Chapter 7

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 $gcd(a, b)$.

Lemma 7.1 (Euclid)**.** *If a, b are natural numbers then $gcd(a, b) = gcd(b, a \, mod \, b)$*

Proof. Let $r = a \, mod \, b$. Then the division algorithm gives $a = qb + r$ for some integer q. SInce $gcd(b, r)$ divides b and r, it divides $qb + r = a$. Therefore $gcd(b, r)$ is a common divisor of a and b, so that that $gcd(b, r) \leq gcd(a, b)$. On the other hand, $r = a - qb$ implies that $gcd(a, b)|r$. Therefore $gcd(a, b)$ is a common divisor of b and r, so $gcd(a, b) \leq gcd(b, r)$, which forces them to be equal. □

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

$$gcd(100, 40) = gcd(40, 20) = gcd(20, 0) = 20.$$

For our purposes, a *diophantine equation* is an equation with integer coefficients where the solutions are also required to be integers. The simplest examples are the linear ones: given integers a, b, c, find all integers m, n such that $am + bn = c$.

Theorem 7.2. *Given integers a, b, c, $am + bn = c$ has a solution with $m, n \in \mathbb{Z}$ if and only if $gcd(a, b)|c$.*

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 $min(a, b)$.

If $min(a, b) = 0$, then one of them, say $b = 0$. Since $a = gcd(a, b)$ divides c by assumption, $(c/a, 0)$ gives a solution of $am + bn = c$. Now assume that

$a'm + b'n = c'$ has a solution whenever $min(a', b') < min(a, b)$ 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 4.1. 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 $m = n'$ and $n = m' - qn'$, then

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

$\square$

Corollary 7.3. *Given $a, b \in \mathbb{Z}$, there exists $m, n \in \mathbb{Z}$ such that $am + bn = gcd(a, b)$.*

We can now finish the proof of the following:

Theorem 7.4. *$m \in \mathbb{Z}_n$ has a multplicative inverse if and only if $gcd(m, n) = 1$ (we also say that m and n are* relatively prime *or* coprime*).*

Proof. If $gcd(m, n) = 1$, then $mm' + nn' = 1$ or $mm' = -n'n + 1$for some integers by corollary 7.3. After replacing (m', n') by $(m' + m''n, n' - m'')$ for some suitable m'', we can assume that $0 \leq m' \leq n$. Since have $r(mm', n) = 1$, $mm' = 1$.

The converse follows by reversing these steps. $\square$

Corollary 7.5. *If p is a prime, then $\mathbb{Z}_p$ is a field.*

Lemma 7.6. *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 $gcd(p, a)$ divides it, $gcd(p, a)$ is either 1 or p. It must be 1, since $gcd = p$ would contradict the fact the p does not divide a. Therefore $pm + an = 1$ for some integers m, n. Multiply this by b to obtain $p(bm + cn) = b$. So $p|b$. $\square$

Corollary 7.7. *Suppose that $p|a_1 \dots a_n$, 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 7.8. *A natural number $N \geq 2$ can be expressed as a product of primes in exactly one way. What that means if $N = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ where $p_1 \leq p_2 \leq \dots p_n$ and $q_1 \leq \dots q_m$ are primes, then $n = m$ and $p_i = q_i$.*

Proof. The existence part has already been done in corollary 5.3. We will prove that given increasing finite sequences of primes such that

$$p_1 \dots p_n = q_1 \dots q_m, \tag{7.1}$$

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 (7.1) 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 $q_i = p_1 \leq p_j \leq q_1$. Canceling p_1 from (7.1) leads to an equation $p_2 \ldots p_n = q_2 \ldots q_m$. By induction, we are done. $\square$

7.9 Exercises

1. Carry out the procedure explained after lemma 7.1 to calculate $gcd(882, 756)$. (Do this by hand.)

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

3. 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.

4. 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.)

5. Prove corollary 7.7.

6. Use the fact that 101 is prime to determine how many elements of $\mathbb{Z}_{101^2}$ have a multiplicative inverse. Note that unless you have a lot of patience, you may as come up with a theoretical argument which works for $\mathbb{Z}_{p^2}$ when p is a prime.