2 - p < a_1, \\ &\dots \\ 0 < a_{n-1} &= a_{n-2} r_{n-1} - p < a_{n-2} \\ a_n &= a_{n-1} r_n = 1. \end{aligned}$$

These equations give rise to the following congruences:

$$\begin{aligned} a_1 &\equiv ar_1 \bmod p, \\ a_2 &\equiv a_1 r_2 \bmod p, \\ &\dots \\ a_{n-1} &\equiv a_{n-2} r_{n-1} \bmod p, \\ 1 = a_n &\equiv a_{n-1} r_n \bmod p. \end{aligned}$$

Starting with the last and working our way up we get

$$1 = a_n \equiv a_{n-1} r_n equiv a_{n-2} r_{n-1} r_n \dots \equiv a_1 r_2 r_3 \cdots r_n \equiv a r_1 r_2 \cdots r_n \bmod p.$$

This shows that $b \equiv r_1 r_2 \cdots r_n \bmod p$ is the multiplicative inverse of $a \bmod p$. □

Here's an example: let us compute the inverse of the residue class [5] in $\mathbb{Z}/13\mathbb{Z}$. We find $a = 5$, $p = 13$, $r_1 = \lceil \frac{13}{5} \rceil = 3$, hence $a_1 = ar_1 - p = 2$. Repeating this step provides us with $r_2 = \lceil \frac{13}{2} \rceil = 7$ and $a_2 = a_1 r_2 - p = 1$. Thus $r_1 r_2 \equiv 3 \cdot 7 \equiv 8 \bmod 13$, and $[5][8] = [1]$.

Remark. Fields F have very nice properties; one of them is that linear equations $ax = b$ with $a, b \in F$ and $a \neq 0$ always have a unique solution: in fact, since $a \neq 0$, it has an inverse element $a^{-1} \in F$, and multiplying through by a^{-1} we get $x = a^{-1}b$. This does not work in general rings: the equation $2x = 1$ does not have a solution in $\mathbb{Z}/4\mathbb{Z}$, and the linear equation $2x = 2$ has two solutions, namely $x = [1]$ and $x = [3]$.

The main result on which unique factorization will be built is the following:

Proposition 4.11. *Irreducibles in $\mathbb{Z}$ are prime.*

Proof. Assume that p is irreducible and that $p \mid ab$. If $p \nmid a$ and $p \nmid b$, then $[a]$ and $[b]$ are invertible modulo p; but then $[ab]$ has an inverse (if $[a][r] = [b][s] = [1]$, then $[ab][rs] = [1]$), and therefore $p \nmid ab$. This proves that $p \mid a$ or $p \mid b$. □

This means in particular that every integer in $\mathbb{Z}$ has a factorization into primes. We will prove in a minute that this factorization is unique; here we will give an example showing that this is not obvious: consider the monoid $M = \{1, 5, 9, 13, \ldots\}$ of positive integers of the form $4n + 1$ (this example is actually due to Hilbert). It is clear that every integer in M has a factorization into irreducibles, but it is not unique: for example, we have $21 \cdot 33 = 9 \cdot 77$, and 9, 21, 33 and 77 are all irreducible in M The reason why unique factorization fails is the existence of irreducibles that aren't prime.

The theorem of unique factorization asserts that every integer has a prime factorization, and that it is unique up to the order of the factors.

Theorem 4.12. *Every integer $n \geq 2$ has a prime factorization $n = p_1 \cdots p_r$ (with possibly repeated factors). This factorization is essentially unique, that is: if $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ are prime factorizations of an integer n, then $r = s$, and we can reorder the q_j in such a way that $p_j = q_j$ for $1 \leq j \leq r$.*

A partial result in the direction of Theorem 4.12 can already be found in Euclid's elements; the first explicit statement and proof was given by Gauss in 1801.

Proof. We already know that prime factorizations exist, so we only have to deal with uniqueness. This will be proved by induction on $\min\{r, s\}$, i.e. on the minimal number of prime factors of n. We may assume without loss of generality that $r \leq s$.

If $r = 0$, then $n = 1$, and $n = 1 = q_1 \cdots q_s$ implies $s = 0$.

