Soham Chatterjee
Email: sohamc@cmi.ac.in
Course: Algebra and Computation

Assignment - 2
Roll: BMC202175
Date: May 19, 2024

Problem 1 Problem Set 2: P1

Let p be a prime number and n a positive integer. Then by *explicit data* for $\mathbb{F}_{p^n}$ we mean a set of n^3 elements $(a_{i,j,k})_{i,j,k=1}^n$ of the prime field $\mathbb{F}_p$ such that $\mathbb{F}_{p^n}$ becomes a field with the ordinary addition and multiplication by elements of $\mathbb{F}_p$ and the multiplication determined by

$$e_ie_j = \sum_{k=1}^n a_{i,j,k}e_k$$

where $e_1, e_2, \dots, e_n$ denotes the standard basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. If we know an irreducible polynomial of degree n, then such explicit data for $\mathbb{F}_{p^n}$ can be directly computed. Show conversely. given explicit data for $\mathbb{F}_{p^n}$ one can find an irreducble polynomial over $\mathbb{F}_p[x]$ of degree n via a dieterministic polynomial-time (in $\log p$ and n) algorithm.
Lenstra gave a deterministic polynomial time to *find* an isomorphism between two explicitly given finite fields of the same cardinality. Till date, we do not know any deterministic polynomial time (in $\log p$, n) algorithm to find an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.

Solution: We will use the paper [Len91]. Suppose $n = \prod_{i=1}^k p_i^{t_i}$. Suppose γ_i be an t_i degree an element of $\mathbb{F}_q$ where $q = p^n$ over $\mathbb{F}_p$. Then we can say

$$\mathbb{F}_p \subset \mathbb{F}_p(\gamma_1) \subset \mathbb{F}_p(\gamma_1, \gamma_2) \subset \cdots \subset \mathbb{F}_p(\gamma_1, \dots, \gamma_k) = \mathbb{F}_{p^n}$$

where γ_i has minimal polynomial $p_i^{t_i}$. Hence finding these γ_i and their minimal polynomials will help us find the polynomial f such that $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/\langle f \rangle$.

1. Finding Minimal Polynomial of $\gamma = \sum_{i=1}^k \gamma_i$ from Minimal Polynomial of γ_i's

Now suppose g_i is the minimal polynomial of γ_i of degree $p_i^{t_i}$. Then we have to find the minimal polynomial of $\gamma = \sum_{i=1}^k \gamma_i$. Now if α, β are numbers with minimal polynomial $h_1(x) = \sum_{l=0}^m a_l x^l$ and $h_2(x) = \sum_{l=0}^n b_l x^l$ then α is eigen values of the corresponding matrix $A = \left[\begin{array}{c|c} 0 & -a_0 \\ \hline I_{m-2} & \begin{array}{c} \vdots \\ -a_{m-1} \end{array} \end{array}\right]$ since the characteristic polynomial of A is $h_1(x)$. Similarly we obtain B for β. Let u_1 and u_2 are the eigen vectors of A and B. Then the matrix $A \otimes I + I \otimes B$ has eigen vector $u_1 \otimes u_2$ with eigen value $\alpha + \beta$ since

$$(A \otimes I + I \otimes B)(u_1 \otimes u_2) = Au_1 \otimes Iu_2 + Iu_1 \otimes Bu_2 = \alpha(u_1 \otimes u_2) + \beta(u_1 \otimes u_2)$$

So $\alpha + \beta$ root of the characteristic polynomial of $A \otimes I + I \otimes B$ and since $\alpha + \beta$ should have minimal polynomial mn and degree of characteristic polynomial of $A \otimes I + I \otimes B$ is mn we have the characteristic polynomial as the minimal polynomial of $\alpha + \beta$. Using this way we can obtain the minimal polynomial of $\gamma = \sum_{i=1}^k \gamma_i$.

2. Finding g_i from γ_i for $i \in [k]$

Suppose we have γ_i. It has a $p_i^{t_i}$ degree minimal polynomial over $\mathbb{F}_p$. γ_i is an element of degree $p_i^{t_i}$ over $\mathbb{F}_p$. So let

$$\gamma_i^{p_i^{t_i}} = \sum_{k=0}^{p_i^{t_i}-1} c_k \gamma_i^k$$

with $c_k \in \mathbb{F}_p$. Then the polynomial $\tilde{g}_i = x^{p_i^{t_i}} - \sum_{k=0}^{p_i^{t_i}} c_k \gamma_i^k$ is minimal polynomial of γ_i. So $\tilde{g}_i = g_i$. This we can do in $poly(n, \log p)$ steps.

