[Number Theory] HW 6

Connor Li, csl2192

March 24, 2025

Problem 1

If $x \equiv a \bmod n$, then we can express x as follows for some $c \in \mathbb{Z}$.

$$x = nc + a$$

We also know that c must either be even or odd. Consider the first case, where c is even and we can express $c = 2k$ for some $k \in \mathbb{Z}$. Substituting this into the expression above, we get $x = 2nk + a$, which implies that $x \equiv a \bmod 2n$ since $a < n < 2n$.

Now, consider the case where c is odd. We can express $c = 2m + 1$ for some $m \in \mathbb{Z}$. Substituting this into the expression above, we get $x = n(2m+1) + a = 2nm + (n+a)$. Since $a < n \implies a + n < 2n$, then we know that $x \equiv a + n \bmod 2n$.

Thus, we have shown for any $x \in \mathbb{Z}$, if $x \equiv a \bmod n$, then $x \equiv a \bmod 2n$ or $x \equiv a + n \bmod 2n$.

Problem 2

We have the following expression, $5^{45} \bmod 11$. Using Fermat's Little Theorem, we have that $5^{10} \bmod 11 \equiv 1 \bmod 11$.

$$\begin{aligned} 5^{45} \bmod 11 &\equiv 5^5 \cdot \left(5^{10} \bmod 11\right)^4 \bmod 11 \\ &\equiv 5^5 \bmod 11 \\ &\equiv (5^2 \bmod 11)^2 \cdot (5 \bmod 11) \bmod 11 \\ &\equiv 9 \cdot 5 \bmod 11 \\ &\equiv 1 \bmod 11 \end{aligned}$$

This means that $5^{45} \bmod 11 \equiv 1 \bmod 11 \in [1]_{11}$.

Problem 3

Our goal is to prove that if $\gcd(a, 35) = 1$, then $a^{12} \equiv 1 \bmod 35$. To begin, let's use Fermat's Little Theorem on each prime factor of 35, which states that if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \bmod p$.

Consider the prime factor 5 first. Using the theorem, we have the following.

$$a^4 \equiv 1 \bmod 5 \implies a^{12} \equiv 1 \bmod 5$$

Now, consider the prime factor 7. Using the theorem, we have the following.

$$a^6 \equiv 1 \bmod 7 \implies a^{12} \equiv 1 \bmod 7$$

Using the Chinese Remainder Theorem and the fact that 5 and 7 are coprime, we can combine the two congruences above to get the following.

$$a^1 2 \equiv 1 \bmod \operatorname{lcm}(5, 7) \implies a^{12} \equiv 1 \bmod 35$$

Thus, we have shown the original claim, if $\gcd(a, 35) = 1$, then $a^{12} \equiv 1 \bmod 35$.

Problem 4

If $7 \nmid a$, then we can express $a = 7c + b$ for some $c \in \mathbb{Z}$ and for some $b \in [1, 2, 3, 4, 5, 6]$. Using the binomial expansion, we can expand the term of interest a^3 as follows.

$$\begin{aligned}(7c + b)^3 &= (7c)^3 + (7c)^2 b + (7c)b^2 + b^3 \\ &= 7 \cdot (\quad \cdots \quad) + b^3\end{aligned}$$

This means that the terms $a^3 + 1$ and $a^3 - 1$ are only divisible by 7 if $b^3 + 1$ and $b^3 - 1$, respectfully, are divisible by 7. Using the table below, for every value of b, I will show that one of $b^3 + 1, b^3 - 1$ is divisible by 7.

b	$b^3 + 1$	$b^3 - 1$
1	$\cancel{2}$	0
2	$\cancel{9}$	7
3	28	$\cancel{26}$
4	$\cancel{65}$	63
5	126	$\cancel{124}$
6	217	$\cancel{215}$

Thus, we have shown for any $c \in \mathbb{Z}$ and $b \in [1, 2, 3, 4, 5, 6]$, we have that $7 \mid (7c + b)^3 + 1$ or $7 \mid (7c + b)^3 - 1$. Finally, we can conclude that if $7 \nmid a$, then $7 \mid a^3 + 1$ or $7 \mid a^3 - 1$.

