# Chapter 2

# Arithmetic

We denote the set of all integers by $\mathbb{Z}$. The arithmetic operations $+$, $-$, $\times$ are defined on $\mathbb{Z}$. In general we cannot **divide** one integer by another because this operation takes us outside the set $\mathbb{Z}$ into rational numbers. However, the following theorem alllows us to **divide with remainder**.

**Theorem 2.1** (The Division Theorem)**.** Let $a$ and $b$ be integers with $b > 0$. Then there exist unique integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < b$.

**Definition.** We call $q$ the **quotient** and $r$ the **remainder** on dividing $a$ by $b$.

Just to reiterate, the remainder must be **non-negative** and **less than** $b$.

**Proof**. The proof of the Division Theorem consists of two parts, existence and uniqueness.

**Existence:** Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. The set

$$R = \{a - bp \mid p \in \mathbb{Z},\ a - bp \geq 0\}.$$

is non-empty: if $a \geq 0$ then $a - b0 \in R$ (the integer $a - b0$ is non-negative) whereas if $a < 0$ then $a - ba = (b-1)(-a) \in R$ (the integer $(b-1)(-a)$ is non-negative). A non-empty set of non-negative integers contains least element so let

$$r = \min R$$

and let $q$ be the integer such that $r = a - bq$. Since $r \in R$, we have $r \geq 0$. It remains to prove that $r < b$. Assume for contradiction that $r \geq b$. Then $a - b(q+1) = r - b \geq 0$ so that $a - b(q+1)$ is an element of $R$ which is less than $r = \min R$, contradiction.

Thus, the integers $q$ and $r$ satisfy $a - bq = r$ and $0 \leq r < b$. Existence is proved.

**Uniqueness:** we take two pairs, $(q_1, r_1)$ and $(q_2, r_2)$ for which

$$a = bq_1 + r_1 = bq_2 + r_2, \qquad 0 \le r_1, r_2 < b.$$

and show that these pairs are equal. Assume $r_1 \le r_2$. Since $(bq_1 + r_1) - (bq_2 + r_2) = 0$, we have $b(q_1 - q_2) = r_2 - r_1$ so $0 \le q_1 - q_2 = \frac{r_2 - r_1}{b} \le \frac{r_2}{b} < 1$. Since $q_1 - q_2$ is an integer, $q_1 - q_2 = 0$ and $q_1 = q_2$. Also, $r_1 = a - bq_1 = a - bq_2 = r_2$. Uniqueness is proved. □

**Remark.** The Division Theorem tells us that the quotient and remainder exist and are unique. It is easy to **verify** that $q$ and $r$, once found, are indeed the quotient and remainder: one checks that $a = bq + r$, that $r \ge 0$ and that $r < b$.

But in applications, we need to **find** $q$ and $r$. A classical method for this is **long division** of integers. Students are expected to master this method which is applicable not only to positive integers but to decimal fractions, polynomials etc.

In practice, $q$ can be found by dividing $a$ by $b$ on a calculator, but verification of the three conditions as above is necessary, and the students need to understand what they are doing. The calculator method will not be demonstrated in the course.

**Example.** Let $b = 41$ and $a = 166361$. Long division of $a$ by $b$:

$$\begin{array}{r|r}
\multicolumn{1}{r}{} & 004043 \\ \cline{2-2}
41 & 166361 \\
\multicolumn{1}{r}{} & 161720 \\ \cline{2-2}
\multicolumn{1}{r}{} & 4641 \\
\multicolumn{1}{r}{} & 4043 \\ \cline{2-2}
\multicolumn{1}{r}{} & 598
\end{array}$$

So $166361 = 41 \times 4043 + 598$, hence $q = 4043$ and $r = 598$.

Now, what is the quotient and remainder on dividing $a = -166361$ by $b = 4043$?

From the above we have, on multiplying by $-1$,

$$\begin{aligned}
-166361 &= (-41) \times 4043 - 598 \qquad \textit{but } -598 \textit{ is not the remainder as it is negative} \\
&= (-42) \times 4043 + 4043 - 598 \\
&= (-42) \times 4043 + 3445,
\end{aligned}$$

all because the remainder has to be *non-negative*. Thus $q = -42$ and $r = 3445$.

