Computational Number Theory

HW 2

CS20BTECH11042

1 Question 1

- Using Chinese Remainder Theorem, we can say that solutions of $x^2 - 1$ in $\mathbb{Z}_{17}$ and $x^2 - 1$ in $\mathbb{Z}_{19}$ are the solutions we require.
- $\mathbb{Z}_{17}$

$$\begin{aligned}(x-1)(x+1) &= 0 \mod 17\\ \Rightarrow x &= 1, 16 \mod 17\end{aligned}$$

- $\mathbb{Z}_{19}$

$$\begin{aligned}(x-1)(x+1) &= 0 \mod 19\\ \Rightarrow x &= 1, 18 \mod 19\end{aligned}$$

- $\mathbb{Z}_{17\times 19}$
  - $x = 1 \mod 17$ and $x = 1 \mod 19 \Rightarrow x = 1 \mod 17 \times 19$
  - $x = 16 \mod 17$ and $x = 1 \mod 19 \Rightarrow x = 305 \mod 17 \times 19$
  - $x = 1 \mod 17$ and $x = 18 \mod 19 \Rightarrow x = 18 \mod 17 \times 19$
  - $x = 16 \mod 17$ and $x = 18 \mod 19 \Rightarrow x = 322 \mod 17 \times 19$
- Therefore, the roots of $x^2 - 1$ in $\mathbb{Z}_{17\times 19}$ are $\{1, 18, 305, 322\}$

2 Question 2

- We observe that 41 is a prime number and $7 \nmid 41$
- Using Euclids lemma, we find k=23 satisfies the equation, $7k = 1 \mod 40$
- Now, raising both sides of $x^7 = 2 \mod 41$ to the power of 23, we get,

$$\begin{aligned}x^{7\times 23} &= 2^{23} \mod 41\\ x^{161} &= 2^{23} \mod 41\\ x &= 2^{23} \mod 41 \ (\because \text{Fermat's Little Theorem})\\ x &= 8 \mod 41\end{aligned}$$

3 Question 3

- Given, p is an odd prime number and $d|(p-1)$
- Let $S : \{a \in \mathbb{Z}_p : a^d = 1\}$
- Let $T : \{a^{(p-1)/d} : a \in \mathbb{Z}_p\}$. Here, since p is prime, $\mathbb{Z}_p = \mathbb{Z}_p^*$
- Now, for every element $x \in T$, we can see that $x^d = \left(a^{(p-1)/d}\right)^d = a^{p-1} = 1$. Therefore, $\forall x \in T, x \in S \Rightarrow T \subset S$
- Consider the equation $x^d - 1 = 0$, which has $p-1$ roots in $\mathbb{Z}_p$, denoted by the set S.
- We know that this equation has d distinct roots in $\mathbb{Z}_p$ and we see that

4 Question 4

4.1 Part a

- Given $dk \equiv 0 \mod n$, it implies n divides dk. Therefore, k must be a multiple of $\frac{n}{\gcd(d,n)}$.
- Hence, let $f(d)$ represents the count of multiples of $\frac{n}{\gcd(d,n)}$ within the range $0 \leq k \leq n-1$.
- The count of multiples of m within $0 \leq k \leq n-1$ is given by $\left\lfloor \frac{n}{m} \right\rfloor$.
- $\implies f(d) = \left\lfloor \frac{n}{\frac{n}{\gcd(d,n)}} \right\rfloor = \gcd(d,n)$.
- Therefore, $|\{0 \leq k \leq n-1 : dk \equiv 0 \mod n\}| = \gcd(d,n)$.

4.2 Part b

- Given that $x^d = 1 \mod p$
- We raise both sides by k to get: $x^{dk} = 1 \mod p$
- $\implies dk = \gcd(d, p-1) \mod p-1$
- From part a, we know that the number of solutions to above equation is $\gcd(d, p-1)$
- That is if we find an arbitrary solution as a primitive root, then the rest of the solutions are powers of the primitive root.
- Therefore, the number of roots of $x^d - 1$ in Zp is $\gcd(d, p-1)$

5 Question 5

- We need to find the roots of the equation $x^2 - 4$ in $\mathbb{Z}_{343}$
- $\mathbb{Z}_7$

$$\begin{aligned}(x-2)(x+2) &= 0 \mod 7 \\ \Rightarrow x &= 2, 5 \mod 7\end{aligned}$$

- $\mathbb{Z}_{49}$, we use **Hensel Lifting**,
  - Let x be of the form $7y + b$ where $b \in \{2, 5\}$
  - Now, when b = 2,

$$\begin{aligned} x^2 &= 4 \mod 49 \\ \Rightarrow (7y+2)^2 &= 4 \mod 49 \\ \Rightarrow 28y + 4 &= 4 \mod 49 \\ \Rightarrow 28y &= 0 \mod 49 \\ \Rightarrow y &= 7k, k \in \mathbb{Z} \\ \Rightarrow x &= 2 \end{aligned}$$

  - Now, when b = 5,

$$\begin{aligned} x^2 &= 4 \mod 49 \\ \Rightarrow (7y+5)^2 &= 4 \mod 49 \\ \Rightarrow 70y + 25 &= 4 \mod 49 \\ \Rightarrow 70y &= -21 \mod 49 \\ \Rightarrow 10y &= -3 \mod 7 \\ \Rightarrow y &= 7k + 6 \\ \Rightarrow x &= 47 \end{aligned}$$

- $\mathbb{Z}_{343}$, we use **Hensel Lifting** again
  - Let x be of the form $49y + b$ where $b \in \{2, 47\}$
  - Now, when b = 2,

$$\begin{aligned} x^2 &= 4 \mod 343 \\ \Rightarrow (49y+2)^2 &= 4 \mod 343 \\ \Rightarrow 98y + 4 &= 4 \mod 343 \\ \Rightarrow 98y &= 0 \mod 343 \\ \Rightarrow y &= 7k, k \in \mathbb{Z} \\ \Rightarrow x &= 2 \end{aligned}$$

  - Now, when b = -2, we can see that $x = 341 \mod 343$

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