

DISCRETE MATHEMATICS

W W L CHEN

© W W L Chen, 1981, 2003.

This chapter originates from material used by the author at Imperial College, University of London, between 1981 and 1990.

It is available free to all individuals, on the understanding that it is not to be used for financial gains, and may be downloaded and/or photocopied, with or without permission from the author.

However, this document may not be kept on any information storage and retrieval system without permission from the author, unless such system is not accessible to any individuals other than its owners.

Chapter 4

DIVISION AND FACTORIZATION

4.1. Division

DEFINITION. Suppose that $a, b \in \mathbb{Z}$ and $a \neq 0$. Then we say that a divides b , denoted by $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. In this case, we also say that a is a divisor of b , or b is a multiple of a .

EXAMPLE 4.1.1. For every $a \in \mathbb{Z} \setminus \{0\}$, $a \mid a$ and $a \mid -a$.

EXAMPLE 4.1.2. For every $a \in \mathbb{Z}$, $1 \mid a$ and $-1 \mid a$.

EXAMPLE 4.1.3. If $a \mid b$ and $b \mid c$, then $a \mid c$. To see this, note that if $a \mid b$ and $b \mid c$, then there exist $m, n \in \mathbb{Z}$ such that $b = am$ and $c = bn$, so that $c = amn$. Clearly $mn \in \mathbb{Z}$.

EXAMPLE 4.1.4. If $a \mid b$ and $a \mid c$, then for every $x, y \in \mathbb{Z}$, $a \mid (bx + cy)$. To see this, note that if $a \mid b$ and $a \mid c$, then there exist $m, n \in \mathbb{Z}$ such that $b = am$ and $c = an$, so that $bx + cy = amx + any = a(mx + ny)$. Clearly $mx + ny \in \mathbb{Z}$.

PROPOSITION 4A. Suppose that $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $b = aq + r$ and $0 \leq r < a$.

PROOF. We shall first of all show the existence of such numbers $q, r \in \mathbb{Z}$. Consider the set

$$S = \{b - as \geq 0 : s \in \mathbb{Z}\}.$$

Then it is easy to see that S is a non-empty subset of $\mathbb{N} \cup \{0\}$. It follows from the Well-ordering principle that S has a smallest element. Let r be the smallest element of S , and let $q \in \mathbb{Z}$ such that $b - aq = r$. Clearly $r \geq 0$, so it remains to show that $r < a$. Suppose on the contrary that $r \geq a$. Then $b - a(q + 1) = (b - aq) - a = r - a \geq 0$, so that $b - a(q + 1) \in S$. Clearly $b - a(q + 1) < r$, contradicting that r is the smallest element of S .

Next we show that such numbers $q, r \in \mathbb{Z}$ are unique. Suppose that $b = aq_1 + r_1 = aq_2 + r_2$ with $0 \leq r_1 < a$ and $0 \leq r_2 < a$. Then $a|q_1 - q_2| = |r_2 - r_1| < a$. Since $|q_1 - q_2| \in \mathbb{N} \cup \{0\}$, we must have $|q_1 - q_2| = 0$, so that $q_1 = q_2$ and so $r_1 = r_2$ also. \circ

DEFINITION. Suppose that $a \in \mathbb{N}$ and $a > 1$. Then we say that a is prime if it has exactly two positive divisors, namely 1 and a . We also say that a is composite if it is not prime.

REMARK. Note that 1 is neither prime nor composite. There is a good reason for not including 1 as a prime. See the remark following Proposition 4D.

Throughout this chapter, the symbol p , with or without suffices, denotes a prime.

