Homework 9

CMPSC 360

Kinner Parikh

April 1, 2022

Question 1: Show that if x is an odd integer, then x^2 has the form $8k+1$, for some $k \in \mathbb{Z}$

Proof:
Assume that x is an odd integer.
By definition of odd, $x = 2t+1$ where $t \in \mathbb{Z}$.
This also means that $x = 4t+1$ and $x = 4t+3$.
Case 1: $(x = 4t+1)$

$$\begin{aligned} x^2 &= (4t+1)^2 \\ &= 16t^2 + 8t + 1 \\ &= 8(2t^2 + t) + 1 \\ &= 8k + 1 \text{ such that } k \in \mathbb{Z} \text{ where } k = 2t^2 + t \end{aligned}$$

So we know when $x = 4t+1$, that x^2 has the form $8k+1$
Case 2: $(x = 4t+3)$

$$\begin{aligned} x^2 &= (4t+3)^2 \\ &= 16t^2 + 24t + 9 \\ &= 16t^2 + 24t + 8 + 1 \\ &= 8(2t^2 + 3t + 1) + 1 \\ &= 8k + 1 \text{ such that } k \in \mathbb{Z} \text{ where } k = 2t^2 + 3t + 1 \end{aligned}$$

So we know when $x = 4t+3$, that x^2 has the form $8k+1$
Both cases hold true. Therefore, when x is an odd integer, then x^2 has the form $8k+1$. $\square$

Question 2: Solve for $23^3 \pmod{30}$

$$\begin{aligned} 23^3 \pmod{30} &= 23^{1+2} \pmod{30} \\ &= ((23^1 \bmod 30)(23^2 \bmod 30)) \bmod 30 \\ &= (23 \cdot 19) \bmod 30 \\ &= 437 \bmod 30 \\ &= 17 \end{aligned}$$

Question 3: Show that if an integer n is not divisible by 3, then $n^2 - 1$ is always divisible by 3. Similarly, show that if an integer n is not divisible by 3, then $n^2 - 1 \equiv 0$

Proof:
Assume that $3 \nmid n$ such that $n \in \mathbb{Z}$
We need to prove that $3 \mid (n^2 - 1)$ and $n^2 - 1 \equiv 0$, which means $n^2 = 1 (\text{mod } 3)$
This means that $n = 3x + 1$ or $n = 3x + 2$ such that $x \in \mathbb{Z}$
Case 1: $(n = 3x + 1)$

$$\begin{aligned} n^2 - 1 &= (3x+1)^2 - 1 \\ &= 9x^2 + 6x + 1 - 1 \\ &= 9x^2 + 6x \\ &= 3(3x^2 + 2x) \\ &= 3t \text{ where } t \in \mathbb{Z} \text{ and } t = 3x^2 + 2x \end{aligned}$$

By definition of divides, when $n = 3x + 1$, then $3 \mid (n^2 + 1)$.
Case 2: $(n = 3x + 2)$

$$\begin{aligned} n^2 - 1 &= (3x+2)^2 - 1 \\ &= 9x^2 + 12x + 4 - 1 \\ &= 9x^2 + 12x + 3 \\ &= 3(3x^2 + 4x + 1) \\ &= 3t \text{ where } t \in \mathbb{Z} \text{ and } t = 3x^2 + 4x + 1 \end{aligned}$$

By definition of divides, when $n = 3x + 2$, then $3 \mid (n^2 + 1)$.
Since both cases hold, we know that if $3 \nmid n$ such that $n \in \mathbb{Z}$, then $3 \mid (n^2 - 1)$. $\square$

Question 4: Find GCD of 2947 and 3997 using Euclidean Theorem.

$$\begin{aligned} 3997 &= 2947(1) + 1050 \\ 2947 &= 1050(2) + 847 \\ 1050 &= 847(1) \quad + 203 \\ 847 &= 203(4) \quad + 35 \\ 203 &= 35(5) \quad + 28 \\ 35 &= 28(1) \quad + 7 \\ 28 &= 7(4) \quad + 0 \end{aligned}$$

So, $gcd(2947, 3997) = 7$

Question 5: Express $gcd(128469, 12818)$ as a linear combination of 128469 and 12818 using extended Euclid algorithm.

Applying Euclid's algorithm:

i	r_i	r_{i+1}	q_{i+1}	r_{i+2}	s_i	t_i
0	128469	12818	10	289	1	0
1	12818	289	44	102	0	1
2	289	102	2	85	1	-10
3	102	85	1	17	-44	441
4	85	17	5	0	89	-892
5					-133	1333

$gcd(128469, 12818) = (-133)(128469) + (1333)(12818)$

Question 6: Prove that if $a \mid bc$ with $gcd(a, b) = 1$, then $a \mid c$

Proof:
Assume that $a \mid bc$ and $gcd(a, b) = 1$
By definition of divides, we know that $bc = at$ where $t \in \mathbb{Z}$
Dividing both sides by b, we get $c = \frac{at}{b}$
Since we know that $gcd(a, b) = 1$, it must mean that $t \mid b$.
Therefore, we can say that $\frac{t}{b} \in \mathbb{Z}$
This means that $c = ax$ where $x = \frac{t}{b}$
Thus, by the definition of divides, we can say that $a \mid c$. $\square$

Question 7: Prove that $gcd(a^2, b^2) = gcd(a, b)^2$ using Bezout's identity.