Problem 5

To show that the units digit of a and a^5 are the same, let's first prove a theorem.

Theorem: For any integer a with a units digit a_0, we have that $a^5 \bmod 10 \equiv (a_0)^5 \bmod 10$.

Proof: Consider any integer a. We can represent a in terms of its digits as follows where a_0 is the units place and a is "n digits long".

$$a = \sum_{i=0}^{n} a_i \cdot 10^i$$

Now, consider the term a^5.

$$\begin{aligned} a^5 &= \left(\sum_{i=0}^{n} a_i \cdot 10^i\right)^5 \\ &= (a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_1 \cdot 10 + a_0)^5 \\ &= 10 \cdot (\quad \cdots \quad) + (a_0)^5 \end{aligned}$$

This implies that $a^5 \bmod 10 \equiv (a_0)^5 \bmod 10$.

Now, let's use this theorem to prove the original claim. Since the units digit of a^5 is $a^5 \bmod 10 \equiv (a_0)^5 \bmod 10$, we can show that, for every choice of a_0, we have $a_0 \equiv (a_0)^5 \bmod 10$.

a_0	$(a_0)^5$	$(a_0)^5 \bmod 10$
0	0	0
1	1	1
2	32	2
3	243	3
4	1024	4
5	3125	5
6	7776	6
7	16807	7
8	32768	8
9	59049	9

The above table concludes our proof that the units digit of a and a^5 are the same for any choice of $a \in \mathbb{Z}$.

Problem 6

Using Wilson's Theorem, we have that $(p-1)! \equiv -1 \bmod p$ if and only if p is prime. We can use this theorem to show that 17 is prime by showing that $16! \equiv -1 \bmod 17$.

Instead of expanding 16!, let's consider the product using modular inverses in $\mathbb{Z}_{17}$.

$$\begin{aligned}
16! \bmod 17 &\equiv (1) \cdot \overbrace{(2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14)}^{\text{Paired Inverses in } \mathbb{Z}_{17}} \cdot (16) \bmod 17 \\
&= (1) \cdot (16) \bmod 17 \\
&= -1 \bmod 17
\end{aligned}$$

Thus, since we have shown that $16! \equiv -1 \bmod 17$, we can conclude that 17 is prime by Wilson's Theorem.

Problem 7

In order to find the unique solutions to $x^2 \equiv 1 \bmod 35$, we can use the Chinese Remainder Theorem and first find the solutions to $x^2 \equiv 1 \bmod 5$ and $x^2 \equiv 1 \bmod 7$.

Consider the equation $x^2 \equiv 1 \bmod 5$. Let's find the solutions exhaustively.

x	$x^2 \bmod 5$
0	0
1	1
2	4
3	4
4	1

Thus, the solutions to $x^2 \equiv 1 \bmod 5$ are $x \in [1, 4]_5$.

Similarly, consider the equation $x^2 \equiv 1 \bmod 7$.

x	$x^2 \bmod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Thus, the solutions to $x^2 \equiv 1 \bmod 7$ are $x \in [1, 6]_7$.

By the Chinese Remainder Theorem, since 5 and 7 are corpime, then every pair $(a \bmod 5, b \bmod 7)$ corresponds to exactly one solution $x \bmod 35$. This guarantees exactly 4 unique solutions, listed out in tabular form.

$a \bmod 5$	$b \bmod 7$	$x \bmod 35$
1	1	1
1	6	6
4	1	29
4	6	34

Finally, we can conclude that there are 4 solutions to $x^2 \equiv 1 \bmod 35$ in the form of $\pm 1, \pm 6 \bmod 35$.