MAT1026: SOLUTIONS UN-ASSESSED COURSEWORK 3

Question 1: Assume $a \geq 2$ is odd, then $a^m + 1$ is even for every natural number m and therefore it cannot be a prime.

Question 2: Use the theory of congruences to show that the polynomials given below have no integer roots:
(a) $x^3 + x^2 - x + 3$;
(b) $x^3 - x^2 - x + 11$.

Solution for (a) : We work modulus five. Then any integer $a = 5q + r$, where $r = 0, \pm 1, \pm 2$. Thus we have (the simbol $\not\equiv$ means not congruent):

$$f(0) = 3 \not\equiv 0 \pmod{5};$$

$$f(1) = 4 \not\equiv 0 \pmod{5};$$

$$f(2) = 13 \not\equiv 0 \pmod{5};$$

$$f(-1) = 4 \not\equiv 0 \pmod{5};$$

$$f(-2) = 1 \not\equiv 0 \pmod{5}.$$

Hence the polynomial (a) has no integer roots.
Solution for (b) : Here we work modulus three. Then any integer $a = 3q + r$, where $r = 0, 1, 2$. Thus we have:

$$f(0) = 11 \not\equiv 0 \pmod{3};$$

$$f(1) = 10 \not\equiv 0 \pmod{3};$$

$$f(2) = 13 \not\equiv 0 \pmod{3}.$$

Hence the polynomial (b) has no integer roots.

Question 3: Where it exists, find the general solution of the linear congruences (give detailed reasons for your answers):

a) $10x \equiv 6 \pmod{14}$;

b) $7x \equiv 2 \pmod{9}$;

c) $9x \equiv 7 \pmod{6}$.

Solution for a): By denoting by $g(a,b)$ the *greatest common factor* of the integers (a,b) we have, $g(10,14) = 2$, which divides 6 and so the congruence is solvable. We know that if x_0 is any particular solution, then the general solution is $x = x_0 + (14/2)t = x_0 + 7t$, with t any integer. By inspection we can see that $x_0 = 2$ is a particular solution and therefore we have $x = 2 + 7t$.

Solution for b): Here we have $g(7,9) = 1$, which divides 2 and so the congruence is solvable. We know that if x_0 is any particular solution, then the general solution is $x = x_0 + (9/1)t = x_0 + 9t$, with t any integer. By inspection we can see that $x_0 = 8$ is a particular solution and therefore we have $x = 8 + 9t$.

Solution for c): Here we have $g(9,6) = 3$, which does not divide 7 and so the congruence is not solvable.

Question 4: By using Fermat's Little Theorem:
(a) Show that 6 is the least non-negative residue of $2^{68} \pmod{19}$, that is, show that $2^{68} \equiv 6 \pmod{19}$.
(b) Find the least non-negative residue of $3^{91} \pmod{23}$.

Solution for (a) : Since 19 is prime and since 2 is not divisible by 19 we can apply Fermat's Little Theorem. So $2^{18} \equiv 1 \pmod{19}$. Now $68 = 18 \cdot 3 + 14$ and so

$$2^{68} = (2^{18})^3 \cdot 2^{14} \equiv 1^3 \cdot 2^{14} \equiv 2^{14} \pmod{19}.$$

Also we have

$$2^{14} = (2^4)^3 \cdot 2^2 \equiv (-3)^3 \cdot 2^2 \equiv -27 \cdot 4 \equiv -8 \cdot 4 \equiv -32 \equiv 6 \pmod{19}.$$

Hence $2^{68} \equiv 6 \pmod{19}$.

Solution for (b) : Similarly to (a) we have: $3^{22} \equiv 1 \pmod{23}$. Therefore $3^{88} \equiv 1 \pmod{23}$. Hence $3^{91} = 3^3 \cdot 3^{88} \equiv 27 \cdot 1 = 27 \equiv 4 \pmod{23}$.