Math 25 Fall 2022

Midterm 1 – Vindication

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) The Pell sequence is defined by the recursive formula

$$a_1 = 1, a_2 = 2, \quad a_{n+2} = 2a_{n+1} + a_n \quad n \geq 1.$$

Prove that $\gcd(a_n, a_{n+1}) = 1$ for all $n \geq 1$.

Solution. We proceed by induction. The base case $\gcd(a_1, a_2) = 1$ is clear. We assume for the sake of induction that $\gcd(a_n, a_{n+1}) = 1$. Then by Bezout we may find integers x, y so that

$$xa_n + ya_{n+1} = 1.$$

But $a_{n+2} - 2a_{n+1} = a_n$, so

$$x(a_{n+2} - 2a_{n+1}) + ya_{n+1} = xa_{n+2} + (y - 2x)a_{n+1} = 1.$$

In other words, $\gcd(a_{n+1}, a_{n+2}) \mid 1$, i.e., it *is* 1. This shows the result for n implies the result for $n + 1$, and by induction the result is true in general. □

(2) (10 points) Compute $11^{1001} \mod 101$.

Solution. Note 101 is prime, so by Fermat's little Theorem

$$11^{1001} \equiv 11^{1000} \cdot 11 \equiv 11 \mod 101.$$

□

(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 well-defined (the image of every element lies in the indicated codomain) and is injective.

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 p be an odd prime and let $a \in \mathbb{Z}$ be coprime to p. If a has order d modulo p, then a also has order d modulo p^2.*

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

Solution. The result is false. We consider $a = 4$ and $p = 3$. Then the order of $a \pmod 3$ is one, but its order modulo 9 is not 1, since $a \not\equiv 1 \pmod 9$. □

(5*) (Bonus, 4 points) Let p be a prime and let k be a positive integer. Prove that

$$\sum_{a=0}^{p-1} a^k \pmod p \equiv \begin{cases} -1 & \text{if } p-1 \mid k \\ 0 & \text{otherwise} \end{cases}.$$

The jargon for this is *orthogonality of characters*.

Solution. We first consider when $p-1 \mid k$. We write $k = (p-1)m$ and then by FLT

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

Next, when $p-1 \nmid k$, then we choose a primitive element $\alpha \in \mathbb{Z}/p\mathbb{Z}^\times$. To be in this case we must have $p > 2$, so $\alpha \not\equiv 1 \pmod p$. Then $\mathbb{Z}/p\mathbb{Z}^\times = \{1, \alpha, \dots, \alpha^{p-2}\}$, so

$$\sum_{a=0}^{p-1} a^k \equiv \sum_{j=1}^{p-2} \alpha^{kj} \equiv \frac{\alpha^{p-1} - 1}{\alpha - 1} \pmod p.$$

As noted before, the denominator is a unit modulo p, so this expression is well-defined. By FLT, the numerator is 0, so the sum is 0 modulo p as expected. □

(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.)**