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

Assignment - 1
Roll: BMC202175
Date: May 19, 2024

Problem 1 Problem Set 1: P5

For a prime p and a positive integer e, prove that $\mathbb{Z}_{p^e}^*$ is cyclic.

Solution: We will prove this in 3 stages: $e = 1$, $e = 2$, $e > 2$.

Case 1: $e = 1$

Lemma 1. $\sum\limits_{d|n} \varphi(d) = n$

Proof: Consider the list of numbers $S = \left\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\right\}$. If we express every number in S as simplified form i.e. $\frac{p}{q}$ form where $gcd(p, q) = 1$. Then the denominators are all the divisors of n.

Then for any $k \in [n]$ we have

$$\frac{k}{n} = \frac{\frac{k}{gcd(k,n)}}{\frac{n}{gcd(k,n)}}$$

Denote $d_k := \frac{n}{gcd(k,n)}$ then d_k is a factor of n. And since $gcd\left(\frac{k}{gcd(k,n)}, \frac{n}{gcd(k,n)}\right) = 1$ we have $\frac{k}{gcd(k,n)} \in \mathbb{Z}_{d_k}^*$. Let $k \in \mathbb{Z}_d^*$ then suppose l is such that $d \times l = n$ then the fraction $\frac{k}{d} = \frac{k \times l}{n} \in S$ and its simplified form is infact $\frac{k}{d}$.

Hence for any $d \mid n$, the number of fractions with denominator d is $\varphi(d)$, since for all such fractions the numerators are the elements of $\mathbb{Z}_d^*$. Therefore we have $\sum\limits_{d|n} \varphi(d) = n$. □

Now define for d such that $d \mid p-1$, $S_d = \{a \in \mathbb{Z}_p^* \mid ord(a) = d\}$. Then we have the following lemma:

Lemma 2. $|S_d| = \varphi(d)$

Proof: First we will show that $|S_d| \in \{0, \varphi(d)\}$ then we will show that $|S_d| = \varphi(d)$. Now if $|S_d| \neq 0$ then $\exists\ a \in S_d$ such that $ord(a) = d$. Then consider the polynomial $x^d - 1$ over $\mathbb{F}_p$. $1, a, a^2, \dots, a^{p-1}$ are its distinct roots. Since the degree is d these are the only roots of the polynomial. Now a^k has order $\frac{d}{gcd(d,k)}$. Then the elements which has order d are a^k where $gcd(k, d) = 1$. Hence there are $\varphi(d)$ many powers of a which has order d. Therefore $|S_d| \in \{0, \varphi(d)\}$.

Now we have by Lemma 1

$$\sum_{d|p-1} \varphi(d) = p - 1$$

Now $\{S_d : d \mid p-1\}$ is a partition of $\mathbb{Z}_p^*$. Therefore $\sum\limits_{d|p-1} |S_d| = p - 1$. Hence

$$p - 1 = \sum_{d|p-1} |S_d| \leq \sum_{d|p-1} \varphi(d) = p - 1 \iff |S_d| = \varphi(d)\ \forall\ d \text{ such that } d \mid p-1$$

□

Hence the number of elements in $\mathbb{Z}_p^*$ which has order d such that $d \mid p - 1$

Now we will introduce another definition. Let H be a group. Then Exponent of H is the smallest number n such that $\forall a \in H$, $a^n = 1$. Now we will show that every finite abelian group has an element which has the order to be exponent of the group. Then we will show that $\mathbb{Z}_p^*$ has exponent $p - 1$. With that we can say $\mathbb{Z}_p^*$ has an element which has order $p - 1$. Therefore $\mathbb{Z}_p^*$ is cyclic since $|\mathbb{Z}_p^*| = p - 1$ because $\mathbb{Z}_p^*$ is a finite abelian group.

