A primer on elementary number theory

Leopold Kronecker asserted: *Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.* (Dear God has created the whole numbers, everything else is man's work.) The whole numbers or integers are the central objects of study in number theory. We denote by $\mathbb{Z}$ the set $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ of integers. $\mathbb{Z}$ is a ring under addition and multiplication of integers. In fact, $\mathbb{Z}$ is an integral domain endowed with many interesting properties. The only units in $\mathbb{Z}$ are ± 1.

The set $\mathbb{N}=\{1,2,3,\ldots\}$ of natural numbers or positive integers is also often referred in number theory. It is our convention not to treat the integer 0 (zero) as a natural number.[1] We use the special symbol $\mathbb{Z}_+$ to denote the set $\{0,1,2,3,\ldots\}$ of non-negative integers. Neither $\mathbb{N}$ nor $\mathbb{Z}_+$ is a ring or even a group. Both are monoids under multiplication of integers. $\mathbb{Z}_+$ is also a monoid under integer addition, whereas $\mathbb{N}$ is just a semigroup under addition.

For studying the properties of the integers it is often necessary to study more complex man-made objects like the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers. It is quite surprising (but still true) that a good amount of complex analysis had been developed in order to prove the so-called *prime number theorem* (PNT) which attempts to give a formula of the number of primes less than or equal to a given positive real number. More recently, the theory of number fields[2] and that of elliptic curves[3] came into existence during attempts to prove *Fermat's last theorem* (FLT) which states that there are no solutions of the equation $x^n+y^n=z^n$ with $x,y,z,n\in\mathbb{N}$ and with $n\geqslant 3$. Both the PNT and the FLT have been proved and in the process we have got beautiful branches of number theory, namely, *analytic number theory* and *algebraic number theory*.

Unfortunately, however, human pursuit of understanding the integers is far from complete even with these sophisticated gadgets. Lots of simple questions involving integers are still left unresolved. Many mathematicians believe that the amount of mathematics we know till date is little too inadequate to answer these profound questions.

In what follows I summarize (without proofs) some elementary results of *multiplicative number theory*, the branch of number theory that deals with the multiplicative properties of integers.

1. The fundamental theorem of arithmetic

The reader should already know that every (nonzero) integer can be expressed uniquely as a product of primes. Here is a formal approach to the story.

Definition An integer a is said to divide an integer b, if there is an integer x such that $b=ax$. When this happens, we write $a|b$ and also say that a is a *divisor* or *factor* of b and that b is an (integral) *multiple* of a. By this definition, every integer divides 0, whereas 0 divides no integer other than 0.

Corollary Let $a,b,c,x,y\in\mathbb{Z}$.
a) If $a|b$ and $b|c$, then $a|c$.
b) If $a|b$ and $a|c$, then $a|(bx+cy)$.
c) If $a|b$, then $|a|\leqslant|b|$.
d) $a|b$ and $b|a$ if and only if $a=\pm b$.

[1] Zero had to be invented. It was not available in nature. It is a contrived concept to make an attempt to quantify "nothing". In modern language 0 is the additive identity in the ring $\mathbb{Z}$. But then you have heard that there is a multinational company that manufactures and sells rings containing only natural resources like gold, diamond and gem stones!

[2] A number field is a finite (and hence algebraic) field extension of $\mathbb{Q}$.

[3] An elliptic curve is a plane curve of genus one. It can be described by an equation of the form: $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$. Caution: Ellipses are not elliptic curves.

Definition A *prime number* p is an integer $\neq 0, \pm 1$ such that $p = uv$ with $u, v \in \mathbb{Z}$ implies that either u or v is a unit (in $\mathbb{Z}$). An integer $\neq 0, \pm 1$ is called *composite*, if it is not prime. It is often convenient to restrict our attention on positive primes only. We reserve the symbol $\mathbb{P} = \{2, 3, 5, 7, 11, 13, \ldots\}$ to denote the set of (positive) prime numbers.

Theorem Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. Then $p|ab$ implies $p|a$ or $p|b$. Equivalently, if $p \not| a$ and $p \not| b$, then $p \not| ab$.

Definition Let $p \in \mathbb{P}$ and $a \in \mathbb{Z}$, $a \neq 0$. Then there exists an integer $v \in \mathbb{Z}_+$ such that $p^v | a$ but $p^{v+1} \not| a$. In this case we call v the *multiplicity* of p in a and denote[4] this as $v = \mathrm{v}_p(a)$. It is customary to take $\mathrm{v}_p(0) = \infty$. For every $v \in \mathbb{Z}_+ \cup \{\infty\}$ we adopt the conventions: $v + \infty = \infty + v = \infty$, $\min(v, \infty) = v$ and $\max(v, \infty) = \infty$.

Corollary Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. Then
a) $\mathrm{v}_p(a + b) \geqslant \min(\mathrm{v}_p(a), \mathrm{v}_p(b))$ with equality holding if $\mathrm{v}_p(a) \neq \mathrm{v}_p(b)$.
b) $\mathrm{v}_p(ab) = \mathrm{v}_p(a) + \mathrm{v}_p(b)$.
c) $a|b$ if and only if $\mathrm{v}_p(a) \leqslant \mathrm{v}_p(b)$ for all $p \in \mathbb{P}$.

Theorem [The fundamental theorem of arithmetic] Every non-zero integer a has a unique factorization of the form:

$$a = \sigma(a) \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(a)},$$

where $\sigma(a)$ denotes the sign of a (± 1) and where almost all (i.e., all except finitely many, perhaps none, of) the exponents $\mathrm{v}_p(a)$ are zero.

The factorization of a nonzero integer a can also be written as $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $r \in \mathbb{Z}_+$, $p_1, \ldots, p_r$ are (pairwise) distinct (positive) primes and $\alpha_1, \ldots, \alpha_r$ are positive (or nonnegative) numbers. Note that an empty product is treated as 1 (and an empty sum as 0).

An important corollary to the fundamental theorem of arithmetic is the following:

Theorem There are infinitely many primes. That is, the set $\mathbb{P}$ is infinite.

Definition Let a and b be integers not both zero.[5] The *greatest common divisor* or the *gcd* of a and b is defined to be the (positive) integer:

$$\gcd(a, b) := \prod_{p \in \mathbb{P}} p^{\min(\mathrm{v}_p(a), \mathrm{v}_p(b))}.$$

Clearly, $\gcd(a, b) = \gcd(b, a)$. If $a \neq 0$, it follows that $\gcd(a, 0) = |a|$. Furthermore, if $a|b$, then $\gcd(a, b) = |a|$. Two integers a and b (not both zero) are said to be *coprime* or *relatively prime*, if $\gcd(a, b) = 1$.

Factorization of a and b clearly gives us $\gcd(a, b)$. But they say that factorization is too tiring![6] Thanks to Euclid, we have a short-cut for computing $\gcd(a.b)$.

Theorem [Euclidean division] Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q and r satisfying $a = qb + r$ and $0 \leqslant r < |b|$.

The integers q and r in the last theorem are respectively called the *quotient* and the *remainder* of Euclidean

[4] Why v after all? $m_p(a)$ could have been more appropriate.
My answer: Why not v? Germans call multiplicity 'Vielfachheit'. A large part of modern mathematics has been developed in central Europe – Germany, France etc. English-speaking mathematicians do not hesitate to accept certain central European conventions. If you buy this idea too, keep yourself happy with v and have m free for denoting other things (say, the integers you are carrying in your bag). Or else use the other popular notation $p^v || a$ to mean $v = \mathrm{v}_p(a)$.

[5] 0 and 1 are not both zero, whereas 1 and 2 are both non-zero.

[6] Proving the primality or compositeness of an integer and factoring a composite integer are some of the central problems in number theory. With the advent of digital computers these problems have received special attention. While the primality of an integer can be checked reasonably fast using the so-called randomized algorithms, factoring large composite integers continues to remain a very difficult computational problem.

division of a by b. We follow the notations: $q = a \operatorname{quot} b$ and $r = a \operatorname{rem} b$. It follows that $b|a$ if and only if $a \operatorname{rem} b = 0$.

Theorem [Euclidean gcd] Let $a, b \in \mathbb{Z}$ be not both zero. Then for any $c \in \mathbb{Z}$ we have $\gcd(a, b) = \gcd(a - bc, b)$. In particular, if $b \neq 0$, then taking $c = a \operatorname{quot} b$ gives $\gcd(a, b) = \gcd(b, r)$, where $r = a \operatorname{rem} b$.

If we denote $r_0 := a$ and $r_1 := b$, then our task is to find $\gcd(r_0, r_1)$. Without loss of generality we may assume that $r_0 \geqslant r_1 \geqslant 0$. (The case $r_0 = r_1 = 0$ is to be excluded.) If $r_1 = 0$, then $\gcd(r_0, r_1) = r_0$. So assume that $r_1 > 0$ and reduce the computation of $\gcd(r_0, r_1)$ to that of $\gcd(r_1, r_2)$, where $r_2 := r_0 \operatorname{rem} r_1$. If $r_2 = 0$, we have $\gcd(r_1, r_2) = r_1$, otherwise we compute $\gcd(r_2, r_3)$, where $r_3 := r_1 \operatorname{rem} r_2$. This process must terminate after finitely many steps since we have $r_0 \geqslant r_1 > r_2 > r_3 > \cdots$, that is, we would eventually get $r_j = 0$ for some j.

Theorem [Bézout] Let $a, b \in \mathbb{Z}$ not both zero. Then there exist $u, v \in \mathbb{Z}$ (not unique, in general) such that $\gcd(a, b) = ua + vb$.

The integers u and v in Bézout's theorem can be computed with little additional effort during computation of $\gcd(a, b)$ using Euclid's algorithm. One initializes $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$. For $k = 2, 3, \ldots$ denote $q_k := r_{k-2} \operatorname{quot} r_{k-1}$. We get the new remainder as $r_k := r_{k-2} - q_k r_{k-1}$. We identically update the u and v values as $u_k := u_{k-2} - q_k u_{k-1}$ and $v_k := v_{k-2} - q_k v_{k-1}$. In this way we maintain the relationship $r_k = u_k a + v_k b$ for all $k = 0, 1, 2, \ldots$. If $r_j = 0$, then we have $\gcd(a, b) = r_{j-1} = u_{j-1} a + v_{j-1} b$, the desired *Bézout relation*.

We conclude this section after stating some properties of gcds.

