Exercises

(1) Let p be a prime and $a_1, \dots, a_n$ be integers. Show that if $p \mid a_1 \dots a_n$ then there is a j with $1 \le j \le n$ such that $p \mid a_j$.
(2) Find the remainder $r \in [0, 16]$ so that $2^{2023} \equiv r \mod 17$.
(3) Let p be a prime and $p \nmid a$. Show that $\{a, 2a, \dots, (p-1)a\} \mod p$ has cardinality $p - 1$.
(4) Let $\text{GCD}(m, n) = 1$ and $a \in \mathbb{N}$. Show that if $m \mid a$ and $n \mid a$ then $mn \mid a$.
(5) Solve the system of congruences

$$x \equiv 1 \mod 2, \quad x \equiv 4 \mod 5, \quad x \equiv -2 \mod 7.$$

(6) Using the following method of contradiction show that there are infinitely many primes $p \equiv -1 \mod 4$: Assume that there are only finitely many such primes $p_1, \dots, p_k$. Show that any prime factor p of $N = 4p_1 \dots p_k - 1$ is $\equiv 1 \mod 4$. Using this complete the proof.
(7) From the definition (and not using the formula) that for any prime p and natural number k we have $\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right)$. Here φ is the totient function.
(8) If there exists $e \ge 0$ so that $z^e \equiv 1 \mod n$ show that $\text{GCD}(z, n) = 1$.
(9) Show that $\sum_{d|n} \varphi(d) = n$.
(10) Let z be a primitive root mod p. Show that the order of z^e is $\frac{p-1}{\text{GCD}(e,p-1)}$.
(11) Find all elements in $\mathbb{Z}/17\mathbb{Z}^\times$ with order 4.
(12) For any $n, k \in \mathbb{N}$ show that $\varphi(n^k) = n^{k-1}\varphi(n)$.
(13) For any $n > 2$ show that $\phi(n)$ is even.
(14) Find $\left(\frac{39}{41}\right)$ and $\left(\frac{38}{43}\right)$.
(15) Find all solutions of $x^2 = -1 \mod 29$.
(16) Find all solutions of $x^2 = -1 \mod 37$.
(17) Show that $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) = 0$.
(18) Show that $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$ for any $a, b \in \mathbb{N}$.
(19) Recall the convergence $\frac{s_n}{t_n}$ of the continued fraction expansion of a real number. Show that s_n and t_n are increasing sequence.

(20) Recall the algorithm for continued fraction expansion and the quantities a_n and ρ_n. If $r = [a; a_1, a_2, \dots]$ show that $r = [a; a_1, a_2, \dots, a_{n-1}, \rho_n]$.
(21) Show that $[\bar{1}] = \frac{1+\sqrt{5}}{2}$.
(22) Find the value of $[\overline{2; 1}]$ and $[3; 5, \overline{2, 1}]$.
(23) Show that $\sqrt{n^2+1} = [n; \overline{2n}]$.
(24) Find continued fraction expansion of $\sqrt{11}$ and find the first three convergents.
(25) Let r_n be the convergence of an irrational number r. Show that $r_{2j} < r < r_{2j+1}$.
(26) Show that if a periodic continued fraction has period 0 or 1 then it must be a quadratic algebraic number.
(27) Let $d \in \mathbb{N}$ such that $\sqrt{d}$ has periodic continued fraction expansion with even period. Show that $x^2 - dy^2 = -1$ has no solution.
(28) Find all solutions to $x^1 - 17y^2 = \pm 1$ and $x^2 - 10y^2 = \pm 1$ and $x^2 - 11y^2 = \pm 1$.
(29) If $s^2 - dt^2 = s'^2 - dt'^2 = \pm 1$ for $s, s', t, t' \geq 0$ and $s + t\sqrt{d} < s' + t'\sqrt{d}$ show that $s < s'$ and $t < t'$.
(30) Write $13, 17$ as sums of two squares.
(31) Write 65 as sums of two squares in two different ways.
(32) What are the rings of integers of $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{14})$, $\mathbb{Q}(\sqrt{7}i)$.
(33) Calculate the unit groups in the rings of integers in $\mathbb{Q}(\sqrt{97}i)$ and $\mathbb{Q}(\sqrt{26})$.
(34) Let $d < 0$ and $d \equiv 2, 3 \mod 4$. Find the group of units in $\mathbb{Z}[\sqrt{d}]$.