Lemma 3. *If G is a finite abelian group with exponent n then $\exists\ g \in G$ such that $ord(g) = n$.*

Proof: By structure theorem we have

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$$

where $q_1, \ldots, q_m$ are primes powers. Now $\forall\ g \in G$, $ord(g) \mid lcm(q_1, \ldots, q_m)$. The element in $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_m}$, $(1, 1, \ldots, 1)$ has order $lcm(q_1, \ldots, q_m)$. So the exponent of G is $lcm(q_1, \ldots, q_m)$ and the corresponding element of $(1, \ldots, 1)$ has order $lcm(q_1, \ldots, q_m)$. □

Lemma 4. *$\mathbb{Z}_p^*$ has exponent $p-1$.*

Proof: Over $\mathbb{F}_p$ the equation $x^{p-1}-1$ has $p-1$ roots which are all the elements of $\mathbb{Z}_p^*$. There does not exists any polynomial of lower degree which satisfies this property. Hence the exponent of $\mathbb{Z}_p^*$ is $p-1$. □

Therefore there exists an element of $\mathbb{Z}_p^*$ which has order $p-1$. Therefore the group $\mathbb{Z}_p^*$ is cyclic.

Case 2: $e = 2$

Lemma 5. *Let g be generator of the group $\mathbb{Z}_p^*$. Then either g or $g+p$ is generator for $\mathbb{Z}_{p^2}^*$.*

Proof: We have $|\mathbb{Z}_{p^2}^*|\varphi(p^2) = p(p-1)$. Let g has order m in $\mathbb{Z}_{p^2}^*$. Then $g^p \equiv 1 \bmod p$. Hence $p-1 \mid m$. Therefore $m = p(p-1)$ or $m = p-1$ since $m \mid p(p-1)$. If its the first case then we are done. For the later take the element $g+p$. Again let its order is m'. Then $(g+p)^{m'} \equiv 1 \bmod p$. So $p-1 \mid m'$. Hence m' can be either $p-1$ or $p(p-1)$. If it is also $p-1$ then we have

$$\begin{aligned} 1 \equiv (g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p + p^2(\cdots) \bmod p^2 \\ &\equiv g^{p-1} + p(p-1)g^{p-2} \bmod p^2 \\ &\equiv 1 + p(p-1)g^{p-2} \bmod p^2 \end{aligned}$$

Therefore

$$p(p-1)g^{p-2} \equiv 0 \bmod p^2 \iff p \mid (p-1)g^{p-2}$$

which is not possible since $gcd(p, p-1) = 1$ and $gcd(p, g) = 1$. Contradiction. Hence at least one of g and $g+p$ has order $p(p-1)$. □

With this lemma we have an element of $\mathbb{Z}_{p^2}^*$ which has order $p(p-1) = |\mathbb{Z}_{p^2}^*|$. So $\mathbb{Z}_{p^2}^*$ is cyclic.

Case 3: $e > 2$

Lemma 6. $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$

Proof:

$$\begin{aligned} (1+p)^{p^k} &\equiv ((1+p)^p)^{p^{k-1}} \\ &\equiv \left(1 + p^2 + \binom{p}{2}p^2\right)^{p^{k-1}} \bmod p^{k+2} \\ &\equiv 1 + p^2 \times p^{k-1} \bmod p^{k+2} \\ &\equiv 1 + p^{k+1} \bmod p^{k+2} \end{aligned}$$

□

Therefore

$$(1+p)^{p^{k+1}} \equiv (1+p^{k+1})^p \equiv 1 + p \times p^{k+1} \equiv 1 + p^{k+2} \equiv 1 \bmod p^{k+2}$$

Hence $(1+p)$ has order p^{k+1} in $\mathbb{Z}^*_{p^{k+2}}$. Or we can say $1+p$ has order p^{e-1} is $\mathbb{Z}^*_{p^e}$.

Let g be the generator of $\mathbb{Z}^*_p$. Then let the order of g in $\mathbb{Z}^*_{p^e}$ is m. Then $p-1 \mid m$. So g has order $p^k(p-1)$. Therefore the number $g(1+p) \bmod p^e$ has order $p^{e-1}(1-p) = \varphi(p^e)$. Therefore $\mathbb{Z}^*_{p^e}$ is a cyclic group.