The case where the remainder is $0$ deserves a special definition.

**Definition** (Divisor)**.** An integer $b$ is a **divisor** of an integer $a$ (or: $b$ **divides** $a$) if there exists an integer $c$ such that $a = bc$. Notation: $b \mid a$.

**Remark** (Every integer divides zero)**.** $0$ is divisible by **all** integers, whereas $0$ divides only $0$.

**Definition** (GCD)**.** Let $a$ and $b$ be integers. The **greatest common divisor** of $a$ and $b$ is

$$\gcd(a,b) = \max\{c \in \mathbb{Z} : (c \mid a) \wedge (c \mid b)\}.$$

If $a = b = 0$, all integers divide $a$ and $b$ so $\max$ does not exist; by convention, $\mathbf{gcd(0,0) = 0}$.

**Remark** (GCD exists)**.** If $(a,b) \neq (0,0)$, the set of integers $c$ such that $c \mid a$ and $c \mid b$ is finite. Indeed, if $a \neq 0$ and $c \mid a$, then $kc = a$ for some integer $k$ so $|c| \leq |a|/|k| \leq |a|$. This leaves finitely many possibilities for $c$. Each finite set of integers has a maximum element, so $\gcd(a,b)$ is well defined.

**Remark** (Easy rules for $\gcd(a,b)$)**.** These rules help find $\gcd(a,b)$ in simple cases and should be used before **Euclid's algorithm** given below.

- $\gcd(0,b) = |b|$. Indeed, the common divisors of $0$ and $b$ are simply the divisors of $b$. By the previous remark, the maximal divisor of $b$ is $|b|$.
- $\gcd(a,b) = \gcd(|a|,|b|)$. This is because $a$ and $|a|$ have exactly the same divisors.

**Algorithm** (Euclid)**.** Let $a, b \in \mathbb{N}$. Repeated division with remainder leads to a series of equations

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ &\vdots \end{aligned}$$

Repeat until the next remainder, say $r_{j+1}$, is zero:

$$\begin{aligned} &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Output $r_j$, the last non-zero remainder.

**Theorem 2.2** (Euclid's Algorithm works)**.** Euclid's algorithm terminates after finitely many steps. The output value, $r_j$, is $\gcd(a, b)$.

**Proof**. The process cannot go on forever: by the Division Theorem, the remainders obtained are non-negative and strictly decreasing, $b > r_1 > r_2 > \ldots$, so will eventually reach zero where the process stops.

We now need the following

*Claim.* For $a, b, q \in \mathbb{Z}$, $\gcd(a, b) = \gcd(b, a - bq)$.

*Proof of Claim.* If $c$ is a common divisor of $a$ and $b$ then $a = kc$, $b = \ell c$ so $a - bq = (k - \ell q)c$ where $k, \ell$ and also $k - \ell q$ are integers. Hence $c$ is a common divisor of $b$ and $a - bq$. In the same way, if $d$ is a common divisor of $b$ and $a - bq$, then $b = md$, $a - bq = nd$ so $a = (a - bq) + bq = (n - qm)d$ and $d$ is a common divisor of $a$ and $b$. Hence the pairs $(a, b)$ and $(b, a - bq)$ have the same set of common divisors. In particular, they have the same greatest common divisor. The Claim is proved.

By the Claim, $\gcd(a, b) = \gcd(b, r_1)$ because $r_1 = a - bq_1$. Now apply the Claim to $(b, r_1)$ to conclude that $\gcd(b, r_1) = \gcd(r_1, r_2)$ as $r_2 = b - r_1 q_2$. Continuing in the same way, we show that $\gcd(a, b)$ is equal to $\gcd(r_j, 0)$ which is $r_j$. Theorem 2.2 is proved. □

**Example** (Use of Euclid's Algorithm)**.** Calculate $\gcd(598, 455)$.

**Solution.** Use Euclid's algorithm:

$$598 = 455 \times 1 + 143.$$

The remainder $r_1 = 143$ is not zero — continue:

$$\begin{aligned} 455 &= 143 \times 3 + 26, \\ 143 &= 26 \times 5 + 13, \\ 26 &= 13 \times 2 + 0. \end{aligned}$$

Remainder $0$ has been obtained so the algorithm stops. Hence $\gcd(598, 455) = 13$.

