Math 25 Fall 2022

Midterm 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.

The Honor Principle requires that you neither give nor receive any aid on this 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!

Honor statement: I have neither given nor received any help on this exam, and I attest that all of the answers are my own work.

Signature: _____

Long Answer Questions

(1) (10 points) Compute $5^{1234} \pmod{11}$.

Solution. Write $1234 = 123 \cdot 10 + 4$. By Fermat's little theorem we have

$$5^{1234} \equiv 5^{1230} \cdot 5^4 \equiv 1 \cdot (5^2)^2 \equiv 3^2 \equiv 9 \pmod{11}.$$

□

(2) (10 points) Let a, b be coprime integers. Prove that $\gcd(ab, a+b) = 1$.

Solution. Let p be a prime dividing ab, which implies that $p \mid a$ or $p \mid b$. Assume WLOG that $p \mid a$. Then p does not divide $a+b$, as otherwise

$$p \mid (a+b) - a = b$$

and $\gcd(a, b) = 1$, meaning they have no common prime divisors. In particular, ab and $a+b$ have no common prime divisors, so their gcd is 1. $\square$

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

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

is well-defined (the image of every element lies in the indicated codomain) and is injective. **Remark:** The Corollary from yesterday only covers the case where n_1, n_2 are prime powers.

Solution. To show this map is well-defined, we need to show that any unit u is sent to a pair of units. Let v be an element such that $uv \equiv 1 \pmod{nm}$. Then

$$\psi(uv) = (1, 1) = (uv \bmod n, uv \bmod m).$$

In particular, v reduces to an inverse of u modulo both n and m, so the residues of u remain units.

For injectivity, let x, y both reduce to the pair (a, b). The CRT promises a unique lift, so $x = y$. Thus this map is injective. □

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

Theorem (?)**.** *Let α be a primitive root modulo n and let* $\gcd(e, \phi(n)) = 1$*. Then α^e is a primitive root modulo n.*

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

Solution. The statement is indeed true. The gcd condition ensures that we can find a solution x to the congruence

$$ex \equiv 1 \pmod{n}.$$

Then $(\alpha^e)^x \equiv \alpha \pmod{n}$. The order d of α^e then satisfies

$$\alpha^d \equiv ((\alpha^e)^x)^d \equiv (\alpha^{ed})^x \equiv 1 \pmod{n}$$

Thus d is at least the order of α, which is $\phi(n)$. On the other hand, $d \leq \phi(n)$, which is the order of α by Euler's theorem. Thus $d = \phi(n)$ and we are done. $\square$

(5*) (4 points) Let $f(x), g(x)$ be polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$. If there exist polynomials $a(x), b(x)$ such that

$$a(x)f(x) + b(x)g(x) \equiv c(x) \pmod{p}$$

show that $f(x)$ and $g(x)$ have at most $\deg(c(x))$ roots in common. (You may assume $c(x) \neq 0$.)

Solution. Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$. Then

$$f(\alpha)a(\alpha) + g(\alpha)b(\alpha) \equiv c(\alpha) \pmod{p}.$$

In particular if $f(\alpha) = g(\alpha) \equiv 0 \pmod{p}$, then the left hand side is necessarily zero. On the other hand, $c(x)$ is a polynomial mod p, so has at most $\deg(c(x))$ roots. $\square$

(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.)**