Theorem Let $a, b, c \in \mathbb{Z}$ with a and b not both zero. Denote $d := \gcd(a, b)$. Then:
a) If $c \neq 0$, then $\gcd(ac, bc) = |c| d = |c| \gcd(a, b)$.
b) $\gcd(a/d, b/d) = 1$.
c) If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$ (provided that all these gcds are defined).
d) If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Exercises

1. Prove that for $a \in \mathbb{Z}$ the following conditions are equivalent:
(1) a is not divisible by the square of an integer greater than 1.
(2) a is not divisible by the square of a prime.
(3) $\mathrm{v}_p(a) \leqslant 1$ for every $p \in \mathbb{P}$.
If $a \in \mathbb{Z}$ satisfies one of these equivalent conditions, we say that a is *square-free*. Show that every $n \in \mathbb{Z}$ can be written as $n = ab^2$ with $a, b \in \mathbb{Z}$, where a is square-free. What is the largest number of consecutive square-free integers?

2. Let $m, n \in \mathbb{N}$ with $m \geqslant 2$. Prove that $\sqrt[m]{n}$ is irrational if n is not the mth power of an integer.

3. Let $n \in \mathbb{N}$ and $p \in \mathbb{P}$. Prove that $\mathrm{v}_p(n!) = \sum_{k \in \mathbb{N}} \lfloor n/p^k \rfloor$, where $\lfloor x \rfloor$ denotes the floor[7] of a real number x. Deduce that the number of trailing zero digits in the decimal representation of $n!$ is equal to $\mathrm{v}_5(n!)$. Compute the number of trailing zero digits in the decimal representation of 1234!.

4. Let $m, n \in \mathbb{N}$. Show that if $m^4 + 4^n$ is prime, then either $m = n = 1$ or m is odd and n is even. In particular, $m^4 + 4^m$ is prime only for $m = 1$.

5. Let $a, n \in \mathbb{N}$, $a \geqslant 2$. Show that:

(a) The *Mersenne number* $M_n := 2^n - 1$ is prime only if n is prime. (**Remark:** Marin Mersenne studied integers of the form $M_p := 2^p - 1$, $p \in \mathbb{P}$. For every $p \in \mathbb{P}$ the integer M_p need not be prime. Mersenne made a list of all values of $p \leqslant 255$ for which M_p is prime. Since digital computers were not invented in the times of Mersenne, he

[7] For a real number x the largest integer $\leqslant x$ is called the *floor* of x and is denoted by $\lfloor x \rfloor$, whereas the smallest integer $\geqslant x$ is called the *ceiling* of x and is denoted by $\lceil x \rceil$. For example, $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, $\lfloor -\pi \rfloor = -4$ and $\lceil -\pi \rceil = -3$. It is evident that $\lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil$ with equalities holding if and only if $x \in \mathbb{Z}$.

made a few mistakes. At the time of writing this note there are only 39 Mersenne primes known, the largest of which is $M_{13\,466\,917} = 2^{13\,466\,917} - 1$ which has 4 053 946 decimal digits and is the largest known prime. It is not known if there are infinitely many Mersenne primes.)

(b) The (generalized) *Fermat number* $a^n + 1$ is prime only if a is even and n is a power of 2. (**Remark:** Pierre de Fermat studied integers of the form $\mathrm{F}_n := 2^{2^n} + 1$. He found that F_n is prime for $n = 0, 1, 2, 3$ and 4 and conjectured that all F_n are prime. The next Fermat number F_5 was too big for Fermat to be treated by hand calculations. It, however, turned out that F_5 is not a prime. In fact, for no $n \geqslant 5$ the Fermat number F_n is known to be prime. Some mathematicians nowadays conjecture that all F_n, $n \geqslant 5$, are composite, but this conjecture is far from being settled.)

6. For $n \in \mathbb{N}$ define $\sigma(n) := \sum_{d|n} d$, where the sum is over all positive integral divisors of n.

* **(a)** Let $n_1, n_2 \in \mathbb{N}$ with $\gcd(n_1, n_2) = 1$. Show that $\sigma(n_1 n_2) = \sigma(n_1)\sigma(n_2)$.

(b) Show that for $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$ we have $\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = (p^{\alpha+1} - 1)/(p - 1)$.

(c) Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the canonical prime factorization of n. Deduce a formula for $\sigma(n)$.

7. An integer $n \in \mathbb{N}$ is called a *perfect number* if $\sigma(n) = 2n$, that is, if n equals the sum of its positive divisors smaller than itself.

(a) Let $M_p = 2^p - 1$ be a Mersenne prime. Show that the integer $2^{p-1} M_p$ is a perfect number. (**Remark:** The first four perfect numbers are of this form and are 6, 28, 496 and 8128. It can be shown that every *even* perfect number must be of the form $2^{p-1} M_p$, where M_p is a Mersenne prime. It is, therefore, not known if there are infinitely many even perfect numbers.)

(b) No odd perfect numbers are known. It is also not known if there is any odd perfect number. Explain the fallacy in the following example discovered by Descartes: Let $n = 198585576189 = 3^2 \times 7^2 \times 11^2 \times 13^2 \times 22021$. Then

$$\begin{aligned}
\sigma(n) &= (1+3+3^2)(1+7+7^2)(1+11+11^2)(1+13+13^2)(1+22021) \\
&= 13 \times 57 \times 133 \times 183 \times 22022 \\
&= 397171152378 = 2n\,.
\end{aligned}$$

* **8.** Let $m \in \mathbb{N}$ with $m \geqslant 2$. Show that $\sigma(m)$ is a power of two if and only if m is a product of (pairwise) distinct Mersenne primes.

9. Prove that $\gcd(a^n, b^n) = (\gcd(a, b))^n$, where $a, b, n \in \mathbb{N}$ and a and b are not both zero.

10. **(a)** Let $a, b, c, n \in \mathbb{N}$, $\gcd(a, b) = 1$ and $ab = c^n$. Prove that $a = x^n$ and $b = y^n$ for some $x, y \in \mathbb{N}$.

(b) Let $a, b, m, n \in \mathbb{N}$, $\gcd(m, n) = 1$ and $a^m = b^n$. Show that $a = x^n$ and $b = x^m$ for some $x \in \mathbb{N}$.

11. Let a and b be nonzero integers. The *least common multiple* or the *lcm* of a and b is defined to be the (positive) integer $\mathrm{lcm}(a, b) := \prod_{p \in \mathbb{P}} p^{\max(\mathrm{v}_p(a), \mathrm{v}_p(b))}$. Let $d := \gcd(a, b)$ and $m := \mathrm{lcm}(a, b)$. Show that:

(a) $m|d$.

(b) If m' is a common multiple of a and b, then $m|m'$.

(c) $dm = |ab|$.

(d) $\gcd(m/a, m/b) = 1$.

(e) $\mathrm{lcm}(ca, cb) = |c|m$ for every $c \in \mathbb{Z} \setminus \{0\}$.

12. Let $d, m \in \mathbb{N}$ with $d|m$. Show that the number of ordered pairs $(a, b) \in \mathbb{N}^2$ with $\gcd(a, b) = d$ and $\mathrm{lcm}(a, b) = m$ is 2^k, where k is the number of distinct prime divisors of m/d.

13. **(a)** Does there exist a polynomial $f(x)$ of degree > 1 with integer coefficients such that $f(n)$ is prime for every $n \in \mathbb{N}$? (**Hint:** Let $f(n) = p \in \mathbb{P}$ for some $n \in \mathbb{N}$. Then $p|f(n + kp)$ for every $k \in \mathbb{Z}_+$.)

(b) Does there exist a polynomial $g(x)$ of degree > 1 with integer coefficients such that $g(n)$ is composite for every $n \in \mathbb{N}$?

14. **(a)** Show that every positive integer of the form $4k + 3$ has a prime factor of the same form,

* **(b)** Show that there are infinitely many primes of the form $4k + 3$.

15. The sequence of Fibonacci numbers is defined as $F_0 := 0$, $F_1 := 1$ and $F_m := F_{m-1} + F_{m-2}$ for $m \geqslant 2$. The first few Fibonacci numbers are $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Show that:

(a) $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$ for all $m \in \mathbb{Z}_+$ and $n \in \mathbb{N}$. (**Hint:** Use induction on n.)

(b) $\gcd(F_m, F_{m+1}) = 1$ for all $m \in \mathbb{Z}_+$. (**Hint:** Use induction on m.)

* **(c)** $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \in \mathbb{N}$. (**Hint:** Use Parts (a) and (b) and follow the Euclidean gcd loop for computing $\gcd(m, n)$.)

(d) $F_m = \frac{1}{\sqrt{5}}(\rho^m - \bar{\rho}^m)$ for all $m \in \mathbb{Z}_+$, where $\rho = \frac{1+\sqrt{5}}{2}$ and $\bar{\rho} = \frac{1-\sqrt{5}}{2}$. (**Hint:** Use induction on m.)

** **(e)** For every $n \in \mathbb{N}$ there is an $m \in \mathbb{N}$ such that $n | F_m$. (**Hint:** For each $m \in \mathbb{N}$ define $f_m := F_m \operatorname{rem} n$. First show that the sequence $f_0, f_1, f_2, \ldots$ is periodic.)

* **16.** Show that for $n \in \mathbb{N}$, $n \geqslant 2$, the *harmonic number* $H_n := \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} \in \mathbb{Q}$ is not an integer. (**Hint:** Consider $t \in \mathbb{N}$ such that $2^t \leqslant n < 2^{t+1}$.)

** **17.** Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Show that for any $c \in \mathbb{N}$ there exists $x \in \mathbb{N}$ such that $\gcd(a + bx, c) = 1$. (**Hint:** You may choose x to be a suitable divisor of c.)

** **18.** Prove that if the number $(a^2 + b^2)/(1 + ab)$ with $a, b \in \mathbb{N}$ is a positive integer, then it is a perfect square. (**Hint:** Let $(a^2 + b^2)/(1 + ab) = n \in \mathbb{N}$ with $a > b$. Look at the two roots of the equation $(x^2 + b^2)/(1 + xb) = n$.)

[Exercises marked * are somewhat difficult, whereas those marked ** are really difficult (to the best of my knowledge).]

2. Congruences

Congruence is a handy notation about divisibility. This allows us the build the quotient ring $\mathbb{Z}_m := \mathbb{Z}/\mathbb{Z}m$ without any knowledge of algebra.[8]

Definition Let $m \in \mathbb{N}$. Two integers a and b are said to be *congruent modulo* m, denoted $a \equiv b \pmod{m}$, if $m | (a - b)$, or equivalently if $a \operatorname{rem} m = b \operatorname{rem} m$.

