CS5610 Assignment 2

Gautam Singh
CS21BTECH11018

1) The given equation is
$$x^2 - 1 = 0,\ x \in \mathbb{Z}_n. \tag{1}$$
Factoring n into its prime divisors 17 and 19, and considering (1) modulo these primes yields the equation
$$x^2 - 1 = 0,\ x \in \mathbb{Z}_p,\ p \in \{17, 19\}. \tag{2}$$
By Lagrange's Theorem in $\mathbb{Z}_p$, (2) may be rewritten as
$$(x+1)(x-1) = 0, \tag{3}$$
giving $x \in \{1, p-1\}$ for both values of p. Consider the bijection
$$f : \mathbb{Z}_n \to \mathbb{Z}_{17} \times \mathbb{Z}_{19},\ f(x) = (x \bmod 17, x \bmod 19). \tag{4}$$
Thus, any solution to (1) will also satisfy
$$x \equiv \pm 1 \bmod 17 \tag{5}$$
$$x \equiv \pm 1 \bmod 19. \tag{6}$$
Using the Chinese Remainder Theorem gives us four solutions (one for each combination of signs) $x \in \{1, 18, 305, 322\}$.
2) The equation is $x^7 = 2$ in $\mathbb{Z}_{11}$. Clearly, $x = 0$ is not a solution, thus $x \in \mathbb{Z}_{11}^*$. Fermat's Little Theorem gives $x^{10} = 1$. Since $\gcd(7, 10) = 1$, we use Euclid's Algorithm to find integers a, b such that
$$7a + 10b = 1. \tag{7}$$
One such solution is $(a, b) = (3, -2)$. Thus, we have
$$x = x^{7(3)+10(-2)} = \left(x^7\right)^3 = 2^3 = 8. \tag{8}$$
Hence, the unique solution is $x = 8$.
3) Clearly, $a = 0$ is not a solution to $a^d = 1$ in $\mathbb{Z}_p$. Let g be a generator of the multiplicative group Z_p^*. Letting $a = g^k$ for some $k \in \mathbb{Z}$, we can rewrite the equation as
$$g^{kd} = g^0 = 1. \tag{9}$$
Hence, we must have $kd = n(p-1)$ for some $n \in \mathbb{Z}$. Since $d \mid p-1$, we obtain $k = \frac{n(p-1)}{d}$. Thus, $a = (g^n)^{\frac{p-1}{d}}$. Since g generates $\mathbb{Z}_p^*$ and $n \in \mathbb{Z}$, the set of solutions to the given equation is $\left\{a^{\frac{p-1}{d}}\ :\ a \in \mathbb{Z}_p^*\right\}$, as required.
4) a) Define $g \triangleq \gcd(d, n)$. Then, by Bezout's Lemma, there exist integers a and b such that
$$da + nb = g. \tag{10}$$
Multiplying throughout by k and taking residues modulo n, as well as applying the condition that $dk \equiv 0 \bmod n$, we get
$$adk + nbk = gk \implies gk \equiv 0 \bmod n \implies k = \frac{nm}{g},\ m \in \mathbb{Z}. \tag{11}$$

However, we have $0 \leq k < n$. Thus, $0 \leq m < g$. Hence,

$$|\{0 \leq k \leq n-1 : dk \equiv 0 \bmod n\}| = \gcd(d,n). \tag{12}$$

b) We know that for an integer a and positive integers m, n, we have

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1. \tag{13}$$

Consider the polynomials $f(x) = x^d - 1$ and $g(x) = x^{p-1} - 1$ in $\mathbb{Z}_p[x]$. Since Euclid's algorithm works in $\mathbb{Z}_p$, (13) holds in $\mathbb{Z}_p[x]$. By Fermat's Little Theorem, all elements of $\mathbb{Z}_p^*$ are roots of $g(x)$. Hence, any root of $f(x)$ will also be a root of $\gcd(f(x), g(x)) = x^{\gcd(d,p-1)} - 1$, as $x = 0$ is clearly not a root of $f(x)$.
We also know that $x^k - 1$ has k roots if $k \mid p-1$. Taking $k = \gcd(d, p-1)$, there are $\gcd(d, p-1)$ roots of $f(x)$ in $\mathbb{Z}_p$.

5) Consider in $\mathbb{Z}_7$ the equation

$$x^2 - 4 = (x-2)(x+2) = 0. \tag{14}$$

Using Lagrange's Theorem in $\mathbb{Z}_7$, we see that the roots of (14) are $x = \pm 2$ or $x = 2, 5$.
Now consider (14) in $\mathbb{Z}_{7^2}$. Any solution must be of the form $x = 7k \pm 2$. Substituting and working in $\mathbb{Z}_{7^2}$, we get

$$(7k \pm 2)^2 - 4 = 0 \implies \pm 28k = 0 \implies k = 0. \tag{15}$$

Thus, the solutions in $\mathbb{Z}_{7^2}$ are $x = \pm 2$ or $x = 2, 47$. Again, any solution to (14) in $\mathbb{Z}_{7^3}$ must be of the form $x = 7^2 k \pm 2$. Substituting and working in $\mathbb{Z}_{7^3}$,

$$\left(7^2 k \pm 2\right)^2 - 4 = 0 \implies \pm 196k = 0 \implies k = 0. \tag{16}$$

Therefore, the solutions of (14) in $\mathbb{Z}_{343}$ are $x = 2, 341$.