2 Integer Properties I

The set of all integers (positive, negative, and zero) is written as $\mathbb{Z}$.

We will assume that the usual properties of addition, subtraction, multiplication, and division are known. (See Buchmann 1.1 for some basic properties of numbers which you should know by now.)

2.1 Divisibility

Reference Buchmann 1.2

Definition 2.1. Given two integers x and y with $x \neq 0$, we say that x *divides* y (x is a *divisor* or *factor* of y, or y is a *multiple* of x) if $\dfrac{y}{x}$ is an integer; in other words, if there is some integer q such that $y = xq$.

We write $x \mid y$ in such a case. If x does not divide y, we write $x \nmid y$. □

Example 2.1.

The following results on divisibility seem clear but, nevertheless, require proof.

Theorem 2.2. Let $a, b, c \in \mathbb{Z}$.

(i) $a \mid a$ provided $a \neq 0$.

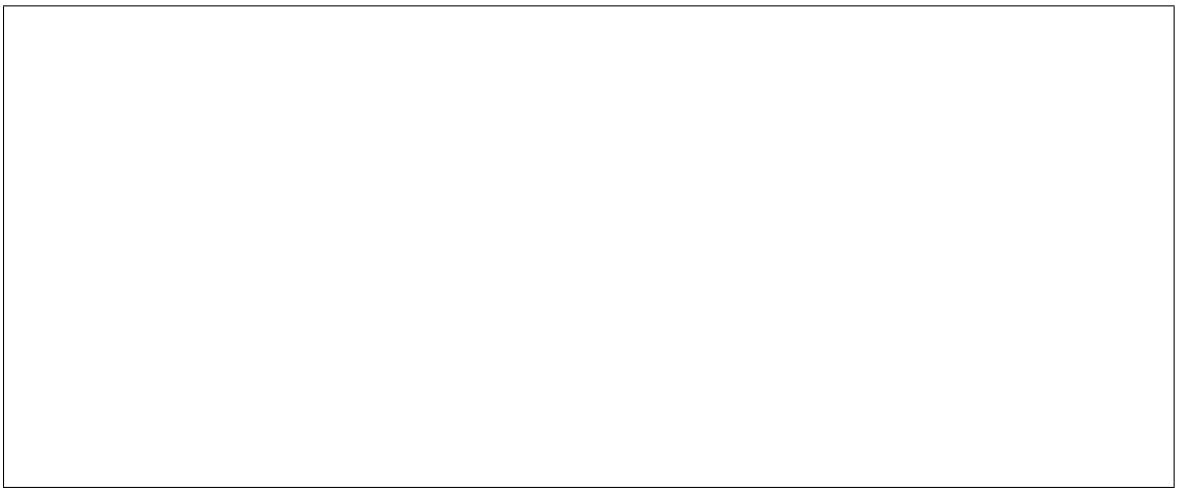
(ii) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

(iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(iv) If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m and n.

(v) If $a \mid b$, then $|a| \leq |b|$.

Proof. See Buchmann, Theorem 1.2.3 for most of the proofs. However, we will prove (iii).



- Part (iv) of the last theorem will be used repeatedly. In words, it says that if a divides b and a divides c, then a divides any *linear combination* of b and c.

We can divide an integer by another to get a *quotient* and a *remainder*. For example, if we divide 7 by 3, the quotient is 2 and the remainder is 1. More generally, we have the following.

Theorem 2.3. (The Division Algorithm for integers.) If a and b are integers with $b \geq 1$, then there are *unique* integers q (the quotient) and r (the remainder) such that $a = qb + r$ and $0 \leq r < b$.

Example 2.2.

Proof. Buchmann, Theorem 1.2.4.

A cryptographic application. Suppose a 15-person federal committee has to vote to approve the President's executive order. Members prefer to keep their votes anonymous. Here is a way so that everyone votes *Yes*, *No*, or *Abstain*, and simultaneously ensures each vote is kept secret.

The chair takes a blank piece of paper, writes a large number, say 5963, on it, and passes it on to the next member. In turn, that member adds 16 for *Yes*, 1 for *No*, and 0 for *Abstain* to this number, and writes the new number on a blank piece of paper and passes it on to the next member to repeat. This process continues until the chair receives a number from the last member on the committee, at which time they add 16 for *Yes*, 1 for *No*, or 0 for *Abstain*. Say the final sum is 6096. How does the chair determine the number of *Yes* votes, *No* votes, and *Abstain* votes?

2.2 Primes

Reference Buchmann 1.11

A *positive* integer n is called a *prime* if the only positive divisors of n are the trivial divisors 1 and n. If n is not prime, it is called *composite*. (For technical reasons, 1 is *not* defined to be a prime.)

Example 2.3.