Corollary Let $m \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. Then:

a) If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$, $a - b \equiv c - d \pmod{m}$ and $ab \equiv cd \pmod{m}$.
b) If $a \equiv b \pmod{m}$ and if $f(x)$ is a polynomial with integer coefficients, then $f(a) \equiv f(b) \pmod{m}$.
c) If $a \equiv b \pmod{m}$ and $d | m$, then $a \equiv b \pmod{d}$.
d) If $a \equiv b \pmod{m}$ and $c \in \mathbb{N}$, then $ac \equiv bc \pmod{mc}$.
e) $ca \equiv cb \pmod{m}$ if and only if $a \equiv b \pmod{m/\gcd(m, c)}$.
f) If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.
g) If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Congruence is an equivalence relation on $\mathbb{Z}$.

Lemma Let $m \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then:

a) $a \equiv a \pmod{m}$.
b) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

The equivalence class of $a \in \mathbb{Z}$ under the relation 'congruence modulo m' is denoted by $[a]_m$. In fact, $[a]_m = \{a + km \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\} \subseteq \mathbb{Z}$. There are m (pairwise) disjoint equivalence classes modulo m. The set of all equivalence classes modulo m is denoted by $\mathbb{Z}_m$. $\mathbb{Z}_m$ is a ring (often called the *residue class ring modulo* m) with m elements and with addition and multiplication defined as: $[a]_m + [b]_m := [a+b]_m$ and $[a]_m [b]_m := [ab]_m$. One can easily check that these operations are well-defined, i.e., independent of the representatives of $[a]_m$ and $[b]_m$.

An integer $a \in \mathbb{Z}$ is said to be *invertible modulo* m, if there exists a $u \in \mathbb{Z}$ with the property that $ua \equiv 1 \pmod{m}$. The set of all $[a]_m$ such that a is invertible modulo m is the multiplicative group of

[8] Let R be a commutative ring and $\mathfrak{a}$ an ideal of R. We say that two elements a and b of R are congruent modulo $\mathfrak{a}$ if $a - b \in \mathfrak{a}$, or equivalently if the cosets $a + \mathfrak{a}$ and $b + \mathfrak{a}$ are equal. This is denoted as $a \equiv b \pmod{\mathfrak{a}}$. If $\mathfrak{a}$ is a principal ideal generated by $m \in R$, then it is customary to write $a \equiv b \pmod{m}$. Every ideal in $\mathbb{Z}$ is principal. Therefore, congruence of two integers modulo a nonzero integer is nothing but a special case of this algebraic notation.

units in $\mathbb{Z}_m$ and is denoted by $\mathbb{Z}_m^*$. Bézout's theorem provides the following important characterization of the elements of $\mathbb{Z}_m^*$.

Theorem Let $m \in \mathbb{N}$. An integer a is invertible modulo m if and only if $\gcd(a, m) = 1$.

If $\gcd(a, m) = 1$, then extended gcd calculation gives us integers u and v with $ua + vm = 1$, i.e., $ua \equiv 1 \pmod m$. In this case, we write $[u]_m = [a]_m^{-1}$ or $u \equiv a^{-1} \pmod m$.

$\mathbb{Z}_m$ is a field if and only if every integer not divisible by m is invertible modulo m. It easily follows that:

Theorem $\mathbb{Z}_m$ is a field if and only if m is a prime.

If m is composite, then $\mathbb{Z}_m$ is not even an integral domain, since it contains nonzero zero divisors. For example, $[3]_{15}[5]_{15} = [0]_{15}$.

Definition The cardinality of $\mathbb{Z}_m^*$ is denoted by $\phi(m)$. This function $\phi : \mathbb{N} \to \mathbb{N}$ is called *Euler's totient function* or *Euler's phi function*. Clearly, $\phi(m) = m - 1$ if and only if m is a prime.

We have the following explicit formula for $\phi(m)$.

Theorem Let $m \in \mathbb{N}$ have the canonical prime factorization $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with pairwise distinct (positive) primes $p_1, \ldots, p_r$ and with $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$. Then:

$$\phi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1) = m \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} \left(1 - \frac{1}{p}\right).$$

The following two theorems are extremely important in number theory:

Theorem [Fermat's little theorem] Let $p \in \mathbb{P}$. If $a \in \mathbb{Z}$ is coprime to (i.e., not divisible by) p, then $a^{p-1} \equiv 1 \pmod p$. For any $b \in \mathbb{Z}$ we have $b^p \equiv b \pmod p$.

Theorem [Euler's theorem] Let $m \in \mathbb{N}$. If $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod m$. For any $b \in \mathbb{Z}$ we have $b^m \equiv b^{m - \phi(m)} \pmod m$.

Clearly, Fermat's little theorem is a special case of Euler's theorem.

Congruences, like equations[9], can be solved for the unknowns appearing in the congruences. We start with the simple case of linear congruences.

Theorem The linear congruence $ax \equiv b \pmod m$ is solvable for x if and only if $d := \gcd(a, m)$ divides b. If $d|b$, the solution is unique modulo m/d and can be obtained as $x \equiv (a/d)^{-1}(b/d) \pmod{m/d}$.

Long back in human history, Chinese generals devised a nice trick to compute the number of soldiers in a troop. Assume that a certain troop is known to have no more than a thousand soldiers. The general asked the soldiers to stand in groups of 7. When the soldiers did that, the general counted the number of soldiers in the last group (which is $\leqslant 7$). He then repeated the procedure twice with 7 replaced by 11 and 13 respectively. Then he applied a magic formula by which he could compute (using the three numbers he got) the exact number of soldiers in his troop. The secret lies in the following theorem:

Theorem [Chinese remainder theorem (CRT)] Let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise relatively prime.[10] Given integers $a_1, \ldots, a_r$ there exists an integer x, unique modulo $m_1 \cdots m_r$, which satisfies the following congruences simultaneously:

$$x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}.$$

In order to construct such an integer x we denote $M := m_1 \cdots m_r$ and $M_i := M/m_i$ for all $i = 1, \ldots, r$. Since $\gcd(M_i, m_i) = 1$ by hypothesis, there exists an integer u_i such that $M_i u_i \equiv 1 \pmod{m_i}$. We then take $x \equiv \sum_{i=1}^r M_i u_i a_i \pmod{m_1 \cdots m_r}$.

[9] A congruence modulo m is actually an equation in $\mathbb{Z}_m$.

[10] The integers 4, 5 and 6 are *relatively prime*, since $\gcd(4, 5, 6) = 1$, but not *pairwise relatively prime* since $\gcd(4, 6) \neq 1$.

In algebraic terms the above theorem can be stated as $\mathbb{Z}_{m_1\cdots m_r} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$, where the isomorphism is that of rings. What is not immediate but still true is that $\mathbb{Z}^*_{m_1\cdots m_r} \cong \mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_r}$, where the isomorphism is that of multiplicative groups. This gives us a powerful insight in the structure of the groups $\mathbb{Z}^*_m$, if the factorization of m is known. We will discuss this topic in Section 3.

Let us come back to the problem of solving congruences. Let $f(x)$ be a polynomial with integer coefficients such that all the coefficients of f are not zero modulo m. We assume that the degree of f modulo m is at least 2 (since degree 1 polynomials have been already taken care of) and try to solve the congruence $f(x) \equiv 0 \pmod{m}$. If $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the canonical prime factorization of m, then we solve the congruences $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ for all $i = 1, \ldots, r$, and combine together the solutions of these congruences by using the CRT to get all the solutions of $f(x) \equiv 0 \pmod{m}$. It is, therefore, sufficient to be able to solve $f(x) \equiv 0 \pmod{p^\alpha}$ for $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$. To that end we proceed by induction on β and solve the congruences $f(x) \equiv 0 \pmod{p^\beta}$ for $\beta = 1, 2, \ldots, \alpha$ in succession. As the induction base let us assume, for the time being, that all the solutions of $f(x) \equiv 0 \pmod{p}$ are available. The inductive step of *lifting* the solutions modulo higher powers of p is illustrated in the following theorem.

Theorem [Hensel lifting] Assume that all the solutions of $f(x) \equiv 0 \pmod{p^\beta}$ are available for some $\beta \geqslant 1$. Let $x_\beta \pmod{p^\beta}$ be such a solution. Then this solution *lifts* to the solutions $x_\beta + kp^\beta \pmod{p^{\beta+1}}$ of $f(x) \equiv 0 \pmod{p^{\beta+1}}$ for all $k \pmod{p}$ satisfying the linear congruence $f'(x_\beta)k \equiv -\frac{f(x_\beta)}{p^\beta} \pmod{p}$, where f' denotes the (formal) derivative of f with respect to x. As x_β ranges over all the solutions of $f(x) \equiv 0 \pmod{p^\beta}$, we indeed get *all* the solutions of $f(x) \equiv 0 \pmod{p^{\beta+1}}$ by this lifting process.

Since we know how to solve linear congruences, the problem essentially reduces to solving congruences of the form $f(x) \equiv 0 \pmod{p}$ for $p \in \mathbb{P}$. An algorithm for finding roots of polynomials over a finite field (like $\mathbb{Z}_p$) can be used for that matter. We will not discuss these root finding algorithms in this note.

The relevant steps for solving the congruence $f(x) \equiv 0 \pmod{m}$ can be summed up as follows:

Goal: To find all the solutions of $f(x) \equiv 0 \pmod{m}$.

Steps:

1. Compute the factorization $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
2. For each $i = 1, \ldots, r$ compute the solutions $x_{i1}, x_{i2}, \ldots, x_{in_i}$ modulo $p_i^{\alpha_i}$ as follows:
   a) Use a root finding algorithm to compute the solutions of $f(x) \equiv 0 \pmod{p_i}$.
   b) For $j = 2, \ldots, \alpha_i$ in succession lift the solutions of $f(x) \equiv 0 \pmod{p_i^{j-1}}$ to those of $f(x) \equiv 0 \pmod{p_i^j}$.
3. For each $i = 1, \ldots, r$ and each $j = 1, \ldots, n_i$ use the CRT to compute an integer $x \pmod{m}$ satisfying simultaneously the congruences $x \equiv x_{ij} \pmod{p_i^{\alpha_i}}$ for $i = 1, \ldots, r$.

It follows that the number of solutions of $f(x) \equiv 0 \pmod{m}$ is $n_1 \cdots n_r$, i.e., the product of the numbers n_i of solutions of $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ for $i = 1, \ldots, r$. In particular, if one of the congruences $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ does not have a solution, then $f(x) \equiv 0 \pmod{m}$ also has no solutions.