□

Problem 2 Problem Set 1: P6

Let $N = p_1 p_2 \cdots p_k$ be a Carmichael number and p_i's are primes. In class we have seen that given N as input, a single pass of Miller-Robin primality test outputs a nontrivial factor of N with probability $\geq \frac{1}{2}$. We can do a finer calculation and get better success probability. Show that a single pass of Miller-Robin primality test outputs a nontrivial factor of N with probability $1 - \frac{1}{2^{k-1}}$.

Solution: Let ϕ be the isomorphism of

$$\mathbb{Z}^*_N \cong \mathbb{Z}^*_{p_1} \times \cdots \times \mathbb{Z}^*_{p_k}$$

Now suppose $N-1 = 2^v m$ where m is odd. Let $a \in \{2,\dots,N-2\}$ Let l_a be the minimum such that $a^{2^{l_a+1}m} \bmod N \equiv 1$. Surely for all a, $l_a > 0$ and $l_a \leq N-1$ Now take $l = \max\{l_a \mid a \in \{2,\dots,N-2\}\}$. Therefore $l > 0$ and $l \leq N-1$. For all $k < l$ there exists $a \in \{2,\dots,N-2\}$ such that $a^{2^{k+1}m} \not\equiv 1 \bmod N$.

Now consider the group

$$G_N = \{a \in \mathbb{Z}^*_N \mid a^{2^l m} \equiv \pm 1 \bmod N\}$$

Now there exists at least one $\tilde{a}$ such that $\tilde{a}^{2^l m} \equiv -1 \bmod N$ since otherwise for all $a \in \{2,\dots N-2\}$, $l_a \leq l-1$. Then $\max\{l_a \mid a \in \{2,\dots,N-2\}\} \leq l-1$ which contradicts that the value we got is l. Hence there exist a $\tilde{a} \in \mathbb{Z}^*_N$ such that $\tilde{a}^{2^l m} \equiv -1 \bmod N$.

Now $\phi(\tilde{a}^{2^l m}) = (-1,\dots,-1)$. Suppose $\phi(\tilde{a}) = (\tilde{a}_1,\dots,\tilde{a}_k)$. Then we have

$$\forall\, i \in [k],\ \tilde{a}_i^{2^l m} \equiv -1 \bmod p_i$$

Now for any $i \in [k]$ the corresponding element in $\mathbb{Z}^*_N$ of $(1,\dots,1,\tilde{a}_i,1,\dots,1)$ denote by g. Then $g^{2^l m} \not\equiv -1 \bmod N$. There are k many slots here and in each slot we have 2 options 1 or $\tilde{a}_i$. Hence with above like construction we can have at most 2^k many elements. Among these the elements $(1,\dots,1)$ and $(\tilde{a}_1,\dots,\tilde{a}_k)$ are in G_N. All the other elements remain in distict cosets of G_N in $\mathbb{Z}^*_N/G_N$. Hence

$$Pr_{a \in_R \mathbb{Z}^*_N}[a \in \mathbb{Z}^*_N - G_N] \geq \frac{2^k - 2}{2^k} = 1 - \frac{1}{2^{k-1}}$$

Hence

$$Pr[\text{Primality Test outputs a nontrivial factor of } N] \geq 1 - \frac{1}{2^{k-1}}$$

□

Problem 3 Problem Set 1: P7

Design a randomized polynomial time algorithm such that given N and $\varphi(N)$ as inputs, it outputs a nontrivial factor of N with probability at least $\frac{1}{2}$, where $\varphi(\cdot)$ is the Euler's totient function

Solution: We first run Miler-Robin Test. If it outputs prime then we output that. Otherwise if it outputs a factor we also output that. If it outputs 'Composite' then we do the following:

Let $\varphi(N) = 2^s t(p-1)$ where $p \mid N$ and t is odd. If a is a non quadratic residue then

$$a^{\frac{\varphi(N)}{2^{s+1}}} \bmod N \equiv \left[a^{\frac{p-1}{2}}\right]^t \bmod p \equiv -1 \bmod p$$

