Chapter 2

Divisibility

2.1 Common Divisors

Definition 2.1.1. Let a and b be integers. A *common divisor* of a and b is any integer that divides both a and b. Suppose that a and b are not both zero. By Proposition 1.3.8, there exists a greatest common divisor, which is positive. It is denoted by

$$\gcd(a, b) \ .$$

Note that in the proof of Proposition 1.3.8 we proved that, for integers a and b which are not both zero, the set $S = \{x \in \mathbb{Z} \ : \ x \mid a, \ x \mid b\}$ has a maximum. Thus,

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

Example 2.1.2. The common divisors of 12 and 30 are: $-6, -3, -2, -1, 1, 2, 3, 6$. These are also the common divisors of -12 and 30, and of 6 and 0. Hence,

$$\gcd(12, 30) = \gcd(-12, 30) = \gcd(6, 0) = 6 \ .$$

Theorem 2.1.3.* Let a and b be integers, not both of which are zero. Then there exist integers x and y such that

$$ax + by = \gcd(a, b) \ .$$

Example 2.1.4. Verifying Theorem 2.1.3 in one case: $12(-2) + 30(1) = \gcd(12, 30)$.

Proposition 2.1.5. Let a and b be integers, not both zero. Then any common divisor of a and b is a divisor of $\gcd(a, b)$.

Definition 2.1.6. Let a and b be positive integers. By Proposition 1.3.9, there exists a least common positive multiple of a and b. It is denoted by

$$\mathrm{lcm}(a, b) \ .$$

It follows from the proof of Proposition 1.3.9 that for positive integers a and b

$$\mathrm{lcm}(a, b) = \min\{x \in \mathbb{Z} \ : \ x > 0, \ a \mid x, \ b \mid x\} \ .$$

Proposition 2.1.7. Let a and b be positive integers. Then any common multiple of a and b is a multiple of $\text{lcm}(a, b)$.

Proposition 2.1.8. Let a, b and d be positive integers. If d is a common divisor of a and b, then ab/d is a common multiple of a and b.

Proposition 2.1.9. Let a, b and m be positive integers. If m is a common multiple of a and b and m divides ab, then ab/m is a common divisor of a and b.

Proposition 2.1.10. If a and b are positive integers, then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

2.2 Relatively Prime Integers

Definition 2.2.1. Let a and b be integers, not both zero. If $\gcd(a, b) = 1$, then a and b are said to be *relatively prime*. Notice that the only common divisors of relatively prime integers are 1 and -1.

Proposition 2.2.2. Let a and b be integers that are not relatively prime. Then there exists a prime that divides both a and b.

Proposition 2.2.3. Let a and b be relatively prime positive integers and let c be an integer. If $a|c$ and $b|c$, then $ab|c$.

Lemma 2.2.4 (Euclid's Lemma)**.** Let a and b be relatively prime integers. If c is an integer and $a|bc$, then $a|c$.

Proposition 2.2.5. Let a and b be integers, not both zero. If $d = \gcd(a, b)$, then a/d and b/d are relatively prime.

Proposition 2.2.6. Let p be a prime and a an integer. If p does not divide a, then p and a are relatively prime.

Theorem 2.2.7 (Euclid's First Theorem)**.** Let p be a prime and let a and b be integers. If $p|ab$, then $p|a$ or $p|b$.

Proposition 2.2.8.* Let $a_1, a_2, \ldots, a_n$ be integers and let $a = a_1 a_2 \cdots a_n$. If p is a prime and p divides a, then there exists k such that p divides a_k.

Proposition 2.2.9. Let $a_1, a_2, \ldots, a_n$ be integers and let $a = a_1 a_2 \cdots a_n$. If b is a nonzero integer and b is relatively prime to each a_k, then a and b are relatively prime.

Proposition 2.2.10. Let $a_1, a_2, \ldots, a_n$ be integers greater than 1 and let $a = a_1 a_2 \cdots a_n$. Then $a + 1$ is not divisible by any of the a_k.

Theorem 2.2.11 (Euclid's Second Theorem)**.*** There exist infinitely many primes.

2.3 Factoring Integers into Primes

Proposition 2.3.1. Let a be an integer greater than 1. Then there exists a positive integer n and there exist primes $p_1, p_2, \ldots, p_n$ such that $p_1 \leq p_2 \leq \cdots \leq p_n$ and

$$a = p_1 p_2 \cdots p_n.$$

Theorem 2.3.2 (The Fundamental Theorem of Arithmetic)**.** Any integer greater than 1 has a unique representation as a product of primes in their natural order.

