2

Basic Properties of the Integers

In this chapter we consider some of the elementary properties of the integers. Many of them are *really* elementary and known to every school child. The algebraist's approach to such things as greatest common divisors (alias "highest common factors") and similar things may, however, be experienced as refreshingly different. We shall use, as before, the notation $\mathbb{Z}$ for the set of all integers, i.e. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$.

Much of modern Cryptology is based on arithmetic (or Number Theory, which at the level we aim at, would be a more appropriate appellation) as we shall show in later chapters, so we promise that you will eventually see this return to these concepts as justifiable.

2.1 Divisibility

As before, we have the following

Definitions Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then a is called a *divisor* or *factor* of b if there exists a $q \in \mathbb{Z}$ such that $b = q \cdot a$, and b is then said to be *divisible by* a, or a *multiple* of a. We denote this by $a|b$. Thus, by definition,

$$a|b \implies \exists q \in \mathbb{Z} \text{ such that } b = qa.$$

q is called the *quotient*.

Theorem *For all $a, b, c \in \mathbb{Z}$, with $a \neq 0$*

- $a|a,\ 1|a$;
- $a|b \Longrightarrow a|-b$;
- $a|b$ *and* $a|c \Longrightarrow a|(b+c)$;
- $a|b$ *and* $b|c \Longrightarrow a|c$;
- $a|b$ *and* $b|a \Longrightarrow a = \pm b$.

A.R. Meijer, *Algebra for Cryptologists*, Springer Undergraduate Texts in Mathematics and Technology,
DOI 10.1007/978-3-319-30396-3_2

Proof The proofs are trivial with the possible exception of that for the last statement: From the given statements we conclude that there exist integers q_1, q_2 such that $b = q_1 a$ and $a = q_2 b$, so that $a = q_2 q_1 a$, so that $q_1 q_2 = 1$. The only possibilities are that $q_1 = q_2 = 1$, in which case $a = b$, or that $q_1 = q_2 = -1$, in which case $a = -b$.

Any integer a is trivially divisible by ± 1 and by $\pm a$. If an integer p ($\neq \pm 1$) has only these trivial divisors it is called *prime*, otherwise it is called *composite*. The first (positive) primes are 2, 3, 5, 7, 11, 13, ... The numbers ± 1 are (by definition) not considered prime. 2 is the only even prime. (This is in itself not a profound statement: one might as well make the observation that 8923 has the remarkable property of being the only prime which is divisible by 8923. Nevertheless, the prime 2 seems, in many cases, to call for treatment different from that of odd primes.)

The **Fundamental Theorem of Arithmetic** states that every integer can be written as the product of primes in an essentially unique way:

Every nonzero integer n can be expressed as a product of the form

$$n = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

where the p_i are r distinct positive primes and the e_i are integers with $e_i > 0$. This representation is unique up to the order in which the factors are written.[1]

Note that if $n = \pm 1$, then $r = 0$, and the product of no terms at all is, by convention, equal to 1.

We shall not prove the Fundamental Theorem, assuming that everyone is aware of it (and believes that it is true). Those who would like to see a proof are referred to Victor Shoup's book *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2005, available online at www.shoup.net/ntb/ntb.v1.pdf.

We shall also make a lot of use of the following theorem:

Division with Remainder Property
For all $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.

Clearly $q = \lfloor \frac{a}{b} \rfloor$ and $r = a - b \cdot \lfloor \frac{a}{b} \rfloor \geq 0$.

Proof Consider the set $\{a - zb | z \in \mathbb{Z} \text{ and } a - zb \geq 0\}$. This set is clearly nonempty and therefore contains a smallest element.[2] Let r be this smallest element, so $r \geq 0$ and $r = a - qb$ for some $q \in \mathbb{Z}$. Also $r < b$, since otherwise we could write $a = (q + 1)b + (r - b)$, and $r - b \geq 0$, so that $r - b$ belongs to the set under discussion, contradicting the choice of r as the smallest element in that set.

It remains to prove that q and r are uniquely determined. Suppose that we have $a = qb + r$ and $a = q'b + r'$, with $0 \leq r, r' < b$. Then, subtracting and rearranging, we have $r - r' = (q' - q)b$. In this equation the left-hand side has absolute value less than $|b|$, whereas if

[1] If we, foolishly, decided that 1 should be considered to be a prime, the uniqueness of this decomposition into primes would no longer hold! This would, at the very least, be inconvenient for mathematicians.

[2] The principle that any nonempty set of positive integers contains a smallest element is equivalent to the principle of mathematical induction, as the reader is invited to prove. Here "equivalent" means that assuming either one of these principles, the other one can be proved as a theorem.

$q \neq q'$ the right-hand side has absolute value at least $|b|$. Hence $q = q'$, from which $r = r'$ follows.

Exercises

1. Let a, b, c, d be integers such that $c|a$ and $d|b$. Prove that $cd|ab$.
2. Show that any product of four consecutive integers is divisible by 24.
3. Prove that $4 \not| n^2 + 2$ for any integer n.
4. Prove by induction that $5|n^5 - n$ for every positive integer n.
5. Let n be a positive composite number. Show that there exists at least one prime divisor p of n satisfying $p \leq \sqrt{n}$.
6. Establish a one-to-one correspondence between the divisors of a positive integer n which are less than $\sqrt{n}$ and those that are greater than $\sqrt{n}$.
7. Prove the "Division with remainder property" in the following form: For all $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $-b/2 < r \leq b/2$.

2.2 Ideals and Greatest Common Divisors

We introduce the concept of *ideals* in $\mathbb{Z}$.

Definition A nonempty set $I \subseteq \mathbb{Z}$ is called an *ideal* in $\mathbb{Z}$ if the following two conditions hold:

$$\forall a, b \in I, \quad a + b \in I,$$

$$\forall a \in I \text{ and } \forall z \in \mathbb{Z}, \quad za \in I.$$

In other words, the set I is closed under addition, as well as under multiplication by *any* integer (and *not* just under multiplication by numbers belonging to I).

Two trivial examples of ideals in $\mathbb{Z}$ are, firstly, the set $\{0\}$ consisting only of the integer 0, and, secondly, the set $\mathbb{Z}$ itself.

Note that if I is an ideal in $\mathbb{Z}$, and $a, b \in I$, then also $a - b \in I$, since, by the second condition $-b = (-1)b \in I$, and therefore, by the first condition $a + (-b) = a - b \in I$. Consequently, if I is any ideal in $\mathbb{Z}$, then $0 \in I$.

We introduce the following notation:

$$a\mathbb{Z} = \{x | x = az \text{ for some } z \in \mathbb{Z}\}.$$

Thus $a\mathbb{Z}$ consists precisely of all multiples of a. We leave as an exercise the easy proof that the set $a\mathbb{Z}$ is an ideal. It is called the *principal ideal generated by a*.

What makes the integers interesting[3] is that the principal ideals are in fact the only ideals in $\mathbb{Z}$. Even the two trivial ideals are of this kind: $\{0\} = 0\mathbb{Z}$ and $\mathbb{Z} = 1\mathbb{Z}$.

Theorem *Every ideal in $\mathbb{Z}$ is principal.*

Proof Let I be an ideal in $\mathbb{Z}$. If $I = \{0\}$, we are through, so assume that $I \neq \{0\}$. Then I contains a positive integer, since (as we noted) if $x \in I$ then also $-x \in I$. Let a be the least positive element of I. We prove that $I = a\mathbb{Z}$.