Now assume that every integer that is a product of at most $r - 1$ prime factors has a unique prime factorization, and consider $n = p_1 \cdots p_r = q_1 \cdots q_s$. Since p_1 is a prime that divides $n = q_1 \cdots q_s$, it must divide one of the factors, say $p_1 \mid q_1$ (after rearranging the q_i if necessary). But q_1 is prime, so its only positive divisors are 1 and q_1; since p_1 is a prime, it is a nonunit, and we conclude that $p_1 = q_1$. Canceling p_1 shows that $p_2 \cdots p_r = q_2 \cdots q_s$, and by induction assumption we have $r = s$, and $p_j = q_j$ after rearranging the q_i if necessary. □

Remark. There is a simple reason for doing induction on the minimal number of prime factors and not simply on the number of prime factors of n: the fact that the number of prime factors of an integer is well defined is a consequence of the result we wanted to prove! In fact, in $M = \{1, 5, 9, \ldots\}$ numbers may have factorizations into irreducibles of different lengths: an example is $225 = 9 \cdot 5 \cdot 5 = 15 \cdot 15$.

Some Applications

We have already seen that integers are squares of rational numbers if and only if they are squares of integers. Here we shall use unique factorization to show that $\sqrt{p}$ is irrational. For assume not: then $p = r^2/s^2$ for $r, s \in \mathbb{N}$, and assume that r and s are coprime (if they are not, cancel). Thus $ps^2 = r^2$. Thus $p \mid r^2$, and since p is prime, we must have $p \mid r$, say $r = pt$. Then $ps^2 = p^2t^2$, hence

$s^2 = pt^2$. But then $p \mid s^2$, hence $p \mid s$ since p is prime, and this is a contradiction, since we now have shown that $p \mid r$ and $p \mid s$ although we have assumed that they are coprime.

4.4 Greatest Common Divisors in $\mathbb{Z}$

We will now introduce greatest common divisors: we say that d is a greatest common divisor of $a, b \in \mathbb{Z}$ and write $d = \gcd(a, b)$ if d satisfies the following two properties:

1. $d \mid a$, $d \mid b$;
2. if $e \in \mathbb{Z}$ satisfies $e \mid a$ and $e \mid b$, then $e \mid d$.

We can use the unique factorization property to give a formula for the gcd of two integers. Before we do so, let us introduce some notation. We can write an $a \in \mathbb{Z}$ as a product of primes. In fact fact we can write $a = \pm \prod p_i^{a_i}$, where the product is over all irreducible elements p_1, p_2, p_3, $\ldots$, and where at most finitely many a_i are nonzero. In order to avoid the $\pm$ in our formulas, let us restrict to positive integers from now on.

Lemma 4.13. *For integers $a, b \in \mathbb{N}$ we have $b \mid a$ if and only if $b_i \leq a_i$ for all i, where $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$ are the prime factorizations of a and b.*

Proof. We have $b \mid a$ if and only if there is a $c \in \mathbb{N}$ such that $a = bc$. Let $c = \prod p_i^{c_i}$ be its prime factorization. Then $c_i \geq 0$ for all i, and $a_i = b_i + c_i$, hence $b \mid a$ is equivalent to $a_i \geq b_i$ for all i. □

Here's our formula for gcd's:

Theorem 4.14. *The gcd of two nonzero integers*

$$a = \prod p_1^{a_i} \quad \text{and } b = \prod p_i^{b_i}$$

is given by

$$d = \prod p_i^{\min\{a_i, b_i\}}.$$

Proof. We have to prove the two properties characterizing gcd's:

1. $d \mid a$ and $d \mid b$. But this follows immediately from Lemma 4.13.
2. If $d' \mid a$ and $d' \mid b$, then $d' \mid d$. In fact, write down the prime factorization $d' = \prod p_i^{d'_i}$ of d'. Then $d' \mid a$ and $d' \mid b$ imply $d'_i \leq \min(a_i, b_i) = d_i$, hence $d' \mid d$.

Now assume that d and d' are gcd's of a and b. Then $d \mid d'$ by 2. since d' is a gcd, and $d' \mid d$ since d is a gcd, hence $d' = \pm d$. □

For the ring $\mathbb{Z}$ of integers, we have much more than the mere existence of gcd's: the gcd of two integers $a, b \in \mathbb{Z}$ has a "Bezout representation",[2] that is, if $d = \gcd(a, b)$, then there exist integers $m, n \in \mathbb{Z}$ such that $d = am + bn$.

Theorem 4.15 (Bezout's Lemma)**.** *Assume that $d = \gcd(a, b)$ for $a, b \in \mathbb{Z}$; then d has a Bezout representation.*

Proof. Consider the set $D = a\mathbb{Z} + b\mathbb{Z} = \{am + bn : m, n \in \mathbb{Z}\}$. Clearly D is a nonempty set, and if $c \in D$ then we also have $-c \in D$. In particular, D contains positive integers.

