Computational Number Theory - Theory Assignment 2

Vishal Vijay Devadiga (CS21BTECH11061)

Question 1

Find all roots of $x^2 - 1$ in $\mathbb{Z}_n$ where $n = 17 \times 19$.

Solution

$x^2 = 1 \pmod{n}$

17 and 19 are prime numbers.

$x^2 = 1 \pmod{17}$ and $x^2 = 1 \pmod{19}$.

$x^2 = 1 \pmod{17}$ has roots $x = 1, -1$.

$x^2 = 1 \pmod{19}$ has roots $x = 1, -1$.

There are 4 cases:

1. $x = 1 \pmod{17}$ and $x = 1 \pmod{19}$. This gives $x = 1 \pmod{323}$.
2. $x = -1 \pmod{17}$ and $x = -1 \pmod{19}$. This gives $x = 322 \pmod{323}$.
3. $x = 1 \pmod{17}$ and $x = -1 \pmod{19}$. This gives $x = 18 \pmod{323}$.
4. $x = -1 \pmod{17}$ and $x = 1 \pmod{19}$. This gives $x = 305 \pmod{323}$.

Thus, the roots of $x^2 - 1$ in $\mathbb{Z}_{323}$ are $\boxed{1, 18, 305, 322}$.

Question 2

Find the unique solution to $x^7 = 2$ in $\mathbb{Z}_{41}$.

Solution

41 is a prime number.

$gcd(7, 41 - 1) = 1$

$gcd(2, 41) = 1$

There exists a unique solution to $x^7 = 2$ in $\mathbb{Z}_{41}$ given by $x = 2^k$ where $k = 7^{-1} \pmod{40}$.

$7^{-1} \pmod{40} = 23$

Thus, $x = 2^{23} \pmod{41}$.

$2^{23} \pmod{41} = 8$

Thus, the unique solution to $x^7 = 2$ in $\mathbb{Z}_{41}$ is $\boxed{x = 8}$.

Question 3

Let p be an odd prime number and $d|(p-1)$. Show that $\{a \in \mathbb{Z}_p : a^d = 1\} = \{a^{\frac{p-1}{d}} : a \in \mathbb{Z}_p^*\}$.

Solution

Let $a \in \mathbb{Z}_p$ such that $a^d = 1$.

Since $d|(p-1)$ and $a^{p-1} = 1$, we have $a^{p-1} = (a^d)^{\frac{p-1}{d}} = 1$.

Thus, $a^{\frac{p-1}{d}}$ is a root of $x^d - 1$.

For all $a \in \mathbb{Z}_p^*$, $a^{\frac{p-1}{d}}$ is a root of $x^d - 1$.

Thus, $\{a \in \mathbb{Z}_p : a^d = 1\} \subseteq \{a^{\frac{p-1}{d}} : a \in \mathbb{Z}_p^*\}$.

Let $a \in \mathbb{Z}_p^*$ such that $a^{\frac{p-1}{d}} = 1$.

Thus, we have $a^{p-1/d*d} = 1$.

Thus, $a^{p-1} = 1$.

Thus, we can write $\{a \in \mathbb{Z}_p : a^d = 1\} \supseteq \{a^{\frac{p-1}{d}} : a \in \mathbb{Z}_p^*\}$.

Thus, $\{a \in \mathbb{Z}_p : a^d = 1\} = \{a^{\frac{p-1}{d}} : a \in \mathbb{Z}_p^*\}$.

Question 4

Part A

Let d, n be integers such that $1 \leq d \leq n$. Find $|\{0 \leq k \leq n-1 : dk \equiv 0 \pmod{n}\}|$.

Solution

$dk \equiv 0 \pmod{n}$ if and only if $n|dk$.

$gcd(dk, n) = n$

$gcd(\frac{dk}{gcd(d,n)}, n/gcd(d,n)) = n/gcd(d,n)$

Since $n|dk$, $gcd(d,n) = d$.

Thus, $gcd(\frac{dk}{d}, n/d) = n/d$.

$gcd(k, n/d) = n/d$

Thus, $k \equiv 0 \pmod{n/d}$.

Thus, $|\{0 \leq k \leq n-1 : dk \equiv 0 \pmod{n}\}| = n/d$.

Part B

Let $1 \leq d \leq p-1$ where p is an odd prime. Find the number of roots of $x^d - 1$ in $\mathbb{Z}_p$.

Solution

$x^d \equiv 1 \pmod{p}$.

Also, $x^{p-1} \equiv 1 \pmod{p}$.

Thus, $x^{gcd(d,p-1)} \equiv 1 \pmod{p}$ as $gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$.

Let $e = gcd(d, p-1)$.

Since, $gcd(e, p-1) = e$, $x^e \equiv 1 \pmod{p}$ has e roots in $\mathbb{Z}_p$. These are the roots of $x^d - 1$.

Thus, the number of roots of $x^d - 1$ in $\mathbb{Z}_p$ is $gcd(d, p-1)$.

Question 5

Find the roots of $x^2 - 4$ in $\mathbb{Z}_{343}$.

Solution

$343 = 7^3$.

$x^2 - 4 = (x - 2)(x + 2)$.

In Z_7, $x^2 - 4 = (x - 2)(x + 2)$ has roots $2, -2$.

In Z_{49}, $x = 7k + 2$ or $7k - 2$.

For $x = 7k + 2$

$x^2 - 4 = (7k + 2)^2 - 4 = 28k \equiv 0 \pmod{49}$.

Thus, $4k \equiv 0 \pmod{7}$.

Thus, $k = 0 \pmod{7}$.

For $x = 7k - 2$

$x^2 - 4 = (7k - 2)^2 - 4 = -28k \equiv 0 \pmod{49}$.

Thus, $-4k \equiv 0 \pmod{7}$.

Thus, $k = 0 \pmod{7}$.

Thus, $x = 2$ or $x = -2$ in $\mathbb{Z}_{49}$.

In $\mathbb{Z}_{343}$, $x = 7k + 2$ or $7k - 2$.

Similar to the above, we get $x = 2$ or $x = -2$ in $\mathbb{Z}_{343}$.

Thus, the roots of $x^2 - 4$ in $\mathbb{Z}_{343}$ are $\boxed{2, 341}$.