For let b be any element of I. By the theorem above on division with remainder, there exist integers q and r, with $0 \leq r < a$ such that $b = qa + r$, i.e.

$$r = b - qa.$$

But $qa \in I$ (by the second condition on ideals) and since $b \in I$, we have that $r \in I$, by the first condition. But a was the least positive element of I, so the only way this can happen is for r to be 0. Hence, $b = qa \in a\mathbb{Z}$. We have therefore proved that

$$I \subseteq a\mathbb{Z}.$$

The reverse inclusion is obvious, since any multiple of an element of an ideal must also belong to the ideal, so that

$$a\mathbb{Z} \subseteq I,$$

which completes the proof.

Notation A principal ideal $a\mathbb{Z}$ of $\mathbb{Z}$ will also sometimes be denoted by $< a >$.

Theorem *Let $a, b \in \mathbb{Z}$. Then $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b|a$.*

Example

$$6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, 18, \ldots\},$$
$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\},$$

so $6\mathbb{Z} \subset 3\mathbb{Z}$, corresponding to the fact that $3|6$.

We leave the (easy) proof of the above theorem as an exercise.

What happens if we have two ideals, neither of which is contained in the other? Let I and J be two such ideals, so $I \nsubseteq J$ and $J \nsubseteq I$. Any ideal containing both I and J must contain all sums of elements $x \in I$ and $y \in J$. But it is straightforward to verify that the set

$$K = \{x + y | x \in I\ ,\ y \in J\}$$

[3]Or boring, depending on one's taste. Rings for which the following condition holds, the "principal ideal rings", are certainly easier to work with than a lot of other rings. We shall in Chap. 5 have occasion to consider an important family of other principal ideal rings which will turn out to be extremely useful in the construction of different kinds of symmetric key ciphers.

is itself already an ideal, so it must be the smallest ideal that contains both I and J. In fact, if $I =< a >$ and $J =< b >$, then K consists of all "linear combinations" of a and b:

$$K = \{ra + sb | r, s \in \mathbb{Z}\}.$$

We usually call the ideal K the *sum* of the ideals I and J: $K = I + J$.

But now something interesting can be noted. All ideals are principal, so $K =< d >$, for some integer d:

$$< a > + < b >=< d > .$$

Now $< a > \subseteq < d >$, so $d|a$, and similarly $d|b$, so that d is a *common divisor* of a and b. Suppose that d' is another divisor of both a and b. Then $< a > \subseteq < d' >$ and $< b > \subseteq < d' >$, so that $K \subseteq < d' >$, or $< d > \subseteq < d' >$, i.e. $d'|d$. Hence d is not only a common divisor of a and b, but *any common divisor of a and b is a divisor of d*. Thus d may be regarded as the *greatest common divisor* of a and b.

Definition If $a, b \in \mathbb{Z}$ then a greatest common divisor d of a and b is an integer such that

- $d|a$ and $d|b$;
- if $c|a$ and $c|b$, then $c|d$.

What we have therefore proved is that any two integers have a greatest common divisor. It is easy to see, and left to the reader as an exercise, that this result can easily be extended: any finite set of integers has a greatest common divisor. Note also that, following from the first theorem in this chapter, any two greatest common divisors differ at most simply by their sign: If d and d' are greatest common divisors of some (finite) set of integers, then $d = \pm d'$. When we speak of *the* greatest common divisor, we shall simply assume henceforth that we mean the positive one.

Notation Given two integers a and b we shall denote their greatest common divisor by $gcd(a, b)$.

We have, in the process, also proved an important property of the greatest common divisor of two integers:

If $d = gcd(a, b)$ then there exist integers x, y such that $xa + yb = d$.

This result is known as *Bezout's identity*.[4] It is, of course, immediate from the fact that $< a > + < b >=< d >$.

For example, the greatest common divisor of 56 and 36 is 4, which we can write as $4 = 2 \cdot 56 + (-3) \cdot 36$.

Definition Two integers a and b are called *relatively prime* if $gcd(a, b) = 1$.

[4]Incorrectly, strictly speaking. In the form in which we have just given it, as a theorem in Number Theory, the result is due to Claude Gaspard Bachet de Méziriac, like Bezout a Frenchman, who lived a century before Bezout.

Theorem *If a, b, c are integers such that $a|bc$ and $gcd(a, b) = 1$, then $a|c$.*

Proof By the previous observation, there exist integers x, y such that

$$xa + yb = 1.$$

Multiplying this equation by c we get

$$xac + ybc = c.$$

Now a is a divisor of each of the terms on the left-hand side, so a must be a divisor of c.

This result has the immediate

Corollary *Let $p > 0$ be a prime. If $p|ab$, then $p|a$ or $p|b$.*

Proof Suppose $p \not| a$. Since p is prime, its only divisors are ± 1 and $\pm p$, so that $gcd(p, b) = 1$ or $gcd(p, b) = p$. By the result just proved, the first case cannot hold. Hence $p|b$.

It is obvious that this result can be generalised: If p is a prime factor of $\prod_{i \in S} a_i$, where $\{a_i\}_{i \in S}$ is some finite set of integers, then $p|a_j$ for some $j \in S$.

Finally, we mention the following fact, which will occasionally prove useful:

If $gcd(a, b) = d$, then $gcd(a/d, b/d) = 1$. This also follows from the fact that $xa + yb = d$ for some integers x, y, and therefore

$$x\frac{a}{d} + y\frac{b}{d} = 1.$$

This means that any common divisor of a/d and b/d must be a divisor of 1, and therefore must be ± 1.

Exercises

1. Prove that the intersection $I \cap J$ of two ideals is itself an ideal. If $I =< a >$ and $J =< b >$, how can you describe $I \cap J$ in terms of a and b?
2. Define, for integers a, b, a *least common multiple* of a and b as an integer m such that

   1. $a|m$ and $b|m$

   and

   2. $\forall\, k \in \mathbb{Z}$ ($a|k$ and $b|k \Longrightarrow m|k$).

   Use the result from the previous exercise to show that any two integers have a least common multiple.
3. An ideal M in $\mathbb{Z}$ is called *maximal* if there is no ideal J such that $M \subset J \subset \mathbb{Z}$. Prove that an ideal M is maximal if and only if $M =< p >$ for some prime number p.
4. Prove that $\gcd(n, n + 2) = 1$ or 2 for every $n \in \mathbb{Z}$.
5. Prove that $a|bc$ if and only if $\frac{a}{\gcd(a,b)}|c$.

2.3 The Euclidean Algorithm

The "Division with Remainder" property can be used to prove the uniqueness of the factorization property of the integers, i.e. the Fundamental Theorem of Arithmetic, as shown in e.g. the book by Victor Shoup to which we referred in Sect. 2.1. Instead, however, we shall take uniqueness of factorisation as a fact, and doing so, it is easy to see that if we take two integers n and m with factorization into primes as

$$n = \prod_{i=0}^{r} p_i^{e_i},$$

$$m = \prod_{j=0}^{s} q_j^{f_j},$$

then $m|n$ if and only if every $q_j = p_i$ for some i and the corresponding $f_j \leq e_i$.

