6 Algorithms and Recursion

An algorithm is a logical step-by-step procedure for solving a problem in a finite number of steps. Many algorithms are recursive, meaning that after one or more initial steps, a general method is given for determining each subsequent step on the basis of steps already taken. As an example of a recursive algorithm, we will later discuss Euclid's algorithm for finding the greatest common divisor of two non-zero integers.

First, recall the **Division Algorithm**: For $a, b \in \mathbb{N}$, we have that $\exists!\, q, r \in \mathbb{Z}$ such that $b = aq + r$ where $0 \leq r < a$.

Remark. *The Division Algorithm can be extended to $a, b \in \mathbb{Z}$ when $a \neq 0$: $\exists!\ q, r \in \mathbb{Z}$ such that $b = aq + r$, where $0 \leq r < |a|$.*

Let $n \in \mathbb{N}$. An immediate consequence of the Division Algorithm is that $\forall\, b \in \mathbb{Z}$, $\exists!\, r \in \mathbb{Z}$ such that $b \equiv r \pmod{n}$ with $0 \leq r < n$. Hence, we partition $\mathbb{Z}$ into n congruence classes modulo n. For $n \geq 3$, these congruence classes are as follows.

$$\begin{aligned}
[0] &= \{b \in \mathbb{Z} :\ b \equiv 0 \pmod{n}\} = n\mathbb{Z}, \\
[1] &= \{b \in \mathbb{Z} :\ b \equiv 1 \pmod{n}\} = 1 + n\mathbb{Z}, \\
[2] &= \{b \in \mathbb{Z} :\ b \equiv 2 \pmod{n}\} = 2 + n\mathbb{Z}, \\
[3] &= \{b \in \mathbb{Z} :\ b \equiv 3 \pmod{n}\} = 3 + n\mathbb{Z}, \\
&\vdots \\
[n-1] &= \{b \in \mathbb{Z} :\ b \equiv n-1 \pmod{n}\} = (n-1) + n\mathbb{Z}.
\end{aligned}$$

Definition 6.1. *Let $a, b, c \in \mathbb{Z}$. We say that c is a **common divisor** of a and b if $c \mid a$ and $c \mid b$.*

Note that 1 is always a common divisor of a and b, and if $a \neq 0$, no integer larger than $|a|$ can be a common divisor of a and b. Further note that every $x \in \mathbb{Z}$ is a divisor of 0 since $0 = 0 \cdot x$.

Definition 6.2. *Let $a, b \in \mathbb{Z}$ with a, b not both equal to 0. We denote by $\gcd(a, b)$ (or equivalently hcf (a, b)), the **greatest common divisor** of a and b, that is $\gcd(a, b)$ is the largest positive divisor that divides both a and b.*

Remark. *Note that $\gcd(0, 0)$ does not exist since every integer is a divisor of 0. This follows since, for $x \in \mathbb{Z}$, we have that $0 = x \cdot 0$, so $x \mid 0$. However, for $a \in \mathbb{Z}$ with $a \neq 0$, we have that $\gcd(a, 0) = |a|$.*

We have the following theorem.

Theorem 6.3. *Let $a, b \in \mathbb{Z}$ with a, b not both equal to 0, and let $\gcd(a, b) = c$. Then $\exists\, s, t \in \mathbb{Z}$ such that $c = as + bt$.*

Proof. Let A be the following set.

$$A = \{as + bt :\ (s, t \in \mathbb{Z}) \wedge (as + bt > 0)\ \}.$$

This is a subset of $\mathbb{N}$ which is non-empty, and it is bounded below by 1, so it has a minimum value. We denote this minimum value by d and take $s, t \in \mathbb{Z}$ such that $d = as + bt$. Note that $c \mid d$ since $c \mid a$ and $c \mid b$. Hence, $c \leq d$.

Now, take $q, r \in \mathbb{Z}$ such that $a = dq + r$ with $0 \leq r < d$. Then

$$r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq).$$

If $r > 0$, then $r \in A$ with $r < d$, contrary to how we chose d. Hence, we must have that $r = 0$, which means $d \mid a$. Similarly, we can show that $d \mid b$, so d is a common divisor of a and b. Since $c = \gcd(a, b)$, we have that $d \leq c$. Since $c \leq d$ and $d \leq c$, it follows that $c = d$. Hence, $\gcd(a, b) = c = d = as + bt$. □

Note that, for $a, b \in \mathbb{Z}$ with a, b not both equal to 0, this proof shows the existence of some $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$, but it does not give us the actual values of s and t. **Euclid's Algorithm** will produce these values:

To explain the steps in Euclid's Algorithm, we need the following proposition.

Proposition 6.4. *Let $a, b, x \in \mathbb{Z}$ with with a, b not both equal to 0. Then* $\gcd(|a|, |b|) = \gcd(a, b) = \gcd(b, a + bx)$.

