1. Define / describe / state the following things: the Euclidean algorithm, the prime factorization of an integer, a residue class modulo m, the multiplicative inverse of a unit, a zero divisor, the Chinese remainder theorem, successive squaring, the order of a unit modulo m, Fermat's little theorem, Euler's φ-function, Euler's theorem, a primitive root modulo m, repeating decimal expansions, Rabin encryption, RSA encryption, zero-knowledge proofs, the Fermat and Miller-Rabin tests, factorization algorithms.

2. 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) $a = 5567$, $b = 12445$.
   (c) $a = 2019$, $b = 20223$.
   (d) $a = 377$, $b = 233$.

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

4. 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 order of 2 modulo 55.

5. 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 number of primitive roots modulo 97.
   (q) The value $0.1\overline{25}$ as a rational number.
   (r) The period of the repeating decimal of $7/11$.

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 a positive integer. If $p|a^2$, prove that $p|a$.
   (c) 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.
   (d) Show that 3 is a primitive root modulo 7.
   (e) 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.
   (f) Prove any two consecutive perfect squares (i.e., the integers k^2 and $(k+1)^2$) are relatively prime.
   (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) If p is a prime, prove that $\gcd(n, n+p) > 1$ if and only if $p|n$.
   (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 $\gcd(a, b) = \text{lcm}(a, b)$ if and only if $a = b$.