PROPOSITION 4B. Suppose that $a, b \in \mathbb{Z}$, and that $p \in \mathbb{N}$ is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

PROOF. If $a = 0$ or $b = 0$, then the result is trivial. We may also assume, without loss of generality, that $a > 0$ and $b > 0$. Suppose that $p \nmid a$. Let

$$S = \{b \in \mathbb{N} : p \mid ab \text{ and } p \nmid b\}.$$

Clearly it is sufficient to show that $S = \emptyset$. Suppose, on the contrary, that $S \neq \emptyset$. Then since $S \subseteq \mathbb{N}$, it follows from the Well-ordering principle that S has a smallest element. Let $c \in \mathbb{N}$ be the smallest element of S . Then in particular,

$$p \mid ac \quad \text{and} \quad p \nmid c.$$

Since $p \nmid a$, we must have $c > 1$. On the other hand, we must have $c < p$; for if $c \geq p$, then $c > p$, and since $p \mid ac$, we must have $p \mid a(c - p)$, so that $c - p \in S$, a contradiction. Hence $1 < c < p$. By Proposition 4A, there exist $q, r \in \mathbb{Z}$ such that $p = cq + r$ and $0 \leq r < c$. Since p is a prime, we must have $r \geq 1$, so that $1 \leq r < c$. However, $ar = ap - acq$, so that $p \mid ar$. We now have

$$p \mid ar \quad \text{and} \quad p \nmid r.$$

But $r < c$ and $r \in \mathbb{N}$, contradicting that c is the smallest element of S . \circ

Using Proposition 4B a finite number of times, we have

PROPOSITION 4C. Suppose that $a_1, \dots, a_k \in \mathbb{Z}$, and that $p \in \mathbb{N}$ is a prime. If $p \mid a_1 \dots a_k$, then $p \mid a_j$ for some $j = 1, \dots, k$.

4.2. Factorization

We remarked earlier that we do not include 1 as a prime. The following theorem is one justification.

PROPOSITION 4D. (FUNDAMENTAL THEOREM OF ARITHMETIC) Suppose that $n \in \mathbb{N}$ and $n > 1$. Then n is representable as a product of primes, uniquely up to the order of factors.

REMARK. If 1 were to be included as a prime, then we would have to rephrase the Fundamental theorem of arithmetic to allow for different representations like $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$. Note also then that the number of prime factors of 6 would not be unique.

PROOF OF PROPOSITION 4D. We shall first of all show by induction that every integer $n \geq 2$ is representable as a product of primes. Clearly 2 is a product of primes. Assume now that $n > 2$ and that every $m \in \mathbb{N}$ satisfying $2 \leq m < n$ is representable as a product of primes. If n is a prime, then it is obviously representable as a product of primes. If n is not a prime, then there exist $n_1, n_2 \in \mathbb{N}$ satisfying $2 \leq n_1 < n$ and $2 \leq n_2 < n$ such that $n = n_1 n_2$. By our induction hypothesis, both n_1 and n_2 are representable as products of primes, so that n must be representable as a product of primes.

Next we shall show uniqueness. Suppose that

$$(1) \quad n = p_1 \cdots p_r = p'_1 \cdots p'_s,$$

where $p_1 \leq \cdots \leq p_r$ and $p'_1 \leq \cdots \leq p'_s$ are primes. Now $p_1 \mid p'_1 \cdots p'_s$, so it follows from Proposition 4C that $p_1 \mid p'_j$ for some $j = 1, \dots, s$. Since p_1 and p'_j are both primes, we must then have $p_1 = p'_j$. On the other hand, $p'_1 \mid p_1 \cdots p_r$, so again it follows from Theorem 4C that $p'_1 \mid p_i$ for some $i = 1, \dots, r$, so again we must have $p'_1 = p_i$. It now follows that $p_1 = p'_j \geq p'_1 = p_i \geq p_1$, so that $p_1 = p'_1$. It now follows from (1) that

$$p_2 \cdots p_r = p'_2 \cdots p'_s.$$

Repeating this argument a finite number of times, we conclude that $r = s$ and $p_i = p'_i$ for every $i = 1, \dots, r$. \circ

Grouping together equal primes, we can reformulate Proposition 4D as follows.

PROPOSITION 4E. *Suppose that $n \in \mathbb{N}$ and $n > 1$. Then n is representable uniquely in the form*

$$(2) \quad n = p_1^{m_1} \cdots p_r^{m_r},$$

where $p_1 < \cdots < p_r$ are primes, and where $m_j \in \mathbb{N}$ for every $j = 1, \dots, r$.

DEFINITION. The representation (2) is called the canonical decomposition of n .

4.3. Greatest Common Divisor

PROPOSITION 4F. *Suppose that $a, b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ such that*

- (a) $d \mid a$ and $d \mid b$; and
- (b) if $x \in \mathbb{N}$ and $x \mid a$ and $x \mid b$, then $x \mid d$.