Proof. Exercise 4.5. □

Take $a, b \in \mathbb{Z}$ with $b \neq 0$. We will first compute $\gcd(a, b)$, and then we will construct $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.

- Step 1: Choose $q_1, r_1 \in \mathbb{Z}$ such that $a = b \cdot q_1 + r_1$ with $0 \leq r_1 \leq |b|$. If $r_1 = 0$, then we stop. Otherwise, we continue.
- Step 2: Choose $q_2, r_2 \in \mathbb{Z}$ such that $b = r_1 \cdot q_2 + r_2$ with $0 \leq r_2 < r_1$. If $r_2 = 0$, then we stop. Otherwise, we continue.
- Step k: For $k \geq 3$, choose $q_k, r_k \in \mathbb{Z}$ such that $r_{k-2} = r_{k-1} \cdot q_k + r_k$ with $0 \leq r_k < r_{k-1}$. If $r_k = 0$ then we stop. Otherwise, we continue.

Notice that after k steps, we have $|b| > r_1 > r_2 > \cdots > r_k \geq 0$. Hence, the algorithm must terminate after at most $|b|$ steps. If it terminates after 1 step, then $\gcd(a, b) = |b|$, and we know that

$$|b| = \begin{cases} a \cdot 0 + b \cdot 1, & \text{if } b > 0, \\ a \cdot 0 + b \cdot (-1), & \text{if } b < 0. \end{cases}$$

So suppose the algorithm terminates after n steps, for $n > 1$. We claim that $r_{n-1} = \gcd(a, b)$.

We note that $r_1 = a - b \cdot q_1$ and $r_2 = b - r_1 \cdot q_2$, and for $3 \leq k < n$, we have $r_k = r_{k-2} - r_{k-1} \cdot q_k$. Then by Proposition 6.4, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n).$$

Since the algorithm terminates after n steps, we have that $r_{n-1} > 0$ but $r_n = 0$. It follows that $\gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}$. Substituting $r_k = r_{k-2} - r_{k-1} \cdot q_k$ for $3 \leq k < n$, $r_2 = b - r_1 \cdot q_2$, and $r_1 = a - b \cdot q_1$, we get $r_{n-1} = as + bt$.

Example. *We want to compute* $\gcd(1451, 323)$ *and find $s, t \in \mathbb{Z}$ such that* $\gcd(1451, 323) = 1451s + 323t$. *We have*

$$\begin{aligned} 1451 &= 323 \cdot 4 + 159 && [\textit{so } q_1 = 4 \textit{ and } r_1 = 159] \\ 323 &= 159 \cdot 2 + 5 && [\textit{so } q_2 = 2 \textit{ and } r_2 = 5] \\ 159 &= 5 \cdot 31 + 4 && [\textit{so } q_3 = 31 \textit{ and } r_3 = 4] \\ 5 &= 4 \cdot 1 + 1 && [\textit{so } q_4 = 1 \textit{ and } r_4 = 1] \\ 4 &= 1 \cdot 4 + 0 && [\textit{so } q_5 = 4 \textit{ and } r_5 = 0] \end{aligned}$$

Hence $\gcd(1451, 323) = r_4 = 1$. *Solving the above equations for* r_4, r_3, r_2, r_1 *gives us:*

$$\begin{aligned} r_4 &= 1 = 5 - 4 \cdot 1, \\ r_3 &= 4 = 159 - 5 \cdot 31, \\ r_2 &= 5 = 323 - 159 \cdot 2, \\ r_1 &= 159 = 1451 - 323 \cdot 4. \end{aligned}$$

Then

$$\begin{aligned} 1 &= 5 - (159 - 5 \cdot 31) \cdot 1 \\ &= 5 \cdot 32 - 159 \cdot 1 \\ &= (323 - 159 \cdot 2) \cdot 32 - 159 \cdot 1 \\ &= 323 \cdot 32 - 159 \cdot 65 \\ &= 323 \cdot 32 - (1451 - 323 \cdot 4) \cdot 65 \\ &= 323 \cdot 292 - 1451 \cdot 65. \end{aligned}$$

It follows that $\gcd(1451, 323) = 1 = 1451s + 323t$ *where* $s = -65$ *and* $t = 292$.

We have the following definition.

Definition 6.5. *We say that* a, b *are* ***relatively prime*** *if* $\gcd(a, b) = 1$.

As an application of Euclid's Algorithm, we have the following theorem.

Theorem 6.6 (Chinese Remainder Theorem)**.** *Let* $m, n \in \mathbb{N}$ *with* $\gcd(m, n) = 1$. *For any* $a, b \in \mathbb{Z}$, $\exists\, x \in \mathbb{Z}$ *such that*

$$x \equiv a \ (mod\ m) \qquad \text{and} \qquad x \equiv b \ (mod\ n).$$

Further, for $x' \in \mathbb{Z}$, *we have that*

$$x' \equiv a \ (mod\ m) \qquad \text{and} \qquad x' \equiv b \ (mod\ n)$$

if and only if

$$x' \equiv x \ (mod\ mn).$$

Proof. We will prove the first part of the theorem and leave the second part as Exercise 4.7.