3. Finding γ_i for $i \in [k]$

Now all is left to find γ_i. Define the map $\phi_d : \alpha \mapsto \alpha^d$. Denote the numbers $\delta_i = p^{p_i^{t_i}}$. Then $\gamma_i \in \ker\left(\phi_{\delta_i} - id\right)$. We create the matrix for frobenius Map i.e. the map $x \mapsto x^p$ and compose it with itself $p_i^{t_i}$ times which gives us the map for ϕ_{δ_i}, T_i which we can compute in $poly(n, \log p)$ steps. Then we compute the matrix $T_i - I$ and by guassian elimination we compute the basis of a kernel and find a basis element which is in $\mathbb{F}_{p^{p_i^{t_i}}} - \mathbb{F}_{p^{p_i^{t_i}-1}}$ which again we can do in $poly(\log p, n)$ steps.

□

Problem 2 Problem Set 2: P5

Let q be a prime power and $f \in \mathbb{F}_q[x]$ squarefree of degree n with $r \geq 2$ irreducible factors $f_1, \ldots, f_r$, each of degree $d = \frac{n}{r}$. We let $R := \mathbb{F}_q[x]/\langle f \rangle$, $R_1 = \mathbb{F}_q[x]/\langle f_1 \rangle, \ldots, R_r = \mathbb{F}_q[x]/\langle f_r \rangle$ and the Chinese Remainder Isomorphism $\chi = \chi_1 \times \cdots \times \chi_r$ where $\chi(a \bmod f) = (a \bmod f_1, \ldots, a \bmod f_r) = (\chi_1(a), \ldots, \chi_r(a))$. The norm on $R_i \cong \mathbb{F}_{q^d}$ is defined by $N(\alpha) = \alpha \alpha^q \alpha^{q^2} \cdots \alpha^{q^{d-1}} = \alpha^{\frac{q^d-1}{q-1}}$.

(a) Let $\alpha \in R^\times$ be a uniform random element, $\beta = N(\alpha)$ and $1 \leq i \leq r$. Show that $\chi_i(\beta)$ is a root of $x^{q-1} - 1$ and conclude that $\chi_i(\beta)$ is a uniform random element in $\mathbb{F}_q^\times$.

(b) Provided that $q > r$, what is the probability that with the $\chi_i(\beta)$ are distinct for $1 \leq i \leq r$? Prove that the probability is at least $\frac{1}{2}$ if $q - 1 \geq 2(r-1)^2$.

(c) Let $u, v \in \mathbb{F}_q$ be distinct. Prove that probability at least $\frac{1}{2}$, $u + t$ is a square (quadratic residue) and $v + t$ is a nonsquare or vice versa, for a uniformly random $t \in \mathbb{F}_q$.

(d) Use the above exercise to come up with a variant of Cantor-Zassenhaus's equal-degree splitting algorithm to factorize a squarefree monic polynomial $f \in \mathbb{F}_q[x]$ of degree n, where all the irredicble factors of f have degree d.

Hint: Use a polynomial $a \in \mathbb{F}_q[x]$ of degree less than n with $\chi_i(a) \in \mathbb{F}_q$ for all i. Choose $t \in \mathbb{F}_q$ at random. Take gcd of f with $(a+t)^{\frac{q-1}{2}} - 1$. Prove that the failure probability of the algorithm is at most $\frac{1}{2}$ if $a \neq \mathbb{F}_q$.

Solution:

(a) We know for any $i \in [r]$, $R_i = \mathbb{F}_q[x]/\langle f_i \rangle \cong \mathbb{F}_{q^d}$. For any element $\alpha \in R^\times$,

$$\chi_i(N(\alpha)) = N(\chi_i(\alpha)) = [\alpha \bmod f_i]^{\frac{q^d-1}{q-1}} \equiv \alpha^{\frac{q^d-1}{q-1}} \bmod f_i$$

Now for all $a \in R_i$, it is a root of the polynomial $x^{q^d-1} - 1$ or $a^{q^n-1} \equiv 1 \bmod f_i$. Now

$$\left[\alpha^{\frac{q^d-1}{q-1}}\right]^{q-1} - 1 \equiv \alpha^{q^d-1} - 1 \equiv 1 - 1 \equiv 0 \bmod f_i$$

