Math 25 Fall 2022

Problem Solving Exercise 3

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 integers x, y, z such that $55x + 33y + 15z = 1$.

Solution. One can find the solution $(1, -18, 36)$ by inspection, but we proceed more systematically.

First, we want to solve

$$33y' + 15z' = \gcd(33, 15) = 3.$$

By XGCD we see $(y', z') = (1, -2)$.

Next we solve $55x + 3w = 1$. By whatever means we find a solution $(x, w) = 1, -18$. Thus

$$1 = 55(1) + 3(-18) = 55(1) + (33(1) + 15(-2))(-18) = 55 \cdot (1) + 33 \cdot (-18) + 15 \cdot (36).$$

□

(2) (10 points) Determine whether 42 is a quadratic residue modulo 101.

Solution. The Legendre symbol is a square detector, so we just calculate using quadratic reciprocity and properties of the symbol. (Note $101 \equiv 1 \pmod 4$, so the sign term in the reciprocity law is 1.)

$$\begin{aligned}\left(\frac{42}{101}\right) &= \left(\frac{7\cdot 6}{101}\right) \\ &= \left(\frac{7}{101}\right)\cdot\left(\frac{2}{101}\right)\cdot\left(\frac{3}{101}\right) \\ &= \left(\frac{101}{7}\right)\cdot\left(\frac{101}{3}\right)\cdot\left(\frac{2}{101}\right) \\ &= \left(\frac{3}{7}\right)\cdot\left(\frac{2}{3}\right)\cdot\left(\frac{2}{101}\right).\end{aligned}$$

Both $3, 7$ are small enough to directly enumerate the squares:

Squares mod 3:	0, 1
Squares mod 7:	0, 1, 2, 4

So $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{3}{7}\right) = -1$.

On Assignment 5, a method is provided to immediately calculate $\left(\frac{2}{101}\right)$:

$$101 \equiv 5 \pmod 8 \implies \left(\frac{2}{101}\right) = -1.$$

Alternatively, we can use trickery

$$\left(\frac{2}{101}\right) = \left(\frac{-99}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{9}{101}\right)\left(\frac{11}{101}\right).$$

Because $101 \equiv 1 \pmod 4$, $\left(\frac{-1}{101}\right) = 1$. Because 9 is a square, $\left(\frac{9}{101}\right) = 1$. Quadratic reciprocity shows that

$$\left(\frac{11}{101}\right) = \left(\frac{101}{11}\right) = \left(\frac{2}{11}\right) = \left(\frac{-9}{11}\right) = \left(\frac{9}{11}\right)\left(\frac{-1}{11}\right) = -1$$

(also, $11 \equiv 3 \mod 4$).

In total, we see

$$\left(\frac{42}{101}\right) = (-1)(-1)(-1) = -1$$

so 42 is not a square. □

(3) (10 points) Using a similar argument to Euclid's argument, prove that there are infinitely many primes congruent to 5 (mod 6). Alternatively, use whatever method you wish.

Solution. One way is to just smite the problem with Dirichlet's Theorem. However, let's proceed a different way.

We proceed via contradiction alla Euclid. Assume there are only finitely many primes $p_1, \ldots, p_k$ congruent to 5 (mod 6). Of course, 5 is a prime, so this set is non-empty. We consider

$$N := \begin{cases} p_1 \ldots p_k + 4 & k \text{ even} \\ p_1 \ldots p_k + 6 & k \text{ odd} \end{cases}.$$

In either case, $N \equiv 5 \pmod 6$ by construction (note $5 \equiv (-1) \pmod 6$).

Observe $N > 5$ and is coprime to 6, so it admits a prime factorization

$$N = \prod_{i=1}^{\ell} q_i^{e_i}$$

with q_i odd primes congruent to either $\pm 1 \pmod 6$ (i.e, $q_i \notin \{2, 3\}$). Reducing modulo 6 gives

$$-1 \equiv N \equiv \prod_{i=1}^{\ell} (\pm 1)^{e_i} \pmod 6.$$

In particular, at least one $q_i \equiv 5 \pmod 6$. So $q_i = p_j$ for some j. But then

$$p_j \mid N - p_1 \ldots p_k = 4, 6.$$

This is a contradiction, since $2, 3 \not\equiv 5 \pmod 6$. Thus, there must be infinitely many primes of the desired type. $\square$

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

Theorem (?)**.** *Let n, m be positive integers. Then*

$$\phi(nm) = \phi(n)\phi(m).$$

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

Solution. The statement is false, $\phi(4) = 2$, but $\phi(2) \cdot \phi(2) = 1$. □

(5*) (4 points) A polynomial $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is *irreducible* if $\deg f(x) > 0$ and any factorization $f(x) = a(x)b(x)$ has either $\deg a(x) = 0$ or $\deg b(x) = 0$. Prove that there are infinitely many irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$.

Solution. We once again proceed via contradiction alla Euclid. Note that any linear polynomial is irreducible. Assume that there are only finitely many irreducible polynomials $p_1, \ldots, p_k$. We now consider

$$F := p_1 p_2 \ldots p_k + 1.$$

Notice that $\deg(F) > 0$. Unique factorization for $\mathbb{Z}/p\mathbb{Z}[x]$ tells us that F is divisible by some irreducible polynomial q. Thus $q = p_i$ for some i. But then

$$p_i \mid F - p_1 p_2 \ldots p_k.$$

That is, $p_i \mid 1$. This can't happen, because $ap_i = 1$ implies $\deg(a) + \deg(p_i) = 0$, and $\deg(p_i) > 0$ by definition. Thus, we have obtained our contradiction, and so there are infinitely many irreducible polynomials. $\square$

(6**) (0 points) Define a sequence by

$$a_0 = 1, a_1 = 2, \quad a_n = 4a_{n-1} - a_{n-2} \quad n \geq 2.$$

Find an odd prime divisor of of a_{2020}.

Solution. For the sake of entertainment, the solution has been withheld. Double-star questions will not appear on the midterm. □

(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.)**