Notation: Both the *set* and the *ring* of integers will be denoted by $\mathbb{Z}$; the set of natural numbers (= *positive* integers) will be denoted by $\mathbb{N}$.

Lemma 1 (Division with Remainder)**.** *For any two $a, b \in \mathbb{Z}$, $a \neq 0$, there exist unique $k, r \in \mathbb{Z}$ such that $b = ka + r$ and $0 \leq r < |a|$.*

Proof. Consider the smallest non-negative element of the set $\{b - ta;\ t \in \mathbb{Z}\}$ and denote it r; thus, $r = b - ka$ for some $k \in \mathbb{Z}$. Argue that the pair (k, r) is unique. □

Definition. For $a, b \in \mathbb{Z}$, we say that a *divides* b, and write $a|b$, if there exists a $k \in \mathbb{Z}$ such that $b = ka$.

Note that on $\mathbb{N}$, the relation $a|b$ defines a *partial order*.

Definition. If $a, b \in \mathbb{Z}$ (not both equal to 0), the *greatest common divisor* $d = \gcd(a, b)$ of a and b is the largest positive integer dividing both a and b.
We say that $a, b \in \mathbb{Z}$ are *coprime*, or *relatively prime*, if $(a, b) = 1$.
A positive integer with exactly two distinct positive divisors is a *prime number*, or a *prime*.

The following lemma is very important in proofs and in applications.

Lemma 2. *If $d = \gcd(a, b)$, then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$.*

Proof. Argue that the smallest positive element of the set $\{sa + tb;\ s, t \in \mathbb{Z}\}$ is $d = \gcd(a, b)$. □

Both $d = \gcd(a, b)$ and the numbers x, y from Lemma 1.2 can be determined by the *Euclidean algorithm*.

Corollary 3. *Let a, b be integers, not both equal to 0.*

(1) *If $k \in \mathbb{Z}$ is such that $k|a$ and $k|b$, then $k|\gcd(a, b)$.*
(2) *If $\gcd(a, b) = 1$ and if $a|bc$ for some $c \in \mathbb{Z}$, then $a|c$.*
(3) *If p is a prime, then $p|ab$ implies that $p|a$ or $p|b$.*

Proposition 4. *Let $a, b, c \in \mathbb{Z}$ such that a, b are not both equal to zero and let $d = \gcd(a, b)$. The linear Diophantine equation $ax + by = c$ has integer solutions x, y if and only if $d|c$. In such a case, all the solutions have the form $x = x_0 + tb/d$ and $y = y_0 - ta/d$ where x_0, y_0 is some solution and $t \in \mathbb{Z}$.*

Proof. If there is a solution, then clearly $d|c$. Conversely, if $c = dk$, then by Euclid's Algorithm there exist integers x, y such that $ax + by = d$, giving a solution kx, ky of the original equation. Now, if x_0, y_0 and x, y are integer solutions, then $ax_0 + by_0 = c = ax + by$, giving $(x - x_0)a/d = (y_0 - y)b/d$. Since $(a/d, b/d) = 1$, we have $x - x_0 = tb/d$ for some $t \in \mathbb{Z}$, which gives $y_0 - y = ta/d$. □

Exercise 1. Find all integer solutions of $10x - 8y = 42$.

Exercise 2. Find $(6435, 24200)$ using the Euclidean Algorithm. Feel free to use GAP, with commands like `a:=6435; b:=24200; c:=RemInt(a,b)` (E.g. repeatedly say `a:=b; b:=c; c:=RemInt(a,b)` until ...)

Exercise 3. The Fundamental Theorem of Arithmetic. We all know that—more or less—every integer is a product of primes and that there is some uniqueness in this. Give a precise statement of the theorem and prove it.
Also state carefully the well-known description of (a, b) in terms of prime factors $(a, b \in \mathbb{N})$.

Exercise 4. Define the *least common multiple* of two integers in a way similar to the above definition of the gcd. Then state and prove a fact analogous to Corollary 3(1), and also state a description of the lcm in terms of prime factors.

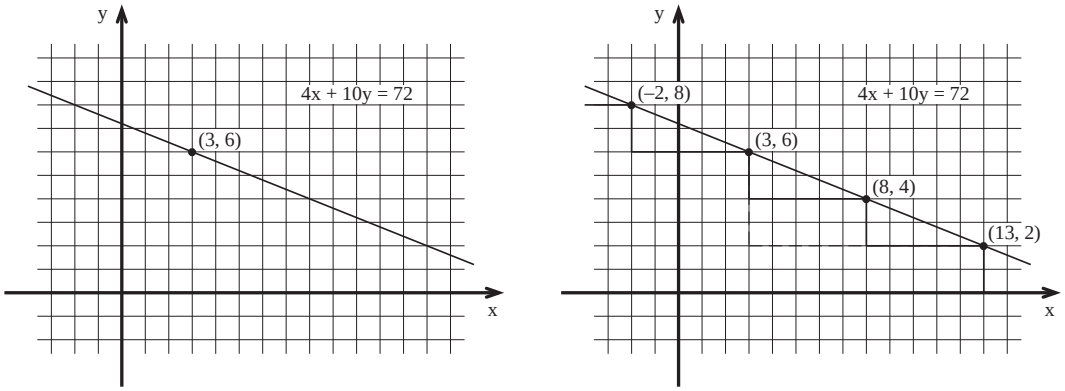
Exercise 5. The Gaussian Integers $\mathbb{Z}[i]$. Define $\mathbb{Z}[i] = \{a+bi\colon a, b \in \mathbb{Z}\}$, where $i^2 = -1$. For $u = a+bi \in \mathbb{Z}[i]$ define $N(u) = u\overline{u} = |u|^2 = a^2 + b^2$.

In $\mathbb{Z}[i]$ one has a division algorithm much like Lemma 1:
given $u, v \in \mathbb{Z}[i]$, $v \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ such that $u = vq + r$ and $N(r) < N(v)$. Prove this, or at least draw a picture which makes this infinitely plausible.

What about uniqueness of quotient and remainder?

Divide $3 + 4i$ by $3 - i$, finding a quotient and a remainder. 'Check' your result using GAP commands like
`R:=GaussianIntegers; i:=E(4); QuotientRemainder(R, 3+4*i, 3-i);`
(Of course, your quotient and remainder need not agree with the one of GAP; a picture will show why.)

Illustration of solutions to the Diophantine equation $ax + by = c$



Example of extended Euclidean algorithm

123456789	1	0
234567890	0	1
123456789	1	0
111111101	−1	1
12345688	2	−1
12345597	−17	9
91	19	−10
82	−2577652	1356659
9	2577671	−1356669
1	−25776691	13566680
0	234567890	−123456789

A simple GAP session

For information about any command, type for example `?Gcdex` at the gap prompt.

```
n := 54;  m := 14;
q := QuoInt(n,m);  r: = RemInt(n,m);
m*q + r = n;
D := Gcdex(n,m);
n * D.coeff1 + m * D.coeff2 = Gcd(n,m);
n * D.coeff3 + m * D.coeff4;
Lcm(n,m) = n * AbsoluteValue(D.coeff3);
Lcm(n,m) = m * AbsoluteValue(D.coeff4);
n := 54;  m := 14;  r := RemInt(n,m);
n := m;  m := r;  r := RemInt(n,m);
n := m;  m := r;  r := RemInt(n,m);
```