Hence $\chi_i(\beta)$ is a root of $x^{q-1}-1$

In the field $\mathbb{F}_{q^d}$ we take the endomorphism $\phi_k : x \mapsto x^k$. Then the $\ker \phi_k = \{a \in \mathbb{F}_{q^d} \mid a^k \equiv 1\}$ which is set of all roots of the equation $x^k - 1$ which can have at most k many roots. So $|\ker \phi_k| \leq k$. Let $S = \left\{ a^{\frac{q^d-1}{q-1}} \mid a \in \mathbb{F}_{q^d} \right\}$. Then $S \subseteq \ker \psi$ where $\psi = \phi_{q-1}$. Hence $|S| \leq |\ker \psi| \leq q-1$. Now

$$q^d - 1 = |\mathbb{F}_{q^d}^\times| = \left|\ker \psi\right| \cdot \left|\mathrm{im}\psi\right| = \left|\ker \psi\right| \cdot |S| \leq \frac{q^d-1}{q-1} \times (q-1) = q^d - 1$$

Therefore $|S| = q-1$. Since S exactly the nonzero elements of $\mathbb{F}_q^\times$ each element of S occurs in different coset of $\mathbb{F}_{q^d}^\times / \ker \psi$. Then

$$\Pr_{a \in \mathbb{F}_{q^d}^\times}\left[a^{\frac{q^d-1}{q-1}} = \alpha \mid \alpha \in S\right] = \frac{\frac{q^d-1}{q-1}}{q^d-1} = \frac{1}{q-1}$$

Hence if we pick α uniformly at random then taking $\alpha^{\frac{q^d-1}{q-1}}$ is a uniformly random element of $\mathbb{F}_q^\times$.

(b) we know $\chi_i(\beta)$ is an uniformly random element of $\mathbb{F}_q^\times$. Now

$$Pr[\chi_i(\beta) \neq \chi_j(\beta) \ \forall \ i, j \in [r], i \neq j] = \frac{(q-1)(q-2)\cdots(q-r)}{(q-1)^r} = \prod_{i=0}^{r-1}\left(1 - \frac{i}{q-1}\right) = \prod_{i=1}^{r-1}\left(1 - \frac{i}{q-1}\right)$$

Given

$$q - 1 \geq 2(r-1)^2 \implies \frac{1}{2(r-1)} \geq \frac{r-1}{q-1} \geq \frac{i}{q-1} \text{ where } i \in [r-1]$$

Hence $1 - \frac{k}{q-1} \geq 1 - \frac{r-1}{q-1} \geq 1 - \frac{1}{2(r-1)}$. Therefore

$$Pr[\chi_i(\beta) \neq \chi_j(\beta) \ \forall \ i, j \in [r], i \neq j] \geq \left[1 - \frac{1}{2(r-1)}\right]^{r-1} \geq 1 - \frac{r-1}{2(r-1)} = \frac{1}{2}$$

(c) Since t is a uniformly random element of $\mathbb{F}_q$. Hence $u+t$ and $v+t$ is are uniformly random element of $\mathbb{F}_q$. Thereofore

$$\Pr_{t \in \mathbb{F}_q}[u + t \text{ is QR } \& v + t \text{ is NQR}] = Pr[u+t] = \Pr_{t \in \mathbb{F}_q}[u + t \text{ is QR}] \Pr_{t \in \mathbb{F}_q}[v + t \text{ is NQR}] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

Similarly $\Pr_{t \in \mathbb{F}_q}[u + t \text{ is NQR } \& v + t \text{ is QR}] = \frac{1}{4}$. Hence probability that one of $u+t, v+t$ is QR and other one is NQR is $\frac{1}{2}$.

(d) We give the algorithm first then we will show the correctness and calculate the probability

Algorithm 1: A Different Variant of Cantor-Zassenhaus Algorithm

Input: Squarefree monic polynomial f of degree n with r irreducible factors of degree d with $q - 1 \geq 2(r-1)^2$

Output: Factor of f if exists otherwise 'FAIL'

```
begin
    Take a ∈ F_q[x] − F_q uniformly at random;
    Compute β ⟵ N(a) mod f using Repeated-Squaring;
    Take t ∈ F_q uniformly at random;
    Compute g ⟵ (β + t)^((q−1)/2) mod f using Repeated-Squaring;
    Compute h ⟵ gcd(f, g);
    if h ≠ 1 and h is nontrivial then
        return h
    else
        return 'FAIL'
```

