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. Show that every non-zero element $x \in \mathbb{Z}_p$ for $p$ a prime has a multiplicative inverse, i.e. there is a $y \in \mathbb{Z}_p$ such that $xy = 1$. Using this show that $(p - 1)! = -1 \pmod{p}$.

6. Prove that if for $a \in \mathbb{Z}_p$, $a^n = 1 \pmod{p}$ for some integer $n$ with $(n, p - 1) = 1$, then $a$ is 1 modulo $p$.

7. (i) If $p_1, \cdots, p_r$ all $> 3$ are primes congruent to 3 modulo 4, show that $4p_1 \cdots p_r + 3$ 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.

8. Show that if $p$ is 3 modulo 4, then it remains irreducible in $\mathbb{Z}[i]$. 
9. Prove that the number of elements of order 2 in $\mathbb{Z}_{p_1 \cdots p_r}^*$ is $2^r$ where $p_i$ are distinct odd primes.

10. Does the polynomial $x^2 + 10x + 1$ have roots modulo 31? Justify your answer.