DEFINITION. The number d is called the greatest common divisor (GCD) of a and b , and is denoted by $d = (a, b)$.

PROOF OF PROPOSITION 4F. If $a = 1$ or $b = 1$, then take $d = 1$. Suppose now that $a > 1$ and $b > 1$. Let $p_1 < \cdots < p_r$ be all the distinct prime factors of a and b . Then by Proposition 4E, we can write

$$(3) \quad a = p_1^{u_1} \cdots p_r^{u_r} \quad \text{and} \quad b = p_1^{v_1} \cdots p_r^{v_r},$$

where $u_1, \dots, u_r, v_1, \dots, v_r \in \mathbb{N} \cup \{0\}$. Note that in the representations (3), when p_j is not a prime factor of a (resp. b), then the corresponding exponent u_j (resp. v_j) is zero. Now write

$$(4) \quad d = \prod_{j=1}^r p_j^{\min\{u_j, v_j\}}.$$

Clearly $d \mid a$ and $d \mid b$. Suppose now that $x \in \mathbb{N}$ and $x \mid a$ and $x \mid b$. Then $x = p_1^{w_1} \cdots p_r^{w_r}$, where $0 \leq w_j \leq u_j$ and $0 \leq w_j \leq v_j$ for every $j = 1, \dots, r$. Clearly $x \mid d$. Finally, note that the representations (3) are unique in view of Proposition 4E, so that d is uniquely defined. \circ

Similarly we can prove

PROPOSITION 4G. *Suppose that $a, b \in \mathbb{N}$. Then there exists a unique $m \in \mathbb{N}$ such that*

- (a) $a \mid m$ and $b \mid m$; and
- (b) if $x \in \mathbb{N}$ and $a \mid x$ and $b \mid x$, then $m \mid x$.

DEFINITION. The number m is called the least common multiple (LCM) of a and b , and is denoted by $m = [a, b]$.

PROPOSITION 4H. *Suppose that $a, b \in \mathbb{N}$. Then there exist $x, y \in \mathbb{Z}$ such that $(a, b) = ax + by$.*

PROOF. Consider the set

$$S = \{ax + by > 0 : x, y \in \mathbb{Z}\}.$$

Then it is easy to see that S is a non-empty subset of \mathbb{N} . It follows from the Well-ordering principle that S has a smallest element. Let d_0 be the smallest element of S , and let $x_0, y_0 \in \mathbb{Z}$ such that $d_0 = ax_0 + by_0$. We shall first show that

$$(5) \quad d_0 \mid (ax + by) \quad \text{for every } x, y \in \mathbb{Z}.$$

Suppose on the contrary that (5) is false. Then there exist $x_1, y_1 \in \mathbb{Z}$ such that $d_0 \nmid (ax_1 + by_1)$. By Proposition 4A, there exist $q, r \in \mathbb{Z}$ such that $ax_1 + by_1 = d_0q + r$ and $1 \leq r < d_0$. Then

$$r = (ax_1 + by_1) - (ax_0 + by_0)q = a(x_1 - x_0q) + b(y_1 - y_0q) \in S,$$

contradicting that d_0 is the smallest element of S . It now remains to show that $d_0 = (a, b)$. Taking $x = 1$ and $y = 0$ in (5), we clearly have $d_0 \mid a$. Taking $x = 0$ and $y = 1$ in (5), we clearly have $d_0 \mid b$. It follows from Proposition 4F that $d_0 \mid (a, b)$. On the other hand, $(a, b) \mid a$ and $(a, b) \mid b$, so that $(a, b) \mid (ax_0 + by_0) = d_0$. It follows that $d_0 = (a, b)$. \square

DEFINITION. We say that the numbers $a, b \in \mathbb{N}$ are said to be coprime (or relatively prime) if $(a, b) = 1$.

It follows immediately from Proposition 4H that

PROPOSITION 4J. *Suppose that $a, b \in \mathbb{N}$ are coprime. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Naturally, if we are given two numbers $a, b \in \mathbb{N}$, we can follow the proof of Proposition 4F to find the greatest common divisor (a, b) . However, this may be an unpleasant task if the numbers a and b are large and contain large prime factors. A much easier way is given by the following result.