Definition 2.3.3. Let a be an integer greater than 1. In the representation given in Proposition 2.3.1, let the distinct primes be $q_1, q_2, \ldots, q_r$, where $q_1 < q_2 < \cdots < q_r$. Suppose that q_i appears k_i times. Then the *canonical form* of a is:

$$a = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r} \ .$$

Proposition 2.3.4. Let a be an integer greater than 1. Then a is a perfect square if, and only if, the exponents in its canonical form are all even integers.

Example 2.3.5. Let $a = 3$, $b = 9$ and $c = 316875$. Here are the representations specified in Theorem 2.3.2 and Definition 2.3.3:

$$\begin{aligned} a &= 3 = 3^1, \\ b &= 3 \cdot 3 = 3^2, \\ c &= 3 \cdot 5 \cdot 5 \cdot 5 \cdot 13 \cdot 13 = 3^1 5^4 13^2 \ . \end{aligned}$$

Exercise 2.3.6. Determine the canonical form of the integer 23! .

2.4 Linear Equations

Remark 2.4.1. In this section, we assume that a, b and c are integers, with $a \neq 0$ and $b \neq 0$. Set $d = \gcd(a, b)$. The object is to investigate the solutions, if any, of the equation

$$ax + by = c \ .$$

Here, x and y are required to be integers. A *positive* solution is one for which both x and y are positive integers.

Proposition 2.4.2. The equation in Remark 2.4.1 has a solution if, and only if, c is a multiple of $\gcd(a, b)$.

Proposition 2.4.3. Suppose, in Remark 2.4.1, that $d = 1$ and that one solution is given by: $x = x_0, y = y_0$. Then the general solution of the equation in Remark 2.4.1 is:

$$x = x_0 + bt, \qquad y = y_0 - at,$$

where t ranges over $\mathbb{Z}$.

Proposition 2.4.4. Suppose, in Remark 2.4.1, that one solution is given by: $x = x_0, y = y_0$. Then the general solution of the equation in Remark 2.4.1 is:

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

where t ranges over $\mathbb{Z}$.

Exercise 2.4.5. Find the general solution of the equation $55x + 65y = 1000$. Find all positive solutions.

Remark 2.4.6. An equation in which the parameters and unknowns are all integers is called a *Diophantine equation*, named for the Greek mathematician Diophantus.

2.5 The Euclidean Algorithm

Remark 2.5.1. Suppose that a and b are positive integers. The purpose here is to see how to determine $\gcd(a, b)$ and to find integers x and y such that

$$ax + by = \gcd(a, b) \ .$$

Definition 2.5.2. Let a and b be integers, with $a > b > 0$. The *Euclidean Algorithm* is a procedure for finding $\gcd(a, b)$. A list of integers

$$a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n$$

is constructed as follows. Let $a_1 = a$ and $a_2 = b$. Let a_3 be the remainder left by a_1 when divided by a_2, let a_4 be the remainder left by a_2 when divided by a_3, and so on. The process stops when the next term would be 0. Hence, all terms are positive and a_{n-1} is a multiple of a_n.

Proposition 2.5.3.* For the list in Definition 2.5.2 it is true that $\gcd(a_1, a_2) = a_n$.

Definition 2.5.4. If $a,\ b,\ c$ and d are integers, set $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. This is called a *determinant*.

Definition 2.5.5. In these notes, a *Euclidean array* is an array of integers of the form

$$\begin{array}{ccccccc} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ & q_2 & \cdots & q_{n-1} & \\ b_1 & b_2 & \cdots & b_{n-1} & b_n \end{array} \ .$$

It is assumed that $n \geq 3$, and that, for $1 < k < n$,

$$a_{k-1} = a_k q_k + a_{k+1} \qquad \text{and} \qquad b_{k-1} = b_k q_k + b_{k+1}$$

Proposition 2.5.6. In Definition 2.5.5, either

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \begin{vmatrix} a_{n-1} & a_n \\ b_{n-1} & b_n \end{vmatrix} \qquad \text{or} \qquad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = - \begin{vmatrix} a_{n-1} & a_n \\ b_{n-1} & b_n \end{vmatrix},$$

according to whether n is even or odd.

2.6 An Example

The two integers of interest here are 275 and 635.