In section 4 we will concentrate on the solvability of quadratic congruences, i.e., congruences of the form $ax^2 + bx + c \equiv d \pmod{m}$.

Exercises

1. Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. Show that:

(a) $\binom{p}{k} \equiv 0 \pmod{p}$ for all $k = 1, \ldots, p-1$, where $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ is the binomial coefficient.

(b) $(a+b)^p \equiv a^p + b^p \pmod{p}$ or, more generally, $(a+b)^{p^\alpha} \equiv a^{p^\alpha} + b^{p^\alpha} \pmod{p}$ for every $\alpha \in \mathbb{N}$.

(c) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

2. Find the simultaneous solution of the congruences: $7x \equiv 8 \pmod{9}$, $x \equiv 9 \pmod{10}$ and $2x \equiv 3 \pmod{11}$.

3. Compute all the solutions of the following congruences:

(a) $x^2 + x + 1 \equiv 0 \pmod{91}$.
(b) $x^2 + x - 1 \equiv 0 \pmod{121}$.
(c) $x^2 + 5x + 24 \equiv 0 \pmod{36}$.
(d) $x^{50} \equiv 10 \pmod{101}$.

4. Let $k \in \mathbb{N}$. Show that:
(a) There exist k consecutive composite integers.
(b) There exist k consecutive integers none of which is square-free.

5. Let $p \in \mathbb{P}$.
(a) Show that

$$\begin{aligned} x^{p-1} - 1 &\equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}, \quad \text{and} \\ x^p - x &\equiv x(x-1)(x-2)\cdots(x-(p-1)) \pmod{p}, \end{aligned}$$

where the congruence of two polynomials modulo p implies the congruences of all of the respective coefficients of the polynomials modulo p.
(b) [Wilson's theorem] Prove that $(p-1)! \equiv -1 \pmod{p}$.
(c) If $m \in \mathbb{N}$ is composite and $\geqslant 4$, then $(m-1)! \equiv 0 \pmod{m}$.

6. Let $p \in \mathbb{P}$ and let $f(x)$ be a nonzero polynomial with integer coefficients and of degree d.
* **(a)** Show that if $f(x) | (x^p - x)$, then the congruence $f(x) \equiv 0 \pmod{p}$ has exactly d solutions.
(b) Let $p = 3k + 1$. How many solutions does the congruence $x^{2k} + x^k + 1 \equiv 0 \pmod{p}$ have?

7. Show that the decimal representation of any rational number is (eventually) periodic. (Note that a terminating decimal representation may be viewed as one padded with an infinite number of trailing zeros.)

8. Let $m, n \in \mathbb{N}$. Show that:
(a) If $m > 2$, then $\phi(m)$ is even.
(b) If $m|n$, then $\phi(m)|\phi(n)$.
(c) If $\gcd(m, n) > 1$, then $\phi(mn) > \phi(m)\phi(n)$.
(d) If $m > 1$, then $\phi(mn) = \phi(n)$ if and only if $m = 2$ and n is odd.
(e) If $m|n$ and $m < n$, then $m - \phi(m) < n - \phi(n)$.

9. For $m \in \mathbb{N}$ define $\psi(m) := \sum_{d|m} \phi(d)$, where the sum is over all positive integral divisors of m. Show that:
(a) $\psi(m_1 m_2) = \psi(m_1)\psi(m_2)$ for $m_1, m_2 \in \mathbb{N}$ with $\gcd(m_1, m_2) = 1$.
(b) $\psi(p^\alpha) = p^\alpha$ for $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$.
(c) $\psi(m) = m$ for every $m \in \mathbb{N}$.

10. [The theoretical foundations of RSA cryptosystems][11]
(a) Let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise relatively prime, $m := m_1 \cdots m_r$. and let $\varphi_i : \mathbb{Z}_{m_i} \to \mathbb{Z}_{m_i}$ be a map for each $i = 1, \ldots, r$. Show that the map $\varphi : \mathbb{Z}_m \to \mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ taking $[a]_m \mapsto (\varphi_1([a]_{m_1}), \ldots, \varphi_r([a]_{m_r}))$ is bijective if and only if each φ_i, $i = 1, \ldots, r$, is bijective.
* **(b)** Let $m \in \mathbb{N}$ be square-free and let $\alpha \in \mathbb{N}$. Show that the exponentiation map $\mathbb{Z}_m \to \mathbb{Z}_m$, $[a]_m \mapsto [a]_m^\alpha = [a^\alpha]_m$, is bijective if and only if $\gcd(\alpha, \phi(m)) = 1$. (**Remark:** Have you already phigured out that I use φ to denote an arbitrary function and ϕ to denote Euler's totient function?)
(c) If $m \in \mathbb{N}$ is not square-free, show that for *no* $\alpha \in \mathbb{N}$, $\alpha \geqslant 2$, the exponentiation map $\mathbb{Z}_m \to \mathbb{Z}_m$, $[a]_m \mapsto [a]_m^\alpha$, is bijective.

[11] In the *RSA protocol* (named after the inventors Ronald L. Rivest, Adi Shamir and Leonard M. Adleman) of message encryption one chooses $m = pq$, where p and q are two distinct sufficiently large (of length 512 bits or more) primes. A *key-pair* (α, β) is selected modulo m with $\gcd(\alpha, \phi(m)) = 1$ and $\alpha\beta \equiv 1 \pmod{\phi(m)}$. The integers α and m are made public, whereas β is kept secret. *Encryption* of a message $x \in \mathbb{Z}_m$ is done by $y := x^\alpha \pmod{m}$, whereas *decryption* is carried out as $x := y^\beta \pmod{m}$. The security of the RSA protocol is based on the fact that it is not known how to compute β *efficiently* from the knowledge of m and α. All known algorithms are based on the factorization of m, which yields p and q and thereby gives $\phi(m) = (p-1)(q-1)$. Factorization of integers $m = pq$ with p, q of size 512 bits or more is at present an infeasible task and takes centuries even on the fastest computers on earth.

3. Structure of $\mathbb{Z}_m^*$

In this section we denote by m a positive integer (usually, $\geqslant 2$). Recall that the set $\{[a]_m \mid \gcd(a, m) = 1\}$ is the multiplicative group of units of the ring $\mathbb{Z}_m$. The cardinality of $\mathbb{Z}_m$ is $\phi(m)$, where ϕ denotes Euler's totient function. If $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the canonical prime factorization of m, then $\mathbb{Z}_m^*$ is canonically isomorphic to the external direct product $\mathbb{Z}^*_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}^*_{p_r^{\alpha_r}}$.

Definition Let $a \in \mathbb{Z}$ be coprime to m. The smallest positive integer h such that $a^h \equiv 1 \pmod m$ is called the *order of a modulo m* and is denoted by $\operatorname{ord}_m a$. That such an integer h exists immediately follows from Euler's theorem: $a^{\phi(m)} \equiv 1 \pmod m$.

Theorem Let $h := \operatorname{ord}_m a$ and $k \in \mathbb{Z}$. Then $a^k \equiv 1 \pmod m$ if and only if $h|k$. In particular, $h|\phi(m)$.

Theorem Let $h := \operatorname{ord}_m a$ and $k := \operatorname{ord}_m b$. If $\gcd(h, k) = 1$, then $\operatorname{ord}_m(ab) = hk$.

Theorem Let $h := \operatorname{ord}_m a$ and $k \in \mathbb{Z}$. Then $\operatorname{ord}_m(a^k) = h/\gcd(h, k)$.

If the factorization of $\phi(m) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is available, the following algorithm computes $\operatorname{ord}_m a$ for a given a coprime to m. Since $\operatorname{ord}_m(a)|\phi(m)$, we must have $\operatorname{ord}_m a = p_1^{\beta_1} \cdots p_r^{\beta_r}$, where each $\beta_i = \mathrm{v}_{p_i}(\operatorname{ord}_m a) \in \{0, 1, \ldots, \alpha_i\}$. Denote $\phi_i := \phi(m)/p_i^{\alpha_i}$. If $a^{\phi_i} \equiv 1 \pmod m$, then β_i is zero, otherwise β_i is the unique positive integer satisfying $a^{\phi_i p_i^{\beta_i}} \equiv 1 \pmod m$ together with $a^{\phi_i p_i^{\beta_i - 1}} \not\equiv 1 \pmod m$.

Definition An integer a is said to be a *primitive element* or a *primitive root modulo m*, if $\operatorname{ord}_m a = \phi(m)$. In that case, the group $\mathbb{Z}_m^*$ is cyclic with $[a]_m$ as a generator.

If $\mathbb{Z}_m^*$ is cyclic and $[a]_m$ is a generator of $\mathbb{Z}_m^*$, then all the generators of $\mathbb{Z}_m^*$ are $[a^k]_m$, $0 \leqslant k < \phi(m)$, $\gcd(k, \phi(m)) = 1$. In particular, in this case $\mathbb{Z}_m^*$ has $\phi(\phi(m))$ primitive roots modulo p.

A question arises naturally: For which values of $m \in \mathbb{N}$ is the group $\mathbb{Z}_m^*$ cyclic? Gauss proved the following characterization of all these values of m.

Theorem [Gauss] The group $\mathbb{Z}_m^*$ is cyclic (i.e., there exist primitive roots modulo m) if and only if $m = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and $\alpha \in \mathbb{N}$. In particular, for every $p \in \mathbb{P}$ the group $\mathbb{Z}_p^*$ is cyclic.

It follows that the group $\mathbb{Z}_{2^\alpha}^*$ is not cyclic for $\alpha \geqslant 3$. This group is actually the internal direct product of the group $\{\pm 1\}$ and the cyclic subgroup of cardinality $2^{\alpha-2}$ generated by $[5]_{2^\alpha}$.

Definition Let $n \in \mathbb{N}$ and $\gcd(a, m) = 1$. We call a an *n-th power residue modulo m* if the congruence $x^n \equiv a \pmod m$ has a solution for x, otherwise a is called an *n-th power nonresidue modulo m*. Second power residues and nonresidues are popularly known as *quadratic residues* and *nonresidues*. Similarly, for $n = 3$ and 4 we respectively speak of *cubic* and *biquadratic* residues and nonresidues.

The following characterization of power residues is very useful.

Theorem Let $\mathbb{Z}_m^*$ be cyclic, $n \in \mathbb{N}$ and $d := \gcd(n, \phi(m))$. For an integer a with $\gcd(a, m) = 1$ the congruence $x^n \equiv a \pmod m$ has d or no solutions according as $a^{\phi(m)/d} \equiv 1 \pmod m$ or not respectively.