**Lemma 2.3** (Bezout's Lemma)**.** Let $a, b \in \mathbb{Z}$. Then there exist $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = am + bn$.

**Proof**. **If $a > 0$, $b > 0$:** we show that in Euclid's Algorithm, each remainder $r_k$ can be written as $am_k + bn_k$ for some integers $m_k$, $n_k$. We denote $r_0 = b$ and use strong induction in $k$. Base cases: $k = 0$, $r_0 = a0 + b1$; $k = 1$, $r_1 = a - bq_1$ so we put $m_1 = 1$ and $n_1 = -q_1$. Inductive step: assume that

$$\begin{aligned} r_{k-1} &= am_{k-1} + bn_{k-1}, \\ r_k &= am_k + bn_k \end{aligned}$$

where $m_{k-1}$, $n_{k-1}$, $m_k$, $n_k$ are integers. Then

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = a(m_{k-1} - m_k q_{k+1}) + b(m_{k-1} - m_k q_{k+1})$$

where the coefficients of $a$ and $b$ are integers, so that the statement is true for $r_{k+1}$. By induction, the statement holds for all $k$. In particular, $\gcd(a, b) = r_j = am_j + bn_j$ for some integers $m_j$, $n_j$. Bezout's Lemma is proved for positive $a$, $b$.

**If $a < 0$, $b > 0$:** by the Easy Rules for GCD, $\gcd(a, b) = \gcd(-a, b) = (-a)m+bn = a(-m)+bn$ where $-m$, $n$ are integers.

**If $a = 0$, $b > 0$:** by the Easy Rules for GCD, $\gcd(0, b) = b = a0 + b1$ where $m = 0$, $n = 1$ are integers.

The cases $b = 0$ and $b < 0$ are similar to the above and are left to the student as an exercise. □

**Example** (Writing $\gcd(a, b)$ as $am + bn$ by working back up Euclid's algorithm)**.** Write $13 = \gcd(598, 455)$ as an *integral linear combination of* 598 *and* 455.

**Solution.** Recall from the previous example:

$$\begin{aligned} (***) \qquad & 598 = 455 \times 1 + 143 \\ (**) \qquad & 455 = 143 \times 3 + 26 \\ (*) \qquad & 143 = 26 \times 5 + \mathbf{13}. \end{aligned}$$

We *start from the line where* 13 *is obtained as a remainder*, marked (*):

$$13 = 143 - 26 \times 5 \qquad (\textit{linear combination of } 143 \textit{ and } 26)$$

Proceed back up to line (**):

$$13 = 143 - (455 - 143 \times 3) = 455(-5) + 143 \times 16 \quad (\textit{linear combination of } 455 \textit{ and } 143)$$

Finally, go back up to line (***):

$$13 = 455(-5) + (598 - 455) \times 16 = 598 \times 16 + 455(-21) \ (\textit{linear combination of } 598 \textit{ and } 455)$$

*Always, always* check your answers by multiplying out the final answer.

**Remark** (Is the pair $(m,n)$ unique?)**.** This method — working back up Euclid's algorithm — gives **one** pair $(m,n)$ such that $am+bn=\gcd(a,b)$. There **always** are **infinitely many** other solutions.

An important case where the GCD is $1$ deserves a special name:

**Definition** (Coprime integers)**.** Two integers $a$ and $b$ are said to be **coprime** if $\gcd(a,b)=1$.

We now give a simple result that has many applications.