Proof:
Bezout's identity states that $gcd(a, b) = as + bt = x$ for some $s, t, x \in \mathbb{Z}$.
Considering x:

$$\begin{aligned}
x^3 &= (as + bt)^3 \\
&= (as)^3 + 3\,(as)^2\,bt + 3as\,(bt)^2 + (bt)^3 \\
&= a^2(as^3 + 3s^2bt) + b^2(3ast^2 + bt^3) \\
x^2 &= a^2\left(\frac{as^3 + 3s^2bt}{x}\right) + b^2\left(\frac{3ast^2 + bt^3}{x}\right) \text{[divide by } x\text{]} \\
&= a^2\left(\frac{a}{x} \cdot s^3 + 3s^2 \cdot \frac{b}{x} \cdot t\right) + b^2\left(\frac{3a}{x} \cdot st^2 + \frac{b}{x} \cdot t^3\right)
\end{aligned}$$

By definition of $gcd(a, b) = x$, we know that $x \mid a$ and $x \mid b$.
So we know that $\frac{a}{x}, \frac{b}{x} \in \mathbb{Z}$
Let $\frac{a}{x}, \frac{b}{x} = y_0, y_1$ respectively, where $y_0, y_1 \in \mathbb{Z}$
Rewriting the equation, we can say that

$$\begin{aligned}
x^2 &= a^2\left(y_0 s^3 + 3s^2 y_1 t\right) + b^2\left(3y_0 st^2 + y_1 t^3\right) \\
&= a^2 \cdot n + b^2 \cdot m \text{ for some } n, m \in \mathbb{Z} \text{ such that } n = y_0 s^3 + 3s^2 y_1 t, m = 3y_0 st^2 + y_1 t^3
\end{aligned}$$

By definition of gcd, we know that $gcd(a^2, b^2) = a^2 s_0 + b^2 t_0$ for some $s_0, t_0 \in \mathbb{Z}$
So we can see that x^2 follows the form of $gcd(a^2, b^2)$
This means that $a^2 s_0 + b^2 t_0 = a^2 n + b^2 m$
And by substitution, we know that $gcd(a^2, b^2) = gcd(a, b)^2$
Therefore, we can conclude that $gcd(a^2, b^2) = gcd(a, b)^2$. $\square$

Question 8: For Z_{11}, find out:

a) $3 \oplus 7$
   $(3+7) \bmod 11 = 10 \bmod 11 = 10$
b) $3 \otimes 7$
   $(3 \cdot 7) \bmod 11 = 21 \bmod 11 = 10$
c) $10 \ominus 7$
   $(10-7) \bmod 11 = 3 \bmod 11 = 3$
d) $10 \oslash 7$
   $10 \otimes 7^{-1} = 10 \otimes 8 = (10 \cdot 8) \bmod 11 = 80 \bmod 11 = 3$
   By definition, $7 \cdot x \bmod 11 = 1$ where $x = 7^{-1}$. So $7^{-1} = 8$

Question 9: Determine whether every element a of $\mathbb{Z}_n$ has an inverse for $n = 5, 6$ and $7, 11$

By definition of an inverse, a number $a \in \mathbb{Z}_n$ has an inverse when a and n are coprimes. This means that a is invertible when $gcd(a,n) = 1$. In the case of $n = 5, 7, 11$, since they are all primes, all $a \in \mathbb{Z}_n$ will be coprime with n. However, for the case of $n = 6$, not every element will have an inverse because 2 and 3 are not coprime with 6.

Question 10: Write the following decimal string 334_{10} to senary (base 6) showing work

$$\begin{aligned} 334 \div 6 &= 55 \;\; R\ 4 \\ 55 \div 6 &= 9 \quad R\ 1 \\ 9 \div 6 &= 1 \quad R\ 3 \\ 1 \div 6 &= 0 \quad R\ 1 \end{aligned}$$

So $334_{10} = 1314_6$.

Question 11: Find the GCD of 846 and 265.

1) $846 = (q_1 = 3) * 265 + (r_1 = 51)$
2) $265 = (q_2 = 5) * r_1 + (r_2 = 10)$
3) $r_1 = (q_3 = 5) * r_2 + (r_3 = 1)$
4) $r_2 = (q_4 = 10) * r_3 + 0$
r_3 is our gcd.
GCD(846, 265) = 1
We have to find the Bezout coefficients a,b such that a*846 + b*265 = GCD(846, 265). For doing this we start backward substitution. So we can write the above steps as:
1) $r_1 = 846 - q_1 * 265$
2) $r_2 = 265 - q_2 * r_1$
3) $r_3 = r_1 - q_3 * r_2$
We start from 3 as r_3 is our gcd and keep on substituting the values of r_1, r_2 and r_3 as above.
$r_3 = r_1 - q_3 * r_2$
$= 846 - q_1 * 265 - [5 * (265 - q_2 * r_1)]$
$= 846 - 3 * 265 - [5 * 265 - 25 * (846 - q_1 * 265)]$
$= 846 - 3 * 265 - [5 * 265 - 25 * (846 - 3 * 265)]$
$= 846 - 3 * 265 - (5 * 265 - 25 * 846 + 75 * 265)$
$= 846 - 3 * 265 - 5 * 265 + 25 * 846 - 75 * 265$
$= 26 * 846 - 83 * 265$