MATH 4573: HOMEWORK 3

INSTRUCTOR: TYLER GENAO

Due: February 6, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to §2.2 of our notes, as well as the Chinese Remainder Theorem from §2.3. Everything else must be proven.**

1. Problems to Submit

Exercise 1.

a) List all integers $1 \leq n \leq 100$ which are congruent to 3 modulo 18.
b) Give a complete residue system modulo 9 comprised of multiples of 4.
c) Give a reduced residue system modulo 14. From this, compute $\varphi(14)$.
d) Give a reduced residue system modulo 11. For each representative r of this residue system, give a multiplicative inverse $r^{-1} \in \mathbb{Z}$ with $0 \leq r^{-1} < 11$.

Exercise 2. Recall the *freshman's dream,* which is the erroneous conclusion that for all real numbers x and y and for any integer $n \geq 2$, one has

$$(x+y)^n = x^n + y^n.$$

In spite of the above, show that for any integers a and b and prime p, one has

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Exercise 3. Show that for prime powers p^e, one has $\varphi(p^e) = p^e - p^{e-1}$.

Exercise 4. Determine all integer solutions to the following congruences. If no solution exists, explain why.

a) $15x \equiv 4 \pmod{35}$.
b) $137x \equiv 64 \pmod{255}$.
c) $63x \equiv 21 \pmod{69}$.

Exercise 5. Show that for any integer $m > 0$, one has that $a \in \mathbb{Z}$ is a root of $x^{\varphi(m)} - 1$ modulo m if and only if $\gcd(a, m) = 1$. Thus, any reduced residue system mod m is equivalent to the set of all roots of $x^{\varphi(m)} - 1 \mod m$, up to congruence mod m.

Exercise 6.

a) Prove that the square of an integer has $0, 1, 4, 5, 6$ or 9 for its unit digit.
b) Prove that the fourth power of an integer has $0, 1, 5$ or 6 for its unit digit.
c) Without using a calculator, prove that $(123456789)^5$ has unit digit 9.

Exercise 7. For each part, use the Chinese Remainder Theorem to determine all integers x which satisfy the simultaneous congruences. If no solution exists, then prove it.

a) $x \equiv 1 \pmod 3$ and $x \equiv 4 \pmod 7$.
b) $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 9$.
c) $8x \equiv 1 \pmod 6$ and $7x \equiv 10 \pmod{15}$.

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §2.1], pages 56–57: $\#1 - 6, 10 - 15, 17, 32$.
From [NZM91, §2.2], pages 62–63: $\#1 - 6, 8 - 9$.
From [NZM91, §2.3], pages 71–72: $\#1 - 4$.

Bonus Exercise 9. Show that for an integer $m \geq 3$, the set $\{0^2, 1^2, \ldots, (m-1)^2\}$ is not a complete residue system modulo m.

Bonus Exercise 10. Show that if $\{x_1, x_2, \ldots, x_r\}$ is a reduced residue system modulo m, then so is $\{x_1^{-1}, x_2^{-1}, \ldots, x_r^{-1}\}$, where each x_i^{-1} is any integer that is a multiplicative inverse to $x_i \bmod m$.

Bonus Exercise 11.

a) Show that for all integers n and k, if $7 \nmid n$ then $7 \mid (n^{6k} - 1)$.
b) Show that for any integer n, one has $42 \mid (n^7 - n)$.

The following two exercises deal with *primitive roots* and *discrete logarithms.* We will talk about the former in §2.8, and the latter is important to cryptography. Both topics are closely connected.

Bonus Exercise 12. Given an integer $m \in \mathbb{Z}^+$, we say that a positive integer g is a *primitive root modulo* m if the powers $g^0 = 1, g, g^2, \ldots, g^{\varphi(m)-1}$ form a reduced residue system modulo m.

a) Show that if g is a primitive root modulo m, then for all integers n coprime to m, there exists a unique integer $0 \leq e < \varphi(m)$ such that $g^e \equiv n \pmod m$. In particular, a primitive root modulo m, if it exists, will generate all reduced residue classes mod m.
b) Determine whether a primitive root exists modulo the following numbers.
   i) Modulo 6.
   ii) Modulo 8.
   iii) Modulo 9.
c) Use Bonus Exercise 10 to show that if g is a primitive root modulo m, then so is $g^{-1} \bmod m$.
d) Use part c) to show that for any prime $p > 3$, the product of primitive roots modulo p is congruent to 1 modulo p.