**Lemma 2.4** (The coprime factor lemma)**.** If $a$ divides $bc$ and $a$ is coprime to $b$, then $a$ divides $c$.

**Proof**. Assume that $a \mid bc$, so that $bc = ak$, $k \in \mathbb{Z}$; and that $\gcd(a,b)=1$, so that by Bezout's Lemma, $am+bn=1$, $m,n\in\mathbb{Z}$. Multiplying both sides by $c$ we obtain $acm+bcn=c$, equivalently $a(cm+kn)=c$. As $cm+kn$ is an integer, $a \mid c$ by definition. □

## Linear Diophantine Equations

**Definition** (linear Diophantine equation)**.** Let $a,b,c\in\mathbb{Z}$. The equation $ax+by=c$ is known as a **linear Diophantine equation** in two unknowns. A solution to this equation is a pair $(x,y)\in\mathbb{Z}^2$.

**Theorem 2.5** (criterion for existence of solutions)**.** The Diophantine equation $ax+by=c$ has solutions, if and only if $\gcd(a,b)\mid c$.

**Proof**. Let $d=\gcd(a,b)$.

$\Longrightarrow$ : assume that the equation has solution $(x_0,y_0)$, i.e., $ax_0+by_0=c$. Recall that $d$ is a common divisor of $a$ and $b$, so that $a=dk$ and $b=d\ell$ for integers $k,\ell$. Then $c=dkx_0+d\ell y_0=d(kx_0+\ell y_0)$. So $d$ divides $c$, as required.

$\Longleftarrow$ : assume $d\mid c$ so that $c=dp$ for some integer $p$. By Bezout's Lemma, $\exists(m,n)\in\mathbb{Z}^2$: $am+bn=d$. Multiplying through by $p$ gives $a(mp)+b(np)=dp=c$. Hence the equation has solution $(mp,np)$. □

**Question.** If a linear Diophantine equation is soluble, is there a method for finding a solution (other than guessing)?

**Example** (Finding a particular solution of a linear Diophantine equation)**.** Check that the equation $598x+455y=-26$ is soluble in integers and find one integer solution.

**Solution. Step 1: Find the GCD of the coefficients $a$, $b$ and check that it divides the constant term $c$.** We need to find $\gcd(598, 455)$. We did this in an earlier Example where used Euclid's Algorithm to obtain $\gcd(598, 455) = 13$. Since $13$ divides $-26$, the equation **has** solutions.

**Step 2: Write the GCD as $am + bn$.** In an earlier example, we worked back up Euclid's Algorithm to write $598 \times 16 + 455(-21) = 13$.

**Step 3: Multiply through by an integer to obtain $ax_0 + by_0 = c$.** Given that $598 \times 16 + 455(-21) = 13$, we multiply through by $-2$ to get

$$598(-32) + 455 \times 42 = -26.$$

Hence $(-32, 42)$ is a solution.

**Terminology.** A single solution $(x_0, y_0)$ to a Diophantine equation is referred to as a **particular solution**.

**Question.** We have seen a method of finding a particular solution by working back up Euclid's Algorithm. How to find all solutions (find the **general solution**)?

**Example.** Find **all** integer solutions to $598x + 455y = -26$.

**Solution.** We continue from the previous example.

**Step 4: Write down the homogeneous equation.** We are solving

$$598x + 455y = -26$$

and we have already found the particular solution

$$598(-32) + 455 \times 42 = -26.$$

Subtracting, we obtain

$$598(x + 32) + 455(y - 42) = 0.$$

A linear equation with constant term $0$ is termed a **homogeneous equation**.

**Step 5: Divide through by GCD to obtain an equation with coprime coefficients.** Divide through by $13$ to obtain an equivalent equation

$$46(x + 32) + 35(y - 42) = 0$$

**Step 6: Use the coprime factor lemma to find the general solution.** Note that the equation is

$$46(x+32) = -35(y-42)$$

where $46$ is coprime to $-35$. By the coprime factor lemma 2.4, $46$ divides $-35(y-42)$ implies that $46 \mid (y-42)$, so

$$y - 42 = 46t, \quad t \in \mathbb{Z}.$$

Substitute this back in the equation: $46(x+32) = -35(46t)$, therefore $x + 32 = -35t$. Hence **all** the solutions are given by

$$(-32-35t,\ 42+46t) \quad \text{for all } t \in \mathbb{Z}. \tag{A1}$$

For example, if one wants to get a solution with positive $x$, one may choose $t = -1$ to get $(3, -4)$. *Check that* $(3, -4)$ *is a solution!*

**Solution** (Second solution)**.** An **alternative**, but also valid, way to proceed when we know $\gcd(a, b)$ is to divide the equation $ax + by = c$ through by $\gcd(a, b)$. Let us demonstrate this.

