Putnam Seminar: Number Theory

November 18, 2020

Here is a question from Putnam 2012 B6:

Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.

Solution 1. **Step 1.** Problem reduction. Since π is defined in terms of power, we only care about the multiplicative structure of $\mathbb{F}_p$, i.e., we only need to focus on $\mathbb{F}_p^\times = \mathbb{Z}/(p-1)$. In this sense, π can be viewed as a permutation on $\mathbb{Z}/(p-1)$ given by $\pi(x) = 3x$. This is much simpler: now π is only a linear function.

Step 2. Cycle types in π. Every cycle in π has the form

$$a \to 3a \to 3^2 a \to \cdots \to 3^r a = a.$$

From this we see that

- For each a, the length of cycle containing a is the smallest positive integer r such that $p-1 \mid (3^r-1)a$. r only depends on $\gcd(a, p-1)$.
- Hence, for any $d \mid p-1$, consider the set of elements a for which $\gcd(a, p-1) = d$: there are $\varphi(\frac{p-1}{d})$ such elements; they are partitioned into cycles of equal length, call it $f(\frac{p-1}{d})$. $f(d)$ is the smallest positive integer such that $3^{f(d)} \equiv 1 \pmod d$.

As a result, π is the permutation consisting of the following cycles: for each $d \mid p-1$, there are $\varphi(d)/f(d)$ number of cycles of length $f(d)$, and the sign of π is

$$\sum_{d : d \mid p-1, 2 \mid f(d)} \varphi(d)/f(d) \pmod 2. \quad (*)$$

Step 3. Analysis of cycle types. Suppose $d = 2^m d_0$, where d_0 is odd. By exponential lifting lemma,

$$3^r \equiv 1 \pmod{2^m} \iff r \in \begin{cases} \mathbb{Z}, & \text{if } m = 1, \\ 2\mathbb{Z}, & \text{if } m = 2, 3, \\ 2^{m-2}\mathbb{Z}, & \text{if } m \geq 3. \end{cases}$$

so

$$f(d)=f(2^m d_0)=\begin{cases} f(d_0), & \text{if } m=0,1\\ \operatorname{lcm}(f(d_0),2), & \text{if } m=2,3,\\ \operatorname{lcm}(f(d_0),2^{m-2}), & \text{if } m\ge 3.\end{cases}$$

Case 1. $p\equiv 3 \pmod 4$. Then for each odd $d\mid p-1$, we have

$$f(2d)=f(d),\varphi(2d)=\varphi(d).$$

By paring d and $2d$ together in $(*)$, we get that $\operatorname{sign}(\pi)=0$.

Case 2. $p\equiv 1 \pmod 4$. Then for each odd $d\mid p-1$, we can still pair d and $2d$. It suffices to consider d for which $4\mid d\mid p-1$. Suppose $d=2^m d_0$,$m\ge 2$. Then

$$\frac{\varphi(d)}{f(d)}=\frac{2^{m-1}\varphi(d_0)}{\operatorname{lcm}(f(d_0),2^{??})}=\begin{cases}\frac{\varphi(d_0)}{f(d_0)}\gcd(f(d_0),2), & \text{if } m=2,\\ 2\frac{\varphi(d_0)}{f(d_0)}\gcd(f(d_0),2^{m-2}), & \text{if } m\ge 3.\end{cases}$$

If $\frac{\varphi(d)}{f(d)}$ is odd, then $m=2$, $f(d_0)$ is odd and $\varphi(d_0)$ is odd. But this only holds if $d_0=1$ and $d=4$. Therefore, π is an odd permutation.

□

Exercise: an explanation of the step

$$3^r\equiv 1 \pmod{2^m} \iff r\in\begin{cases}2^{m-1}\mathbb{Z}, & \text{if } m=1,2,\\ 2^{m-2}\mathbb{Z}, & \text{if } m\ge 3.\end{cases}$$

Note that r is the order of 3 in the group of coprime residues mod 2^m: this is the group

$$(\mathbb{Z}/2^m\mathbb{Z})^\times\cong\begin{cases}\mathbb{Z}/2^{m-1}\mathbb{Z}, \text{ if } m=1,2,\\ (\mathbb{Z}/2)\times(\mathbb{Z}/2^{m-2}\mathbb{Z}), \text{ if } m\ge 3.\end{cases}$$

Thus, r is a power of 2. Furthermore, for $n\ge 1$,

$$v_2(3^{2^n}-1)=v_2((3-1)(3+1)(3^2+1)\cdots(3^{2^{n-1}}+1))=n+2.$$

Solution 2. Note that the sign of π is

$$\prod_{0\le x<y<p}\frac{\pi(x)-\pi(y)}{x-y}\equiv\prod_{0\le x<y<p}(x^2+xy+y^2) \pmod p.$$

Lemma 0.1. *Let* $p\equiv 2 \pmod 3$. *For each* $c\ne 0$, *the number of solutions of*

$$x^2+xy+y^2\equiv c \pmod p$$

is $p+1$.