We will explore primitive roots more closely in §2.8.

Bonus Exercise 13. Given a primitive root g modulo m, we can define a *discrete logarithm modulo m with base g* as follows. As noted in Bonus Exercise 12, for each integer b there exists a unique integer $0 \leq e < m$ with $g^e \equiv b \pmod{m}$. This e is called the *discrete logarithm of b modulo m,* written as $\log_g(b) := e$. The discrete logarithm depends on the choice of g.

a) Compute the following powers modulo 13, reducing them to representatives between 0 and 12.
   i) 2^3.
   ii) 2^9.
   iii) 2^{11}.

b) Compute the following discrete logarithms modulo 13, with base 2.
   i) $\log_2(6)$.
   ii) $\log_2(5)$.
   iii) $\log_2(7)$.

Computing discrete logarithms mod m for large m can take an extremely long time, even with a computer (though there are ways to get around this if m is a "vulnerable" or unsafe modulus). The computational intractability of the discrete logarithm makes it an important component of many algorithms in public-key cryptography.

Bonus Exercise 14. This problem explores primes and their connection to numbers of the form $n! + 1$ for integers $n > 0$. Wilson's theorem gives one such connection.

a) Show that if p is prime, then $(p-1)! + 1$ is a power of p if and only if $p \leq 5$.
b) Using part a) and Wilson's theorem, show that there are infinitely many integers $n > 0$ such that $n! + 1$ is divisible by at least two distinct primes.

In contrast to part b), it is an open problem to determine whether $n! + 1$ is prime for infinitely many $n \in \mathbb{Z}^+$. Such primes are called *factorial primes.* Some of the known factorial primes are listed on the OEIS: A002981.

Bonus Exercise 15. Prove that no polynomial $f(x) \in \mathbb{Z}[x]$ of degree greater than one has the property that $f(n)$ is prime for all $n \in \mathbb{Z}^+$. See also the Bunyakovsky conjecture (HW 2, Bonus Exercise 12).

Bonus Exercise 16. This is a continuation of Bonus Exercise 13 in HW 2. In [NZM91, Theorem 2.12] and [NZM91, Lemma 2.13], it was shown that for odd primes p, one has

$$p \equiv 1 \pmod{4} \Leftrightarrow \exists\, a, b \in \mathbb{Z} : p = a^2 + b^2 \Leftrightarrow x^2 + 1 \text{ has a root modulo } p.$$

In this exercise, we will give another equivalency, and study how prime numbers $p \in \mathbb{Z}$ behave in the *Gaussian integer ring*

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

This ring is generated over $\mathbb{Z}$ by i, which is a root of $x^2 + 1$ over $\mathbb{C}$.

a) Prove the following.

   Theorem. *A prime p satisfies $p \equiv 1 \pmod{4}$ if and only if p* splits *in $\mathbb{Z}[i]$, i.e., $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ with $\alpha \neq \beta$.*

b) Show that if a prime p splits in $\mathbb{Z}[i]$, then $x^2 + 1$ splits into distinct linear polynomials modulo p. Show that the converse also holds.
c) Using parts a) and b), show that an odd prime p is an *irreducible* element in $\mathbb{Z}[i]$ iff $p \equiv 3 \pmod 4$, iff $x^2 + 1$ is irreducible modulo p.
d) How does $p = 2$ factorize in $\mathbb{Z}[i]$? How does $x^2 + 1$ factor modulo 2?

This exercise shows that for any prime p, its behavior in $\mathbb{Z}[i]$ is determined by the factorization of $x^2 + 1$ modulo p. This is not a coincidence – in a more general setting, this is a consequence of a theorem of Dedekind and Kummer.

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).