Example 2.4. (A historical problem.) For all positive integers n, the Fermat numbers F_n are defined by

$$F_n = 2^{(2^n)} + 1.$$

So, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. (Note that if $m > 1$ is not a power of two, then $2^m + 1$ is composite.) Now these are all prime and Fermat (1601–1665) conjectured that all Fermat numbers were prime.

But Euler (1732) showed that

$$F_5 = 641 \times 6700417$$

and Landry (1880) showed that

$$F_6 = 274177 \times 67280421310721,$$

so F_5 and F_6 are not prime. Since then, many F_n's have been proved composite, so that Fermat's conjecture was not a happy one. Currently, $F_5, F_6, \ldots, F_{32}$ have all been shown to be composite. It is now thought (though not yet proven) that there are only a *finite* number of Fermat primes.

See Buchmann, Example 1.11.6 for a fairly recent account of Fermat primes. □

- In comparison with the last example, Mersenne numbers M_n are numbers of the form

$$M_n = 2^n - 1.$$

Named after the French monk Marin Mersenne (1588–1648), a Mersenne prime is a Mersenne number that is prime and it is conjectured, but again not proved, that there are an infinite number of such primes. Check out the Great Internet Mersenne Prime Search (GIMPS).

The next theorem is the *Fundamental Theorem of Arithmetic*. It says that every integer greater than one is either a prime or can be factored into a product of primes in exactly one way.

Theorem 2.4. Every integer $n \geq 2$ can be written as a product of primes and this is unique except for order. If we write (as we usually do) the primes in increasing order, then we have *uniquely*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

with $p_1 < p_2 < \cdots < p_k$ prime and $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$.

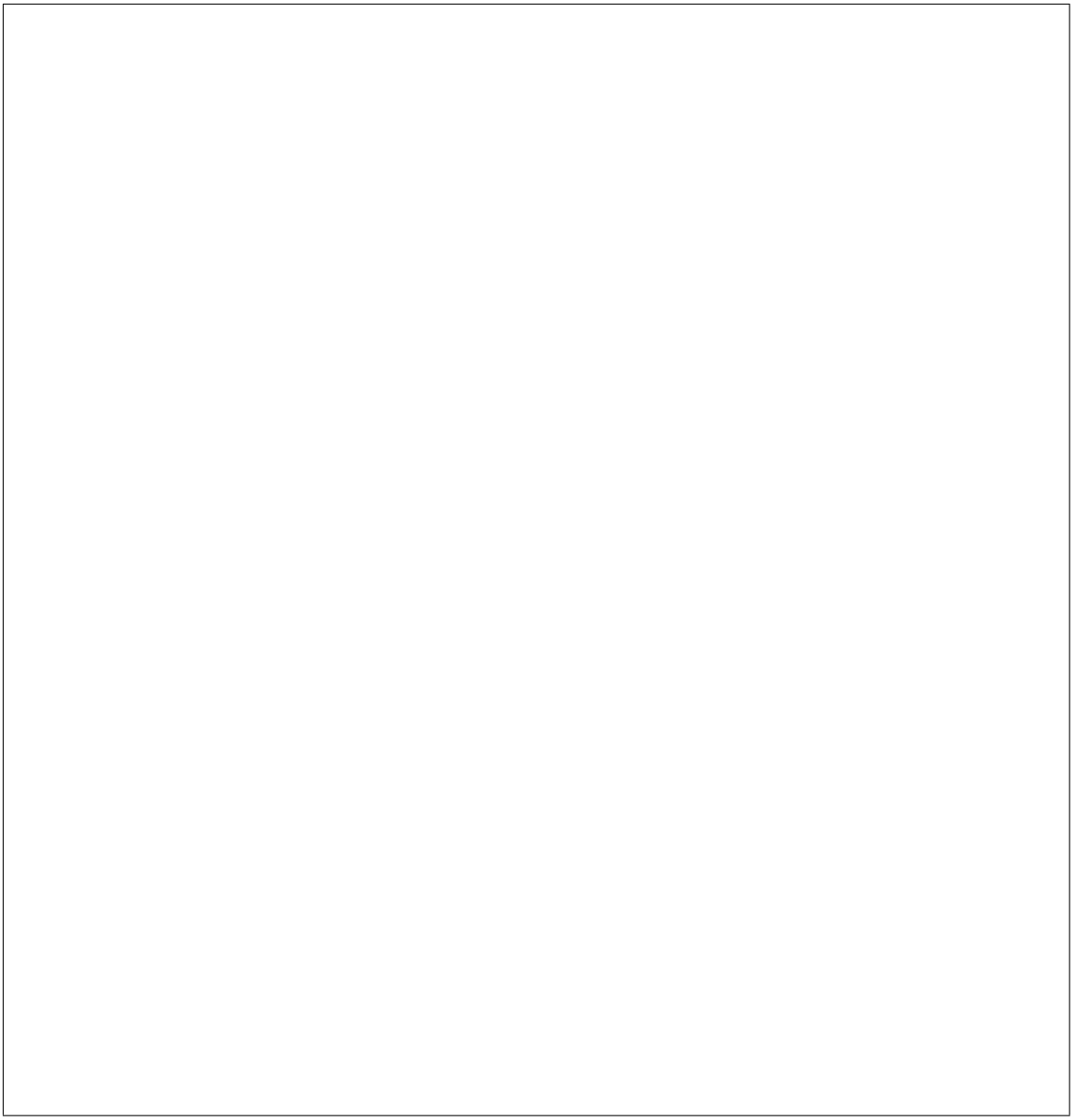
Example 2.5.

