Submission for DHW-GRF

OTIS (internal use)

YOUR NAME HERE

December 28, 2024

> **Example** (Romania TST 2015/2/1, 0♣)**.** Let a and n be integers with $n \geq 1$. Show that n divides
> $$\sum_{k=1}^{n} a^{\gcd(k,n)}.$$

15ROUTST21

Walkthrough. Assume $a > 0$. Consider the following question:

> Given a necklace of n beads, and each could be one of a colors, what is the number of distinct necklaces (up to rotation) that can be formed?

We will apply Burnside lemma to compute this number.

(a) Describe a group action of $G = \mathbb{Z}/n\mathbb{Z}$ on the set of a^n necklaces (before modding out by rotation), so the question above asks for the number of orbits of G on the set of a^n necklaces.

(b) Fix $k \in G = \mathbb{Z}/n\mathbb{Z}$. Find, as a function of a, k, n, the size of the stabilizer of k.

(c) Use Burnside lemma to show the answer to the counting question is
$$\frac{1}{n} \sum_{k} a^{\gcd(k,n)}.$$

(d) Conclude the desired result.

> **Example** (HMMT 2017 A9, 0♣)**.** What is the period of the Fibonacci sequence modulo 127?

17HMMTA9

Walkthrough. In what follows let $p = 127$. Our hope is to use the Fibonacci formula
$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Unfortunately:

(a) Show that $(5/p) = -1$. Thus we cannot find $\alpha, \beta \in \mathbb{F}_p$.

The idea is that we need to instead work in the so-called finite field

$$\mathbb{F}_{p^2} \coloneqq \mathbb{F}_p[\sqrt{5}] = \left\{ a + b\sqrt{5} \mid a, b \in \mathbb{F}_p \right\}.$$

I'll explain the reason for the notation $\mathbb{F}_{p^2}$ later, but for not, just think of it as that field $a + b\sqrt{5}$. Note that this field $\mathbb{F}_{p^2}$ still has a copy of $\mathbb{F}_p$ inside it, namely the numbers of the form $a = a + 0\sqrt{5}$. They still behave as we expect, for example, $a^p \equiv a \pmod{p}$ since $p \mid a^p - a$.

(b) Convince yourself this really is a field. How many elements does it have?

(c) Show that $x^{p^2-1} = 1$ for any nonzero $x \in \mathbb{F}_{p^2}$. (This is the analog of Fermat's little theorem.)

Now we take advantage of the fact that $\alpha, \beta \in \mathbb{F}_{p^2}$.

(d) Consider the so-called Frobenius endomorphism

$$\sigma \colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2} \qquad \sigma(t) = t^p.$$

Determine its fixed points. (Hint: you should already know the roots of $X^p - X$.)

(e) Deduce that $\sigma(\alpha) = \alpha^p \neq \alpha$.

(f) Prove that $\sigma(x + y) = \sigma(x) + \sigma(y)$ by using the binomial theorem, and also that $\sigma(xy) = \sigma(x)\sigma(y)$. Thus the Frobenius endomorphism deserves its name.

(g) Consider the polynomial

$$P(X) = X^2 - X - 1.$$

Prove that $P(\sigma(x)) = \sigma(P(x))$ for any $x \in \mathbb{F}_{p^2}$. (Actually, this holds for any $P \in \mathbb{F}_p[X]$.)

(h) Put together (e) and (g) to deduce that $\sigma(\alpha) = \alpha^p = \beta$, by showing $\sigma(\alpha)$ is a root of P not equal to α.

(i) Find $\sigma(\beta)$.

Now we are in business: we can compute Fibonacci numbers using

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

(j) Using (h) and (i), show that $F_p \equiv -1 \pmod{p}$, $F_{p+1} \equiv 0 \pmod{p}$.

(k) Prove that $F_{2p+1} \equiv 1 \pmod{p}$ and $F_{2p+2} \equiv 0 \pmod{p}$.

(l) Conclude that the period of the Fibonacci sequence modulo p divides $2p + 2 = 256$ but not $p + 1 = 128$. Deduce the answer 256.

The solution notes contain some extended comments about the higher algebra that this problem introduces.

Practice problems

Instructions: Solve [24♣]. If you have time, solve [30♣].

> I forbid any of you from studying for your midterms! It's not a punishment; there are simply other things you should be studying first. I'm responsible, too, for having forgotten to teach them.
>
> Koro-sensei in *Assassination Classroom*, Season 2, Episode 6

Required Problem 1 (9♣)

Write the blog post described in the previous section. Also specify whether you would want your post to be added to the running list above.