This observation allows one to express the least common multiple of two integers, once their factorisations into primes are known. For let

$$a = \prod_{i=0}^{r} p_i^{e_i},$$

$$b = \prod_{i=0}^{r} p_i^{f_i},$$

where the set of primes has been made the same for the two factorisations, by inserting exponents 0 where necessary, then

$$\gcd(a, b) = \prod_{i=0}^{r} p_i^{\min\{e_i, f_i\}}.$$

Also, for the least common multiple one has

$$\mathrm{lcm}(a, b) = \prod_{i=0}^{r} p_i^{\max\{e_i, f_i\}}.$$

This may be called the "high school method" of determining greatest common divisors and least common multiples. Note, incidentally, that this also shows that

$$\mathrm{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Example

$$32170781418 = 2^1 \times 3^1 \times 19^4 \times 41143,$$
$$1323248675872933 = 2^0 \times 3^0 \times 19^1 \times 41143^3,$$

so that their gcd is

$$2^0 \times 3^0 \times 19^1 \times 41143^1 = 781717.$$

The disadvantage of this method is clearly that one needs to be able to factorise the integers in order to apply it, and factorisation is, in general, a non-trivial problem. It is therefore good to know that there exists an efficient algorithm which does not require this prior knowledge. This is called the "Euclidean Algorithm" and appears already in the famous book of Euclid of Alexandria (ca. 350 BCE). The efficiency of this method actually allows one to reverse the process: instead of using factorisation in order to find greatest common divisors, the technique of finding greatest common divisors is a standard component of methods for finding factors.

Let a and b be the two integers whose greatest common divisor we wish to determine, and assume without loss of generality that $0 < b < a$. By the division with remainder theorem we can write

$$\begin{aligned} a &= q_0 b + r_0 & 0 \le r_0 < b \\ b &= q_1 r_0 + r_1 & 0 \le r_1 < r_0 \\ r_0 &= q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 \le r_3 < r_2 \end{aligned}$$

etc. This process cannot continue indefinitely, because the r_i form a strictly decreasing sequence of non-negative integers. The set $\{r_0, r_1, r_2, \dots\}$ must contain a smallest element, and this smallest element must be 0, since otherwise we could use division with remainder once more to get a still smaller remainder. Thus we must eventually reach an n such that

$$r_{n-2} = q_n r_{n-1} + r_n,$$
$$r_{n-1} = q_{n+1} r_n + 0.$$

We now claim that $r_n = \gcd(a, b)$. Indeed, $r_n | r_{n-1}$, so that, by the second to last equation, we find that $r_n | r_{n-2}$. Moving up one equation, we see that $r_n | r_{n-3}$. Continuing in this way, we eventually arrive at $r_n | r_2, r_n | r_1, r_n | r_0$ and finally at $r_n | b$ and $r_n | a$. Thus r_n is indeed a common divisor of a and b.

On the other hand, suppose that c is a common divisor of a and b, i.e. that $c | a$ and $c | b$. This time we move downwards through the equations. The first equation shows that $c | r_0$. Using this, we see from the second equation that $c | r_1$. Continuing in this way, we eventually arrive at $c | r_n$. Thus any common divisor of a and b is a divisor of r_n.

Example To find gcd(6035,1921) we note that

$$\begin{aligned} 6035 &= 3 \times 1921 + 272, \\ 1921 &= 7 \times 272 + 17, \\ 272 &= 16 \times 17 + 0, \end{aligned}$$

and we conclude that the greatest common divisor is 17.

Working backwards through this example, we also note how we can express 17 as a linear combination of 6035 and 1921:

$$\begin{aligned} 17 &= 1921 - 7 \times 272 \\ &= 1921 - 7 \times (6035 - 3 \times 1921) \\ &= 22 \times 1921 - 7 \times 6035. \end{aligned}$$

Since writing the gcd of two integers as a linear combination of those two integers will turn out to be an exceedingly useful trick, we formalise the above in a general way.

Let, as before, a and b be positive integers, with $b < a$ and let

$$\begin{aligned} a &= q_0 b + r_0, \\ b &= q_1 r_0 + r_1, \\ r_0 &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\cdots\cdots\cdots\cdots\cdots \\ r_{k-1} &= q_{k+1} r_k + r_{k+1}, \\ &\cdots\cdots\cdots\cdots\cdots \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

We shall define two sequences $\{P_i\}$ and $\{Q_i\}$ such that, for every $i = 0, 1, \ldots, n$

$$r_i = (-1)^i Q_i a + (-1)^{i+1} P_i b.$$

If, for consistency, we put $r_{-2} = a$ and $r_{-1} = b$, then this equation is satisfied for $i = -2$ and $i = -1$ if we choose $Q_{-2} = 1, Q_{-1} = 0, P_{-2} = 0$ and $P_{-1} = 1$. Now define, for $i \geq 0$, P_i and Q_i recursively by

$$\begin{aligned} P_i &= q_i P_{i-1} + P_{i-2}, \\ Q_i &= q_i Q_{i-1} + Q_{i-2}. \end{aligned}$$

An inductive argument then shows that the above equation holds for all i:

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_k r_k \\ &= (-1)^{k-1} Q_{k-1} a + (-1)^k P_{k-1} b \\ &\quad -q_k[(-1)^k Q_k a + (-1)^{k+1} P_k b] \\ &= (-1)^{k-1}[Q_{k-1} + q_k Q_k]a + (-1)^k [P_{k-1} + q_k P_k]b \\ &= (-1)^{k+1} Q_{k+1} a + (-1)^{k+2} P_{k+1} b. \end{aligned}$$

Note, in particular, that since $r_{n+1} = 0$,

$$\gcd(a, b) = r_n = (-1)^n Q_n a + (-1)^{n+1} P_n b,$$

as we were hoping to get, and that, since $r_{n+1} = 0$

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{a}{b}.$$

It is not hard to show (although we shall refrain from doing so) that the pairs P_i, Q_i consist of relatively prime integers. This implies that in the equation $\frac{P_{n+1}}{Q_{n+1}} = \frac{a}{b}$, the left-hand side cannot be simplified by cancelling out any common factors, or, in other words, the left-hand side represents the fraction $\frac{a}{b}$ in its lowest terms.

Example Let $a = 489$ and $b = 177$. We obtain

$$\begin{aligned} 489 &= 2 \times 177 + 135, \\ 177 &= 1 \times 135 + 42, \\ 135 &= 3 \times 42 + 9, \\ 42 &= 4 \times 9 + 6, \\ 9 &= 1 \times 6 + 3, \\ 6 &= 2 \times 3 + 0, \end{aligned}$$

so our quotients are as follows

i	0	1	2	3	4	:	5
q_i	2	1	3	4	1	:	2

Using the initial values and the recursion relations, we can complete the table as follows:

i	-2	-1	0	1	2	3	4	5
q_i			2	1	3	4	1	2
P_i	0	1	2	3	11	47	58	163
Q_i	1	0	1	1	4	17	21	59

Calculation confirms that $(-1)^4 Q_4 a + (-1)^5 P_4 b = 21 \times 489 - 58 \times 177 = 3 = r_4$ is indeed the greatest common divisor of 489 and 177.

