1. (i) Let $x^7 = 1 \in \mathbb{C}$. Define $\alpha_1 = x + x^2 + x^4$, $\alpha_2 = x^3 + x^5 + x^6$. Show that $\alpha_1 + \alpha_2 = 1$ and $\alpha_1 \alpha_2 = 2$. Hence evaluate $\alpha_1$ and $\alpha_2$.

(ii) Show that $x, x^2, x^4$ solve the cubic equation $X^3 - \alpha_1 X^2 + \alpha_2 X - 1 = 0$.

2. Given that $1 + 473^2 + 751^2 = 21.37511$, where 37511 is a prime, apply the method of descent to write 37511 as a sum of 4 squares. NB: Since $37511 \equiv 7 \pmod{8}$, 37511 cannot be written as a sum of three squares.

3. Suppose that $p$ is an odd prime. Use Wilson’s Theorem $(p-1)! \equiv -1 \pmod{p}$, to show that

$$1^23^25^2 \ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}}.$$ 

4. Suppose that $p \equiv 3 \pmod{4}$ and that $q = 2p + 1$ is also prime. (For example, take $p = 29$, $q = 59$ or $p = 113$, $q = 227$)

(i) Show that 2 is a square $x^2 \pmod{q}$ and hence $2^p \equiv x^{2p} \pmod{q}$.

(ii) Hence show that $2^p - 1 \equiv 0 \pmod{q}$ and so $2^p - 1$ is not a prime. So $2^{29} - 1$ and $2^{113} - 1$ are not primes.

5. (i) Give an example of a number $\equiv \pm 1 \pmod{5}$ which is not divisible by a prime $\equiv \pm 1 \pmod{5}$.

(ii) Show that a number of the form $5n \pm 2$ cannot be a product only of primes $\equiv \pm 1 \pmod{5}$. Hence show that there are infinitely many primes of the form $5n \pm 2$. Hint: If $p_1p_2 \ldots p_n$ are primes greater than 5 and $\equiv \pm 2 \pmod{5}$, consider $N = 5p_1p_2 \ldots p_n + 2$.

6. Use $x^2 + 4 = ((x + 1)^2 + 1)((x - 1)^2 + 1)$, to show that $-4$ is a fourth power modulo $p > 3$ if and only if $p \equiv 1 \pmod{4}$.

7. (i) Show that if $p$ is an odd prime divisor of a number $N = x^4 - x^2 + 1$, then $x^6 + 1 \equiv 0 \pmod{p}$ and so $p \equiv 1 \pmod{12}$.

(ii) Hence show that there are infinitely many primes $p \equiv 1 \pmod{12}$. 