What happens if 1 is considered prime?

Proof. If n is composite, it has a positive divisor d_1 such that $1 < d_1 < n$ and so we can write $n = d_1 d_2$ where d_1 and d_2 are strictly smaller than n. Each of d_1 and d_2 are either

primes or by the same reasoning, can be further written as a product of two smaller integers. Because this process cannot continue for ever, we end up with n written as a product of primes.

Now consider the problem of uniqueness. (This part of the proof is a bit more tricky. Nevertheless, it's worth understanding how it works.)



Corollary 2.5. If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. By Theorem 2.4, p must appear in the prime factorization of a or b (otherwise

it doesn't appear in ab). □

Corollary 2.6. (Euclid.) There are infinitely many primes.

Proof.

The last corollary says that the list of *all* integers contains an infinite number of primes. But do lists like

$$4, 7, 10, 13, 16, 19, 22, \ldots$$

$$3, 8, 13, 18, 23, 28, 33, \ldots$$

and

$$1, 101, 201, 301, 401, 501, 601, \ldots$$

also contain an infinite number of primes? It turns out that the answer is yes!

Theorem 2.7. (Dirichlet, 1837) Let a and b be positive integers with no common factor greater than one. Then

$$a, a + b, a + 2b, a + 3b, \ldots$$

contains infinitely many primes.

2.3 Greatest Common Divisor (GCD)

Reference Buchmann 1.7, 1.8

Definition 2.8. Let a and b be integers. The *positive* integer d is the *greatest common divisor* of a and b if

(i) $d \mid a$ and $d \mid b$, that is, d is a *common divisor* of a and b, and

(ii) if $c \mid a$ and $c \mid b$, then $c \leq d$, that is, d is the *greatest* of all common divisors.

We write $d = \gcd(a, b)$. □

(Note that our definition is slightly different to Buchmann's but completely equivalent.)

Example 2.6.

If we know the prime decomposition of a and b, then it is easy to find $\gcd(a, b)$.

Example 2.7.

In general, if

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

then

$$\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

where, for each i, the integer γ_i is the *smaller* of α_i and β_i.

Exercise 2.8. For integers a, b, and c, show that if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$, that is, any common divisor of a and b *divides* the $\gcd(a, b)$.

In practice, finding the prime decomposition of large numbers is computationally quite difficult and may well be impossible for numbers of the order of 10^{200}. There is an alternate method for finding gcds which is extremely efficient and avoids the decomposition problem. It is called *Euclid's Algorithm* and depends on the following theorem.

Theorem 2.9. Let a and b be integers. If $a = qb + r$ for integers q and r, then

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

Proof.

Example 2.9. Find $d = \gcd(343, 280)$.

In general, we have the following theorem.

Theorem 2.10. Let a and b be integers. If $d = \gcd(a, b)$, then there exist integers m and n such that

$$d = ma + nb.$$

The procedure for finding the greatest common divisor of two integers as illustrated in the last example is *Euclid's Algorithm*. It is computationally very efficient (see Buchmann, Theorem 1.8.6). If $a \geq b$, then $\gcd(a, b)$ can be calculated in at most the order of $\log a$ steps. So even if a and b are of the order 10^{200} (the order of magnitude of numbers used in RSA cryptography–see later), finding $\gcd(a, b)$ is quite feasible.

Definition 2.11. Two integers a and b are *relatively prime* or *coprime* if $\gcd(a, b) = 1$. □

Note that, since $p \mid a$ and $p \mid b$ implies that $p \mid \gcd(a, b)$ (see Exercise 2.8), this is

equivalent to the condition that a and b have no prime factor in common.

Example 2.10.

Example 2.11. Show that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Exercise 2.12. Prove the result in the last example using prime factorisation.

Note also that if a and b are coprime, then there exist integers m and n such that $ma + nb = 1$. Again, Euclid's Algorithm provides a very efficient way not only to check whether or not a and b are coprime, but to find m and n. Finding m and n is a crucial part of the cryptosystems we look at later.

Example 2.13. Show that 314 and 159 are coprime, and find integers m and n such that $314m + 159n = 1$.

Exercise 2.14. Show that for any integer t,

$$m = -40 + 159t \text{ and } n = 79 - 314t$$

is also a solution to $314m + 159n = 1$ in the last example.