Let for p_i the corresponding s, t are denoted by s_i, t_i. WLOG assume $s_1 \geq s_2 \geq \cdots \geq s_k$. Then if a is a Non-Quadratic Residue wrt p_1 and Quadratic Residue wrt p_2 then

$$a^{\frac{\phi(N)}{2^{s_1+1}}} \bmod N \equiv \left[a^{\frac{p_1-1}{2}}\right]^{t_1} \bmod p_1 \equiv -1 \bmod N \text{ but } \left[a^{\frac{\phi(N)}{2^{s_2+1}}}\right]^{2^{s_2-s_1}} \bmod p_1 \equiv \left[a^{\frac{p_2-1}{2}}\right]^{2^{s_2-s_1}\cdot t_1} \bmod p_2 \equiv 1 \bmod p_2$$

Hence

$$a^{\frac{\varphi(N)}{2^{s_1+1}}} \not\equiv \pm 1 \bmod N$$

Now probability that any number is Non-Quadratic Residue modulo p_1 but Quadratic residue modulo p_2 is $\frac{1}{4}$. Therefore $a^{\frac{\varphi N}{2^{t_1+1}}}$ has a common factor p_1 with N but N does not divides it.

Therefore in the algorithm if the Miller Robin test returns 'Composite' then we will take a random $a \in \{2, \ldots, N-2\}$ then we will compute lowest number l such that $\left[a^{\frac{\phi(N)}{2^{l+1}}}\right]^m \equiv 1 \bmod N$ where m is odd and $\phi(N) = 2^k \cdot m$ then we will take $gcd\left(\left[a^{\frac{\phi(N)}{2^{l+1}}}\right]^m, N\right)$. This will return a nontrivial factor of N. We will do this procedure 3 times if the gcd returned is 1. And after 3 times gcd returned 1 we will output prime.

Hence this procedure fails to give a nontrivial factor is $1 - \left(1 - \frac{1}{4}\right)^3 = 1 - \frac{27}{64} > \frac{1}{2}$.

□

Problem 4 Problem Set 1: P13

Design a deterministic polynomial time algorithm to compute the gcd of two univariate polynomials using resultants and linear system solving.

Solution: Let $p, q \in \mathbb{F}[x]$ where $\deg p = m$ and $\deg q = n$. The Sylvester matrix generated by p, q is $S_{p,q}$. Let for any $k \in \mathbb{N}$, $\mathbb{F}_k := \{f \in \mathbb{F}[x] \mid \deg f < k\}$. Then for $(u, v) \in \mathbb{F}_n \times \mathbb{F}_m$, $S_{p,q}(u, v) = up + vq$.

Let $gcd(p, q) = h$ and $\deg h = d$.

Lemma 7. $\dim \ker S_{p,q} = \deg gcd(p, q)$

Proof: Let $(x, y) \in \ker S_{p,q}$. Then $px + qy = 0$. Now denote $p = hp_0$ and $q = hq_0$. Hence $gcd(p_0, q_0) = 1$. Therefore

$$px + qy = 0 \iff p_0x + q_0y = 0 \iff p_0x = -q_0y$$

Therefore $q_0 \mid x$ and $p_0 \mid y$. So let $x = q_0g_x$ and $y = p_0g_y$. Then

$$p_0x + q_0y = 0 \iff p_0q_0g_x + q_0p_0g_y = 0 \iff p_0q_0(g_x + g_y) = 0 \iff g_x = -g_y$$

So denote $g = g_x = -g_y$. So $x = q_0g$, $y = -p_0g$. Now

$$\deg x < \deg q \iff \deg q_0 + \deg g < \deg q_0 + \deg h \iff \deg g < \deg h$$

Hence for each $(x, y) \in |S\rangle_{p,q}$ there exists unique $g \in \mathbb{F}_d$ such that $x = q_0g$ and $y = -p_0g$ and also for each $g \in \mathbb{F}_d$ we have $x = q_0g$ and $y = -p_0g$ such that $px + qy = 0$. Hence there exists a bijection $\mathbb{F}_d \cong \ker S_{p,q}$ by $g \mapsto (q_0g, -p_0g)$ □