Let d be the smallest positive integer in D; we claim that $d = \gcd(a, b)$. There are two things to show:
Claim 1: d is a common divisor of a and b. By symmetry, it is sufficient to show that $d \mid a$. Write $a = rd + s$ with $0 \leq s < d$; from $d = am + bn$ we get $s = rd - a = r(am + bn) - a = a(rm - 1) + b(rn)$, hence $s \in D$. The minimality of d implies $s = 0$, hence $d \mid m$.
Claim 2: if e is a common divisor of a and b, then $e \mid d$. Assume that $e \mid a$ and $e \mid b$. Since $d = am + bn$, we conclude that $e \mid d$.

The existence of the Bezout representation is a simple consequence of the fact that $d \in D$. □

Note that the key of the proof is the existence of a division with remainder.

Bezout's Lemma can be used to give an important generalization of the property $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$ of primes p:

Proposition 4.16. *If $m \mid ab$ and $\gcd(m, b) = 1$, then $m \mid a$.*

Proof. Write $ab = mn$; by Bezout, there are $x, y \in \mathbb{Z}$ such that $mx + by = 1$. Multiplying through by a gives $a = max + aby = max + mny = m(ax + ny)$, that is, $m \mid a$. □

Finally, observe that canceling factors in congruences is dangerous: we have $2 \equiv 8 \bmod 6$, but not $1 \equiv 4 \bmod 6$. Here's what we're allowed to do:

Proposition 4.17. *If $ac \equiv bc \bmod m$, then $a \equiv b \bmod \frac{m}{\gcd(m,c)}$.*

Proof. We have $m \mid (ac - bc) = c(a - b)$. Write $d = \gcd(m, c)$, $m = dm'$, $c = dc'$, and note that $\gcd(m', c') = 1$. From $dm' \mid dc'(a - b)$ we deduce immediately that $m' \mid c'(a - b)$; since $\gcd(m', c') = 1$, we even have $m' \mid (a - b)$ by Prop 4.16, i.e. $a \equiv b \bmod \frac{m}{\gcd(m,c)}$. □

4.5 The Euclidean Algorithm

In most modern textbooks, Unique Factorization is proved using the Euclidean algorithm; it has the advantage that a similar proof can also be used for other rings, e.g. polynomial rings $K[X]$ over fields K. The Euclidean algorithm

[2] Etienne Bezout: 1730 (Nemours, France) – 1783 (Basses-Loges, France)

is a procedure that computes the gcd of integers without using their prime factorization (which may be difficult to obtain if the numbers involved are large). Moreover, it allows us to compute a Bezout representation of this gcd (note that our proof of Thm. 4.15 was an existence proof, giving no hint at how to compute such a representation).

Given integers m and n, there are uniquely determined integers q_1 and r_1 such that $m = q_1 n + r_1$ and $0 \leq r_1 < n$. Repeating this process with n and r_1, we get $n = r_1 q_2 + r_2$ with $0 \leq r_2 < r_1$, etc. Since $n > r_1 > r_2 > \ldots \geq 0$, one of the r_i, say r_{n+1}, must eventually be 0:

$$\begin{aligned} m &= q_1 n + r_1 && (4.1)\\ n &= q_2 r_1 + r_2 && (4.2)\\ r_1 &= q_3 r_2 + r_3 && (4.3)\\ &\ldots \\ r_{n-2} &= q_n r_{n-1} + r_n && (4.4)\\ r_{n-1} &= q_{n+1} r_n && (4.5) \end{aligned}$$

Example: $m = 56$, $n = 35$

$$\begin{aligned} 56 &= 1 \cdot 35 + 21\\ 35 &= 1 \cdot 21 + 14\\ 21 &= 1 \cdot 14 + 7\\ 14 &= 2 \cdot 7 \end{aligned}$$

Note that the last r_i that does not vanish (namely $r_3 = 7$) is the gcd of m and n. This is no accident: we claim that $r_n = \gcd(m, n)$ in general. For a proof, we have to verify two things:

Claim 1: r_n is a common divisor of m and n. Equation (4.5) shows $r_n \mid r_{n-1}$; plugging this into (4.4) we find $r_n \mid r_{n-2}$, and going back we eventually find $r_n \mid r_1$ from (4.3), $r_n \mid n$ from (4.2) and finally $r_n \mid m$ from (4.1). In particular, r_n is a common divisor of m and n.

