Question 4 (Unit 4) – 15 marks

(i) Use Wilson's Theorem and its converse to prove that for any positive integer k, the integer $6k+1$ is prime if and only if $(6k-3)! + k \equiv 0 \pmod{6k+1}$. [5]

(ii) This part of the question is concerned with a generalization of Wilson's Theorem to cover a composite modulus. If $n > 4$ is composite, then the product $1 \times 2 \times 3 \times \ldots \times (n-1)$ will always be congruent modulo n to 0. However, suppose that we restrict the numbers in this product to those which are relatively prime to n. For instance, for $n = 10$, of the numbers in $\{1, 2, \ldots, 9\}$, those relatively prime to 10 are 1, 3, 7 and 9. Notice that

$$1 \times 3 \times 7 \times 9 \equiv -1 \pmod{10}.$$

Similarly, for $n = 20$, the numbers in $\{1, 2, 3, \ldots, 19\}$ which are relatively prime to 20 are 1, 3, 7, 9, 11, 13, 17 and 19, and it turns out that

$$1 \times 3 \times 7 \times 9 \times 11 \times 13 \times 17 \times 19 \equiv 1 \pmod{20}.$$

If you care to investigate other composite values of n, you will find that the resulting value is always either 1 or -1. In part (b) of this question you are asked to prove that this is generally true. The result of part (a) should help you along the way.

(a) Let $n > 2$ be an integer, and let a be an integer with $1 \leq a \leq n-1$ which is a solution of the equation $x^2 \equiv 1 \pmod{n}$. Show that $\gcd(a, n) = 1$, and hence that there is a unique b with $1 \leq b \leq n-1$ such that $ab \equiv -1 \pmod{n}$. Show, further, that $b^2 \equiv 1 \pmod{n}$, and that b does not equal a. [4]

(b) Prove that for any integer $n > 2$, the product of those numbers in $\{1, 2, 3, \ldots, n-1\}$ which are relatively prime to n is congruent modulo n to either 1 or -1. [6]

[Hints: In your proof for (b) you should follow the strategy of the proof of Wilson's Theorem given in *Unit 4*. You should start by pairing numbers whose product is congruent to 1 modulo n. For example, in the above expression for the case $n = 20$, the unique solution of $3x \equiv 1 \pmod{20}$ is 7, and so $3 \times 7 \equiv 1 \pmod{20}$. Similarly, $13 \times 17 \equiv 1 \pmod{20}$. Note that all the remaining numbers in the product for this case satisfy $x^2 \equiv 1 \pmod{20}$, and in fact $1 \times 19 \equiv 9 \times 11 \equiv -1 \pmod{20}$.]

$1 < a \leq n-1 \Rightarrow -1 \geq -a \geq -n+1 \Rightarrow n-1 \geq n-a \geq 1$

$b \equiv -a \bmod n \Rightarrow b = kn - a$

But $1 \leq b \leq n-1 \Rightarrow 1 \leq kn - a \leq n-1$

$-n+1 \leq (k-1)n - a \leq -1$

$n-1 \geq a - (k-1)n \geq 1$

Which is only consistent with $n-1 \geq a \geq 1$ if $k = 1$

$\therefore b = n - a$ and b is unique

$b = n - a$