Math 25 Fall 2022

Midterm 1 – Practice

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. It is intended to be the length of a standard midterm. 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) Express 1 as an integer linear combination of 101 and 90.

Solution. We consider the transcript of the XGCD algorithm for $(101, 90)$.

q_j	r_j	$q_j r_j$	x_j	y_j
	101	—	1	0
1	90	90	0	1
8	11	88	1	-1
5	2	10	-8	9
	1	–	41	-46

Therefore, we see $101 \cdot (41) + 90 \cdot (-46) = 1 = \gcd(101, 90)$. □

(2) (10 points) Determine all solutions in $\mathbb{Z}/143\mathbb{Z}$ to the equation

$$x^2 - 56 \equiv 0 \pmod{143}.$$

Note $12^2 = 144$.

Solution. First, notice $143 = 11 \cdot 13$. We consider the system of congruences

$$x^2 \equiv 56 \equiv 1 \pmod{11}, \quad x^2 \equiv 56 \equiv 4 \pmod{13}.$$

We see that the solutions are ± 1 and ± 2, respectively. We next compute the CRT lifting map.

$$13a \equiv 1 \pmod{11}, \quad 11b \equiv 1 \pmod{13}$$

has unique solutions $a = 6, b = 6$ respectively. (Note $13 \equiv 2 \pmod{11}, 11 \equiv (-2) \pmod{13}$, so we see the solutions by inspection.)

This gives a CRT lifting map

$$(x_1, x_2) \mapsto 13 \cdot 6x_1 + 11 \cdot 6x_2 \pmod{143}.$$

The four solutions $(\pm 1, \pm 2)$ then lift to the four solutions

$$6(13 + 22), \quad 6(13 - 22), \quad 6(-13 + 22), \quad 6(-13 - 22) = 6 \cdot 35, 6(-9), 6(9), 6(-35)$$

modulo 143 by the CRT. $\square$

(3) (10 points) Let p be a prime of the form $22k+1$ and let x be a primitive element. Prove that

$$(p+1)x^{88k} + (p+2)x^{44k} + (p-3)x^{22k} + 1 \not\equiv 0 \pmod{p}$$

Solution. Since x is a primitive element, it is non-zero modulo p. Thus, by Fermat's little Theorem

$$(p+1)x^{88k} + (p+2)x^{44k} + (p-3)x^{22k} + 1 \equiv (p+1) + (p+2) + (p-3) + 1 \equiv 1 \pmod{p}.$$

□

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

Theorem (?)**.** *Let $n > 2$ be an integer and let $k := \phi(n)+1$, where ϕ is the Euler totient function. Then for all a, b such that $\gcd(a, n) = \gcd(b, n) = \gcd(a + b, n) = 1$, we have $a^k + b^k \equiv (a + b)^k \pmod{n}$.*

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

Solution. The statement is in fact true. By Euler's Theorem and the fact that $a, b, a + b$ are all units, we have that

$$a^k \equiv a \pmod{n}, \quad b^k \equiv b \pmod{n}, \quad (a + b)^k \equiv (a + b) \pmod{n}.$$

So $a^k + b^k \equiv (a + b)^k \pmod{n}$. □

(5*) (4 points) A positive integer n is *perfect* if the sum of the positive divisors of n (including n itself) is equal to $2n$. For example, $2 \cdot 6 = 1 + 2 + 3 + 6$, so 6 is perfect.

Prove that there are no odd, squarefree, perfect numbers.

Solution. We proceed via contradiction and let n be an odd, squarefree, perfect number. Clearly $n \neq 1$, because then $\sigma(n) = 1$. Let $n = p_1 p_2 \dots p_k$ be the prime factorization of $n > 1$, and note the exponents are all 1 because n is squarefree. Now via the important trick, we have that the sum of the positive divisors of n is given by

$$\sigma(n) := (1 + p_1) \dots (1 + p_k).$$

Because n is odd, each p_i is odd, so $2^k \mid \sigma(n)$. On the other hand, n is perfect, so $\sigma(n) = 2n$. Thus, because n is odd, $2^k \mid 2$, so $k = 0, 1$.

Thus, n has exactly one prime factor p, else it is equal to 1. But then

$$2p = 1 + p \implies p = 1$$

which is a contradiction. Thus there are no odd, squarefree, perfect numbers. $\square$

(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.)**