Claim 2: if e is a common divisor of m and n, then $e \mid r_n$. This is proved by reversing the argument above: (4.1) shows that $e \mid r_1$, (4.2) then gives $e \mid r_2$, and finally we find $e \mid r_n$ from (4.5) as claimed.

The Euclidean algorithm does more than just compute the gcd: take our example $m = 56$ and $n = 35$; writing the third line as $\gcd(m, n) = 7 = 21 - 1 \cdot 14$ and replacing the 14 by $14 = 35 - 1 \cdot 21$ coming from the second line we get $\gcd(m, n) = 21 - 1 \cdot (35 - 1 \cdot 21) = 2 \cdot 21 - 1 \cdot 35$. Now $21 = 56 - 1 \cdot 35$ gives $\gcd(m, n) = 2 \cdot (56 - 1 \cdot 35) - 1 \cdot 35 = 2 \cdot 56 - 3 \cdot 35$, and we have found a Bezout representation of the gcd of 56 and 35.

This works in complete generality: (4.4) says $r_n = r_{n-2} - q_n r_{n-1}$; the line before, which $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$, allows us to express r_n as a $\mathbb{Z}$-linear combination of r_{n-2} and r_{n-3}, and going back we eventually find an expression of r_n as a $\mathbb{Z}$-linear combination of a and b.

Bezout representations have an important practical application: they allow us to compute multiplicative inverses in $\mathbb{Z}/p\mathbb{Z}$. In fact, let $[a]$ denote a nonzero residue class modulo p; since $\mathbb{Z}/p\mathbb{Z}$ is a field, $[a]$ must have a multiplicative inverse, that is, there must be a residue class $[b]$ such that $[ab] = [1]$. Since there are only finitely many residue classes, this can always be done by trial and error (unless p is large): for example, let us find the multiplicative inverse of $[2]$ in $\mathbb{Z}/5\mathbb{Z}$: multiplying $[2]$ successively by $[1]$, $[2]$, $[3]$, $[4]$ we find $[2] \cdot [3] = [6] = [1]$; thus $[2]^{-1} = [3]$ (we occasionally also write $\frac{1}{2} \equiv 3 \bmod 5$).

Computing the inverse of $[2]$ in $\mathbb{Z}/p\mathbb{Z}$ is actually always easy: note that we want an integer b such that $[2b] = [1]$; but $[1] = [p+1]$, hence we can always take $b = \frac{p+1}{2}$.

In general, however, computing inverses is done using Bezout representations. Assume that $\gcd(a, p) = 1$ (otherwise there is no multiplicative inverse), compute integers $x, y \in \mathbb{Z}$ such that $1 = ax + py$; reducing this equation modulo p gives $1 \equiv ax \bmod p$, i.e., $[a][x] = [1]$, or $[a]^{-1} = [x]$.

4.1 Prove that $2 \mid n(n+1)$ for all $n \in \mathbb{N}$
a) using induction
b) directly.

4.2 Prove that $3 \mid n(n^2 - 1)$ for all $n \in \mathbb{N}$. Generalizations?

4.3 Prove that $8 \mid (n^2 - 1)$ for all odd $n \in \mathbb{N}$.

4.4 Prove or disprove: if $n \mid ab$ and $n \nmid a$, then $n \mid b$.

4.5 Show that there are arbitrary long sequences of composite numbers (Hint: observe that $2 \cdot 3 + 2$ and $2 \cdot 3 + 3$ can be seen to be composite without performing any division; generalize!)

4.6 Show that divisibility defines a *partial order* on $\mathbb{Z}$ by writing $a \leq b$ if $b \mid a$.

4.7 Show that, for integers $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, we have

- $a \equiv b \bmod m \Longrightarrow a \equiv b \bmod n$ for every $n \mid m$;
- $a \equiv b \bmod m$ and $c \equiv d \bmod m \Longrightarrow a+c \equiv b+d \bmod m$ and $ac \equiv bd \bmod m$;
- $a \equiv b \bmod m \Longrightarrow ac \equiv bc \bmod m$ for any $c \in \mathbb{Z}$.

