MATH 4573: HOMEWORK 4

INSTRUCTOR: TYLER GENAO

Due: February 13, 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 §2.6 of our notes. Everything else must be proven.**

1. Problems to Submit

Exercise 1.

a) Show that for integers e, f, m where $m > 0$, if

$$e \equiv f \pmod{\varphi(m)},$$

then for all integers a coprime to m one has

$$a^e \equiv a^f \pmod{m}.$$

(*Hint:* Euler's Theorem.)

b) Let p be a prime. Show that for any polynomial $f(x) \in \mathbb{Z}[x]$, there exists $g(x) \in \mathbb{Z}[x]$ of degree less than $p-1$ such that for all $a \in \mathbb{Z}$ coprime to p one has

$$f(a) \equiv g(a) \pmod{p}.$$

c) Show that for all integers a with $13 \nmid a$, one has

$$a^{16} + 42a^{12} + 11a^4 + 1 \equiv 4 - a^4 \pmod{13}.$$

d) Give an interesting example of a polynomial $f(x) \in \mathbb{Z}[x]$ that "reduces" to a polynomial $g(x) \in \mathbb{Z}[x]$ of strictly smaller degree modulo a prime p, in the sense of part b). (One point)

Exercise 2. Prove the following multilinear version of Dirichlet's Theorem on Primes in Arithmetic Progressions.

Theorem. *Given positive integers $m_1, m_2, \ldots, m_r$ which are pairwise coprime, for any integers $a_1, a_2, \ldots, a_r$ where each a_i is coprime to m_i, there exist infinitely many primes p such that for all $1 \leq i \leq r$ one has*

$$p \equiv a_i \pmod{m_i}.$$

(*Hint:* Use the Chinese Remainder Theorem and the original Dirichlet's Theorem from Homework 2, Exercise 4 to prove this.)

Exercise 3.

a) Determine all integers $n \in \mathbb{Z}^+$ for which $\varphi(n)$ is odd.
b) Show that if every prime p which divides m also divides n, then $\varphi(mn) = m\varphi(n)$.

Exercise 4.

a) Prove that the polynomial $f(x) := x^2 + 5x + 24$ has no integer solutions.
b) Using the Chinese Remainder Theorem, prove that $f(x)$ from part a) has solutions modulo 36; **write these solutions as least positive integers mod 36.** Then check that your solutions work by writing their values under $f(x)$ as a multiple of 36.

Exercise 5. Fix a polynomial $f(x) \in \mathbb{Z}[x]$ and a prime p. Suppose that $f(x)$ has a nonsingular root a_1 modulo p. Then by Hensel's Lemma, we can lift a_1 repeatedly to obtain solutions a_{k+1} to $f(x)$ mod p^{k+1} for each $k \geq 1$. These solutions can be described by the formula

$$(*) \qquad a_{k+1} \equiv a_k - f'(a_1)^{-1} \cdot f(a_k) \pmod{p^{k+1}},$$

where $f'(a_1)^{-1}$ represents the multiplicative inverse of $f'(a_1)$ modulo p.

a) Using the formula $(*)$, verify that a_{k+1} is a lift of a_k. Also verify that each $f'(a_k)^{-1}$ is congruent to $f'(a_1)^{-1}$ modulo p.
b) Use the formula for solution lifts from Hensel's Lemma in class to prove the formula $(*)$.
c) Suppose that a is instead a *singular root* modulo p, i.e.,

$$f(a) \equiv 0 \pmod{p}$$

but

$$f'(a) \equiv 0 \pmod{p}.$$

Prove that there are either 0 or p lifts of a modulo p^2. (*Hint:* revisit our proof of Hensel's Lemma and see what happens when $f'(a)$ is not coprime to p.)

Exercise 6. Using Hensel's Lemma by hand, solve the congruence

$$x^4 + 2 \equiv 0 \pmod{27};$$

write your solution(s) as a least positive integer mod 27. Then show directly that your solution(s) works by writing its evaluation under $f(x)$ as a multiple of 27.

Exercise 7. For this computational exercise, **you will need to submit your associated code as a text file onto Carmen.** In particular, your code must run without error if pasted into SageCell by the class grader, and *automatically* print the output you claim in your answer. Note that when you copy-paste your code into Carmen, it might mess some of the formatting up, so you may need to fix it. The deadline for submitting the code is the same as this HW.

a) Create a `Sage` function which takes as input $(f(x), p)$, where $f(x)$ is a polynomial in $\mathbb{Z}[x]$ and p is a prime, and outputs a list of solutions for $f(x)$ modulo p, via plugging each integer in $[0, p-1]$ directly into $f(x)$ and reducing mod p. If no such solutions exist, have it return a message saying as much.

Run output for this function for $f(x) := x^2 + 1$, over all primes $p \leq 101$.

b) What patterns do you notice in part a)? (One point)

c) Using your function from part a), create another function which takes as input $(f(x), p^k)$ where $f(x) \in \mathbb{Z}[x]$ and p^k is a prime power, and applies Hensel's Lemma to $f(x)$ modulo p^k, via the formula $(*)$ given in Exercise 5. **Have your code output solutions as least positive integers mod p^k.**

(*Hint:* You may find `ZZ.valuation()` useful for returning the exponent k in p^k, as well as `inverse_mod(a,m)` for computing multiplicative inverses mod m, and `derivative()` for computing derivatives. Note, however, that some object types might mismatch, in which case you may have to turn several objects into integers to have them interact; `Integer()` can be useful for this.)

Use this code to output solutions to $f(x) := x^2 + 1$ modulo p^3 for all primes $p \leq 101$.

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

2. Other Recommended Problems

From [NZM91, §2.3], pages 72–73: $\#7 - 8, 10 - 15, 17, 32$.
From [NZM91, §2.6], page 91: $\#1 - 3, 5 - 7$.

Bonus Exercise 9. Prove that for integers $m, n \in \mathbb{Z}^+$ with $m > 1$, if

$$\varphi(mn) = \varphi(n)$$

then $m = 2$ and n is odd. Characterize the set of positive integers n satisfying

$$\varphi(2n) = \varphi(n).$$

Bonus Exercise 10. Show that for a fixed integer $n \in \mathbb{Z}^+$, the equation

$$\varphi(x) = n$$

has a finite number of solutions.

Bonus Exercise 11. This exercise explores which positive integers are not in the image of Euler's totient function $\varphi(x)$.

a) Show that for an odd integer $n > 0$, the equation

$$\varphi(x) = n$$

has a solution if and only if $n = 1$. Thus, the image $\varphi(\mathbb{Z}^+)$ contains no odd $n \geq 3$.

b) Show that there does not exist a solution to $\varphi(x) = 14$.

c) Show that 14 is the *smallest* positive even integer not in $\varphi(\mathbb{Z}^+)$. Then determine the next smallest such integer.

Bonus Exercise 12. Extend Exercise 7 via the Chinese Remainder Theorem: program a function in `Sage` where given polynomial $f(x) \in \mathbb{Z}[x]$ and integer $m > 0$, the function takes as input $(f(x), m)$ and outputs the list of all solutions to $f(x)$ modulo m.

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).