The group $\mathbb{Z}_p^*$ is cyclic for $p \in \mathbb{P}$. The last theorem can be restated for this case as:

Theorem [Generalized Euler criterion] Let $p \in \mathbb{P}$ and $\gcd(a, p) = 1$. The congruence $x^n \equiv a \pmod p$ has $\gcd(n, p-1)$ or no solutions according as $a^{(p-1)/\gcd(n,p-1)} \equiv 1 \pmod p$ or not respectively.

Specializing further for the case $n = 2$ gives:

Theorem [Euler criterion (for quadratic residues)] Let p be an *odd* prime. An integer a coprime to p is a quadratic residue (resp. nonresidue) modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$ (resp. $a^{(p-1)/2} \equiv -1 \pmod p$).

Corollary Let $p \in \mathbb{P}$. The congruence $x^2 \equiv -1 \pmod p$ is solvable if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Equivalently, the congruence $x^2 \equiv -1 \pmod p$ is not solvable if and only if $p \equiv 3 \pmod 4$.

In general, it is difficult to find out a primitive root modulo m, even when we know that $\mathbb{Z}_m^*$ is cyclic. However, if the complete prime factorization of $\phi(m)$ is available, then the following simple randomized algorithm works nicely.

> **Goal:** Given that $\mathbb{Z}_m^*$ is cyclic and given the prime factorization $\phi(m) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, to compute a primitive root a modulo m.
>
> **Steps:**
> 1. Choose a random integer a coprime to m.
> 2. If $a^{\phi(m)/p_i} \not\equiv 1 \pmod{m}$ for all $i = 1, \ldots, r$, return a, otherwise go to Step 1.

Exercises

1. Let $p \in \mathbb{P}$ and $\operatorname{ord}_p a = 3$. Show that $\operatorname{ord}_p(1+a) = 6$.

2. Let p be an odd prime number and $M_p = 2^p - 1$ the Mersenne number corresponding to p. If q is a prime divisor of M_p, show that $q \equiv 1 \pmod{2p}$. (**Hint:** Look at $\operatorname{ord}_q 2$.)

3. Let $p \in \mathbb{P}$ and $k \in \mathbb{Z}$. Show that $1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid k, \\ -1 \pmod{p} & \text{if } (p-1) \mid k. \end{cases}$

4. Let $m, n \in \mathbb{N}$ with m odd. Show that $\gcd(2^m - 1, 2^n + 1) = 1$. (**Hint:** Assume otherwise, let p be a prime divisor of $\gcd(2^m - 1, 2^n + 1) = 1$ and consider $\operatorname{ord}_p 2$.)

5. Show that for any $h \in \mathbb{N}$ there exist $m, a \in \mathbb{N}$ with $\gcd(a, m) = 1$ such that $\operatorname{ord}_m a = h$.

6. Let $h := \operatorname{ord}_m a$ and $k := \operatorname{ord}_m b$. Show that $\operatorname{ord}_m(ab) | \operatorname{lcm}(h,k)$. Give an example where $\operatorname{ord}_m(ab) < \operatorname{lcm}(h,k)$.

7. **(a)** Let p be a prime of the form $4k+1$. Show that a is a primitive root modulo p if and only if $-a$ is a primitive root modulo p.

(b) Let p be a prime of the form $4k+3$. Show that a is a primitive root modulo p if and only if $\operatorname{ord}_p(-a) = (p-1)/2$.

8. Let p be an odd prime and let g and g' be two primitive roots (not necessarily distinct) modulo p. Show that gg' is not a primitive root modulo p.

9. Let p be a prime, $d | (p-1)$ and g a primitive root modulo p. Show that an integer a not divisible by p is a d-th power residue modulo p if and only if $a \equiv g^{kd} \pmod{p}$ for some $k \in \mathbb{Z}$.

*** 10.** **(a)** Let $m, n \in \mathbb{N}$. How many solutions does the congruence $x^n \equiv x \pmod{m}$ have? (**Hint:** In view of the CRT the problem reduces to the case $m = p^\alpha$ for some $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$. In that case $[0]_m$ is the only solution in $\mathbb{Z}_m \setminus \mathbb{Z}_m^*$. For counting the solutions in $\mathbb{Z}_m^*$ separately consider the cases that $\mathbb{Z}_m^*$ is cyclic and that it is not.)

(b) Compute the number of solutions of $x^3 \equiv x \pmod{10^{10}}$.

11. Let $m \in \mathbb{N}$ be odd and composite. Show that if there exists $[b]_m \in \mathbb{Z}_m^*$ for which $b^{m-1} \not\equiv 1 \pmod{m}$, then at least half of the elements $[a]_m \in \mathbb{Z}_m^*$ satisfy $a^{m-1} \not\equiv 1 \pmod{m}$.

*** 12.** Let $m \in \mathbb{N}$, $m > 1$.

(a) Show that the number of solutions of $x^{m-1} \equiv 1 \pmod{m}$ is $\prod_{\substack{p \in \mathbb{P} \\ p | m}} \gcd(p-1, m-1)$.

(b) Let m be composite. Then m is called a *Carmichael number*[12] if $a^{m-1} \equiv 1 \pmod{m}$ for every a coprime to m. Show that m is a Carmichael number if and only if m is square-free and $(p-1) | (m-1)$ for every $p | m$.

---

[12] If m is a prime, then every a coprime to m satisfies the Fermat congruence: $a^{m-1} \equiv 1 \pmod{m}$. Based on this observation a naïve primality testing algorithm can be designed like this:

> **Goal:** Given an odd integer $m > 1$ to check if m is prime.
>
> **Steps:**
> 1. For $i = 1, \ldots, t$ do the following:
>   a) Choose a random integer $a_i \in \{2, \ldots, m-1\}$.
>   b) If $a_i^{m-1} \not\equiv 1 \pmod{m}$, return "$m$ is composite".
> 2. Return "m is prime".

(c) Let $k \in \mathbb{N}$ be such that $p_1 := 6k+1$, $p_2 := 12k+1$ and $p_3 := 18k+1$ are all primes. Show that $p_1p_2p_3$ is a Carmichael number.

(d) Show that there are no even Carmichael numbers.

(e) Show that a Carmichael number must be the product of at least three distinct odd primes.

(f) Deduce that $561 = 3 \times 11 \times 17$, $41041 = 7 \times 11 \times 13 \times 41$, $825265 = 5 \times 7 \times 17 \times 19 \times 73$ and $321197185 = 5 \times 19 \times 23 \times 29 \times 37 \times 137$ are Carmichael numbers. (**Remark:** These are the smallest Carmichael numbers having three, four, five and six prime factors respectively.)

4. Quadratic residuosity and reciprocity

In this section we concentrate our attention on quadratic congruences of the form $Ay^2 + By + C \equiv 0 \pmod{m}$. From the results of Section 2 it follows that we need to concentrate only on the case that $m = p$ is a prime. Since we are dealing with a quadratic congruence we may assume without loss of generality that $\gcd(A, p) = 1$, i.e., that $p \not| A$. Moreover, since the case $p = 2$ is easy to handle, we let p be an odd prime, so that 2 has an inverse modulo p. In this case, the given congruence reduces to the form $x^2 \equiv a \pmod{p}$, where $x \equiv y + (2A)^{-1}B \pmod{p}$ and $a \equiv (4A^2)^{-1}(B^2 - 4AC) \pmod{p}$. It follows that the solutions of the congruence $Ay^2 + By + C \equiv 0 \pmod{m}$ are in one-to-one correspondence with those of $x^2 \equiv a \pmod{p}$.

In view of the argument in the last paragraph it is sufficient to consider quadratic congruences of the form:

$$x^2 \equiv a \pmod{p}, \quad p \text{ an odd prime.}$$

In the last section we have seen that if $\gcd(a, p) = 1$, then this equation has exactly two or no solutions according as whether a is a quadratic residue or a nonresidue modulo p respectively. On the other hand, if $p|a$, then the congruence $x^2 \equiv a \pmod{p}$ has a unique solution, namely $0 \pmod{p}$. The following notation helps us summarize these facts:

Definition Let p be an odd prime and $a \in \mathbb{Z}$. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \text{ and} \\ 0 & \text{if } p|a. \end{cases}$$

With this notation, the congruence $x^2 \equiv a \pmod{p}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions.

Note that if a is a quadratic residue modulo p and if $\xi^2 \equiv a \pmod{p}$, then the other root of $x^2 \equiv a \pmod{p}$ is $-\xi$ (i.e., $p - \xi$) modulo p. Since p is assumed to be odd, we have $\xi \not\equiv -\xi \pmod{p}$.

Theorem There are exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic nonresidues modulo an odd prime p.

Let Q_p denote the set of all (congruence classes of) quadratic residues modulo p. Then Q_p is a subgroup of $\mathbb{Z}_p^*$ of index $[\mathbb{Z}_p^* : Q_p] = 2$. The map $\eta : \mathbb{Z}_p^* \to \mathbb{Z}_p^*/Q_p = \{\pm 1\}$ taking $[a]_p$ to $\left(\frac{a}{p}\right)$ is a group homomorphism and is called the *quadratic character* modulo p. The following theorem is a direct consequence of these observations and of Euler's criterion discussed in Section 3.

If some a_i does not satisfy the Fermat congruence, m is certainly composite. However, if all a_i satisfy the congruence, we cannot guarantee that m is really prime. First assume that m is composite, but *not* a Carmichael number. By Exercise 11 each a_i satisfies the Fermat congruence with probability at most $1/2$. Thus m passes the above primality test with probability no more than $1/2^t$. Taking t sufficiently large (say, $t = 50$) we can make this failure probability arbitrarily small. On the other hand, if m *is* a Carmichael number, then every a coprime to m satisfies the Fermat congruence, that is, the above primality test fails with certainty, unless we come across an a_i with $\gcd(a_i, m) \neq 1$. But the probability of finding an element $a \in \{2, \ldots, m-1\}$ with $\gcd(a, m) \neq 1$ is, in general, very very low. In fact, finding such an a is computationally as difficult as factoring n.

R. D. Carmichael first found the existence of his numbers in 1910, studied their properties and conjectured that there are infinitely many of them. This conjecture has been proved by Alford, Granville and Pomerance in 1994. All the Carmichael numbers $< 10^5$ are 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 and 75361.