We know by part (a) for all $i \in [r]$ $\chi_i(\beta)$ is an uniformly random element of $\mathbb{F}_q^\times$. Now By part (b) with probability $\geq \frac{1}{2}$ for $i \neq j$, $i, j \in [r]$ we have $\chi_i(\beta) \neq \chi_j(\beta)$. So By part (c) with probability $\frac{1}{2}$, one of $[\chi_i(\beta)+t]^{\frac{q-1}{2}}$ and $\left[\chi_j(\beta)+t\right]^{\frac{q-1}{2}}$ is QR and other one is NQR. Suppose $[\chi_i(\beta)+t]^{\frac{q-1}{2}}$ is QR. Then

$$f_i \mid [\chi_i(\beta)+t]^{\frac{q-1}{2}} - 1 \qquad \text{but} \qquad f_j \nmid [\chi_i(\beta)+t]^{\frac{q-1}{2}} - 1$$

Hence $f_i \mid gcd\left(f, [\chi_i(\beta)+t]^{\frac{q-1}{2}}\right)$ but not f_j. Therefore the gcd is nontrivial. Hence the gcd h yields a nontrivial factor of f.

□

Problem 3 Problem Set 2: P6

Finding roots of a polynomial is clearly a special case of polynomial factorization. This exercise shows conversely how factoring over $\mathbb{F}_{p^k}$ can be reduced to root finding over $\mathbb{F}_p$. Let $q = p^k$ be a prime power for some positive $k \in \mathbb{N}$, $f \in \mathbb{F}_q[x]$ monic squarefree of degree n, $R = \mathbb{F}_q[x]/\langle f \rangle$ and $\mathcal{B} = \{a \bmod f \in R \colon a^p \equiv a \bmod f\}$

(a) Let $b \in \mathbb{F}_q[x]$ such that $b \bmod f \in \mathcal{B}$. Prove that $f = \prod\limits_{a \in \mathbb{F}_p} gcd(f, b-a)$

(b) Let y be a new indeterminate and $r = \mathrm{Res}_x(f, b-y) \in \mathbb{F}_q[x,y]$. Show that r has some roots in $\mathbb{F}_p$ and that any root of r in $\mathbb{F}_p$ leads to a nontrivial factor of f if $b \notin \mathbb{F}_p$.

(c) Make this to a deterministic polynomial time reduction from factoring in $\mathbb{F}_q[x]$ to root finding in $\mathbb{F}_p[x]$

Solution:

(a) $b \bmod f \in \mathcal{B}$. Hence

$$b^p - b \equiv 0 \bmod f \implies \prod_{a \in \mathbb{F}_p} (b-a) \equiv 0 \bmod f$$

Hence $gcd\left(f, \prod\limits_{a \in \mathbb{F}_p}(b-a)\right) = f$. Now for any two $a, a' \in \mathbb{F}_p$, $a \neq a'$, we have $gcd(b-a, b-a') = 1$ as $(a'-a)^{-1}((g-a)-(g-a')) = 1$. Hence $gcd\left(f, \prod_{a \in \mathbb{F}_p}(b-a)\right) = \prod\limits_{a \in \mathbb{F}_p} gcd(f, b-a)$. Therefore

$$f = gcd\left(f, \prod_{a \in \mathbb{F}_p}(b-a)\right) = \prod_{a \in \mathbb{F}_p} gcd(f, b-a)$$

(b) Since $f = \prod\limits_{a \in \mathbb{F}_p} gcd(f, b-a)$ there exists at least one $a \in \mathbb{F}_p$ such that $gcd(f, b-a) \neq 1$. Hence we have $\mathrm{Res}(f, b-a) = 0$ in $\mathbb{F}_q[x]$. Now we can say

$$\mathrm{Res}(f, b-a) = 0 \iff \mathrm{Res}_x(f, b-y) \equiv 0 \pmod{y-a}$$

where the RHS is in the ring $\mathbb{F}_q[x,y]$. Hence we can say $\mathrm{Res}_x(f, b-y)$ has a root at $y = a$ where $a \in \mathbb{F}_p$ in $\mathbb{F}_q[x,y]$. Therefore $\mathrm{Res}_x(f, b-y)$ has some roots in $\mathbb{F}_p$.