Proof of Lemma. Note that $4x^2 + 4xy + 4y^2 = (2x + y)^2 + 3y^2$. After change of variables, it suffices to count the number of solutions of

$$x^2 + 3y^2 \equiv c \pmod{p}.$$

Key observation: the number of solutions depends only on the quadratic residue type of c.

- $c = 0$. Since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1$, $(x, y) = (0, 0)$ is the only solution.
- c is a quadratic residue. We can take $c = 1$. Then the number of solution is

$$\begin{aligned}\sum_{x\in\mathbb{F}_p} 1 + \left(\frac{(1-x^2)3^{-1}}{p}\right) &= p - \sum_{x\in\mathbb{F}_p} \left(\frac{x-1}{p}\right)\left(\frac{x+1}{p}\right) \\ &= p - \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)\left(\frac{x+2}{p}\right) = p + 1.\end{aligned}$$

- c is a non quadratic residue. There are $\frac{p-1}{2}$ of them.

□

By symmetry, the number of solutions ($c \neq 0$)

$$x^2 + xy + y^2 \equiv c \pmod{p}$$

restricting to $0 \leq x < y < p$ is

$$\frac{1}{2}\left(p - \left(\frac{3^{-1}c}{p}\right)\right) = \frac{1}{2}\left(p + \left(\frac{-c}{p}\right)\right).$$

This gives

$$\prod_{0\leq x<y<p} (x^2 + xy + y^2) = \prod_{c=1}^{p-1} c^{\frac{1}{2}\left(p+\left(\frac{-c}{p}\right)\right)}.$$

There are two cases:

- $p \equiv 1 \pmod{4}$. Since $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$, we can parametrize $c = g^m$ with $m = 1, 2, \ldots, p-1$. This reduces to an explicit computation.
- $p \equiv 3 \pmod{4}$. Verify yourself.

□

How can we generalize this problem?

1. Change $\pi(x)$ to, for example, $\pi(x) \equiv x^5 \pmod p$, where $5 \nmid p-1$. In this case, we need to consider

$$\sum_{d:d|p-1, 2|f(d)} \varphi(d)/f_5(d) \pmod 2.$$

Note that

$$5^r \equiv 1 \pmod{2^m} \Longleftrightarrow r \in \begin{cases} \mathbb{Z}, & \text{if } m = 1, 2, \\ 2^{m-2}\mathbb{Z}, & \text{if } m \geq 3. \end{cases}$$

Therefore, for odd d,

$$f_5(d) = f_5(2d) = f_5(4d), f_5(2^n d) = \operatorname{lcm}(f_5(d), 2^{n-2}), n \geq 3.$$

By pairing d and $2d$ when d is odd, we only need to consider d with $4 \mid d \mid p-1$. But in this case we have

$$\frac{\varphi(d)}{f_5(d)} = \begin{cases} 2\frac{\varphi(d_0)}{f_5(d_0)}, \text{ if } n = 2, \\ 2\frac{\varphi(d_0)}{f_5(d_0)} \gcd(2^{n-2}, f_5(d_0)), \text{ if } n \geq 3 \end{cases}$$

is even. So π is always an even permutation.

2. (A generalization of 1). Change $\pi(x)$ to $\pi(x) \equiv x^k \mod p$, where $\gcd(k, p-1) = 1$. In this case, we need to consider the order of k mod 2^m. This is:

$$k^r \equiv 1 \pmod{2^m} \Longleftrightarrow r \in \begin{cases} \mathbb{Z}, & \text{if } m \leq v_2(k-1), \\ 2\mathbb{Z}, & \text{if } v_2(k-1) < m \leq v_2(k^2-1), \\ 2^{m-v_2(k^2-1)+1}\mathbb{Z}, & \text{if } m > v_2(k^2-1) \end{cases}$$

3. Change p to any integer n such that $3 \nmid n$. Ex. $n = p^m$. Then we only care about $(\mathbb{Z}/p^m)^\times = \mathbb{Z}/(p^{m-1}(p-1))$.

4. Change p to other finite fields, ex. $\mathbb{F}_{p^2}$? This is essentially the same: we only care about the multiplicative group $(\mathbb{F}_{p^2})^\times = \mathbb{Z}/(p^2-1)$

5. If π has a multiplicative formula, then it only depends on the multiplicative structure and under this multiplicative structure π can be viewed as a group automorphism (isomorphism with itself). So the question we can ask is: given a finite group G and an automorphism π of G, what can we say about π as a permutation?

6. Change even permutation to something else?

7. For a fixed prime p, what is the set of polynomials $f(x)$ such that $f(a) \equiv f(b) \pmod p$ if and only if $a \equiv b \pmod p$?