No PUID

Problem 2 (Napkin 4B, 2♣)

Prove that the rings $\mathbb{C}[x]/(x^2 - x)$ and $\mathbb{C} \times \mathbb{C}$ are isomorphic.

NAP4B

Let $I = x^2 - x$ in $\mathbb{C}[x]$. The cosets of I are given by $(ax + b)I$ where $a, b \in \mathbb{C}$.

Required Problem 3 (Napkin 5D, 3♣)

Let R be an integral domain with finitely many elements. Prove that R is a field.

NAP5D

Let $r \in R$ be nonzero. Consider the map $\phi : R \to R$ given by $x \to rx$.

We claim this map is injective. Indeed, if $rx = ry$, then $r(x - y) = 0$, and since $r \neq 0$, we have $x = y$.

Since R is finite, this map must also be bijective. So, there is some x such that $rx = 1$. This is the multiplicative inverse of r.

Since every nonzero element has a multiplicative inverse, R is a field.

Problem 4 (Burnside's lemma, 3♣)

Let G be a finite group which acts on a finite set X. For each $g \in G$, let $\operatorname{FixPt} g$ denote the set of $x \in X$ for which $g \cdot x = x$. Prove that the number of orbits of this action is given exactly by $\frac{1}{|G|} \sum_{g \in G} \operatorname{FixPt} g$.

Z33FA3B5

We count ordered pairs (g, x) such that $g \cdot x = x$ in two ways. First, it is equal to $\sum_{g \in G} \operatorname{FixPt} g$. It is also the sum of the sizes of the stabilizers, which we can write as

$$\sum_{x \in X} |\operatorname{stab}(x)| = \sum_{x \in X} \frac{|G|}{|\operatorname{orb}(x)|} = |G| \sum_{x \in X} \frac{1}{|\operatorname{orb}(x)|}.$$

But, notice that $\sum_{x \in X} \frac{1}{|\operatorname{orb}(x)|}$ just counts the number of orbits, giving us the result.

Problem 5 (Napkin 4G; also USA TST 2016/3, 3♣)

Define $\Psi\colon \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ by

$$\Psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i x^{p^i}.$$

Let S denote the image of Ψ.

(a) Show that S is a ring with addition given by polynomial addition, and multiplication given by *function composition*.

(b) Prove that $\Psi\colon \mathbb{F}_p[x] \to S$ is then a ring isomorphism.

NAP4G

Problem 6 (Napkin 5G, 3♣)

How many prime ideals of the ring $R = \mathbb{Z}[\sqrt{2017}]$ are *not* maximal ideals?

NAP5G

Problem 7 (Napkin 1G, 5♣)

Find the smallest integer n such that the symmetric group S_n has a subgroup isomorphic to the dihedral group D_{2018} of order 2018.

NAP1G

Note that D_{2018} has an element of order 1009, namely, the smallest rotation. Since 1009 is prime, a permutation has order 1009 only when it contains cycle of length 1009. So, $n \geq 1009$.

However, $n = \boxed{1009}$ works if we consider the natural action of D_{2018} on a 1009-gon.

Problem 8 (Putnam 2009 A5, 5♣)

Is there a finite abelian group G such that the product of all the orders of its elements is 2^{2009}?

09PTNMA5

Problem 9 (Putnam 2007 A5, 5♣)

Let p be a prime. Let G be a finite group, and suppose there are exactly n elements of order p. Prove that either $n = 0$ or p divides $n + 1$.

07PTNMA5

Problem 10 (Napkin 16F, 5♣)

Does there exist a faithful transitive action of S_5 on a six-element set?

NAP16F

Problem 11 (Shortlist 2005 C5, 3♣)

There are n markers, each with one side white and the other side black. In the beginning, these n markers are aligned in a row so that their white sides are all up. In each step, if possible, we choose a marker whose white side is up (but not one of the outermost markers), remove it, and reverse the closest marker to the left of it and also reverse the closest marker to the right of it. Prove that, by a finite sequence of such steps, one can achieve a state with only two markers remaining if and only if $n - 1$ is not divisible by 3.

05SLC5

Problem 12 (PRIMES 2018 M5, 3♣)

Let G be a group with presentation given by

$$G = \left\langle a, b, c \mid ab = c^2a^4,\ bc = ca^6,\ ac = ca^8,\ c^{2018} = b^{2019} \right\rangle.$$

Determine the order of G.

18PRIMESM5

Problem 13 (PRIMES 2021 M5, 9♣)

Suppose G is a nonabelian finite group and $\varphi\colon G \to G$ a homomorphism. Denote by $0 \le k \le 1$ the fraction of elements $g \in G$ which satisfy

$$\varphi(g) = g^2.$$

Find the largest possible value of k across all nonabelian finite groups G.

21PRIMESM5