Chapter 6

Linear Diophantine equations

Given two integers \(a, b\), a common divisor is an integer \(d\) such that \(d | a\) and \(d | b\). The greatest common divisor is exactly that, the common divisor greater than or equal to all others (it exists since the set of common divisors is finite). We denote this by \(\text{gcd}(a, b)\).

**Lemma 6.1 (Euclid).** If \(a, b\) are natural numbers then \(\text{gcd}(a, b) = \text{gcd}(b, a \mod b)\)

**Proof.** Let \(r = a \mod b\). Then the division algorithm gives \(a = qb + r\) for some \(q\). It follows from exercise 2 of the chapter 4 that \(\text{gcd}(b, r) | a\). Since \(\text{gcd}(b, r) | b\), we can conclude that \(\text{gcd}(b, r) \leq \text{gcd}(a, b)\). On the other hand, \(r = a - qb\) implies that \(\text{gcd}(a, b) | r\). Therefore \(\text{gcd}(a, b)\) is a common divisor of \(b\) and \(r\), so \(\text{gcd}(a, b) \leq \text{gcd}(b, r)\).

This lemma leads to a method for computing gcgs. For example

\[
\text{gcd}(100, 40) = \text{gcd}(40, 20) = \text{gcd}(20, 0) = 20.
\]

A **Diophantine equation** is an equation where the solutions are required to be integers or rationals. The simplest examples are the linear ones: given integers \(a, b, c\), find all integers \(m, n\) such that \(am + bn = c\). If a solution exists, then \(\text{gcd}(a, b)\) must divide \(c\) by exercise 2 of chapter 3. The converse is also true:

**Theorem 6.2.** Given integers \(a, b, c\), \(am + bn = c\) has a solution with \(m, n \in \mathbb{Z}\) if and only if \(\text{gcd}(a, b) | c\).

**Proof.** Since \((m', n') = (\pm m, \pm n)\) is a solution of \(\pm an' + \pm bm' = c\), we may as well assume that \(a, b \geq 0\). We now prove the theorem for natural numbers \(a, b\) by induction on the minimum \(\text{min}(a, b)\).

If \(\text{min}(a, b) = 0\), then one of them, say \(b = 0\). Since \(a = \text{gcd}(a, b)\) divides \(c\) by assumption, \((c/a, 0)\) gives a solution of \(am + bn = c\). Now assume that the theorem that \(a'm + b'n = c'\) has a solution whenever \(\text{min}(a', b') < \text{min}(a, b)\) and
the other conditions are fulfilled. Suppose \( b \leq a \), and let \( r = r(a, b) = a \mod b \) and \( q = q(a, b) \) be given as in theorem 2.6. Then \( rm' + bn' = c \) has a solution since \( \min(r, b) = r < b = \min(a, b) \) and \( \gcd(b, r) = \gcd(a, b) \) divides \( c \). Let \( m = m' \) and \( n = n' \), then

\[
am + bn = an' + b(m' - qn') = bm' + rn' = c.
\]

\[ \square \]

**Corollary 6.3.** Given \( a, b \in \mathbb{Z} \), there exists \( m, n \in \mathbb{Z} \) such that \( am + bn = \gcd(a, b) \).

The proof yields a method for finding a solution. For simplicity assume that \( a \geq b \geq 0 \). Then a solution to \( am + bn = c \) is given by \( m = s_1(a, b, c), n = s_2(a, b, c) \) where these functions are given recursively:

\[
s_1(a, b, c) = \begin{cases} 
c/a & \text{if } b=0 \\
s_2(b, r(a, b), c) & \text{otherwise}
\end{cases}
\]

\[
s_2(a, b, c) = \begin{cases} 
0 & \text{if } b=0 \\
s_1(b, r(a, b), c) - q(a, b)s_2(b, r(a, b), c) & \text{otherwise}
\end{cases}
\]

This is easy to implement in Maple:

\[
> s1 := (a,b,c) \rightarrow \text{if } (b=0) \text{ then } c/a \text{ else } s2(b,\text{irem}(a,b),c) \text{ fi};

> s2 := (a,b,c) \rightarrow \text{if } (b=0) \text{ then } 0 \text{ else } s1(b, \text{irem}(a,b),c) - \text{iquo}(a,b)*s2(b,\text{irem}(a,b),c) \text{ fi};
\]

**Lemma 6.4.** If \( p \) is prime number, then for any integers, \( p|ab \) implies that \( p|a \) or \( p|b \).

**Proof.** Suppose that \( p \) does not divide \( a \), then we have to show that it divides \( b \). By assumption, we can write \( ab = cp \) for some integer \( c \). Since \( p \) is prime, and \( \gcd(p, a)|p \), \( \gcd(p, a) \) is either 1 or \( p \). It must be 1, since \( \gcd = p \) would contradict the first statement. Therefore \( pm + an = 1 \) for some integers \( m, n \). Multiply this by \( b \) to obtain \( p(bm + cn) = b \). So \( p|b \).

**Corollary 6.5.** Suppose that \( p|a_1 \ldots a_n \), then \( p|a_i \) for some \( i \).

The proof of the corollary is left as an exercise.

We can now finish the proof of the fundamental theorem of arithmetic.

**Theorem 6.6.** A natural number \( N \geq 2 \) can be expressed as a product of primes in exactly one way. What that means is that \( N = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m \) where \( p_1 \leq p_2 \leq \ldots p_n \) and \( q_1 \leq \ldots q_m \) are primes, then \( n = m \) and \( p_i = q_i \).

**Proof.** The existence part has already been done in corollary 4.3. We will prove that given increasing finite sequences of primes such that

\[
p_1 \ldots p_n = q_1 \ldots q_m,
\]

(6.1)
then $m = n$ and $p_i = q_i$ by induction on the minimum $\min(n, m)$. We will interpret the initial case $\min(m, n) = 0$ to mean that 1 is not a product of primes, and this is clear. Now suppose that (6.1) holds, and that $0 < n \leq m$. Then $p_1$ divides the right side, therefore $p_1$ divides some $q_i$. Since $q_i$ is prime, $p_1 = q_i$. Similarly $q_1 = p_j$ for some $j$. We can conclude that $p_1 = q_1$, since $q_1 \leq q_i$ and $q_i = p_1 \leq p_j \leq q_i$. Canceling $p_1$ from (6.1) leads to an equation $p_2 \ldots p_n = q_2 \ldots q_m$. By induction, we are done.

\[ \square \]

### 6.7 Exercises

1. Carry out the procedure explained after lemma 6.1 to calculate $\gcd(882, 756)$.
   (Do this by hand.)

2. Prove that any common divisor of $a$ and $b$ divides $\gcd(a, b)$, and conversely that any divisor of the gcd is a common divisor.

3. The least common multiple $\text{lcm}(a, b)$ of two natural numbers $a, b$ is the smallest element of the set of numbers divisible by both $a$ and $b$. Prove that $\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$.

4. Given integers $a, b$, determine all integer solutions to $am + bn = 0$. Assuming the existence of one solution $(m_0, n_0)$ to $am + bn = c$, determine all the others.

5. In how many ways, can you express $10$ as a sum of dimes and quarters? (This is a linear diophantine equation with an obvious constraint.)

6. Find one solution for $120m + 131n = 1$ (either by hand or using Maple).

7. Prove corollary 6.5.