MATH 4573: HOMEWORK 4

INSTRUCTOR: TYLER GENAO

Due: February 16.

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. The day this HW was assigned, the last thing we did was prove Hensel's lemma.

1. Problems to Submit

Exercise 1. In this exercise, you will prove the following "multilinear version" of Dirichlet's theorem on primes in arithmetic progression. See Exercise 4 from HW 2 for a statement of the original result, which you should use to prove this one.

Theorem. *Given pairwise coprime integers $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$, for any integers $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ 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*

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

Exercise 2. This exercise will study some arithmetic properties of Euler's totient function $\phi(n)$.

a) Determine all integers $n \in \mathbb{Z}^+$ for which $\phi(n)$ is odd.
b) Show that if every prime p which divides m also divides n, then $\phi(mn) = m\phi(n)$.
c) Prove that if $\phi(mn) = \phi(n)$ and $m > 1$, then $m = 2$ and n is odd. Characterize the set of positive integers satisfying $\phi(2n) = \phi(n)$.

Exercise 3. Show that for a fixed integer $n \in \mathbb{Z}^+$, the equation $\phi(x) = n$ has a finite number of solutions.

Exercise 4.

a) Show that for $e, f, m \in \mathbb{Z}$ with $m > 0$, if $e \equiv f \pmod{\phi(m)}$, then for all integers a coprime to m, one has $a^e \equiv a^f \pmod{m}$.
b) Show that modulo 13, one has for all integers a with $13 \nmid a$ that

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

c) Show that for any polynomial $f(x) \in \mathbb{Z}[x]$, there exists a polynomial $g(x) \in \mathbb{Z}[x]$ of degree $< p$ such that for all $a \in \mathbb{Z}$ with $p \nmid a$, one has

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

Exercise 5. Fix a polynomial $f(x) \in \mathbb{Z}[x]$ and prime $p \in \mathbb{Z}^+$, and suppose that $f(x)$ has a nonsingular root $a \in \mathbb{Z}$ modulo p. By Hensel's lemma, we can inductively lift the solution a to obtain solutions a_k modulo p^k, and these solutions are described by the formula

$$a_{k+1} \equiv a_k - A_k \cdot f(a_k) \pmod{p^{k+1}},$$

where $A_k \in \mathbb{Z}$ represents $(f'(a_k))^{-1} \mod p$.

a) Using the formula above, show directly that a_{k+1} is a lift of a_k.
b) Show that the integers A_k can be chosen independently of $k \geq 1$.
c) Suppose that a is instead a *singular root* modulo p, i.e., $f'(a) \equiv 0 \pmod{p}$. Prove that there are either 0 or p lifts of a modulo p^2.

Exercise 6. Using Hensel's lemma, solve the congruence $x^4 + 2 \equiv 0 \pmod{27}$. Then check directly that your solution(s) works by writing it as a multiple of 27.

Exercise 7. With proof, solve the equation $x^2 + 5x + 24 \equiv 0 \pmod{36}$. Then check that your solution(s) works by writing it as a multiple of 36.

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

2. Other Recommended Problems

From the textbook, pages $71 - 73$: $\#1, 3, 6, 8, 10 - 17, 19, 20, 25, 27, 30$.
Page 91: $\#1 - 3, 5 - 7$.

Bonus Exercise 9. This exercise explores which positive integers are not in the image of Euler's totient function $\phi(x)$.

a) Show that for odd $n \in \mathbb{Z}^+$, the equation $\phi(x) = n$ has a solution if and only if $n = 1$. Thus, the image $\phi(\mathbb{Z}^+)$ has no odd numbers except $n = 1$.
b) Show that there does not exist a solution to $\phi(x) = 14$.
c) Show that 14 is the *smallest* positive even integer not in $\phi(\mathbb{Z}^+)$. Then determine the next smallest such integer.

Bonus Exercise 10. Create a program which does the following: given a polynomial $f(x) \in \mathbb{Z}[x]$, a prime power p^e and an integer a such that $f(a) \equiv 0 \pmod{p^e}$, it uses Hensel's Lemma to check whether a lifts to a root of $f(x)$ modulo p^{e+1}. The code also returns whether the root a is singular or not, and if it is singular, it returns the p lifts of a mod p^{e+1}.

You could also write code that does the following: given $f(x) \in \mathbb{Z}[x]$ and a prime power p^e, it determines all roots of $f(x)$ mod p^e.

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).