It should be clear that any implementation of the Euclidean algorithm can, with very little extra effort, be extended to keep track of the P_i and Q_i at the same time and thus output at the end not only the greatest common divisor but also two integers x and y such that $xa + yb = \gcd(a, b)$. Such an implementation is commonly referred to as an implementation of the *Extended Euclidean Algorithm*.

One final comment may be made about the Euclidean algorithm: it is amazingly efficient. Its complexity is linear in the logarithm of its inputs, so finding the gcd of two 100 digit integers will take only twice as many steps as finding the gcd of two 10 digit integers.

The connections between this algorithm and the theory of continued fraction approximations to real numbers are not of any interest to cryptologists; with the possible exception of a (now outdated) technique for factoring,[5] its relevance to cryptology is minimal in any case. Factoring itself is relevant, and probably crucial, in breaking the RSA algorithm, as we shall see in Sect. 4.1.

Exercises

1. Find the gcd d of $a = 233968$ and $b = 282015$ and integers x, y such that $ax + by = d$.
2. Show that there are infinitely many pairs of integers (x, y) such that $x + y = 133$ and $\gcd(x, y) = 7$.

2.3.1 Stein's gcd Algorithm

Stein's version of the Euclidean algorithm is an adaptation convenient for machine implementation. Generally, division is a computationally demanding operation, whereas division by 2 is a simple right shift. Also, determining whether a given integer is even or odd, is a simple check on the least significant bit. Stein's implementation therefore makes no use of division except when it can be done by shifting.

Stein's algorithm depends on the following three observations, each of which allows one to reduce the size of at least one of the inputs by half:

1. If a and b are both even and not both zero, then $\gcd(a, b) = 2 \cdot \gcd(a/2, b/2)$.
2. If a is even and b is odd, then $\gcd(a, b) = \gcd(a/2, b)$.
3. If a and b are both odd, then $\gcd(a, b) = \gcd(\frac{a-b}{2}, b)$.

Stein's algorithm (also known as the Binary Algorithm) for finding greatest common divisors is faster than the standard method, because it does not require costly (in terms of time) integer divisions, even though it requires more iterations. The constants that are

[5] Lehmer, D.H.; Powers, R.E.: On Factoring Large Numbers; Bulletin of the American Mathematical Society **37** (10) (1931), pp. 770–776.

required in Bezout's identity, thereby obtaining an "extended" version of Stein's algorithm, can be found in a manner analogous to how it is done in the Euclidean algorithm.[6]

Still other algorithms are known, such as the Schönhage–Strassen algorithm, which are faster than either Euclid's or Stein's, but their efficiency only becomes apparent when the inputs are of the order of $2^{2^{15}}$ or more.

Please note that those Bezout constants will turn out to be quite important when we start dealing with $\mathbb{Z}_p$ (p prime) as a *field.* And to do that we clearly need to find out first of all what $\mathbb{Z}_p$ is supposed to mean.

2.4 Congruences

We recall the following from our introductory chapter:

Definition Let n be any nonzero integer. Two integers a and b are said to be *congruent modulo n* if $n|a-b$. We denote this by $a \equiv b \mod n$.

The relation $a \equiv b \bmod n$ is called a *congruence relation* or simply a *congruence*, and the integer n appearing in it is called the *modulus* of that congruence.

From the "division with remainder" property, the next theorem follows immediately:

Theorem *For any integers a and n with $n \neq 0$, there exists a unique integer $b \in \{0, 1, \ldots, n-1\}$ such that $a \equiv b \mod n$.* (We shall, possibly with an abuse of notation, denote this integer by $a \bmod n$. The reader is, however, warned that not all computer languages interpret $a \bmod n$ this way. The C language, for one, does not, and may return a negative value for $a \bmod n$.)

The following theorem, which we have already seen in Chap. 1, shows that a congruence is in fact an equivalence relation:

Theorem *Let a, b, c and $n \neq 0$ be integers. Then*

- $a \equiv a \bmod n$*;*
- *if* $a \equiv b \bmod n$ *then* $b \equiv a \bmod n$*;*
- *If* $a \equiv b \bmod n$ *and* $b \equiv c \bmod n$*, then* $a \equiv c \bmod n$*.*

Our next theorem shows that the arithmetical operations of addition (and subtraction) and multiplication on $\mathbb{Z}$ "carry over" to operations on the resulting set of equivalence classes. These equivalence classes are also known as *congruence* or *residue classes*, and we shall frequently use this terminology.

[6]See, for example, Joux, A.: *Algorithmic Cryptanalysis*, CRC Press, Boca Raton, 2009, pp. 30–32. Pseudocode for the extended Stein algorithm can be found in Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A.: *Handbook of Applied Cryptography*, CRC Press, 1997, p. 606.

Theorem *Let a, b, a', b' and $n \neq 0$ be integers such that $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$. Then*

$$a + b \equiv a' + b' \bmod n,$$
$$a \cdot b \equiv a' \cdot b' \bmod n.$$

Proof $n|a - a'$ and $n|b - b'$, so there exist integers q_1, q_2 such that $a - a' = q_1 n$ and $b - b' = q_2 n$. But then $(a+b)-(a'+b') = (q_1+q_2)n$ and $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = aq_2 n + q_1 nb' = (aq_2 + q_1 b')n$.

We can therefore define operations of "addition" and "multiplication" of the (finite) set of *equivalence classes*: Denote, temporarily, the equivalence class containing the integer x by $\overline{x}$, and keep the modulus n fixed. Then the theorem states that

$$\overline{a} + \overline{b} = \overline{a + b}$$

and

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Examples In the following examples we shall, by a common abuse of notation, denote the equivalence class containing a by a, rather than by the more correct $\overline{a}$.

1. Let $n = 6$. Then the set of equivalence classes is $\{0, 1, 2, 3, 4, 5\}$ and the tables for the addition and the multiplication of these classes are

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

and

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Let $n = 5$. Then the set of equivalence classes is $\{0, 1, 2, 3, 4\}$, and the tables are

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. Now let $n = 2$. In this case there are only two equivalence classes, viz. $\overline{0}$ (which is the class of all even integers) and $\overline{1}$ (the class of all odd integers), and the tables are as follows:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Note that the first table corresponds to the exclusive or (XOR, $\oplus$) operation. The second corresponds to the logical AND. (Alternatively, one might interpret these tables as "odd + even yields odd", "odd times odd yields odd", etc.)

Notation If n is a nonzero integer, then we shall refer to the set of congruence classes modulo n with the above definitions for addition and multiplication of such classes as the *ring of integers modulo n*, and denote this ring by $\mathbb{Z}_n$. We leave to the next chapter the answer to the question which immediately arises from this terminology: What is a ring? (Or, to avoid facetious replies: "What does an algebraist mean when he or she uses the word 'ring' in his or her professional capacity?")

2.5 Fermat's Factoring Method

The problem of finding the (prime or otherwise) factors of composite integers has been studied for centuries, but has in recent decades achieved greater attention because of its importance in the RSA public key system: it is generally assumed that a system based on RSA can be broken only by factoring the (publicly known) modulus used in the particular implementation.[7] One way of attempting to find a factorisation of an integer n would, of course, be to try the prime numbers less than $\sqrt{n}$, one by one, until one is found that divides neatly (i.e. without remainder) into n. This works fine if n is a small integer, but such an "exhaustive search" becomes totally impracticable when n has been selected to have only large prime factors.