Now we can assume $\deg b < \deg f$ since otherwise we can write $b = qf + r$ where $\deg r < \deg f$ and now $gcd(f, b-a) = gcd(f, r-a)$. If $b \notin \mathbb{F}_p$. Then $\deg(b-r) < \deg f$ for any $r \in \mathbb{F}_p$. Hence if $\mathrm{Res}_x(f, b-a) = 0$ for some $a \in \mathbb{F}_p$ since $b - a \neq 0$ we have $gcd(f, b-a)$ nontrivial which actually gives a factor of f. Hence finding a root leads to a anontrivial factor of f if $b \notin \mathbb{F}_p$

(c) So given f we have to find a nontrivial solution for the map $h^p - h \bmod f$. Now the map $T : h \mapsto h^p - h$ for $h \in \mathbb{F}_q[x]$ is a linear map over $\mathbb{F}_p$. So we create the matrix for T modulo f. with respect to the polynomials basis $x^{n-1} \bmod f, \ldots, x \bmod f, 1 \bmod f$. Now we will compute the basis of the kernel of this map using guassian elemination. Now

$$f \text{ is irreducible} \iff \operatorname{rank} T = n - 1$$

So if the computed basis has a non-constant polynomial g then that is our desired polynomial for a nontrivial solution of $h^p - h \equiv \bmod f$. Using this g now we can try to find a root of the polynomial $\mathrm{Res}_x(f, g - y)$ in $\mathbb{F}_p$ which will help us to find a factor as discussed in the part (b).

□

Problem 4 Problem Set 2: P9

Every prime $p \equiv 1 \pmod 4$ can be expressed as a sum of two squares. Give an efficient algorithm to find two integers x and y such that $p = x^2 + y^2$. Here *efficient* means randomized or deterministic polynomial time in the input size (number of bits to represent the given prime in binary).
Helpful keywords: Fermat sum of squares, quadratic non-residue, Euclid's GCD algorithm/Gauss- Lagrange 2-dimensional lattice reduction algorithm.

Solution:

Lemma 1. *Let $c = \sqrt{-1} \pmod p$ and $gcd(p, c - i) = a + bi$. Then $p = a^2 + b^2$*

Proof: First we will show if we find a nontrivial guassian integer whcih divides p then we can get the integers a, b. Let $\alpha \mid p$ completely. Then by conjugating we have $\overline{\alpha} \mid p$. Hence $\alpha\bar{e}\alpha \mid p^2$. Now $\alpha\overline{\alpha} \in \mathbb{Z}$. So $\alpha\bar{e}\alpha$ is a nontrivial factor of p. And the only nontrivial factor of p^2 is p. So $p = \alpha\bar{e}\alpha$. Let $\alpha = a + ib$. Then $\alpha\overline{\alpha} = a^2 + b^2$. So $p = a^2 + b^2$. Hence finding a nontrivial guassian integer which divides p is enough to find the integers whose square sum is p.

Now suppose we found α, β nontrivial guassian integers such that $pq = \alpha\beta$ and $p \nmid \alpha, \beta$. Then $gcd(\alpha, p)$ divides p completely. We will show if this is the case then $gcd(\alpha, p) \neq 1, p$. If gcd was p then $p \mid \alpha$ which contradicts the assumption that $p \nmid \alpha$. Hence the gcd is 1. Then $\alpha \mid q$. Therefore $\frac{q}{\alpha} = \frac{\beta}{p}$. Hence p divides β completely but that contradicts the assumption. So $gcd(\alpha, p) \neq 1, p$. So the gcd gives a nontrivial factor of p.

Now if we found $c \bmod p$ such that $c^2 \equiv 1 \bmod p$ or we can say $c^2 - 1 + pg = 0$ for some $g \in \mathbb{Z}[i]$. Then $c^2 + 1 + pg = (c + i)(c - i) + pg = 0$ in $\mathbb{Z}[i]$. Therefore

$$(c + i)(c - i) = -pg$$

Now $p \nmid c \pm i$. Hence by the above proof we have $gcd(p, c + i)$ nontrivial factor of p in $\mathbb{Z}[i]$. From that we get the integers a, b such that $p = a^2 + b^2$ □

So now we have to find an element of $a < p$ such that $a^2 \equiv -1 \bmod p$. If we can find a quadratic non-residue $a \in \mathbb{Z}_p$ then we have $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ then we can take $a^{\frac{p-1}{4}}$ to be the desired element. Now in the group $\mathbb{Z}_p$ we can select a non quadratic residue by picking an element uniformly at random and with probability $\frac{1}{2}$ we can obtain a quadratic non residue.

□

References

[Len91] Hendrik W Lenstra. Finding isomorphisms between finite fields. *mathematics of computation*, 56(193):329–347, 1991.