(1) To find the greatest common divisor of 275 and 635, apply the Euclidean Algorithm:

$$635 \quad 275 \quad 85 \quad 20 \quad 5 \ .$$

That is, 635 leaves a remainder 85 when divided by 275, and so on. Hence,

$$\gcd(275, 635) = 5 \ .$$

(2) The object now is to solve the equation

$$275x + 635y = \gcd(275, 635) \ .$$

A Euclidean array will be constructed. The second row consists of the quotients found, but not shown, when applying the Euclidean Algorithm:

$$\begin{array}{ccccc} 635 & 275 & 85 & 20 & 5 \\ & 2 & 3 & 4 & \end{array}$$

The third row is constructed from right to left. The best way to start is to put 1 and 0 beneath 20 and 5. The first and third rows are related to the second row in exactly the same way, even though they are constructed in opposite directions. The array is:

$$\begin{array}{ccccc} 635 & 275 & 85 & 20 & 5 \\ & 2 & 3 & 4 & \\ 30 & 13 & 4 & 1 & 0 \end{array}$$

That is, 30 leaves a remainder 4 when divided by 13, and so on. The computations are:

$$4 = 1 \cdot 4 + 0, \quad 13 = 4 \cdot 3 + 1, \quad 30 = 13 \cdot 2 + 4 \ .$$

The first row has an odd number of entries. By Proposition 2.5.6,

$$\begin{vmatrix} 635 & 275 \\ 30 & 13 \end{vmatrix} = - \begin{vmatrix} 20 & 5 \\ 1 & 0 \end{vmatrix} \ .$$

Hence, $635 \cdot 13 - 275 \cdot 30 = 5$. That is, $275 \cdot (-30) + 635 \cdot (13) = 5$.

(3) We now consider the equation

$$275x + 635y = \gcd(275, 635) \ .$$

By Proposition 2.4.4, the general solution is:

$$x = -30 + 127t, \quad y = 13 - 55t,$$

where t ranges over $\mathbb{Z}$.

2.7 Problems

Problem 2.7.1. Let $q_1 = 2$. For $n \geq 2$, let q_n be the smallest prime divisor of the integer $1 + q_1 q_2 \cdots q_{n-1}$. Show that the q_k are distinct, and thereby give another proof of Theorem 2.2.11. Verify that the first five terms are 2, 3, 7, 43, 13. Find the next two terms.

Problem 2.7.2. Determine all ways to make \$2.35 with dimes and quarters.

Problem 2.7.3. Five hundred ducats were used to buy one hundred animals of three types. The burros cost 11 ducats each, the camels cost 9 ducats each, and the dogs cost 2 ducats each. How many animals of each kind were there?

Problem 2.7.4. Find the general solution of: $2669x + 3825y = \gcd(2669, 3825)$.

Problem 2.7.5. Find the general solution of: $3409x + 1488y = 1$.

Problem 2.7.6. Solve: $1234x - 4321y = 1$.

Problem 2.7.7. Solve: $4275x + 2983y = \gcd(4275, 2983)$.

2.8 Projects

Project 2.8.1. By Proposition 1.4.8, the product of any two consecutive integers is a multiple of 2. Prove that the product of any three consecutive integers is a multiple of 6. What can you say about the product of any four consecutive integers?

Project 2.8.2. Suppose that a and b be relatively prime integers, both greater than 1. Look into the question of for which integers c the equation $ax + by = c$ has a positive solution. It will help to deal with three cases

$$c < a + b, \qquad c > ab, \qquad a + b \leq c \leq ab \ .$$

Project 2.8.3. In addition to the representations for integers given in Theorem 2.3.2 and Definition 2.3.3, there is a third method that is useful when dealing with more than one integer at the same time. For $n \geq 1$, let p_n be the n-th prime. For example, $p_1 = 2$ and $p_2 = 3$. Any positive integer can be expressed using non-negative powers of the first n primes, for sufficiently large n. For example, to represent the integer c in Example 2.3.5 using the first eight primes, we write

$$316875 = 2^0 3^1 5^4 7^0 11^0 13^2 17^0 19^0 \ .$$

Use such representations to illuminate some of the propositions and definitions in Sections 2.1 and 2.2. Assume that all the integers being considered are positive.

2.9 Proofs and Suggestions

Proof of Theorem 2.1.3.

(1) Let a and b be integers, not both zero.

(2) Let $S = \{z : z > 0, \text{ there exist } x \text{ and } y \text{ such that } z = ax + by\}$.

(3) The integer $a \cdot a + b \cdot b$ is an element of S, and so S is nonempty.

(4) 0 is a lower bound for S.

(5) By Axiom 16, there exists a least integer in S. Call it c. By (2), c is positive.

(6) There exist integers x and y such that $c = ax + by$.

(7) By Proposition 1.4.1, there exist integers q and r such that $a = qc + r$ and $0 \leq r \leq c - 1$.

(8) Let $x' = 1 - qx$ and $y' = -qy$.

(9) $r = a - qc = a - q(ax + by) = a(1 - qx) + b(-qy)$.