4.8 Show that there are infinitely many primes of the form $3n - 1$.

4.9 Try to extend the above proof to the case of primes of the form $3n + 1$ (and $5n - 1$). What goes wrong?

4.10 Show that primes $p = c^2 + 2d^2$ satisfy $p = 2$ or $p \equiv 1, 3 \bmod 8$.

4.11 Show that primes $p = c^2 - 2d^2$ satisfy $p = 2$ or $p \equiv 1, 7 \bmod 8$.

4.12 Show that primes $p = c^2 + 3d^2$ satisfy $p = 3$ or $p \equiv 1 \bmod 3$.

4.13 Compute $d = \gcd(77, 105)$ and write d as a $\mathbb{Z}$-linear combination of 77 and 105.

4.14 Check the addition and multiplication table for the ring $\mathbb{Z}/3\mathbb{Z}$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

4.15 Compute addition and multiplication tables for the rings $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

4.16 Compute the multiplicative inverse of $[17]$ in $\mathbb{Z}/101\mathbb{Z}$.

4.17 Compute $\gcd(2^m - 1, 2^n - 1)$ for small values of $m, n \geq 1$ until you discover a general formula for d.

4.18 Let $U_1 = U_2 = 1$, and $U_{n+1} = U_n + U_{n-1}$ denote the Fibonacci numbers. Find a formula for $\gcd(U_m, U_n)$.

4.19 Show that the Fermat numbers $F_n = 2^{2^n} + 1$ are pairwise coprime.

4.20 Show that there are infinitely many primes of the form $p = 4n + 3$.

4.21 Show that there are infinitely many primes of the form $p = 3n + 2$.

4.22 Compute $\gcd(x^2 + 2x + 2, x^2 - x - 2)$ over $\mathbb{Z}/m\mathbb{Z}$ for $m = 2, 3, 5$ and 7, and find its Bezout representation.

4.23 Let $a, b \in \mathbb{N}$ be coprime, and let $r \in \mathbb{N}$ be a divisor of ab. Put $u = \gcd(a, r)$ and $v = \gcd(b, r)$, and show that $r = uv$.

4.24 Assume that $M_p = 2^p - 1$ is a prime. List the complete set of (positive) divisors of $N_p = 2^{p-1}M_p$, and compute their sum. Conclude that if M_p is prime, then N_p is a perfect number (a number n is called perfect if the sum of its (positive) divisors equals $2n$).

Euler later proved that every even perfect number has the form $2^{p-1}M_p$ for some Mersenne prime M_p. It is conjectured (but not known) that odd perfect numbers do not exist.

4.25 Compute the last two digits of 27^{19}.

4.26 For primes $p \in \{3, 5, 7, 11, 13\}$, compute $A \equiv (\frac{p-1}{2})! \bmod p$. Can you find a pattern? If not, compute $B \equiv A^2 \bmod p$. Formulate a conjecture.

4.27 Check which of the primes $p \in \{3, 5, 7, 11, 13\}$ can be written as $p = a^2 + b^2$ with integers $a, b \in \mathbb{N}$ (e.g. $5 = 1^2 + 2^2$). Formulate a conjecture.

4.28 For some small primes $p = 4n + 1$, compute the smallest residue (in absolute value) of $a \bmod p$, where $a = \binom{2n}{n}$. (Example: for $p = 5$, we have $n = 1$ and $\binom{2}{1} = 2 \equiv 2 \bmod 5$.) Compare with the results from the preceding Exercise. Formulate a conjecture and test it for a few more primes.

4.29 a) Given a 5-liter jar and a 3-liter jar and an unlimited supply of water, how do you measure out 4 liters exactly?
b) Can you also measure out 1, 2 and 3 liters?
c) Which quantities can you measure out if you are given a 6-liter and a 9-liter jar?
d) Formulate a general conjecture. Can you prove it (at least partially)?

4.30 Show that a number $n = d_n \dots d_1 d_0 = d_n 10^n + \dots + d_1 \cdot 10 + d_0$ satisfies the congruence $n \equiv d_n + \dots + d_1 + d_0 \bmod 9$: the residue class modulo 9 of any integer is congruent to the sum of the digits of n.

4.31 Show that a number $d_n \dots d_1 d_0 = d_n 10^n + \dots + d_1 \cdot 10 + d_0$ satisfies the congruence $n \equiv (-1)^n d_n + \dots + d_2 - d_1 + d_0 \bmod 11$.

4.32 Invent a simple method to compute the residue class of $n = d_n \dots d_1 d_0 = d_n 10^n + \dots + d_1 \cdot 10 + d_0$ modulo 7.

4.33 Compute the last digit of 7^{100}. Compute the last two digits of 3^{65}.