Theorem Let p be an odd prime and $a, b \in \mathbb{Z}$.

a) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$. [Euler's criterion]

b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

c) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. In particular, $\left(\frac{a}{p}\right) = \left(\frac{a \operatorname{rem} p}{p}\right)$.

d) If $p \not| a$, then $\left(\frac{a^2}{p}\right) = 1$.

e) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Euler's criterion gives us a nice way to check if a given integer is a quadratic residue modulo an odd prime. While this is much faster than the brute-force strategy of enumerating all the quadratic residues, it is still not the best solution, because it involves a modular exponentiation. We can, however, employ a gcd-like procedure for a faster computation. The development of this method demands further results which are otherwise interesting in themselves as well. The first important result is known as the *law of quadratic reciprocity*. Euler, Kronecker and Legendre, among others, studied this law and provided partial results. The first complete proof was given by Gauss in 1796. In fact, Gauss deemed the result so important that he gave eight proofs for it. At present about 200 published proofs exist in the literature.

Theorem [The law of quadratic reciprocity] Let p and q be two distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$, or equivalently $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$.

This law can be restated in the following different way. Consider the two congruences: $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$ for distinct odd primes p and q. If both p and q are congruent to 3 modulo 4, then exactly one of these congruences is solvable. On the other hand, if either p or q is congruent to 1 modulo 4, then either both these congruences are solvable or both are unsolvable.

In order to make the law of quadratic reciprocity a computational weapon for determining the Legendre symbol $\left(\frac{a}{p}\right)$ we need to consider the value of $\left(\frac{2}{p}\right)$ also.

Theorem Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$. In particular, 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 8$.

As an example let us compute $\left(\frac{360}{997}\right)$. Since $360 = 2^3 \times 3^2 \times 5$, we have $\left(\frac{360}{997}\right) = \left(\frac{2}{997}\right)\left(\frac{5}{997}\right) = (-1)^{\frac{997^2-1}{8}}\left(\frac{5}{997}\right) = -\left(\frac{5}{997}\right) = -(-1)^{\frac{(5-1)(997-1)}{4}}\left(\frac{997}{5}\right) = -\left(\frac{997}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{\frac{5^2-1}{8}} = 1$. Thus 360 is a quadratic residue modulo 997. In fact, the solutions of $x^2 \equiv 360 \pmod{997}$ are 193 and 804 modulo 997.

The apparent attractiveness of this method is beset by the fact that it demands the factorization of several integers (e.g. 360 in the above example) and as such does not lead to a practical algorithm. We need further machineries in order to have an efficient algorithm. First we define a generalization of the Legendre symbol.

Definition Let a, b be integers with $b > 0$ and odd. We define the *Jacobi symbol* $\left(\frac{a}{b}\right)$ as

$$\left(\frac{a}{b}\right) := \begin{cases} 0 & \text{if } \gcd(a,b) \neq 1, \\ 1 & \text{if } b = 1, \\ \prod_{i=1}^{t} \left(\frac{a}{p_i}\right) & \text{if } \gcd(a,b) = 1 \text{ and } b = p_1 \ldots p_t, \end{cases}$$

where in the last case $p_1, \ldots, p_t$ are all the prime factors of b (not necessarily all distinct).

Note that if $\left(\frac{a}{b}\right) \neq 1$, then a is not a quadratic residue modulo b. However, the converse is not always true, that is, $\left(\frac{a}{b}\right) = 1$ does not necessarily imply that a is a quadratic residue modulo b (Example: $a = 2$ and $b = 9$).[13] Of course, if b is an odd prime and if $\gcd(a,b) = 1$, the Legendre and Jacobi symbols $\left(\frac{a}{b}\right)$

[13] If $\gcd(a,b) = 1$, we could have defined $\left(\frac{a}{b}\right)$ to be 1 (resp. -1) if a is a quadratic residue (resp. nonresidue) modulo b. But this definition turns out not to be useful. Thus we opted for losing the direct connection of $\left(\frac{a}{b}\right)$ with the quadratic residuosity of a modulo b. What we gained is that the law of quadratic reciprocity continues to remain valid for this general definition. This is precisely what mathematics is: Do the right thing to achieve the desired goal.

correspond to the same value and meaning.

The properties of the Jacobi symbol are very similar to those of the Legendre symbol.

Theorem For $a, a' \in \mathbb{Z}$ and odd positive $b, b' \in \mathbb{Z}$ we have:
a) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$.
b) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$.
c) If $a \equiv a' \pmod{b}$, then $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$. In particular, $\left(\frac{a}{b}\right) = \left(\frac{a \operatorname{rem} b}{b}\right)$.

Theorem Let a and b be odd positive integers. Then:
a) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ and $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.
b) $\left(\frac{a}{b}\right) = (-1)^{\frac{(a-1)(b-1)}{4}}\left(\frac{b}{a}\right)$. Moreover, if $\gcd(a, b) = 1$, then $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{(a-1)(b-1)}{4}}$.

Now we can calculate the Legendre symbol $\left(\frac{360}{997}\right)$ without factoring as: $\left(\frac{360}{997}\right) = \left(\frac{2^3}{997}\right)\left(\frac{45}{997}\right) = \left(\frac{2}{997}\right)\left(\frac{45}{997}\right) = (-1)^{\frac{997^2-1}{8}}\left(\frac{45}{997}\right) = -\left(\frac{45}{997}\right) = -(-1)^{\frac{(45-1)(997-1)}{4}}\left(\frac{997}{45}\right) = -\left(\frac{997}{45}\right) = -\left(\frac{7}{45}\right) = -(-1)^{\frac{(7-1)(45-1)}{4}}\left(\frac{45}{7}\right) = -\left(\frac{45}{7}\right) = -\left(\frac{3}{7}\right) = -(-1)^{\frac{(3-1)(7-1)}{4}}\left(\frac{7}{3}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$. Note that here we still had to extract all the factors of 2 from certain integers. But that is easy. Nobody demanded the full factorization of integers.

Now we have a satisfactory computational procedure for determining the solvability of $x^2 \equiv a \pmod{p}$. The next question that arises is to compute a square root x of a modulo p, when we know that $\left(\frac{a}{p}\right) = 1$. This is a somewhat involved problem. The two easy cases are discussed first.

If $p \equiv 3 \pmod{4}$, then $x \equiv a^{\frac{p+1}{4}} \pmod{p}$.

If $p \equiv 5 \pmod{8}$, then $x \equiv \begin{cases} a^{\frac{p+3}{8}} \pmod{p} & \text{if } a^{\frac{p-1}{4}} \equiv 1 \pmod{p}, \\ 2a(4a)^{\frac{p-5}{8}} \pmod{p} & \text{if } a^{\frac{p-1}{4}} \equiv -1 \pmod{p}. \end{cases}$

In the remaining case, that is, $p \equiv 1 \pmod{8}$, one may use the following algorithm due to Tonelli and Shanks:

Steps:
1. Write $p - 1 = 2^v q$ with q odd.
2. The 2-Sylow subgroup G of $\mathbb{Z}_p^*$ is of order 2^v and is cyclic. Find a quadratic nonresidue b modulo p and compute a generator $g \equiv b^q \pmod{p}$ of G.
3. Find an even integer e, $0 \leqslant e < 2^v$, with $a^q \equiv g^e \pmod{p}$.
4. Compute the square root $x \equiv a^{\frac{q+1}{2}}(g^{\frac{e}{2}})^{-1} \pmod{p}$ of a modulo p.

This algorithm is randomized, because in Step 2 we need a random quadratic nonresidue modulo p. While it is easy to find deterministically a random quadratic residue modulo p, this is not the case with nonresidues. Since $\mathbb{Z}_p^*$ contains $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues, we expect to find a b with $\left(\frac{b}{p}\right) = -1$ after a few random values of b are tried. The algorithm can be made deterministic by choosing $b = 2, 3, \ldots$ in succession. This version behaves efficiently, given that there is a small quadratic nonresidue modulo p. It is easy to show that the least quadratic nonresidue modulo p has to be less than $1 + \sqrt{p}$. If the Extended Riemann Hypothesis (ERH)[14] is true, then the least quadratic nonresidue modulo p is $\leqslant 2\ln^2 p$ and the deterministic version of Tonelli and Shanks' algorithm runs in time polynomial in $\ln p$.

[14] Here is a short cultural introduction to the Riemann Hypothesis and its extended version:

The famous *prime number theorem* gives an asymptotic estimate of the number of primes smaller than or equal to a positive real number. Gauss conjectured this result in 1791. Many mathematicians tried to prove it during the nineteenth century and came up with partial results. The first complete proof (based mostly on the ideas of Riemann and Chebyshev) was given independently by the French mathematician Hadamard and by the Belgian mathematician de la Vallée Poussin in 1896. Their proof is regarded as one of the major achievements of modern mathematics.

Exercises

1. Let p be an odd prime and let $\gcd(a,p) = 1$. Show that the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ has exactly $1 + \left(\frac{b^2-4ac}{p}\right)$ solutions.

2. Find all the solutions of the following congruences:

(a) $x^2 \equiv 71 \pmod{713}$. (**Remark:** $713 = 23 \times 31$).

(b) $x^2 + x + 1 \equiv 0 \pmod{437}$. (**Remark:** $437 = 19 \times 23$).

3. **(a)** Find all the quadratic residues and nonresidues modulo 17 in the set $\{1, 2, \ldots, 16\}$.

Theorem [Prime Number Theorem (PNT)] Let $\pi(x)$ denote the number of primes less than or equal to a real number $x > 0$. As $x \to \infty$ we have $\pi(x) \to x/\ln x$ (i.e., the ratio $\pi(x)/(x/\ln x) \to 1$). In particular, for $n \in \mathbb{N}$ the density $\pi(n)/n$ of primes among the natural numbers $\leqslant n$ asymptotically approaches $1/\ln n$ as $n \to \infty$. It also follows that the nth prime is approximately equal to $n \ln n$.

Given the PNT it follows that $\pi(x)$ approaches $x/(\ln x - \xi)$ for any real ξ. It turns out that $\xi = 1$ is the best choice. Gauss's Li function is also an asymptotic estimate for $\pi(x)$, where for real $x > 0$ one defines:

$$\mathrm{Li}(x) := \text{ The principal value of the integral } \int_{\xi=0}^{x} \frac{d\xi}{\ln \xi}$$

Gauss conjectured that $\mathrm{Li}(x)$ asymptotically equals $\pi(x)$. The PNT is in fact equivalent to this conjecture. Furthermore, de la Vallée Poussin proved that $\mathrm{Li}(x)$ is a better approximation to $\pi(x)$ than $x/(\ln x - \xi)$ for any real ξ.