(10) $r = ax' + by'$ and $0 \leq r < c$.

(11) $r = 0$, since c is the least integer in S.

(12) c divides a.

(13) Similarly, c divides b.

(14) c is a common divisor of a and b and $c > 0$.

(15) Any common divisor of a and b divides $ax + by$.

(16) $c = \gcd(a, b)$. □

Suggestion for Proposition 2.1.5. Use Theorem 2.1.3.

Suggestion for Proposition 2.1.7. Let $m = \text{lcm}(a, b)$, and let c be a common multiple. Show that if r is the remainder left by c when divided by m, then r is also a common multiple, and must be 0.

Suggestion for Proposition 2.1.8. Notice that $\dfrac{ab}{d} = a\,\dfrac{b}{d} = \dfrac{a}{d}\,b$.

Suggestion for Proposition 2.1.9. Let $k = \dfrac{ab}{m}$. Verify that $a = k\,\dfrac{m}{b}$ and $b = k\,\dfrac{m}{a}$.

Suggestion for Proposition 2.1.10. Let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Use Proposition 2.1.8 to show that $\dfrac{ab}{d} \geq m$. Use Propositions 2.1.7 and 2.1.9 to show that $\dfrac{ab}{m} \leq d$.

Lemma 2.2.4: Use Theorem 2.1.3 to write $ax + by = 1$, and multiply through by c.

Suggestion for Proposition 2.2.5. Use Theorem 2.1.3.

Suggestion for Theorem 2.2.7. If p divides ab but not a, apply Lemma 2.2.4 and Proposition 2.2.6.

Proof of Proposition 2.2.8.

(1) Let p be a prime and let $a_1, a_2, \ldots, a_n$ be integers. Suppose that $p \mid a_1 a_2 \cdots a_n$.

(2) Consider the set

$$S = \big\{ j \in \{1, 2, \ldots, n\} \,:\, p \mid a_j a_{j+1} \cdots a_n \big\}.$$

By (1) $1 \in S$. Clearly $x \leq n$ for each $x \in S$. Thus S is non-empty and bounded above. Therefore S has a maximum. Put $m = \max S$.

(3) Now I shall prove that $p \mid a_m$. There are two cases:

Case 1 $m = \max S = n$.

Then $n \in S$. By the definition of the set S, I conclude that $p \mid a_n$.

Case 2 $1 \leq m < n$.

Then $m+1 \leq n$ and $m+1 \notin S$. Therefore $p \not| a_{m+1} a_{m+2} \cdots a_n$. Since $m \in S$, I conclude that $p \mid a_m a_{m+1} \cdots a_n$. Since

$$p \mid a_m a_{m+1} \cdots a_n \quad \text{and} \quad p \not| a_{m+1} a_{m+2} \cdots a_n,$$

Euclid's Theorem implies that $p \mid a_m$. □

Suggestion for Proposition 2.2.9. Use Proposition 2.2.8.

Suggestion for Proposition 2.2.10. Use Proposition 1.2.8.

Proof of Theorem 2.2.11*, Euclid's proof by contradiction.*

(1) Assume that there exist only finitely many primes, say $p_1, p_2, \ldots, p_n$.

(2) Let $b = 1 + p_1 p_2 \cdots p_n$.

(3) By Proposition 1.6.4, there exists a prime p that divides b.

(4) By Proposition 2.2.10, p does not equal any of the p_k.

(5) That contradicts (1). □

Proof of Proposition 2.3.1.

(1) Let $a \in \mathbb{Z}$ and $a > 1$.

(2) Put

$$S = \left\{ b \ : \ \begin{array}{l} b \in \mathbb{Z},\ b > 1,\ b \mid a,\ b = q_1 \cdots q_k, \text{ where} \\ k \text{ is a positive integer and } q_1, \ldots, q_k \text{ are primes} \end{array} \right\}.$$

(3) By (1) and Proposition 1.6.5 there exists a prime p that divides a. Clearly $p \in S$. Thus $S \neq \emptyset$.

(4) If $x \in S$, then $x > 1$ and $x \mid a$. Therefore $x \leq a$. Thus a is an upper bound for S.

(5) The lines (3) and (5) imply that Proposition 1.3.5 can be applied to the set S and we conclude that S has a maximum. Let $c = \max S$.

(6) Since $c \in S$, we conclude that $c \leq a$.

(7) Let x be an integer in S such that $x < a$. Then $a = xs$ for some integer s. Since $x < a$, we conclude that $s > 1$.

(8) By Proposition 1.6.5 and (7) we conclude that there exist a prime r such that $r \mid s$, that is $s = rt$.