More sophisticated methods of factoring an integer n usually depend on finding two integers a and b (with $a \not\equiv \pm b \bmod n$) such that

$$a^2 \equiv b^2 \bmod n$$

or, equivalently,

$$a^2 - b^2 \equiv 0 \bmod n,$$
$$(a-b)(a+b) \equiv 0 \bmod n.$$

Once this has been achieved, the problem is, for all practical purposes, solved, for this implies that $a - b$ and $a + b$ must have some divisor(s) in common with n, so that $\gcd(a - b, n)$ will be a divisor of n. We have the Euclidean algorithm available for finding that gcd efficiently.

Fermat's method of factoring represents an early, simple, version of this idea. Instead of trying to find a congruence

$$a^2 - b^2 = qn$$

one tries to find an equation

$$a^2 - b^2 = n$$

or

$$a^2 - n = b^2,$$

[7] But this has not been proved! (Or not yet?) It also does not mean that an *implementation* of RSA, or a protocol using RSA for encryption or signing is necessarily secure. An early example of what can go wrong is given by Bleichenbacher's successful attack on version 1 of RSA Data Security's standard PKCS 1 [Bleichenbacher, D.: Chosen ciphertext attacks against protocols based on the RSA Encryption Standard PKCS # 1; Proc. Crypto '98, LNCS 1462, Springer-Verlag, 1998, pp. 1–12].

RSA, by the way, is named after its inventors: **R**abin, **S**hamir and **A**dleman. We shall discuss RSA in some detail in Chap. 4.

whence the obtained factors of n are simply $a-b$ and $a+b$. Finding such an equation is done by, starting at $x = \lceil \sqrt{n} \rceil$, increasing x by 1 in each iteration, until $x^2 - n$ is a perfect square.

Example Factoring 3973 by this method, we start at $x = \lceil \sqrt{3973} \rceil = 64$, and obtain successively

$$64^2 - 3973 = 123 \text{ which is not a perfect square,}$$
$$65^2 - 3973 = 252 \text{ which is not a perfect square,}$$
$$66^2 - 3973 = 383 \text{ which is not a perfect square,}$$
$$67^2 - 3973 = 516 \text{ which is not a perfect square,}$$
$$68^2 - 3973 = 651 \text{ which is not a perfect square,}$$
$$69^2 - 3973 = 788 \text{ which is not a perfect square,}$$
$$70^2 - 3973 = 927 \text{ which is not a perfect square,}$$
$$71^2 - 3973 = 1068 \text{ which is not a perfect square,}$$
$$72^2 - 3973 = 1211 \text{ which is not a perfect square,}$$
$$73^2 - 3973 = 1356 \text{ which is not a perfect square,}$$
$$74^2 - 3973 = 1503 \text{ which is not a perfect square,}$$
$$75^2 - 3973 = 1652 \text{ which is not a perfect square,}$$
$$76^2 - 3973 = 1803 \text{ which is not a perfect square,}$$
$$77^2 - 3973 = 1956 \text{ which is not a perfect square,}$$
$$78^2 - 3973 = 2111 \text{ which is not a perfect square,}$$
$$79^2 - 3973 = 2268 \text{ which is not a perfect square,}$$
$$80^2 - 3973 = 2427 \text{ which is not a perfect square,}$$
$$81^2 - 3973 = 2588 \text{ which is not a perfect square,}$$
$$82^2 - 3973 = 2751 \text{ which is not a perfect square,}$$
$$83^2 - 3973 = 2916 = 54^2 \text{ which IS a perfect square.}$$

From the last step we get that $3973 = 83^2 - 54^2 = (83 - 54)(83 + 54) = 29 \times 137$.

This example shows that the method is still not terribly efficient: in fact the number of steps required is, if $n = ab$, $\frac{a+b}{2} - \lceil \sqrt{ab} \rceil$, in other words approximately equal to the difference

between the arithmetic and the geometric means of a and b. When a and b differ by an order of magnitude, this difference becomes very large.[8]

Exercises

1. What pattern appears in the sequence $\{x_i^2 - 3973\}$ in the example? Could such sequences be used to speed up an implementation of the Fermat algorithm?
2. Use Fermat's method to find the factors of 706711.
3. Given that if $n = 31864033$, then $24779170^2 \equiv 1 \bmod n$, find a factor of n.

2.6 Solving Linear Congruences

We shall start with another example:

Observe that $7 \cdot 13 = 91 \equiv 1 \bmod 15$, and suppose that we are asked to find all x such that $13x + 5 \equiv 12 \bmod 15$.

Now we have observed that all arithmetical operations on $\mathbb{Z}$ "carry over" to modular operations. Thus we may subtract 5 from both sides of this congruence to obtain

$$13x \equiv 12 - 5 \equiv 7 \bmod 15$$

and we may multiply both sides of this congruence by 7, and get

$$7 \cdot 13x \equiv 7 \cdot 7 \equiv 49 \equiv 4 \bmod 15$$

and, since $7 \cdot 13 \equiv 1 \bmod 15$, we get the solution

$$x \equiv 4 \bmod 15$$

(or, if you are fussy, that $x \in \{\ldots, -26, -11, 4, 19, 34, \ldots\}$).

Note that if we had considered a similar congruence $10x + 5 \equiv 10 \bmod 15$, we would have been stumped, for, no matter how long we looked for it, we would not have been able to find a z such that $10z \equiv 1 \bmod 15$. (After all, this would mean that $10z = 1 + 15k$ for some

[8] In a recent paper (#2009/318) published on the IACR ePrint archive (eprint.iacr.org) Erra and Grenier prove that with a more sophisticated search technique the Fermat method will lead to a successful factorisation in polynomial time if $n = p \cdot q$, with p and q both prime, and $|p - q| < n^{1/3}$. "Polynomial time" means that the time taken increases with the length l of n in bits like a polynomial in l. As a general rule, algorithms for solving problems (like searching for a cryptographic key) are considered practicable or feasible if they run in polynomial time. This is a very simple approach, but may through ignoring the degree—and the coefficients—of the polynomials, lead to the rejection of some cryptological primitives which would, in practice, have been quite secure. But that's another story, and we should get back to Algebra. Considering all problems for which a problem can be computed in polynomial time to be easy is just the cryptologists' way of ensuring an adequate safety margin. Cryptologists are very conservative and like *big* safety margins.

integer k, but in that case we have the contradiction that the left-hand side of the equation is divisible by 5, and the right-hand side cannot be.)

Definition Let a and n be two nonzero integers. An integer a' is called a *multiplicative inverse* of a modulo n if $a \cdot a' \equiv 1 \bmod n$.

Thus 7 and 13 are each other's multiplicative inverses modulo 15, whereas 10 does not have a multiplicative inverse modulo 15.

Theorem *Let a, n be integers with $n \neq 0$. Then a has a multiplicative inverse modulo n if and only if a and n are relatively prime.*

Proof This follows immediately from Bezout's identity: a and n are relatively prime if and only if there exist integers s and t such that $as + nt = 1$ which is the case if and only if $as \equiv 1 \bmod n$.