Definition The *Riemann zeta function* $\zeta(s)$ is defined for a complex variable s as

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n \in \mathbb{N}} \frac{1}{n^s}$$

The Riemann zeta function can be shown to have zeros at $s = -2, -4, -6, \ldots$. These are called the *trivial zeros* of $\zeta(s)$. It can be proved that all *non-trivial zeros* of $\zeta(s)$ must lie in the so-called *critical strip*: $0 \leqslant \operatorname{Re} s \leqslant 1$, and are symmetric about the *critical line*: $\operatorname{Re} s = 1/2$. Riemann conjectured:

Conjecture [The Riemann Hypothesis] All non-trivial zeros of $\zeta(s)$ lie *on* the critical line.

In 1900 Hilbert asserted that proving or disproving the RH is one of the most important problems confronting twentieth century mathematicians. The problem continues to remain so even to the twenty-first century mathematicians.

In 1901 von Koch proved that the RH is equivalent to the formula:

Conjecture [An equivalent form of the Riemann Hypothesis]

$$\pi(x) = \mathrm{Li}(x) + \mathrm{O}(x^{1/2} \ln x)$$

Hadamard and de la Vallée Poussin proved that

$$\pi(x) = \mathrm{Li}(x) + \mathrm{O}(x e^{-\alpha\sqrt{\ln x}})$$

for some positive constant α. While this estimate was sufficient to prove the PNT, the tighter bound due to von Koch continues to remain unproved.

Theorem [Dirichlet's theorem on primes in arithmetic progression] Let $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$. The set $\{a + bd \mid d \in \mathbb{Z}_+\}$ contains an infinite number of primes.

Dirichlet's theorem is a powerful generalization of infinitude of primes (which corresponds to $a = b = 1$). One can accordingly generalize the notation $\pi(x)$ as follows:

Definition Let $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$. Then by $\pi_{a,b}(x)$ we denote the number of primes in the set $\{a + bd \mid d \in \mathbb{Z}_+\}$, that are $\leqslant x$.

The PNT gives the estimate:

$$\pi_{a,b}(x) \to \frac{(1 + \mathrm{o}(1))\, x}{\phi(b) \ln x} \quad \text{as } x \to \infty\,.$$

The RH now generalizes to:

Conjecture [The Extended Riemann Hypothesis (ERH)] For $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$

$$\pi_{a,b}(x) = \frac{1}{\phi(b)} \mathrm{Li}(x) + \mathrm{O}(x^{1/2} \ln x)\,.$$

(b) Show that the equation $6x^2 - 17y^2 = 1$ does not have a solution in integers.

4. Let $n \in \mathbb{N}$ be congruent to 3 modulo 4. Show that:

(a) $(0,0,0)$ is the only solution $(x,y,z) \in \mathbb{Z}^3$ of the equation $x^2 + y^2 = nz^2$. (**Hint:** Reduce modulo 4.)

(b) There is no solution $(x,y) \in \mathbb{Q}^2$ of the equation $x^2 + y^2 = n$, i.e., there are no points with rational coordinates on the circle $x^2 + y^2 = n$ with radius $\sqrt{n}$ and center at the origin.

5. Let p and q be two distinct primes of the form $4k+3$, $m := pq$ and a (with $\gcd(a,m) = 1$) a quadratic residue modulo m. Show that a has exactly four square roots modulo m, of which exactly one is a quadratic residue modulo m.

6. Let p be a prime of the form $4k+1$. Find the sum of the quadratic residues (modulo p) in the set $\{1, \ldots, p-1\}$. (**Hint:** Look at $\left(\frac{-1}{p}\right)$.)

*** 7.** Let p be an odd prime. Prove that the product of all quadratic residues (modulo p) in the set $\{1, \ldots, p-1\}$ is congruent to $+1$ or -1 according as p is of the form $4k+3$ or $4k+1$ respectively. (**Hint:** If $\left(\frac{a}{p}\right) = 1$ and $ab \equiv 1 \pmod{p}$, then $\left(\frac{b}{p}\right) = 1$.)

8. Let p be a prime of the form $4k+1$ and let a and b be positive integers with a odd and $a^2 + b^2 = p$. Show that $\left(\frac{a}{p}\right) = 1$. (**Hint:** Use the law of quadratic reciprocity.)

9. Let p be an odd prime. Prove that:

(a) g^k is a quadratic nonresidue modulo p if and only if k is odd, where g is a primitive root modulo p. In particular, every primitive root modulo p is a quadratic nonresidue modulo p.

(b) Every quadratic nonresidue modulo p is a primitive root modulo p if and only if p is of the form $2^{2^n} + 1$ for some $n \in \mathbb{Z}_+$.

10. **(a)** Show that the Fermat number $F := 2^{2^n} + 1$, $n \in \mathbb{N}$, is prime if and only if $3^{(F-1)/2} \equiv -1 \pmod{F}$. (**Hint:** Look at $\left(\frac{3}{F}\right)$.) In particular, if F is prime, then 3 is a primitive root modulo F.

(b) Let p be an odd prime with $q := 2p+1$ also prime, and let $M_p := 2^p - 1$ be the Mersenne number corresponding to p. Show that $q | M_p$ if and only if $p \equiv 3 \pmod{4}$. (**Hint:** Look at $\left(\frac{2}{q}\right)$.)

*** 11.** Let $m \in \mathbb{N}$ and $\gcd(a,m) = 1$. Prove that the numbers of solutions of the congruence $x^2 \equiv a \pmod{m}$ for the following different cases of m are as given in the next table:

m	Number of solutions of $x^2 \equiv a \pmod{m}$
1	1
2	1
4	2 or 0 according as $a \equiv 1 \pmod{4}$ or not
2^α ($\alpha \in \mathbb{N}$ and $\alpha \geqslant 3$)	4 or 0 according as $a \equiv 1 \pmod{8}$ or not
p^α (p an odd prime and $\alpha \in \mathbb{N}$)	$1 + \left(\frac{a}{p}\right)$

Hence compute the number of solutions of $x^2 \equiv a \pmod{m}$ for a general modulus $m \in \mathbb{N}$.

12. Let p be an odd prime and let $a, b \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Show that $\sum_{j=0}^{p-1} \left(\frac{aj+b}{p}\right) = 0$.

*** 13.** Let m be an odd square-free integer > 1 and let $a, b \in \mathbb{Z}$ with $\gcd(a,m) = 1$. Show that $\sum_{j=0}^{m-1} \left(\frac{aj+b}{m}\right) = 0$. (**Hint:** You may start by showing that there is an integer c coprime to m such that $\left(\frac{c}{m}\right) = -1$.)

14. Let $p \in \mathbb{P}$ be odd.

(a) For $j \in \mathbb{N}$ define $S_j := 1^j + 2^j + \cdots + (p-1)^j$. Show that if $1 \leqslant j \leqslant p-2$, then $S_j \equiv 0 \pmod{p}$.

Taking $b = 1$ demonstrates that the RH is a special case of the ERH.

The ERH implies the following:

Conjecture The smallest positive quadratic nonresidue modulo a prime p is $< 2\ln^2 p$.

*** (b)** Let $\gcd(a,p) = 1$ and define $S := \sum_{j=0}^{p-1} \left(\frac{j^2+a}{p}\right)$. Show that $S \equiv -1 \pmod{p}$. (**Hint:** Use Euler's criterion, the binomial theorem and Part (a).)

(c) Conclude that $S = -1$.

*** 15.** Let $p \in \mathbb{P}$.

(a) Let x be an integer not divisible by p. Show that there exist integers a, b satisfying $0 < |a| < \sqrt{p}$, $0 < |b| < \sqrt{p}$ and $a \equiv bx \pmod{p}$. (**Hint:** Let $r := \lfloor \sqrt{p} \rfloor$. Apply the pigeon-hole principle[15] on the $(r+1)^2$ integers $(u+vx) \operatorname{rem} p$ with $u, v \in \{0, 1, 2, \ldots, r\}$.)

(b) Show that p can be expressed in the form $a^2 + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. (**Hint:** The congruence $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.)

(c) Show that p can be expressed in the form $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod{8}$. (**Hint:** The congruence $x^2 \equiv -2 \pmod{p}$ is solvable if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod{8}$.)

(d) Show that p can be expressed in the form $a^2 + 3b^2$ with $a, b \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \pmod{3}$. (**Hint:** The congruence $x^2 \equiv -3 \pmod{p}$ is solvable if and only if $p = 3$ or $p \equiv 1 \pmod{3}$.)

5. Simple continued fractions

John Wallis and Lord William Brouncker in an attempt to solve a problem posed by Pierre de Fermat developed the theory of continued fractions. However, there is evidence that this theory in some form was known to the Indian mathematician Bhaskaracharya in the twelfth century A.D. An expression of the form

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_{k-1} + \cfrac{1}{x_k}}}}$$

with $x_0, x_1, \ldots, x_k \in \mathbb{R}$, all positive except perhaps x_0 is called a (finite) *continued fraction*. If all x_i are integers, then this continued fraction is called *simple*. In that case, the integers x_i are called the *partial quotients* of the continued fraction. Note that by definition x_0 may be positive, negative or zero, whereas all subsequent x_i must be positive.

In order to make continued fractions look less menacing and in order to reduce wastage of paper let us agree to denote[16] the above continued fraction expansion by the short-hand notation $\langle x_0, x_1, x_2, \ldots, x_{k-1}, x_k \rangle$. If we start folding the stair from bottom, we conclude that a finite simple continued fraction $\langle a_0, \ldots, a_k \rangle$ evaluates to a rational number. For example, $\langle 9, 1, 10, 4, 2 \rangle$ represents $1001/101$.

The converse is also true, i.e., given any rational h/k, with $k > 0$ and $\gcd(h, k) = 1$ one can develop a finite simple continued fraction expansion of h/k. This can be done using the procedure for computing the gcd of h and k as the following example illustrates:

$$\begin{aligned} 1001 &= 9 \times 101 + 92 \\ 101 &= 1 \times 92 + 9 \\ 92 &= 10 \times 9 + 2 \\ 9 &= 4 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

[15] *Dirichlet's pigeon-hole principle* (also known as *Dirichlet's box principle*) states that if there are $n+1$ or more pigeons in n holes, then there is a hole containing two or more pigeons. This can be generalized as follows: If there are m objects in n boxes, then there is at least one box containing $\geqslant \lceil m/n \rceil$ objects.

[16] Some authors prefer to use the notation $x_0 + \frac{1}{x_1 +} \frac{1}{x_2 +} \cdots \frac{1}{x_{k-1} +} \frac{1}{x_k}$. This perhaps gives a better feeling of the stair and is, in particular, important if the angular brackets have to be reserved for symbolizing more sacred entities. I also prefer to designate an ideal in a ring generated by the elements $x_0, x_1, \ldots, x_k$ by $\langle x_0, x_1, \ldots, x_k \rangle$ (without even bothering which one is more sacred, an ideal or a continued fraction) with the hope that context makes it clear what is what!

