1. For each pair of integers (a, b), use the Euclidean algorithm to calculate their greatest common divisor $d = \gcd(a, b)$ and also to find integers x and y such that $d = ax + by$.
   (a) $a = 12$, $b = 44$.
   (b) $a = 2022$, $b = 20232$.
   (c) $a = 5567$, $b = 12445$.
   (d) $a = 233$, $b = 144$.

---

2. Decide whether each residue class has a multiplicative inverse modulo m. If so, find it, and if not, explain why not:
   (a) $\overline{10}$ modulo 25.
   (b) $\overline{11}$ modulo 25.
   (c) $\overline{12}$ modulo 25.
   (d) $\overline{30}$ modulo 42.
   (e) $\overline{31}$ modulo 42.
   (f) $\overline{32}$ modulo 42.

---

3. Find the following orders of elements modulo m:
   (a) The orders of 2 and 3 modulo 13.
   (b) The orders of 2, 4, and 8 modulo 17.
   (c) The orders of 2, 4, and 8 modulo 15.
   (d) The orders of 3, 5, and 15 modulo 16.
   (e) The order of 5 modulo 22.
   (f) The orders of 2, 4, 8, 16, and 32 modulo 55.

---

4. Calculate the following things:
   (a) The gcd and lcm of 256 and 520.
   (b) The gcd and lcm of 921 and 177.
   (c) The gcd and lcm of $2^3 3^2 5^4 7$ and $2^4 3^3 5^4 11$.
   (d) The values of $\overline{4} + \overline{6}$, $\overline{4} - \overline{6}$, and $\overline{4} \cdot \overline{6}$ modulo 8.
   (e) The inverses of $\overline{4}$, $\overline{5}$, and $\overline{6}$ modulo 71.
   (f) All units and all zero divisors modulo 14.
   (g) The solution to $5n \equiv 120 \pmod{190}$.
   (h) The solution to $6n \equiv 10 \pmod{100}$.
   (i) All n with $n \equiv 4 \pmod{19}$ and $n \equiv 3 \pmod{20}$.
   (j) All n with $n \equiv 2 \pmod{9}$ and $n \equiv 7 \pmod{14}$.
   (k) The remainder when $10!$ is divided by 11.
   (l) The remainder when 2^{47} is divided by 47.
   (m) The remainder when 6^{20} is divided by 25.
   (n) The values of $\varphi(121)$ and $\varphi(5^5 7^{10})$.
   (o) A primitive root modulo 7.
   (p) The value $0.1\overline{25}$ as a rational number.
   (q) The period of the repeating decimal of $7/11$.

---

5. Briefly justify the following statements:
   (a) The Caesar shift cipher is insecure.
   (b) Rabin encryption is provably equivalent to factorization, but is not suitable for modern use.
   (c) It is believed to be difficult to decrypt an arbitrary message encoded using RSA when the key size is large.
   (d) A zero-knowledge protocol can be used to establish knowledge of secret information without revealing useful information about it.
   (e) It is possible to establish that large integers are prime, or composite, very quickly.
   (f) There is no known procedure for factoring large integers very quickly.

---

6. Prove the following:

(a) Prove that $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$ for every positive integer n.

(b) Suppose p is a prime and a is an integer. If $p|a^2$, prove that $p|a$.

(c) Prove any two consecutive perfect squares (i.e., the integers k^2 and $(k+1)^2$) are relatively prime. [Hint: Use (b).]

(d) If u is a unit and x is a zero divisor in a commutative ring with 1, prove that ux is also a zero divisor.

(e) Show that 5 is a primitive root modulo 18.

(f) Suppose $b_1 = 3$ and $b_n = 2b_{n-1} - n + 1$ for all $n \geq 2$. Prove that $b_n = 2^n + n$ for every positive integer n.

(g) Prove that $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$ for every positive integer n.

(h) Show that 4^{240} is congruent to 16 modulo 239 and to 1 modulo 55. (Note 239 is prime.)

(i) Show that $a^4 \equiv 0$ or $1 \pmod 5$ for every integer a. Deduce that 2024 is not the sum of three fourth powers.

(j) Show that $a^3 - a$ is divisible by 6 for every integer a.

(k) Suppose $d_1 = 2$, $d_2 = 4$, and for all $n \geq 3$, $d_n = d_{n-1} + 2d_{n-2}$. Prove that $d_n = 2^n$ for every positive integer n.

(l) If a and b are positive integers, prove that $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.

(m) Prove that 3 has order 10 modulo 61.

(n) Prove that 101 is the smallest prime divisor of $99! - 1$.

(o) If p is a prime, prove that $\gcd(n, n + p) > 1$ if and only if $p|n$.