1. (i). Define the greatest common divisor $gcd(a, b)$ of two non-zero integers $a$ and $b$.

(ii). Show that if $a$ is an odd integer and $b$ is an even integer then $gcd(a, b) = gcd(a + b, a - b)$. Show that the statement may be false if $a$ and $b$ are both odd.

2. State the Chinese Remainder Theorem, and write down all integers $x$ which satisfy the congruences $x \equiv 3 \pmod{17}$, $x \equiv 8 \pmod{13}$.

3. State the fundamental theorem of arithmetic. Using it prove that the equation $x^2 = 3$ has no solution in the rationals.

4. If $n$ is a positive integer, and $a_1, \cdots, a_{n+1}$ are $n + 1$ integers, then at least two of them are congruent to each other modulo $n$. Prove that there are $n$ integers $b_1, \cdots, b_n$ that are all incongruent modulo $n$.

5. When is a commutative ring $R$ with unit different from zero said to be an integral domain? Prove that for a prime $p$, $\mathbb{Z}_p$ is an integral domain.

6. Show that every non-zero element $x \in \mathbb{Z}_p$ has a multiplicative inverse, i.e. there is a $y \in \mathbb{Z}_p$ such that $xy = 1$.

7. Prove that if $a, b$ are integers such that $gcd(a^3, b^3) = 1$ then $gcd(a, b)$ is also 1.

8. (i) If $p_1, \cdots, p_r$ all > 3 are primes congruent to 3 modulo 4, show that $4p_1...p_r + 3$ is not divisible by any of the $p_i$, and nor by 3.

(ii) Prove that if $a, b$ are integers with $ab$ congruent to 3 modulo 4, then one of $a$ or $b$ is 3 modulo 4.

(iii) Deduce that there are infinitely many primes congruent to 3 modulo 4.
9. (i) Let \( G \) be an abelian group and let \( g, h \in G \) be elements of finite order. Let \( k \) denote the order of \( g \) and \( l \) denote the order of \( h \). Prove that if \( \gcd(k, l) = 1 \) then the order of \( gh \) is \( kl \).

(ii) Find the orders of 2 and 6 in \( \mathbb{Z}_{31}^* \). Use this and (i) to show that 12 is a primitive root modulo 31.

10. Show, by example, that there is a positive integer \( n \) such that there is no primitive root modulo \( n \).

11. Find all positive integers \( n \) such that \( |\mathbb{Z}_n^*| = 1000 \).

12. Let \( p \) and \( q \) be distinct odd primes and let \( a \) be an integer with \( \gcd(a, pq) = 1 \). Prove that if \( a \) is a quadratic residue modulo \( pq \), then the congruence \( x^2 \equiv a \pmod{pq} \) has four distinct solutions modulo \( pq \).

13. Does the polynomial \( x^2 + 10x + 1 \) have roots modulo 17? Justify your answer.

14. State Fermat’s little theorem. Using it, compute \( 3^{1199} \mod 401 \). The answer should be a number between 0 and 400. (If you use that 401 is a prime, prove it!)

15. (i) State precisely the Chinese Remainder Theorem.

(ii) Given integers \( m, n > 1 \) with \( \gcd(m, n) > 1 \), show that there always exist integers \( a, b \) such that the simultaneous congruences \( x \equiv a \pmod{m}, x \equiv b \pmod{n} \) has no solutions with \( x \in \mathbb{Z} \). (This shows that a certain hypothesis in the statement of the Chinese Remainder Theorem cannot be weakened.)

16. Show that if the order of an element \( a \) in \( \mathbb{Z}_p^* \) is odd, then it is the square of an element in \( \mathbb{Z}_p^* \).

17. State Euler’s theorem, and using it compute \( 2^{300} \mod 187 \).