Math 25 Fall 2022

Problem Solving Exercise 1

Your name: _____

INSTRUCTIONS

You may begin the "exam" when ready.

Write your name in the space provided above.

Use of calculators is not permitted on the "exam". They are not likely to be of much help anyways.

Unless otherwise stated, you must justify your solutions to receive full credit. Work that is illegible may not be graded. Work that is scratched out will not be graded.

It is fine to leave you answer in a form such as $\ln(0.02)$ or $\sqrt{123412}$ or $(1341)^4(1231)^{-1}$. However, if an expression can be easily simplified (such as $e^{\ln(0.02)}$ or $\cos\pi$), you should simplify it.

This is not actually an exam!

The "exam" has been created with the intended length of 50 minutes. This midterm is collected at the end of the X-hour.

Good luck!

Long Answer Questions

(1) (10 points) Find a primitive element modulo 13^{100}. Justify why it is primitive.

Solution. First, we observe that 2 is a primitive element modulo 13. This is checked via the primitive element test

$$2^6 \equiv -1 \pmod{13}, \quad 2^4 \equiv 3 \pmod{13}.$$

Now, we know that $(1+13)$ has order 13^{99} modulo 13^{100} from a prior lemma, and that $2^{13^{100}}$ has order 12. Because $\gcd(12, 13) = 1$, we see that the order of $2^{13^{100}} \cdot (1+13)$ is $13^{99} \cdot 12 = \phi(13^{100})$. That is, it is a primitive element. $\square$

(2) (10 points) Find five prime divisors of $3^{10!} - 1$.

Solution. We claim $2, 5, 7, 11, 13$ are five prime divisors. Note 3 is a unit modulo each prime $p = 2, 5, 7, 11, 13$; additionally, we see $p - 1 \mid 10!$ for each p, so by Fermat's Little Theorem we have $3^{10!} \equiv 1 \pmod{p}$. $\square$

(3) (10 points) Let n, m be coprime. Prove that the map

$$\begin{array}{rccc} \psi\colon & (\mathbb{Z}/nm\mathbb{Z})^\times & \to & (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \\ & a & \mapsto & (a \bmod n,\ \ a \bmod m) \end{array}$$

is surjective. You may assume that the map is well-defined and injective.
Remark: The Corollary from Thursday only covers the case where n, m are prime powers.

Solution. Observe that the number of elements in the domain is $\phi(nm)$, and the number of elements in the codomain is $\phi(n) \times \phi(m)$. We know $\phi(nm) = \phi(n)\phi(m)$ because it is a multiplicative function.

Because ψ is injective, we see that its image has size $\phi(nm)$. In particular, its image must be everything, so it is surjective. □

(4*) (10 points) Is the following statement true:

Theorem (?)**.** *Let p be an odd prime and let k be a positive integer such that* $\gcd(p-1,k)=1$. *Then*

$$\sum_{a=0}^{p-1} a^k \equiv 0 \pmod{p}.$$

If the statement is true, provide a proof. If not, provide a counter-example.

Solution. The statement is indeed true. Let α be a primitive element modulo p. Then

$$\sum_{a=0}^{p-1} a^k = 0^k + \sum_{a=1}^{p-1} a^k = \sum_{j=1}^{p-1} (\alpha^j)^k$$

because powers of α enumerate all of the elements of $\mathbb{Z}/p\mathbb{Z}^\times$. But $\gcd(k, p-1)=1$, so α^k is also a primitive element modulo p. In other words

$$\{\alpha^{kj} : 1 \le j \le p-1\} = \mathbb{Z}/p\mathbb{Z}^\times.$$

So

$$\sum_{j=1}^{p-1} (\alpha^j)^k = \sum_{a=1}^{p-1} a.$$

Finally, using a well-known identity

$$\sum_{a=1}^{p-1} a = p \cdot \frac{p-1}{2} \equiv 0 \pmod{p}.$$

This completes the proof. □

(5*) (4 points) Let $f(x), g(x)$ be polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$. Assume that $g(x) \neq 0$. Prove that there exist polynomials $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg r(x) < \deg g(x)$, or $r(x) = 0$. (You *do not* need to show these are unique.)

Solution. Let $m = \deg(g)$ and $n = \deg(f)$. If $n < m$ then we set $q = 0, r = f$. Assume for the sake of a contradiction that there is a counter-example for some pair (f, g). Then there is a counter example with $\deg(f) = n$ minimal. Write

$$f = (a_n x^n + \ldots + a_m x^m) + a_{m-1}x^{m-1} + \ldots + a_0, \quad g = b_m x^m + h.$$

We now set $q = a_n b_m^{-1} x^{n-m}$. Observe that b_m is non-zero modulo p by definition, so it is invertible. Now

$$f - q \cdot g = (a_{n-1} - a_n b_m^{-1} b_{m-1})x^{n-1} + \text{lower order terms}.$$

This polynomial has lower degree, and can be written as $q'g + r'$. But then

$$f - qg = q'g + r' \implies f = (q + q')g + r'.$$

This contradicts that f was a counterexample! Thus the result must be true. $\square$

(This page is intentionally left blank in case you need extra space for any of the problems. **If you use this page for a particular problem, it is essential that you make a note on the page where the problem appears, indicating that your work is continued here.)**