Therefore by Rank-Nullity Theorem

$$\operatorname{rank}(S_{p,q}) + \dim \ker S_{p,q} = m + n$$

Therefore $\operatorname{rank}(S_{p,q}) = m + n - d$. Hence the last d rows of the row echelon form of the $S_{p,q}^T$ are zeros. Let $(S_{p,q}^T)^*$ denote the row echelon form of $S_{p,q}^T$. Let e_i denote the ith row of $(S_{p,q}^T)^*$. Hence the last nonzero row of $(S_{p,q}^T)^*$ is

e_{m+n-d}. We have $\deg e_{m+n-d} \leq d$. Now for $i \in [n]$ the ith row of $S_{p,q}^T$ is just $x^{n-i}p$ and for $n+1 \leq j \leq n+m$ the jth row is $x^{m+n-j}q$. Hence

$$e_{m+n-d} = \sum_{i=1}^{n} \alpha_i x^{n-i} p + \sum_{i=n+1}^{m+n} \alpha_i x^{m+n-i} q$$

The LHS has degree $\leq d$ and the RHS is divisible by h since $h \mid p$ and $h \mid q$. Hence $h = e_{m+n-d}$ up to some unit multiplication. Therefore we can say e_{m+n-d} is the gcd of p, q. Therefore the algorithm will be

Algorithm:

Step 1 Construct $S_{p,q}$

Step 2 Find Row Echelon Form of $S_{p,q}^T$ by Gaussian Elimination

Step 3 Output the last nonzero row

□

Problem 5 Problem Set 1: P14

Give a polynomial time algorithm to compute the gcd of two bivariate polynomials, without using bivariate factorization.

Solution:

Lemma 8. *Let R be an Euclidean Domain. Let $p \in R$ be a prime and $f, g \in R[x]$ be nonzero. Let $h = gcd(f, g) \in R[x]$. Denote $\overline{f} = f \bmod p$ and $\overline{g} = g \bmod p$ and $d = \deg h$ and $\alpha = lc(h)$. Assume $p \nmid b = gcd(lc(f), lc(g)) \in R$ and $\overline{d} = \deg gcd(\overline{f}, \overline{g})$. Then*

1. $\alpha \mid b$
2. $\overline{d} \geq d$
3. $d = \overline{d} \iff \overline{\alpha} \cdot gcd(\overline{f}, \overline{g}) = \overline{h} \iff p \nmid \operatorname{Res}\left(\frac{f}{h}, \frac{g}{h}\right)$

Proof:

1. Now h divides both f, g. Therefore $lc(h)$ divides both $lc(f)$ and $lc(g)$ in R. Hence $\alpha \mid b$
2. Let $u = \frac{f}{h}$ and $v = \frac{g}{h}$. Since $p \nmid b \implies p \nmid lc(h)$. Hence $\deg h = \deg \overline{h} = d$. Now
$$\overline{u}\overline{h} = \overline{f} \text{ and } \overline{v}\overline{h} = \overline{g}$$
Hence $\overline{h} \mid \overline{f}$ and $\overline{h} \mid \overline{g} \implies \overline{h} \mid gcd(\overline{f}, \overline{g})$. Therefore $\deg gcd(\overline{f}, \overline{g}) \geq \deg \overline{h} \implies \overline{d} \geq d$.
3. $d = \overline{d} \iff \deg \overline{h} = \deg gcd(\overline{f}, \overline{g})$. Now $p \nmid b$ and $\alpha \mid b$ so $p \nmid \alpha$. Hence α is a unit in $R/\langle p \rangle$ as $R/\langle p \rangle$ is a field. In a field gcd is always taken to be monic. Now $\overline{\alpha} = lc(\overline{h})$. Since $\deg \overline{h} = \deg gcd(\overline{f}, \overline{g})$ we can say $\overline{h} = u \cdot gcd(\overline{f}, \overline{g})$ for some unit $u \in R/\langle p \rangle$. Now since $gcd(\overline{f}, \overline{g})$ is monic we have $u = \overline{\alpha}$ Therefore $d = \overline{d} \implies \overline{\alpha} \cdot gcd(\overline{f}, \overline{g}) = \overline{h}$. Other direction obviously becomes true as $\overline{\alpha}$ is a unit in $R/\langle p \rangle$.