Therefore, $1001/101 = \langle 1001/101\rangle = \langle 9, 101/92\rangle = \langle 9, 1, 92/9\rangle = \langle 9, 1, 10, 9/2\rangle = \langle 9, 1, 10, 4, 1/2\rangle = \langle 9, 1, 10, 4, 2\rangle$

Let $r := \langle a_0, \ldots, a_k\rangle$. If $a_k > 1$, then the simple continued fraction $\langle a_0, \ldots, a_k - 1, 1\rangle$ also represents r. On the other hand, if $a_k = 1$, then the simple continued fraction $\langle a_0, \ldots, a_{k-1} + 1\rangle$ also represents r. In either case these are the only two simple continued fractions representing r. For example, $\langle 9, 1, 10, 4, 2\rangle$ and $\langle 9, 1, 10, 4, 1, 1\rangle$ are the only simple continued fractions representing $1001/101$.

Finite continued fractions appear not to be so interesting. Assume that an infinite sequence $a_0, a_1, a_2, \ldots$ of integers, all positive except perhaps a_0, is given. We want to assign a meaning (and value) to the *infinite simple continued fraction* $\langle a_0, a_1, a_2, \ldots\rangle$. To this end we inductively define two infinite sequences h_n and k_n as follows:

$$\begin{array}{llll} h_{-2} = 0, & h_{-1} = 1, & h_n = a_n h_{n-1} + h_{n-2} & \text{for } n \geqslant 0 \\ k_{-2} = 1, & k_{-1} = 0, & k_n = a_n k_{n-1} + k_{n-2} & \text{for } n \geqslant 0 \end{array}$$

We also define the rationals $r_n := h_n/k_n$ for $n \geqslant 0$. This makes sense, since we have $1 = k_0 \leqslant k_1 < k_2 < k_3 < \cdots < k_n < \cdots$. Then we have:

Theorem $r_n = \langle a_0, \ldots, a_n\rangle$ for every $n \in \mathbb{Z}_+$. Furthermore, r_n satisfy the inequalities: $r_0 < r_2 < r_4 < \cdots < r_5 < r_3 < r_1$. The limit $\xi := \lim_{n\to\infty} r_n$ exists and for every $m, n \in \mathbb{Z}_+$ we have $r_{2m} < \xi < r_{2n+1}$.

This allows us to assign the unique real number ξ to the infinite continued fraction $\langle a_0, a_1, a_2, \ldots\rangle$, i.e.,

$$\langle a_0, a_1, a_2, \ldots\rangle := \lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n\rangle = \lim_{n\to\infty} r_n = \lim_{n\to\infty} \frac{h_n}{k_n} = \xi\,.$$

Theorem The value of an infinite simple continued fraction is *irrational*. Moreover, two different infinite simple continued fractions evaluates to different values, i.e., if $\langle a_0, a_1, a_2, \ldots\rangle = \langle b_0, b_1, b_2, \ldots\rangle$, then $a_n = b_n$ for all $n \in \mathbb{Z}_+$.

Definition For each $n \in \mathbb{Z}_+$ the rational number r_n is called the *n-th convergent* to the irrational number $\xi = \langle a_0, a_1, a_2, \ldots\rangle$.

The converse question is: Does any irrational ξ expand to an infinite simple continued fraction? The answer is again 'yes'. We inductively generate $a_0, a_1, a_2, \ldots$ with $\xi = \langle a_0, a_1, a_2, \ldots\rangle$ as follows: We start by setting $\xi_0 := \xi$ and $a_0 := \lfloor \xi_0\rfloor$. When $\xi_0, \ldots, \xi_n$ and $a_0, \ldots, a_n$ are known for some $n \geqslant 0$, we calculate: $\xi_{n+1} := 1/(\xi_n - a_n)$ and $a_{n+1} := \lfloor \xi_{n+1}\rfloor$. Since ξ is irrational, it follows that each ξ_n is also irrational. In addition, the integers $a_1, a_2, a_3, \ldots$ are all positive. (a_0 may be positive, negative or zero.)

As an example let us develop the infinite simple continued fraction expansion of $\pi = 3.1415926535\ldots$:

$$\begin{aligned} \xi_0 = \pi &= 3.1415926535\ldots, & a_0 &= \lfloor \xi_0\rfloor = 3\,, \\ \xi_1 = \frac{1}{\xi_0 - a_0} &= 7.0625133059\ldots, & a_1 &= \lfloor \xi_1\rfloor = 7\,, \\ \xi_2 = \frac{1}{\xi_1 - a_1} &= 15.996594406\ldots, & a_1 &= \lfloor \xi_1\rfloor = 15\,, \\ \xi_3 = \frac{1}{\xi_2 - a_2} &= 1.0034172310\ldots, & a_1 &= \lfloor \xi_1\rfloor = 1 \text{ and so on.} \end{aligned}$$

Thus the first few convergents to π are $r_0 = \langle 3\rangle = 3$, $r_1 = \langle 3, 7\rangle = 22/7 = 3.1428571428\ldots$, $r_2 = \langle 3, 7, 15\rangle = 333/106 = 3.1415094339\ldots$ and $r_3 := \langle 3, 7, 15, 1\rangle = 355/113 = 3.1415929203\ldots$. It is apparent that the convergents $r_0, r_1, r_2, r_3, \ldots$ go successively closer to π. This is indeed true in general:

Lemma Let h_n/k_n, $n \in \mathbb{Z}_+$, be the convergents to the irrational number ξ. Then $|\xi - \frac{h_n}{k_n}| < \frac{1}{k_n k_{n+1}}$, or equivalently $|\xi k_n - h_n| < \frac{1}{k_{n+1}}$ for all $n \geqslant 0$.

Theorem Let h_n/k_n, $n \in \mathbb{Z}_+$, be the convergents to the irrational number ξ. Then for all $n \geqslant 1$ we have $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$. In particular, $|\xi - \frac{h_n}{k_n}| < |\xi - \frac{h_{n-1}}{k_{n-1}}|$ for all $n \geqslant 1$.

The convergents h_n/k_n to the irrational ξ are called *best possible approximations* to ξ in the sense that if a rational a/b is closer to ξ than h_n/k_n is, then the denominator b has to be larger than k_n. More precisely:

Theorem Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ with $|\xi - \frac{a}{b}| < |\xi - \frac{h_n}{k_n}|$ for some $n \geqslant 1$. Then $b > k_n$.

Exercises

1. Expand the following irrational numbers as infinite simple continued fractions: $\sqrt{2} - 1$, $1/\sqrt{3}$ and $\sqrt{15}$.

2. Let h_n/k_n be the convergents to an irrational ξ and let F_n, $n \in \mathbb{Z}_+$, denote the Fibonacci numbers (See Exercise 15 of Section 1.).

(a) Show that $k_n \geqslant F_{n+1}$ for all $n \geqslant \mathbb{Z}_+$.

(b) Deduce that $k_n \geqslant \left\lfloor \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} \right\rfloor$ for all $n \in \mathbb{Z}_+$. (**Remark:** This shows that the denominators in the convergents to an irrational number grow quite rapidly (at least exponentially) in n.)

(c) Does there exist an irrational number ξ for which $k_n = F_{n+1}$ for all $n \in \mathbb{Z}_+$?

3. [A lemma from algebra] A real number of the form $\frac{a+\sqrt{b}}{c}$ with $a, b, c \in \mathbb{Z}$, $c \neq 0$ and $b \geqslant 2$ *not* a perfect square is called a *quadratic irrational*. Prove that for $\xi \in \mathbb{R}$ the following conditions are equivalent:
(1) ξ is a quadratic irrational.
(2) ξ is a root of a quadratic polynomial with integer coefficients but of no linear polynomials with integer coefficients.
(3) The minimal polynomial of ξ over $\mathbb{Q}$ is quadratic.

4. An infinite simple continued fraction $\langle a_0, a_1, a_2, \ldots \rangle$ is called *periodic*, if there exist $s \in \mathbb{Z}_+$ and $t \in \mathbb{N}$ such that $a_{n+t} = a_n$ for all $n \geqslant s$. Thus one can rewrite a periodic continued fractions as $\langle a_0, \ldots, a_{s-1}, \overline{b_0, \ldots, b_{t-1}} \rangle$, where the bar over the block of terms $b_0, \ldots, b_{t-1}$ indicates that this block is repeated ad infinitum. If $s = 0$, this continued fraction can be written as $\langle \overline{b_0, \ldots, b_{t-1}} \rangle$ and is called *purely periodic*. Show that a periodic simple continued fraction represents a quadratic irrational. (**Hint:** First consider the case of purely periodic continued fractions and then adapt to the general case.)
(**Remark:** The converse of the result in this exercise is also true, i.e., the simple continued fraction expansion of a quadratic irrational is periodic. However, the proof of this converse is not that easy.)

5. Evaluate the periodic continued fractions $\langle 1, 2, 3, \overline{4} \rangle$ and $\langle 1, 2, \overline{3, 4} \rangle$.

*** 6.** Prove that there are infinitely many solutions in positive integers of both the equations $x^2 - 2y^2 = 1$ and $x^2 - 2y^2 = -1$. (**Hint:** Compute $h_n^2 - 2k_n^2$, where h_n/k_n is the nth convergent to $\sqrt{2}$.)

7. Use individually

(a) the theory of simple continued fractions, and

*** (b)** the pigeon-hole principle

to demonstrate that if ξ is an irrational number, then there exist infinitely many rationals a/b satisfying

$$\left| \xi - \frac{a}{b} \right| < \frac{1}{b^2} .$$

**** 8.** **(a)** Let ξ be an irrational number and let α, β be real numbers with $0 < \alpha < \beta < 1$. Show that there are infinitely many $n \in \mathbb{N}$ such that $\alpha < \{n\xi\} < \beta$, where $\{x\} = x - \lfloor x \rfloor$ denotes the *fractional part* of a real number x. (**Remark:** This exercise states that the real numbers $\{\xi\}, \{2\xi\}, \{3\xi\}, \ldots$ constitute a dense subset of the closed interval $[0, 1]$.)

(b) Demonstrate that there exist infinitely many powers of 2 the four most significant digits in the decimal representation of each of which are 2002, i.e., there exist infinitely many $n \in \mathbb{N}$ such that we have the decimal representation $2^n = 2002\ldots$.