Divide the equation $598x + 455y = -26$ through by $13$ to obtain the equivalent equation

$$46x + 35y = -2.$$

If one is lucky, one can **notice** that

$$46 \times 3 - 35 \times 4 = 138 - 140 = -2,$$

so that $(x_0, y_0) = (3, -4)$ is a particular solution. Subtracting, we obtain

$$46(x-3) + 35(y+4) = 0,$$

so, using that $46$ is coprime to $35$, we conclude that $y + 4$ is divisible by $46$ hence $y + 4 = 46k$, $k \in \mathbb{Z}$. Substituting, $x - 3 = -35k$, so the general general solution is

$$(x, y) = (3-35k,\ -4+46k), \qquad k \in \mathbb{Z}. \tag{A2}$$

**Important remark:** Formulas (A1) and (A2), even though they may look different and were obtained from different particular solutions, give *exactly the same* general solution. This can be seen by putting $k = t + 1$ which leads to $3 - 35k = -32 - 35t$ and $-4 + 46k = 42 + 46t$. Of course, if $t$ runs over the set of all integers, then $k = t + 1$ also runs over the set of all integers.

The above method of solving a linear Diophantine equations leads to the following

**Theorem 2.6** (general solution to a linear Diophantine equation)**.** If $(a, b) \neq (0, 0)$, $ax + by = c$ is soluble and $(x_0, y_0)$ is a solution, then all solutions are given by

$$\Big(x_0 - \frac{b}{\gcd(a,b)}t,\ y_0 + \frac{a}{\gcd(a,b)}t\Big), \qquad \text{with } t \in \mathbb{Z}.$$

**Proof**. *This proof is included in the lecture notes for completeness but will not be given in the lectures. Students are expected to solve linear Diophantine equations following the steps above but can refer to this proof in the notes if they wish.*

We prove the Theorem assuming that $a \neq 0$. The case $a = 0$ is left as an exercise to the student.

Let $d = \gcd(a, b)$. The pair $(x, y) \in \mathbb{Z}^2$ is a solution to $ax + by = c$ iff $ax + by = ax_0 + by_0$ iff $a(x - x_0) + b(y - y_0) = 0$, which is equivalent (after dividing through by $d$ and rearranging) to the equation

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{†}$$

If this holds, $a/d$ divides $-(b/d)(y-y_0)$. Indeed, we can see from equation (†) that $-(b/d)(y-y_0)$ equals $a/d$ times $(x - x_0)$ where $x - x_0$ is an integer.

But $a/d$ is coprime to $b/d$ (*see homework problem sheet*). Hence by the coprime factor lemma 2.4, $a/d$ must divide $-(y - y_0)$ so that $y - y_0 = (a/d)t$ for some $t \in \mathbb{Z}$.

To find $x$, we substitute $y - y_0 = (a/d)t$ in equation (†):

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}\frac{a}{d}t, \qquad t \in \mathbb{Z}.$$

By assumption, $a \neq 0$, so $a/d \neq 0$. Dividing through by $a/d$, we obtain the equivalent equation for $x$:

$$x - x_0 = -\frac{b}{d}t.$$

Thus, every solution has the form

$$x = x_0 - \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t$$

for **some** $t \in \mathbb{Z}$.

It remains to check that, for **all** $t \in \mathbb{Z}$, $\big(x_0 - \frac{b}{d}t,\ y_0 + \frac{a}{d}t\big)$ **is** a solution. This is done by substitution:

$$a\Big(x_0 - \frac{b}{d}t\Big) + b\Big(y_0 + \frac{a}{d}t\Big) = ax_0 + by_0 - \frac{ab}{d}t + \frac{ba}{d}t = ax_0 + by_0 = c$$

as required. □