   Now $p \nmid b \implies p$ divides at most one of $lc(u)$ or $lc(v)$. WLOG assume $p \nmid lc(u)$. We know
$$p \mid \operatorname{Res}(u, v) \iff gcd(\overline{u}, \overline{v}) \neq 1 \text{ in } R/\langle p \rangle$$
   So
$$\begin{aligned} gcd(\overline{f}, \overline{g}) = gcd(\overline{u}, \overline{v}) \cdot \frac{\overline{h}}{\overline{\alpha}} &\iff \overline{\alpha} gcd(\overline{f}, \overline{g}) = gcd(\overline{u}, \overline{v}) \overline{h} \\ &\iff \overline{h} = gcd(\overline{u}, \overline{v}) \overline{h} \\ &\iff gcd(\overline{u}, \overline{v}) = 1 \\ &\iff p \nmid \operatorname{Res}(\overline{u}, \overline{v}) \\ &\iff p \nmid \operatorname{Res}(u, v) \end{aligned}$$

□

Algorithm 1: Modular Bivariate GCD Algorithm

Input:

1. Primitive Polynomials $f, g \in \mathbb{F}[x,y] = R[x]$
2. $\deg_x f = n \geq \deg_x g \geq 1$
3. $\deg_y f, \deg_y g \leq d$

Output: $h = gcd(f,g) \in \mathbb{F}[x,y]$

1 **begin**

2 $b \longleftarrow gcd(lc(f), lc(g))$, $FAIL \longleftarrow 1$

3 **while** $FAIL$ **do**

4 Choose a random monic irreducible polynomial $p \in \mathbb{F}[y]$ with $\deg p = d + 1 + \deg b$

5 $\overline{f} \longleftarrow f \bmod p$, $\overline{g} \longleftarrow g \bmod p$

6 Use Extended Euclidean Algorithm over $\mathbb{F}[y]/\langle p \rangle$ on $\overline{f}$ and $\overline{g}$ to compute the monic $v \in R/\langle p \rangle$

7 Compute $w, f', g' \in R[x]$ with $\deg_y w, \deg_y f', \deg_y g' < \deg p$ such that:

$$w \equiv bv \bmod p \qquad f'w \equiv bf \bmod p \qquad g'w \equiv bg \bmod p$$

8 **if** $\deg_y(f'w) = \deg_y(bf)$ *and* $\deg_y(g'w) = \deg(bg)$ **then**

9 $FAIL \longleftarrow 0$

10 **return** *premitive part of* w *w.r.t* x

Now in $\mathbb{F}[x,y]$ let $gcd(f,g) = h$ and $r = \mathrm{Res}_x\left(\frac{f}{h}, \frac{g}{h}\right) \in \mathbb{F}[y]$. Now $\deg_y b < \deg_y p = \deg p$ and hence $p \nmid b$. Assume $p \nmid r$ then by Lemma 8 we have $\alpha \cdot v \equiv h \bmod p$ and $\alpha \mid b$. Therefore

$$w \equiv bv \equiv \left(\frac{b}{\alpha}\right) h \bmod p$$

Now primitive part of w=premitive part of $\left(\frac{b}{\alpha}\right)h$=$h$. Hence correct result is returned.

Now if $p \mid r$ then by Lemma 8 we have $\deg_x gcd(\overline{f}, \overline{g}) > \deg_x h$. If the degree conditions in step 8 are satisfied then the congruences in step 7 would be equalities and the primitive part of w will be a common divisor of f and g of higher degree than $\deg_x h$. Contradiction. So the degree condtions will not be satisfied.

□