(9) From (7) and (8) we conclude that $a = xrt$. Therefore $xr \mid a$.

(10) Since $x \in S$ there exist primes $u_1, \ldots, u_j$ such that $x = u_1 \cdots u_j$. Therefore $xr = u_1 \cdots u_j r$.

(11) Since clearly $xr > 1$, the lines (9) and (10) imply that $xr \in S$.

(12) Since $r > 1$ and $x > 1$, we have $xr > x$.

(13) The results from the lines (7) through (12) can be summarized as:

Let $x \in S$. If $x < a$, then x is not a greatest integer in S.

(14) The contrapositive of the statement in (13) is

Let $x \in S$. If x is a greatest integer in S, then $x \geq a$.

(15) Since c is a greatest integer in S we conclude from (14) that $c \geq a$.

(16) The lines (6) and (15) imply that $c = a$.

(17) Since $a = c$ and $c \in S$ we conclude that $a \in S$. By (2) it follows that there exist primes $p_1, \ldots, p_n$ such that $a = p_1 \cdots p_n$. □

Suggestion for Theorem 2.3.2. In view of Proposition 2.3.1, the only thing to be proved is the uniqueness of the representation. Let a be an integer greater than 1. Let $m, n \in \mathbb{N}$ and assume that $p_1, p_2, \ldots, p_m$ and $q_1, q_2, \ldots, q_n$ are primes such that

$$\begin{array}{ll} p_1 \le p_2 \le \cdots \le p_m, & q_1 \le q_2 \le \cdots \le q_n, \\ a = p_1 p_2 \cdots p_m, & a = q_1 q_2 \cdots q_n \ . \end{array}$$

(1) Let $k \in \{1, 2, \ldots, n\}$. Since $q_1, q_2, \ldots, q_n$ are primes, the following implication holds: If $k < n$, then $q_1 q_2 \cdots q_k < a$. The contrapositive of this implication is: If $q_1 q_2 \cdots q_k = a$, then $k = n$.
(2) We need to prove that $m = n$ and $p_1 = q_1, \ldots, p_m = q_m$. Notice that by Proposition 2.2.8 we have $p_1 = q_1$.
(3) Assume that $m \le n$ and consider the set

$$S = \big\{ j \in \{1, 2, \ldots, m\} \ : \ p_j \ne q_j \big\}.$$

By Proposition 2.2.8 $1 \notin S$. We will prove by contradiction that $S = \emptyset$. Suppose that $S \ne \emptyset$. Since 1 is a lower bound for S, the set S has a minimum. Set $k = \min S$. Since $1 \notin S$, $1 < k \le m$. Then $1, \ldots, k-1 \notin S$, that is $p_1 = q_1, \ldots, p_{k-1} = q_{k-1}$. By the assumption

$$a = p_1 \cdots p_{k-1} p_k \cdots p_m = q_1 \cdots q_{k-1} q_k \cdots q_n.$$

Therefore, $p_k \cdots p_m = q_k \cdots q_n$. Set $b = p_k \cdots p_m = q_k \cdots q_n$. Since $k \le m$, $b > 1$. By Proposition 2.2.8 applied to b we deduce that $p_k = q_k$. Therefore $k \notin S$. This contradicts $k = \min S$.
(4) By **(3)**, $S = \emptyset$. Therefore, $p_1 = q_1, \ldots, p_m = q_m$. Hence $a = p_1 \cdots p_m = q_1 \cdots q_m$. By **(1)**, $a = q_1 \cdots q_m$ implies $m \ge n$. Since we assumed that $m \le n$, this implies $m = n$.

Suggestion for Exercise 2.4.5. Divide by 5 and try various values of x and y.

Proof of Proposition 2.5.3.

(1) If $n = 2$, then $\gcd(a_1, a_2) = a_2$.

(2) Suppose that $n > 2$.

(3) Let q_k be such that $a_{k-1} = a_k q_k + a_{k+1}$ for $k = 2, 3, \ldots, n-1$.

(4) The common divisors of a_{k-1} and a_k are just the common divisors of a_k and a_{k+1}.

(5) $\gcd(a_{k-1}, a_k) = \gcd(a_k, a_{k+1})$ for each k.

(6) $\gcd(a_1, a_2) = \gcd(a_2, a_3) = \cdots = \gcd(a_{n-1}, a_n) = a_n$. □

Suggestion for Proposition 2.5.6. Verify that $\begin{vmatrix} a_{k-1} & a_k \\ b_{k-1} & b_k \end{vmatrix} = - \begin{vmatrix} a_k & a_{k+1} \\ b_k & b_{k+1} \end{vmatrix}$ for $k = 2, 3, \ldots, n-1$.