CS60094: Computational Number Theory, Spring 2018-19
Class Test 2

CSE 107, 7:30 PM — 9th April, 2019
Duration = 1 hour — Total marks = 20

1. (a) Show that the polynomial $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{F}_3$. **[2]**

Solution: We have $f(0) = 2$, $f(1) = 1$ and $f(2) = 2$. That is, $f(x)$ has no roots in $\mathbb{F}_3$ and is hence irreducible over $\mathbb{F}_3$. (This is true because $\deg f(x) = 3$. Prove it!)

(b) Define $\mathbb{F}_{27} = \mathbb{F}_{3^2} = \mathbb{F}_3(\theta)$ where θ is a root of $f(x)$ i.e., $\theta^3 + \theta^2 + 2 = 0$. Let $\gamma = \theta + 1 \in \mathbb{F}_{27}$. Determine whether γ is a primitive element of $\mathbb{F}_{27}$. **[4]**

Hint: $|F_{27}^*| = 26 = 2 \times 13$. The order of any element in $\mathbb{F}_{27}^*$ must be one of the following: $1, 2, 13, 26$.

Solution: As $\theta^3 + \theta^2 + 2 = 0$, we have $\theta^3 = 2\theta^2 + 1$. To check if γ is a primitive element, it suffices to check if γ has order 2 or 13.

$$\gamma = \theta + 1$$
$$\gamma^2 = \theta^2 + 2\theta + 1$$
$$\gamma^3 = \gamma \cdot \gamma^2 = 2\theta^2 + 2 \neq 1$$
$$\gamma^6 = (\gamma^3)^2 = \theta$$
$$\gamma^{12} = (\gamma^6)^2 = \theta^2$$
$$\gamma^{13} = \gamma^{12} \cdot \gamma = 1$$

γ has order 13 in $\mathbb{F}_{27}^*$ and hence is not a primitive element.

(c) Is $\delta = \theta^2 \in \mathbb{F}_{27}$ a normal element of $\mathbb{F}_{27}$? **[4]**

Solution: δ would be normal if $\delta, \delta^3, \delta^{3^2}$ are linearly independent. We have

$$\delta = \theta^2$$
$$\delta^2 = \theta^2 + \theta + 2$$
$$\delta^3 = \delta \cdot \delta^2 = 2\theta^2 + \theta$$
$$\delta^6 = (\delta^3)^2 = \theta^2 + \theta$$
$$\delta^9 = \delta^3 \delta^6 = 2\theta + 1$$

i.e.,

$$\begin{pmatrix} \delta \\ \delta^3 \\ \delta^9 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}}_{\mathbf{A}} \begin{pmatrix} \theta^2 \\ \theta \\ 1 \end{pmatrix}$$

Clearly, $\det \mathbf{A} = 1$ and $\delta, \delta^3, \delta^9$ are linearly independent. Therefore, δ is a normal element in $\mathbb{F}_{27}$.

2. Let $\mathbb{F}_q$ be a finite field and let $\gamma \in \mathbb{F}_q$ be a primitive element. For every $\alpha \in \mathbb{F}_q^*$, there exists a unique $k \in \mathbb{Z}_{q-1}$ (i.e., $0 \le k \le q-2$) such that $\alpha = \gamma^k$. Denote this k by $\mathrm{ind}_\gamma \alpha$ (index of α with respect to γ).

   (a) Assume that q is odd. Prove that the equation $x^2 = \alpha$ is solvable in $\mathbb{F}_q$ for $\alpha \in \mathbb{F}_q^*$ if and only if $\mathrm{ind}_\gamma \alpha$ is even. **[4]**

   Solution: Suppose that $x^2 = \alpha$ is solvable in $\mathbb{F}_q$. Let $\beta = \gamma^k$ is a solution. Then $\alpha = \beta^2 = \gamma^{2k \pmod{q-1}}$. Since both $2k$ and $q-1$ are even, so is $2k \pmod{q-1} = \mathrm{ind}_\gamma \alpha$.

   Conversely, suppose that $\mathrm{ind}_\gamma \alpha = 2k$ for some integer k. Then $\beta = \gamma^k \in \mathbb{F}_q$ is a solution to $x^2 = \alpha$ as $\beta^2 = \gamma^{2k} = \alpha$.

   (b) Now, let $q = 2^n$. Prove that the equation $x^2 = \alpha$ has a unique solution in $\mathbb{F}_q$ and the solution is given by $\beta = \alpha^{2^{n-1}}$. **[4]**

   Solution: Clearly $\beta = \alpha^{2^{n-1}}$ is a solution to $x^2 = \alpha$ since $\beta^2 = \alpha^{2^n} = \alpha^q = \alpha$. In order to prove uniqueness, suppose that $\beta_1, \beta_2 \in \mathbb{F}_q^*$ are two distinct solutions. Then $\beta_1^2 = \beta_2^2 \implies \left(\beta_1 \beta_2^{-1}\right)^2 = 1$ which means that $\beta_1 \beta_2^{-1}$ is an element of order 2. But the order of any element in $\mathbb{F}_q^*$ must divide $|\mathbb{F}_q^*| = q - 1 = 2^n - 1$, which is odd. Hence the solution to $x^2 = \alpha$ must be unique.

   (c) Again, assume $q = 2^n$. Suppose that $\alpha, \beta \in \mathbb{F}_q^*$ and $\alpha = \beta^2$. Let $k = \mathrm{ind}_\gamma \alpha$ and $\ell = \mathrm{ind}_\gamma \beta$. Express ℓ as an efficiently computable formula in k and q. **[2]**

   Solution: Since $\beta = \alpha^{2^{n-1}}$, we have $\ell = 2^{n-1} k \pmod{2^n - 1}$. Since $n = \log q$, this is efficiently computable. Moreover, ℓ can be obtained by only a cyclic rotation of the bits of k. To see this, suppose that $k = (k_{n-1}, k_{n-2}, \ldots, k_1, k_0)_2$.

$$\begin{aligned} 2^{n-1} k \pmod{2^n - 1} &= 2^{n-1} \left(2^{n-1} k_{n-1} + 2^{n-2} k_{n-2} + \cdots + 2k_1 + k_0\right) \pmod{2^n - 1} \\ &= 2^{n+n-2} k_{n-1} + 2^{n+n-3} k_{n-2} + \cdots + 2^n k_1 + 2^{n-1} k_0 \pmod{2^n - 1} \\ &= 2^{n-2} k_{n-1} + 2^{n-3} k_{n-2} + \cdots + k_1 + 2^{n-1} k_0 \end{aligned}$$

   The last equality follows from the fact that $2^n = 1 \pmod{2^n - 1}$). We have $\mathrm{ind}_\gamma \beta = \ell = k_0 2^{n-1} + k_{n-1} 2^{n-2} + \cdots + k_2 2 + k_1$, which is nothing but a cyclic rotation of the bits of k one position to the right.