MATH 4573: HOMEWORK 3

INSTRUCTOR: TYLER GENAO

Due: February 9.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

Your solutions should not use theorems from sections which come after the day the homework was assigned (i.e., a week before it's due). The day this HW was assigned, we stopped at the proof of the Chinese remainder theorem.

1. Problems to Submit

Exercise 1. Find all integer solutions to the following congruences. If no solution exists, then explain why.

a) $20x \equiv 4 \pmod{30}$;
b) $353x \equiv 254 \pmod{400}$;
c) $64x \equiv 83 \pmod{105}$.

Exercise 2. For each part, determine all integers x which satisfy the simultaneous congruences. If no such solution exists, then prove it.

a) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ and $x \equiv 5 \pmod{2}$;
b) $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$ and $3x \equiv 1 \pmod{7}$;
c) $5x \equiv 1 \pmod{6}$, $4x \equiv 13 \pmod{15}$.

Exercise 3.

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

Exercise 4.

a) Show that for any modulus $m > 0$, one has that $a \in \mathbb{Z}$ is a root of $x^{\phi(m)} - 1$ modulo m if and only if $\gcd(a, m) = 1$. Thus, any reduced residue system modulo m is the set of all roots of $x^{\phi(m)} - 1$ modulo m.
b) Show that for prime $p \in \mathbb{Z}$, one has for all $a \in \mathbb{Z}$ that

$$a^p \equiv a \pmod{p}.$$

(This strengthens Exercise 7 from HW 2.)

Exercise 5.

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 6. Show that if $\{x_1, x_2, \ldots, x_r\}$ is a reduced residue system modulo m, then so is $\{x_1^{-1}, x_2^{-1}, \ldots, x_r^{-1}\}$.

Exercise 7. Given an integer $m \in \mathbb{Z}^+$, we say that an integer $g \in \mathbb{Z}^+$ is a *primitive root modulo* m if the (distinct modulo m) powers $g^0 = 1, g, g^2, \ldots, g^{\phi(m)-1}$ 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 $0 \leq e \leq \phi(m) - 1$ such that $g^e \equiv n \pmod{m}$. In particular, a primitive root modulo m, if it exists, "generates" all reduced residue classes modulo m.
b) Determine with proof whether a primitive root exists modulo the following integers.
   i) Modulo 6;
   ii) Modulo 8;
   iii) Modulo 9.
c) Use Exercise 6 to show that if g is a primitive root modulo m, then so is g^{-1} mod 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.

Exercise 8. Given a primitive root g modulo m, we can define a "discrete logarithm modulo m with base g" as follows. As noted in Exercise 7, 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 modulo m when m is large 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.

Exercise 9. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From the textbook, page 57: $\#14 - 18, 32$.
Pages 62–63: $\#1 - 6$.
Page 72: $\#4$.

Bonus Exercise 10. This problem explores primes and their connection to numbers of the form $n! + 1$ for $n \in \mathbb{Z}^+$. 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 $n \in \mathbb{Z}^+$ 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: https://oeis.org/A002981.

Bonus Exercise 11. Prove that no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 has the property that $f(n)$ is prime for all $n \in \mathbb{Z}^+$. See also the Bunyakovsky conjecture (HW 2, Bonus Exercise 14).

Bonus Exercise 12. This is a continuation of Bonus Exercise 15 in HW 2. In [NZM91, Theorem 2.12] and [NZM91, Lemma 2.13], it was shown that for prime $p > 2$,

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

In this exercise, we will 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 $p \in \mathbb{Z}^+$ 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 $p > 2$ 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 a prime $p > 2$ is irreducible in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$, if and only if $x^2 + 1$ 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 $p \in \mathbb{Z}^+$, its behavior in $\mathbb{Z}[i]$ is determined by the factorization of $x^2 + 1$ modulo p. In a more general setting, this is a consequence of a theorem of Dedekind and Kummer.

Bonus Exercise 13. Try a few problems from Project Euler (this site is a mix of math and computer programming problems).

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).