Theorem *Let a, b, c, n be integers with $n \neq 0$. If a and n are relatively prime then $ab \equiv ac \bmod n$ if and only if $b \equiv c \bmod n$. More generally, if d is the greatest common divisor of a and n, then $ab \equiv ac \bmod n$ if and only if $b \equiv c \bmod n/d$.*

Proof Suppose that $\gcd(a, n) = 1$, and let a' be the multiplicative inverse of a modulo n. Then $ab \equiv ac \bmod n$ implies $a'ab \equiv a'ac \bmod n$ and since $aa' \equiv 1 \bmod n$, this means $b \equiv c \bmod n$.

To prove the general case, note that if $ab \equiv ac \bmod n$, then $ab = ac + kn$ for some integer k. Dividing both sides of this equation by $d = \gcd(a, n)$, we get

$$\frac{a}{d}b = \frac{a}{d}c + k\frac{n}{d}$$

so that

$$\frac{a}{d}b \equiv \frac{a}{d}c \mod \frac{n}{d}$$

and since $\frac{a}{d}$ and $\frac{n}{d}$ are relatively prime, the result follows from the first part of the proof.

The reader may have noticed that we have, rather deviously, changed from referring to a multiplicative inverse to calling it *the* multiplicative inverse. This is because a multiplicative inverse, if it exists, is essentially unique. For suppose that x and x' are both multiplicative inverses of a modulo n. Thus $ax \equiv 1 \bmod n$ and $ax' \equiv 1 \bmod n$. But then

$$x \equiv x \cdot 1 \equiv x(ax') \equiv (xa)x' \equiv 1 \cdot x' \equiv x' \mod n.$$

Note that, whatever n may be, the congruence class 0, i.e. the element $0 \in \mathbb{Z}_n$, will never have an inverse. Looking at the examples at the end of Sect. 2.4, we see that in $\mathbb{Z}_6$, only the elements 1 and 5 have inverses (and both are their own inverses, coincidentally, which follows from the facts that only 1 and 5 are relatively prime to 6, and that $5 \equiv -1 \bmod 6$). On the other hand in $\mathbb{Z}_5$ and $\mathbb{Z}_2$ every nonzero element has an inverse, which follows from the fact that 5 and 2 are primes: If p is a prime, then every integer a such that $p \nmid a$ is relatively

prime to p. $\mathbb{Z}_5$ and $\mathbb{Z}_2$, and generally $\mathbb{Z}_p$, with p a prime, are our first examples of what are known as *finite fields*, about which more in later chapters, where we shall denote them as $GF(p)$, the "GF" standing for "Galois field".[9]

Exercises

1. Calculate in $\mathbb{Z}_{175}$: $37 \times 19,\ 35 \times 25,\ 13 \times (14 + 167),\ 4^{-1}$.
2. Calculate in $\mathbb{Z}_{29}$: $7 \times 13, 7^{-1} \times 13^{-1}, 25^7,\ 12 \times (13 + 14)$.
3. Solve for x:

$$333x + 129 \equiv 234 \mod 911.$$

4. Show that if $p > 2$ is a prime, then the congruence $x^2 \equiv 1 \bmod p$ has exactly two solutions.
5. More generally, show that if p is a prime, then the congruence $x^2 \equiv a^2 \bmod p$ has exactly two solutions. For how many values of a does the equation $x^2 \equiv a \bmod p$ have a solution?
6. The congruence $x^2 \equiv 1 \mod 4033$ has the four solutions (mod 4033) $x = 1, 4032, 110, 3923$. Conclude that 4033 cannot be prime. Find the factorization of 4033, using the given data.
7. Prove: If the congruence $kx \equiv a \bmod n$ has a solution, then it has s solutions, where $s = \gcd(k, n)$.
8. Show that as k runs through the values 1, 2, ..., 28, $2^k \bmod 29$ runs through all the nonzero elements of $\mathbb{Z}_{29}$. (One wonders whether this sort of thing can be done for any prime. The answer is "yes", as we shall show later in Sect. 6.2. But not necessarily with 2 as base, though.)
9. Solve for x and y:

$$2x + 3y \equiv 8 \bmod 17,$$
$$7x - y \equiv 7 \bmod 17.$$

10. A test for divisibility by 9 is (if one uses decimal notation) to add up all the digits of the number: if this gives a multiple of 9, the number is divisible 9. Explain why this works and then devise a similar test for divisibility by 11. Can you devise a test for divisibility by 7? (*Hint*: If $n = 10a + b$ is divisible by 7, then so is $n - 21b$.) If you can, you'll easily find one for divisibility by 37.

[9]This notation is not standardised: many books use the notation $\mathbb{F}_p$, whereas it is also common to denote fields by the letter K and variations on that theme, following the German, where they are known as *Körper*. Much of the early work on these mathematical structures was done in Germany. The rather bland term "field" was introduced into English by American algebraists who had studied in Germany. If an applied mathematician tells you that he is interested in field theory, you will have to enquire further to find out what kind of fields he means: the algebraic ones or, say, electro-magnetic ones.

2.7 The Chinese Remainder Theorem

We next consider solving systems of congruences, or more precisely, solving for a single unknown which must satisfy (linear) congruence relations with respect to different moduli. The theorem and the method concerned, which are known as the *Chinese Remainder Theorem*, sometimes referred to as CRT for short,[10] allows for calculations to be performed modulo smaller integers, with the final result, i.e. the result modulo a large product of moduli, only being calculated at the very end. This is helpful, since arithmetical operations with very large integers (as required, for example, in RSA based systems) may be very time-consuming. (There is a price to pay for this increased efficiency in that use of the CRT leaves the operations more vulnerable to certain attacks, such as those known as "glitch attacks".)

Theorem (CRT) *Let $n_1, n_2, \ldots n_k$ be positive integers which are pairwise relatively prime,*[11] *and let $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then there exists an integer z such that*

$$z \equiv a_i \bmod n_i \quad \forall\ i \in \{1, 2, \ldots, k\}.$$

Moreover, any other integer z' is also a solution to all these congruences if and only if $z \equiv z' \bmod n$, where $n = \prod_{i=1}^{k} n_i$.

Proof Let $n = \prod_{i=1}^{k} n_i$, and define, for $i = 1, 2, \ldots, k$

$$n_i' = n/n_i.$$

From the fact that the n_i are pairwise relatively prime, it is easy to see that $\gcd(n_i, n_i') = 1$ for all $i = 1, 2, \ldots, k$. Therefore there exists, for each i, an integer m_i such that $m_i n_i' \equiv 1 \bmod n_i$.

Now put, for each $i = 1, 2, \ldots, k$,

$$w_i = m_i n_i',$$

then we clearly have that

- $w_i \equiv 1 \bmod n_i$;
- $w_i \equiv 0 \bmod n_j$ for all $j \in \{1, 2, \ldots, k\} \backslash \{i\}$.

Hence, if we put

$$z = \sum_{i=1}^{k} w_i a_i$$

[10] The story goes that a Chinese emperor, wanting to find out how many troops he had, made them march past in rows of 3, then 5, and so on, noting in each case how many soldiers there were in the last incomplete row. He then applied the remainder theorem and computed the size of his army. Hence the name of the theorem. If you believe this story, you will be interested to know that the emperor concerned was taught the theorem by intergalactic aliens whose space ship had crash landed on the island of Atlantis.

[11] I.e., $\gcd(n_i, n_j) = 1$ whenever $i \neq j$.

then

$$z \equiv a_j \bmod n_j \quad \forall j \in \{1, 2, \ldots, k\}.$$

Moreover, if $z' \equiv z \bmod n$, then, since $n_i | n$ for all i, we also have that $z' \equiv z \equiv a_i \bmod n_i$ for all i, so that z' is also a solution of all the congruences.