PROPOSITION 4K. (EUCLID'S ALGORITHM) *Suppose that $a, b \in \mathbb{N}$, and that $a > b$. Suppose further that $q_1, \dots, q_{n+1} \in \mathbb{Z}$ and $r_1, \dots, r_n \in \mathbb{N}$ satisfy $0 < r_n < r_{n-1} < \dots < r_1 < b$ and*

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Then $(a, b) = r_n$.

PROOF. We shall first of all prove that

$$(6) \quad (a, b) = (b, r_1).$$

Note that $(a, b) \mid b$ and $(a, b) \mid (a - bq_1) = r_1$, so that $(a, b) \mid (b, r_1)$. On the other hand, $(b, r_1) \mid b$ and $(b, r_1) \mid (bq_1 + r_1) = a$, so that $(b, r_1) \mid (a, b)$. (6) follows. Similarly

$$(7) \quad (b, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n).$$

Note now that

$$(8) \quad (r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n.$$

The result follows on combining (6)–(8). \circ

EXAMPLE 4.3.1. Consider $(589, 5111)$. In our notation, we let $a = 5111$ and $b = 589$. Then we have

$$\begin{aligned} 5111 &= 589 \cdot 8 + 399, \\ 589 &= 399 \cdot 1 + 190, \\ 399 &= 190 \cdot 2 + 19, \\ 190 &= 19 \cdot 10. \end{aligned}$$

It follows that $(589, 5111) = 19$. On the other hand,

$$\begin{aligned} 19 &= 399 - 190 \cdot 2 \\ &= 399 - (589 - 399 \cdot 1) \cdot 2 \\ &= 589 \cdot (-2) + 399 \cdot 3 \\ &= 589 \cdot (-2) + (5111 - 589 \cdot 8) \cdot 3 \\ &= 5111 \cdot 3 + 589 \cdot (-26). \end{aligned}$$

It follows that $x = -26$ and $y = 3$ satisfy $589x + 5111y = (589, 5111)$.

4.4. An Elementary Property of Primes

There are many consequences of the Fundamental theorem of arithmetic. The following is one which concerns primes.

PROPOSITION 4L. (EUCLID) *There are infinitely many primes.*

PROOF. Suppose on the contrary that $p_1 < \dots < p_r$ are all the primes. Let $n = p_1 \dots p_r + 1$. Then $n \in \mathbb{N}$ and $n > 1$. It follows from the Fundamental theorem of arithmetic that $p_j \mid n$ for some $j = 1, \dots, r$, so that $p_j \mid (n - p_1 \dots p_r) = 1$, a contradiction. \circ

PROBLEMS FOR CHAPTER 4

1. Consider the two integers 125 and 962.
 - a) Write down the prime decomposition of each of the two numbers.
 - b) Find their greatest common divisor.
 - c) Find their least common multiple.
2. Factorize the number 6469693230.
3. Find $(210, 858)$. Determine integers x and y such that $(210, 858) = 210x + 858y$. Hence give the general solution of the equation in integers x and y .
4. Find $(182, 247)$. Determine integers x and y such that $(182, 247) = 182x + 247y$. Hence give the general solution of the equation in integers x and y .

5. It is well-known that every multiple of 2 must end with the digit 0, 2, 4, 6 or 8, and that every multiple of 5 must end with the digit 0 or 5. Prove the equally well-known rule that a natural number is a multiple of 3 if and only if the sum of the digits is a multiple of 3 by taking the following steps. Consider a k -digit natural number x , expressed as a string $x_1x_2\dots x_k$, where the digits $x_1, x_2, \dots, x_k \in \{0, 1, 2, \dots, 9\}$.
- Calculate the value of x in terms of the digits x_1, x_2, \dots, x_k .
 - Calculate the difference between x and the sum of the digits.
 - Show that this difference is divisible by 3.
 - Complete the proof.
6. Let $x, y, m, n, a, b, c, d \in \mathbb{Z}$ satisfy $m = ax + by$ and $n = cx + dy$ with $ad - bc = \pm 1$. Prove that $(m, n) = (x, y)$.