Practice problems

1. Let $m, n \in \mathbb{N}$ with $m < n$. Show that $\mathrm{v}_p(\binom{n}{m}) \leqslant \lfloor \log_p n \rfloor$ for every prime p, i.e., if a prime power p^α divides $\binom{n}{m}$, then $p^\alpha \leqslant n$. In particular, $\binom{n}{m} = p^\alpha$ is a power of a prime only for $n = p^\alpha$ and $m = 1$ or $m = n - 1$. (**Hint:** Use $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ and the well-known formula for $\mathrm{v}_p(k!)$, $k \in \mathbb{N}$.)

2. **(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 $n \in \mathbb{N}$?

3. 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 $r := \lfloor \sqrt{p} \rfloor$. Consider the $(r+1)^2$ integers $(u + vx) \operatorname{rem} p$ with $u, v \in \{0, 1, 2, \ldots, r\}$. Observe that $(r+1)^2 > p$ and apply the pigeon-hole principle.)

(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:** If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = 1$. Let x be a square root of -1 modulo p. Now apply Part (a).)

(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:** For odd p the congruence $x^2 \equiv -2 \pmod{p}$ is solvable if and only if $p \equiv 1$ or $3 \pmod{8}$. In that case let x be a square root of -2 modulo p. Apply Part (a) and show that $a^2 + 2b^2 = 2p$ implies that a is even, so that $b^2 + 2(a/2)^2 = p$.)

(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:** If $p \equiv 1 \pmod{3}$, take x to be a square root of -3 modulo p.)

4. Let $m \in \mathbb{N}$.

(a) Let $d \in \mathbb{N}$ be a divisor of m with $d < m$. Prove that $d - \phi(d) < m - \phi(m)$. (**Hint:** Consider the complete residue systems $\{1, 2, \ldots, d\}$ and $\{1, 2, \ldots, m\}$ of d and m.)

(b) Prove the following generalization of Euler's theorem: $a^m \equiv a^{m - \phi(m)} \pmod{m}$ for any $a \in \mathbb{Z}$. (**Hint:** Use the canonical prime factorization of m, the CRT and Part (a).)

5. **(a)** Let $a, k \in \mathbb{N}$ with $a \geqslant 2$. Show that $k | \phi(a^k - 1)$. (**Hint:** $k = \operatorname{ord}_{a^k - 1} a$.)

(b) Let $m \in \mathbb{N}$. Show that if $p | \phi(m)$ and $p \nmid m$, then there is at least one prime divisor q of m such that $q \equiv 1 \pmod{p}$.

(c) Let $p \in \mathbb{P}$ be given. Show that there exist infinitely many primes q of the form $q \equiv 1 \pmod{p}$. (**Hint:** Let $q_1, \ldots, q_r$ be a collection of such primes. Take $a = pq_1 \cdots q_r$ and $k = p$ in Part (a) and then apply Part (b).)

6. 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.

(b) Every primitive root modulo p is a quadratic nonresidue modulo p.

(c) 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 $n \in \mathbb{Z}_+$.

7. **(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 $\left(\frac{2}{q}\right)$.)

8. Show that $\sum_{d|n} \delta(d)^3 = \left(\sum_{d|n} \delta(d)\right)^2$ for all $n \in \mathbb{N}$, where $\delta(m)$ denotes the number of positive divisors of $m \in \mathbb{N}$. (**Hint:** Use the multiplicative property of δ and relate the formulas for $1 + 2 + \cdots + s$ and $1^3 + 2^3 + \cdots + s^3$.)

9. For $n \in \mathbb{N}$ define $\mathcal{F}(n)$ to be the set of those integers $m \in \mathbb{N}$ such that $\phi(m) = n$. Show that for every $n \in \mathbb{N}$ we have $\sum_{m \in \mathcal{F}(n)} \mu(m) = 0$, where μ denotes the Möbius function. (**Hint:** Only those $m \in \mathcal{F}(n)$, that are square-free, contribute to the sum.)

10. Let F_n, $n \in \mathbb{N}$, denote the Fibonacci sequence. Show that every $m \in \mathbb{N}$ can be written uniquely as $m = F_{n_1} + F_{n_2} + \cdots + F_{n_r}$ with $n_1 \geqslant n_2 + 2$, $n_2 \geqslant n_3 + 2, \ldots, n_{r-1} \geqslant n_r + 2$ and $n_r \geqslant 2$.

11. Do there exist Pythagorean triples (a, b, c) and (α, β, γ) in $\mathbb{N}^3$ such that $a - \alpha = b - \beta = c - \gamma$ is a non-zero integer?

12. 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.

13. For $n, m \in \mathbb{N}$ let $\phi_n(m)$ denote the number of invertible $n \times n$ matrices over $\mathbb{Z}_m$. Note that ϕ_1 coincides with Euler's totient function ϕ.

(a) Show that for a fixed n the number-theoretic function ϕ_n is multiplicative.

(b) Show that for a prime power p^α, $\alpha \geqslant 1$, one has $\phi_n(p^\alpha) = p^{(\alpha-1)n^2}\phi_n(p)$. (**Hint:** An $n \times n$ matrix over $\mathbb{Z}_{p^\alpha}$ is invertible if and only if its canonical image over $\mathbb{Z}_p$ is invertible.)

(c) Show that $\phi_n(p) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{n^2}\left(1 - \frac{1}{p}\right) \cdots \left(1 - \frac{1}{p^n}\right)$. (**Hint:** $\phi_n(p)$ is the number of ordered bases of the n-dimensional $\mathbb{Z}_p$-vector space $\mathbb{Z}_p^n$.)

(d) Prove *Euler's formula*: $\phi_n(m) = m^{n^2} \prod_{p|m} \left(1 - \frac{1}{p}\right) \cdots \left(1 - \frac{1}{p^n}\right)$.

14. **(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 $x^3 \equiv x \pmod{10^{10}}$.

15. 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 $\sqrt{2}$.)