Finally, if z' is any solution of all the congruences, then $z' \equiv z \bmod n_i$, for all i. In other words, $n_i | (z' - z)$ for all i. Since the n_i are relatively prime, this implies that $n | (z' - z)$, i.e. $z' \equiv z \bmod n$.

Examples

1. Consider the congruences

$$x \equiv 1 \bmod 7,$$
$$x \equiv 2 \bmod 23,$$
$$x \equiv 19 \bmod 29.$$

With the notation used in the theorem, we have $n = 7 \cdot 23 \cdot 29 = 4669$, $n_1' = 667$, $n_2' = 203$, $n_3' = 161$, and we can compute

$$m_1 = n_1'^{-1} \bmod n_1 = 667^{-1} \bmod 7 = 4,$$
$$m_2 = n_2'^{-1} \bmod n_2 = 203^{-1} \bmod 23 = 17,$$
$$m_3 = n_3'^{-1} \bmod n_3 = 161^{-1} \bmod 29 = 20.$$

This yields

$$w_1 = n_1' \cdot m_1 = 667 \cdot 4 = 2668,$$
$$w_2 = n_2' \cdot m_2 = 203 \cdot 17 = 3451,$$
$$w_3 = n_3' \cdot m_3 = 161 \cdot 20 = 3220,$$

so that

$$\begin{aligned} z &\equiv 1 \cdot 2668 + 2 \cdot 3451 + 19 \cdot 3220 = 70750 \\ &\equiv 715 \bmod 4669. \end{aligned}$$

2. In attempting to solve the congruence

$$x^2 \equiv 1 \bmod 323$$

we note that $323 = 17 \cdot 19$, so we are actually considering two simultaneous congruences:

$$x^2 \equiv 1 \bmod 17,$$
$$x^2 \equiv 1 \bmod 19.$$

Now, if p is a prime, then Exercise 5 of the previous section shows that the only solutions of a congruence $x^2 \equiv a^2 \bmod p$ are $x \equiv \pm a \bmod p$ for some a. So there are a total of four possibilities, which we solve by means of the Chinese Remainder Theorem:

$x \bmod 17$	1	1	-1	-1
$x \bmod 19$	1	-1	1	-1
$x \bmod 323$	1	18	305	322

Exercises

1. Solve for x: $x \equiv 1 \mod 7$, $x \equiv 2 \mod 11$ and $x \equiv 3 \mod 13$.
2. Find all solutions of the congruence $x^2 \equiv 13 \mod 391$. (*Hint*: $391 = 17 \times 23$.)

2.8 Some Number-Theoretic Functions

2.8.1 Multiplicative Functions

In this section we shall briefly discuss some number-theoretic functions, of which the most important one, by far, is Euler's totient function, better known as Euler's ϕ-function. In order to make the discussion a little more general, we shall discuss this in the context of "multiplicative functions". The proofs involved are a little messy, but not *too* difficult.

But if you want to go straight through to the most important case (for our purposes), the value of $\phi(n)$ where $n = p \cdot q$, the product of two primes, feel free to go to Sect. 2.8.4, where we give an easy proof of our main result for that particular case.

Definitions A function defined on the non-negative (or the positive) integers whose codomain is the field of complex numbers or a subset thereof, is called a *number-theoretic* function. A number-theoretic function f is called *multiplicative* if for any positive integers a and b which are relatively prime

$$f(ab) = f(a) \cdot f(b).$$

The following are immediate consequences of the definition:

- If f is multiplicative and not identically 0, then for any positive integer a such that $f(a) \neq 0$, we have

$$f(a) = f(1 \cdot a) = f(1) \cdot f(a),$$

  so that $f(1) = 1$.
- If f and g are multiplicative functions, then so is the function $f \cdot g$, defined by $(f \cdot g)(a) = f(a) \cdot g(a)$.

- If $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ is the factorization of n into a product of prime powers, and if f is multiplicative, then

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_r^{e_r}).$$

  Thus any multiplicative function is completely determined by its values at the primes and their powers.

Any multiplicative function f gives rise to a related one, as in the following theorem.

Theorem *If f is a multiplicative function and F is defined by*

$$F(n) = \sum_{0<d,d|n} f(d)$$

then F is also multiplicative.

Proof If a, b are relatively prime positive integers, then any divisor d of ab is a product of a divisor of a and one of b, i.e. $d = a' \cdot b'$, where $a'|a$ and $b'|b$. (This factorization may be trivial, of course, with $a' = 1$ or $b' = 1$.) Hence

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1 d_2) \\ &= \sum_{d_1|a, d_2|b} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|a} f(d_1) \right) \left(\sum_{d_2|b} f(d_2) \right) = F(a) F(b), \end{aligned}$$

as required.

Remarkably, the converse of this theorem is also true: If F is multiplicative, then so is f. This is a consequence of the Möbius inversion theorem, which we state and prove in the next subsection.

For now, let f be a multiplicative function, and define F as in the theorem. If p is a (positive) prime, then the only divisors of p^k are $1, p, p^2, \dots p^k$. We know that $f(1) = 1$, and therefore

$$F(p^k) = 1 + f(p) + f(p^2) + \dots + f(p^k) = \sum_{i=0}^{k} f(p_i^k).$$

Hence

$$F(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}) = \prod_{i=1}^{r} \sum_{j=0}^{e_i} f(p_i^j).$$

Example Define f by $f(a) = a$. Trivially, f is multiplicative. If we define s by

$$s(a) = \sum_{d|a} f(d)$$

then $s(a)$ is simply the sum of all the divisors of a. By what we have done so far, we find that if $a = p_1^{e_1} \dots p_r^{e_r}$, then

$$\begin{aligned} s(a) &= [1+p_1+\dots+p_1^{e_1}] \times \dots \times [1+p_r+\dots+p_r^{e_r}] \\ &= \frac{p_1^{e_1+1}-1}{p_1-1} \times \dots \times \frac{p_r^{e_r+1}-1}{p_r-1}. \end{aligned}$$

Thus, for example, the sum of the divisors of $1400 = 2^3 \times 5^2 \times 7$ is $\frac{2^4-1}{2-1} \times \frac{5^3-1}{5-1} \times \frac{7^2-1}{7-1} = 15 \times 31 \times 8 = 3720$.

Exercises

1. If f is any number-theoretic function, explain why

$$\sum_{d|a} f(d) = \sum_{d|a} f(a/d).$$

2. Define $d(a)$ by $d(a) = \sum_{d|a} 1$. Show that a is prime if and only if $d(a) = 2$ if and only if $s(a) = a + 1$ (where s is the function defined in the previous example).
3. A positive integer n is called *perfect* if $s(n) = 2n$, *deficient* if $s(n) < 2n$ and *abundant* if $s(n) > 2n$.

   (a) Show that any power of a prime is deficient.
   (b) Find the first four abundant natural numbers.
   (c) Perform a computer search to find the smallest odd natural abundant number.

   This terminology dates from antiquity, and is important in numerology,[12] but apart from providing some interesting number-theoretical problems (for example: no odd perfect number is known, but there is no proof that such a number cannot exist), there are few, if any, practical applications.

