MATH 2170-19W Problem Set 5

March 8, 2019

Solutions

[2] **Question 1.** Find all solutions to

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 7 \pmod{12} \\ x \equiv 43 \pmod{60} \end{cases}$$

Hint: This question is worth only 2 marks.

One mark is for the correct answer, the other mark is for the insight that this problem does not require any work.

Solution: Notice first that $3|12$ and $12|60$. Furthermore $43 \equiv 7 \pmod{12}$ and $43 \equiv 1 \pmod{3}$.

So the unique solution to this system is $x \equiv 43 \pmod{60}$.

[5] **Question 2.** Find all solutions to $x^3 + x^2 + 3x + 1 \equiv 0 \pmod{21}$.

[Arithmetic help: $1^3 \equiv 2^3 \equiv 4^3 \equiv 1 \pmod{7}$ and $3^3 \equiv 5^3 \equiv 6^3 \equiv -1 \pmod{7}$.]

Remark: Not only was there a typo is the "Help" line (5 instead of 6) which mostly didn't matter; there was a bigger error of some sort in the coefficients of the polynomial. The intended solution had 3 solutions $\pmod{21}$ coming from the unique solution of $x \equiv 1 \pmod{3}$ and the three solutions $x \equiv 1, 2, 4 \pmod{7}$. Somewhere along the line, something got transcribed incorrectly.

Solution: Set $p(x) = x^3 + x^2 + 3x + 1$. We check for solutions modulo 7 and calculate:

x	x^3	x^2	$3x$	$p(x)$
0	0	0	0	1
1	1	1	3	6
2	1	4	6	5
3	-1	2	2	4
4	1	2	5	2
5	-1	4	1	5
6	-1	1	4	3

Since there are no solution modulo 7, there are no solutions modulo 21.

Question 3.

[2] (a) Calculate $\phi(210,000)$.

Solution: $210,000 = 21 \times 10^4 = 3 \times 7 \times 2^4 \times 5^4$.

So $\phi(210000) = 2 \times 6 \times 2^3 \times (5^4 - 5^3) = 96 \times 125 \times 4 = 48,000$.

[3] (b) Find the prime power factorization of $\phi(12!)$.

Solution: $12! = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 11^1 7^1 5^2 3^5 2^{10}$.

$\phi(11) = 10 = 2 \cdot 5$, $\phi(7) = 6 = 2 \cdot 3$, $\phi(25) = 25 - 5 = 20 = 2^2 5$, $\phi(3^5) = 3^5 - 3^4 = 3^4 2$, and $\phi(2^{10}) = 2^9$.

Since ϕ is multiplicative, the prime power factorization of $\phi(12!)$ is $2^{14} 3^5 5^2$.

[3] **Question 4.** Prove that if n has k distinct odd prime factors, then $2^k \mid \phi(n)$.

Proof: $\phi(n) = \prod_{p|n} \left(p^{\alpha_p} - p^{\alpha_p - 1}\right)$, where α_p is the exponent of p in the prime power factorization of n.

But $p^{\alpha_p} - p^{\alpha_p - 1} = p^{\alpha_p - 1}(p-1)$, and since p is odd, $2|(p-1)$. There are k such prime factors, so $2^k \mid \phi(n)$. ∎

[5] **Question 5.** Suppose that $b \equiv a^{53} \pmod{91}$ and that $(a, 91) = 1$. Find a positive number $\overline{k}$ such that $b^{\overline{k}} \equiv a \pmod{91}$. If $b = 67$, what is a?.

Solution: $91 = 7 \times 13$, so $\phi(91) = 6 \times 12 = 72 = 9 \times 8$. We need to solve $1 \equiv 53\overline{k} \pmod{72}$, so since 9 and 8 are relatively prime, we have a fairly easy task: Modulo 9, $1 \equiv 53\overline{k} \equiv -1\overline{k} \pmod{9}$ so $\overline{k} \equiv -1 \pmod{9}$. Thus $\overline{k} = 9t - 1$ for some t, and modulo 8, $1 \equiv 53(9t-1) \equiv 5(t-1) \equiv 5t - 5 \pmod{8}$, so $5t \equiv 6 \pmod{8}$, so $t \equiv 6 \pmod{8}$.

Therefore $t = 8s + 6$ and $\overline{k} = 9(8s+6) - 1 = 72s + 53$. So we can take $\overline{k} = 53$.

Hence $a \equiv b^{53} \pmod{91}$ and so we calculate:

$$b^2 \equiv 30;\ b^4 \equiv 81;\ b^8 \equiv 9;\ b^{16} \equiv 81;\ b^{32} \equiv 9 \pmod{91}$$

and $53 = 32 + 16 + 4 + 1$ so

$$b^{53} \equiv b^{32} b^{16} b^4 b \equiv 9 \cdot 81 \cdot 81 \cdot 67 \equiv 58 \pmod{91}$$

Remark: Any sort of explanation of where "58" came from was acceptable, but I did want to see something. I also accepted using the Euclidean algorithm and $(53, 72) = 1$ to find the multiplicative inverse of 53 modulo 72, although that is not nearly so efficient.