Since $\gcd(m, n) = 1$, we know that there exist $s, t \in \mathbb{Z}$ such that $ms + nt = 1$. Then

$$1 \equiv ms + nt \equiv nt \ (\text{mod } m)$$

and

$$1 \equiv ms + nt \equiv ms \ (\text{mod } n).$$

Now, take $x = msb + nta$. Then

$$x \equiv nta \equiv 1 \cdot a \equiv a \ (\text{mod } m)$$

and

$$x \equiv msb \equiv 1 \cdot b \equiv b \ (\text{mod } n).$$

□

Example. *We want to find $x \in \mathbb{Z}$ such that $x \equiv 4 \pmod 5$ and $x \equiv 7 \pmod 8$.*

We have that $\gcd(5,8) = 1$, so we set $x = msb + nta$, where $a = 4, m = 5, b = 7, n = 8$ and s, t are such that $gcd(5,8) = 5s + 8t$. We have that

$$\begin{aligned} 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

so

$$\begin{aligned} 1 &= 3 - 2 \\ 2 &= 5 - 3 \\ 3 &= 8 - 5 \end{aligned}$$

Then

$$\begin{aligned} gcd(5,8) = 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2(8 - 5) - 5 \\ &= 2 \cdot 8 - 3 \cdot 5 \end{aligned}$$

so $s = -3$ and $t = 2$. Hence, we set

$$x = msb + nta = 5 \cdot -3 \cdot 7 + 8 \cdot 2 \cdot 4 = -105 + 64 = -41.$$

We double check that x indeed satisfies the given congruences:

$$\begin{aligned} x = -41 &\equiv 4 \equiv a \pmod 5 \\ = -41 &\equiv 7 \equiv b \pmod 8 \end{aligned}$$

Note that x' such that $x' \equiv x \pmod{40} = -1, 39, 79, \ldots$ are also solutions.

We have the following propositions.

Proposition 6.7. *Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. If $c \mid ab$ and $\gcd(b, c) = 1$, then $c \mid a$.*

Proof. Exercise 4.4 b). □

Proposition 6.8. *Let $a, b \in \mathbb{Z}$ and suppose $\gcd(a, b) = c$. Take $x, y \in \mathbb{Z}$ such that $a = cx$ and $b = cy$. Then $\gcd(x, y) = 1$.*

Proof. Exercise 4.4 c). □

Definition 6.9. *Let $a, b, c \in \mathbb{Z}$. Then c is a **common multiple** of a and b if both $a \mid c$ and $b \mid c$.*

Definition 6.10. *Let $a, b \in \mathbb{Z}\backslash\{0\}$. Then the **least common multiple** of a and b, denoted by $lcm(a, b)$, is the smallest positive integer which is divisible by both a and b.*

We have the following proposition.

Proposition 6.11. *Let $a, b \in \mathbb{Z}\backslash\{0\}$. Then $lcm(a, b)\gcd(a, b) = |ab|$.*

Proof. Let $\gcd(a, b) = c$. Then $c \mid a$ and $c \mid b$, so $c \mid |ab|$. Hence, $\exists\, m, n, k \in \mathbb{Z}$ such that $a = cm, b = cn$ and $|ab| = ck$. Then $ck = |ab| = |cmb| = |acn|$, so either $k = mb$ or $k = -mb$ and either $k = an$ or $k = -an$. Hence $a \mid k$ and $b \mid k$, so k is a common multiple of a and b. Further, since $|ab| = ck$ and $c \geq 1$, then $k \in \mathbb{N}$.

Now, suppose that $l \in \mathbb{N}$ is also a common multiple of a and b. Then $a \mid l$ and $b \mid l$, so $\exists\, u, v \in \mathbb{Z}$ such that $l = au = bv$. Further, since $gcd(a, b) = c$, $\exists\, s, t \in \mathbb{Z}$ such that $c = as + bt$. Then

$$\begin{aligned} lc &= l(as + bt) \\ &= las + lbt \\ &= bvas + aubt \\ &= ab(vs + ut). \end{aligned}$$

Since $|ab| = ck$, then either $lc = ck(vs + ut)$ or $lc = -ck(vs + ut)$. It follows that either $l = k(vs + ut)$ or $l = -k(vs + ut)$. Since $\pm(vs + ut) \in \mathbb{Z}$, then $k \mid l$. Therefore, $k \leq l$, so k must be the smallest common multiple of a and b, that is $\text{lcm}(a, b) = k$. It follows that

$$\text{lcm}(a, b)\gcd(ab) = ck = |ab|.$$

□

As an immediate consequence of Proposition 6.11, we have the following corollary.

Corollary 6.12. *Let $a, b \in \mathbb{Z}\backslash\{0\}$. If $gcd(a, b) = 1$, then $lcm(a, b) = |ab|$.*