[12] From Oystein Ore's *Number Theory and its History:*—

> Alcuin (735–804), the adviser and teacher of Charlemagne, observes that the entire human race descends from the 8 souls in Noah's ark. Since 8 is a deficient number, he concludes that this second creation was imperfect in comparison with the first, which was based on the principle of the perfect number 6.

We are getting rather far from cryptology.

2.8.2 The Möbius Function

Definition The Möbius function μ is defined as follows: For any positive integer n

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by a square,} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ primes.} \end{cases}$$

Note that, from the definition, μ is a multiplicative function. Also recall that if f is any multiplicative function then $f \cdot \mu$ will also be multiplicative (so that $\mu(1)f(1) = 1$) and note that for a prime p

$$(\mu \cdot f)(p) = \mu(p)f(p) = -f(p),$$
$$(\mu \cdot f)(p^2) = 0.$$

In fact,

$$(\mu \cdot f)(p^k) = 0 \text{ whenever } k \geq 2.$$

Hence, if $n = p_1^{e_1} \dots p_r^{e_r}$, then

$$\sum_{d|n} (\mu \cdot f)(d) = (1 - f(p_1))(1 - f(p_2)) \dots (1 - f(p_r)).$$

In particular, if we take $f(a) = 1$ for all positive integers a, then we get

Property 1 For any integer $n > 1$

$$\sum_{d|n} \mu(d) = 0.$$

Similarly, by taking $f(n) = \frac{1}{n}$, we obtain

Property 2 For any integer $n > 1$

$$\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

The following lemma, which refines Property 1, will be needed in the proof of the main result in this section.

Lemma *Let a and b be integers greater than 1 such that $b|a$. Then*

$$\sum_{d:b|d|a} \mu\left(\frac{a}{d}\right) = \begin{cases} 1 & \text{if } b = a, \\ 0 & \text{otherwise.} \end{cases}$$

Proof Let $a = a' \cdot b$. If $b|d$ and $d|a$, put $d = d' \cdot b$. Then

$$\sum_{d\,:\,b|d|a} \mu(\frac{a}{d}) = \sum_{d'|a'} \mu(\frac{a'}{d'}) = \sum_{d'|a'} \mu(d')$$

according to the first exercise in the preceding subsection, and the last sum equals 0, by property 1, unless $a' = 1$, in which case the sum is just $\mu(1) = 1$.

Theorem (Möbius Inversion Theorem) *Let $f(n)$ be any number-theoretic function, and let F be defined by $F(n) = \sum_{d|n} f(d)$. Then*

$$f(n) = \sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \mu(n/d)F(d).$$

Proof The fact that the two sums are equal should not need explaining. Now observe that

$$\begin{aligned} \sum_{d|n} \mu(n/d)F(d) &= \sum_{d|n} \mu(n/d) \sum_{e|d} f(e) \\ &= \sum_{e|n} f(e) \sum_{d:e|d|n} \mu(n/d). \end{aligned}$$

By the lemma, the inner sum equals 0, except in the case where $e = n$, in which case it is 1. Thus the only nonzero term in the outer sum is the term for which $e = n$, and we have that

$$\sum_{d|n} \mu(n/d)F(d) = f(n),$$

as required.

2.8.3 Euler's ϕ-Function

Euler's *totient function*, usually referred to simply as "Euler's ϕ", is defined as follows:

Definition Let n be any integer greater than 1. Then

$$\phi(n) = \#\{a : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

In other words, $\phi(n)$ is the number of positive integers not exceeding n which are relatively prime to n. Note that $\phi(1) = 1$. (The integers ± 1 are the only ones which are relatively prime to themselves.)

If p is a positive prime, then all the numbers in the set $\{1, 2, 3, \ldots, p-1\}$ are relatively prime to p, so $\phi(p) = p - 1$. Also $\phi(p^k)$ is the number of elements remaining in the set $\{1, 2, 3, \ldots, p^k - 1\}$ after all the multiples of p have been deleted; since there are p^{k-1} such multiples, we get that $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

ϕ is in fact a multiplicative function – as we'll prove in a moment. From that fact we get that if $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, then

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1})\phi(p_2^{e_2}) \ldots \phi(p_r^{e_r}) \\ &= p_1^{e_1}(1 - 1/p_1)p_2^{e_2}(1 - 1/p_2) \ldots p_r^{e_r}(1 - 1/p_r) \\ &= n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Here is the promised theorem:

Theorem *If m and n are relatively prime, then $\phi(mn) = \phi(m) \cdot \phi(n)$.*

Proof Denote the set of residue classes modulo k which have multiplicative inverses by $\mathbb{Z}_k^*$. There are $\phi(k)$ such classes.

Thus we need to prove that if m and n are relatively prime, then

$$\#\mathbb{Z}_{mn}^* = (\#\mathbb{Z}_m^*)(\#\mathbb{Z}_n^*).$$

We do this by simply defining a function

$$p : \ \mathbb{Z}_{mn}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

by $p(x \bmod mn) = (x \bmod m, x \bmod n)$. Since $\gcd(x, mn) = 1$ implies that $\gcd(x, m) = \gcd(x, n) = 1$, the function p is certainly into $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Moreover, the Chinese Remainder Theorem guarantees that $p(x \bmod mn) = p(y \bmod mn)$ if and only if $x \bmod mn = y \bmod mn$, so that p is one-to-one. Finally, for any element of $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$, there exists, by the same theorem, an element of $\mathbb{Z}_{mn}^*$ which gets mapped onto it by p. Thus p is one-to-one and onto, and the two sets have the same cardinality.

Exercises

1. Find $\sum_{k=1}^{n} \phi(p^k)$, where p is a prime.
2. Show that
   (a) $\phi(4n) = 2\phi(2n)$;
   (b) $\phi(4n + 2) = \phi(2n + 1)$;
   (c) $\phi(n^2) = n\phi(n)$.
3. Prove that there does not exist a positive integer n such that $\phi(n) = 2p$ where p is a prime and $2p + 1$ is composite. Conclude that $\phi(n)$ can never equal 14.

2.8.4 The Case $n = p \cdot q$

If you followed our suggestion and skipped the previous few subsections, or if, in the less likely case that you didn't but have already forgotten: if n is a positive integer then $\phi(n)$ is the number of integers in the interval $[1, n]$ which are relatively prime to n.

It is obvious that if p is a prime then $\phi(p) = p - 1$.

In many cryptological applications, such as RSA, numbers of the form $n = p \cdot q$ are used, where both p and q are primes. Now in the interval $[1, n]$ there are q multiples of p, namely $p, 2p, 3p, \ldots, (q-1)p, qp$ and p multiples of q, namely $q, 2q, 3q, \ldots, (p-1)q, pq$. So the number of integers in $[1, pq]$ relatively prime to n is

$$\phi(n) = n - p - q + 1,$$

where the "+1" occurs because we twice counted pq itself. Hence

$$\phi(pq) = pq - p - q + 1 = (p-1)(q-1).$$

Exercise Use the facts that $n = 12509443$ is known to be the product of two primes and $\phi(n) = 12501720$ to find the two prime factors.

http://www.springer.com/978-3-319-30395-6

Algebra for Cryptologists

Meijer, A.R.

2016, XIV, 301 p. 6 illus., Hardcover
ISBN: 978-3-319-30395-6