Indian Institute of Technology Kharagpur

CS60094: Computational Number Theory, Spring 2018-19
End-Semester Examination

30th April, 2019 CSE 107/108, 2PM – 5PM Total marks: 50

Answer all questions. State any assumptions you make. Provide concise answers.

---

1. Represent the finite field $\mathbb{F}_{16} = \mathbb{F}_2(\theta)$ with $\theta^4 + \theta^3 + 1 = 0$. Let $\alpha = \theta^3 + 1$.
   (a) Is α a primitive element of $\mathbb{F}_{16}$? **[3]**
   (b) Is α a normal element of $\mathbb{F}_{16}$? **[3]**
   (c) Compute the minimal polynomial of α over $\mathbb{F}_2$. **[4]**

2. Let $\alpha \in \mathbb{F}_q^*$ with q odd. Prove that the equation $x^2 = \alpha$ has a solution in $\mathbb{F}_q^*$ if and only if $\alpha^{(q-1)/2} = 1$. **[4]**

3. Consider an extension field $\mathbb{F}_q = \mathbb{F}_{p^n}$ for $n \geq 2$. Assume basic operations in $\mathbb{F}_p$ run in $O(1)$ time. Suppose that $\mathbb{F}_q$ is represented by an arbitrary $\mathbb{F}_p$-basis $(\theta_0, \theta_1, \ldots, \theta_{n-1})$. For $\alpha \in \mathbb{F}_q$, α^{-1} is given by α^{q-2} (by Fermat's little theorem). Propose an algorithm that computes α^{-1}, given α, that runs in $O(n^3)$ time. Clearly specify if any precomputation is required and indicate the space required to store precomputed values. **[10]**
   Hint: A system of n linear equations in n unknowns over $\mathbb{F}_p$ can be solved in time $O(n^3)$ using Gaussian elimination.

4. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree 3. Prove that $f(x)$ is irreducible if and only if $f(x)$ has no roots in $\mathbb{F}_q$. **[4]**

5. Find the distinct degree factorisation of $x^8 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. **[4]**

6. Let $f(x), g(x) \in K[x]$ for some field K and let $\deg f(x) = m$, $\deg g(x) = n$. Suppose that $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$ and $g(x) = b(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$ with $a, b \in K$ and α_i's, β_j's are all distinct and belong to some extension field of K. Let $\mathbf{M} = \mathrm{Syl}(f(x), g(x))$, the Sylvester matrix of $f(x)$ and $g(x)$. We know that $\mathrm{Res}(f(x), g(x)) = \det \mathbf{M}$.
   (a) Consider the $(m+n) \times (m+n)$ Vandermonde matrix $\mathbf{V} = (v_{i,j})$ defined by
   $$v_{i,j} = \begin{cases} \beta_j^{m+n-i} & \text{if } j \leq n \\ \alpha_{j-n}^{m+n-i} & \text{if } n+1 \leq j \leq n+m \end{cases}$$
   for $1 \leq i \leq m+n$. Determinant of $\mathbf{V}$ is given by
   $$\det \mathbf{V} = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j) \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j) \prod_{i \in [1,n], j \in [1,m]} (\beta_i - \alpha_j).$$

Show that

$$\det(\mathbf{MV}) = \prod_{i=1}^{n} f(\beta_i) \cdot \prod_{j=1}^{m} g(\alpha_j) \cdot \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j).$$

[7]

(b) Deduce that $\operatorname{Res}(f(x), g(x)) = a^n \prod_{j=1}^{m} g(\alpha_j) = (-1)^{mn} \cdot b^m \prod_{i=1}^{n} f(\beta_i)$. **[5]**

(c) Let K be a field with characteristic 0. Recall that the discriminant of a polynomial $f(x) \in K[x]$ is given by

$$\operatorname{Discr}(f(x)) = (-1)^{m(m-1)/2} \cdot a^{-1} \operatorname{Res}(f(x), f'(x))$$

where $m = \deg f(x)$ and a is the leading coefficient of $f(x)$. Prove that

$$\operatorname{Discr}(f(x)) = a^{2m-2} \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2,$$

where α_i's are the roots of $f(x)$ in some extension field of K. **[6]**