MATH 150 - WRITTEN HOMEWORK # 8

DUE THURSDAY, APRIL 11, 2024 AT 11:59 P.M.

Show your work clearly for each problem so that it can be understood how you arrived at your answer.

(1) *(10 points)*

(a) Find an inverse of 19 modulo 141 in $\mathbb{Z}_{141}$.

(b) Solve the linear congruence $19x \equiv 9 \pmod{141}$. Your answer must be in $\mathbb{Z}_{141}$.

Solution:

(a) We first use the Euclidean algorithm to verify that the gcd$(19, 141) = 1$.

$$\begin{aligned} 141 &= 19(7) + 8 \\ 19 &= 8(2) + 3 \\ 8 &= 3(2) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0. \end{aligned}$$

Thus, gcd$(19, 141) = 1$, so inverse of 19 modulo 141 exists. To find the inverse, we work backwards to compute the Bezout coefficients. From the Euclidean algorithm, we have

$$\begin{aligned} 8 &= 141 - 19(7) \\ 3 &= 19 - 8(2) \\ 2 &= 8 - 3(2) \\ 1 &= 3 - 2(1) = 3 - (8 - 3(2))(1) \\ &= 3(3) - 8 = (19 - 8(2))(3) - 8 \\ &= 19(3) - 8(7) = 19(3) - (141 - 19(7))(7) = 19(52) - 141(7). \end{aligned}$$

Therefore, $19 \cdot 52 \equiv 1 \pmod{141}$, and the inverse of 19 modulo 141 is 52.

(b) Using part (a), we have

$$\begin{aligned} 19 \cdot 52 &\equiv 1 \pmod{141} \\ x &\equiv 52 \cdot 9 \pmod{141} \\ x &\equiv 468 \equiv 45 \pmod{141}. \end{aligned}$$

Hence, the solution x for the given linear congruence in $\mathbb{Z}_{141}$ is 45.

(2) *(10 points)* Use the Chinese Remainder Theorem to find all integer solutions x to the following system of congruences:

$$x - 4 \equiv 1 \pmod{5}$$
$$3x + 2 \equiv 3 \pmod{7}$$
$$5x \equiv 1 \pmod{9}.$$

Solution: Observe that all moduli are relatively prime and thus, we will be able to find a unique solution modulo $m = m_1 m_2 m_3 = 5 \cdot 7 \cdot 9 = 315$. We then isolate x on the left-hand side of the first two congruences to get:

$$x \equiv 0 \pmod{5}$$
$$3x \equiv 1 \pmod{7}$$
$$5x \equiv 1 \pmod{9}.$$

Now we find the inverse of 3 modulo 7 and 5 modulo 9 to further isolate x in the second and third congruences, respectively. Note that the inverse of 3 modulo 7 is 5 since $15 \equiv 1 \pmod{7}$ and the inverse of 5 modulo 9 is 2 since $10 \equiv 1 \pmod{9}$. Thus, we obtain the following system of congruences:

$$x \equiv 0 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$
$$x \equiv 2 \pmod{9}.$$

The solution is $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$, where $a_1 = 0$, $a_2 = 5$, $a_3 = 2$. Thus,

$$x = 5M_2 y_2 + 2M_3 y_3,$$

where $M_2 = 315/7 = 45$, $M_3 = 315/9 = 35$, and y_k is an inverse of M_k modulo m_k for $k = 2, 3$.

Need to find y_2, an inverse of 45 modulo 7, which is equivalent to 3 modulo 7. Thus, $y_2 = 3$ as seen above.

Need to find y_3, an inverse of 35 modulo 9, which is equivalent to -1 modulo 9. Thus, y_3 must satisfy the congruence: $-y_3 \equiv 1 \pmod{9}$. Note that $y_3 = -1$ works, since $1 \equiv 1 \pmod{9}$.

Hence, the solution is

$$x = 5 \cdot 45 \cdot 5 + 2 \cdot 35 \cdot (-1) = 1125 - 70 = 1055.$$

Since $m = 315$, the unique solution in $\mathbb{Z}_{315}$ is: $1055 - 3(315) = 110$. Hence, all integer solutions are given by: $x = 110 + 315k$; $k \in \mathbb{Z}$.

(3) *(10 points)*

(a) Compute 3^{7941} **mod** 7.

(b) Compute 6^{17} **mod** 20.

Solution:

(a) By Fermat's Little Theorem, $3^6 \equiv 1 \pmod 7$. We compute $7941 = 6(1323) + 3$. Thus,
$$3^{7941} = 3^{6(1323)+3} \equiv 1^{1323}\, 3^3 \pmod 7.$$
Now we can conclude the computation by simply calculating $3^3 = 27$ and 27 **mod** 7 = 6.

(b) This is done by repeated squaring. Observe that $17 = 2^4 + 1$. We then compute
$$6^2 = 36 \equiv 16 \pmod{20}$$
$$6^4 \equiv 16^2 \equiv (-4)^2 \equiv 16 \pmod{20}.$$
This is already enough information to observe that 6 raised to any power of 2 will be congruent to 16 mod 20. So
$$6^{17} = 6^{16}\, 6 \equiv (16)(6) \equiv 96 \equiv 16 \pmod{20}.$$

(4) *(10 points)* Find all integers x satisfying
$$4x^2 + 4x - 3 \equiv 0 \pmod{11}.$$
Solution: Factoring the quadratic equation, we have
$$(2x-1)(2x+3) \equiv 0 \pmod{11}.$$
Now we recall the fact that if p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i. Therefore, we have
$$2x - 1 \equiv 0 \pmod{11}, \quad \text{or} \quad 2x + 3 \equiv 0 \pmod{11}$$
$$2x \equiv 1 \pmod{11}, \quad \text{or} \quad 2x \equiv -3 \equiv 8 \pmod{11}.$$
Note that the inverse of 2 modulo 11 is 6 since $12 \equiv 1 \pmod{11}$. Thus,
$$x \equiv 6 \pmod{11}, \quad \text{or} \quad x \equiv 48 \equiv 4 \pmod{11}.$$
Hence, all integer solutions x are:
$$x = 11k + 6, \quad \text{or} \quad x = 11k + 4,$$
for $k \in \mathbb{Z}$.