Math 328K. Fall 2025
Guide for Midterm Exam 2

Prof. Hector E. Lomeli

Solve the following problems.

§3.5 10, 36, 40, 46.
§3.7 2–8.
§4.1 14, 30, 34.
§4.2 2, 8, 9, 12, 18.
§4.3 4, 10, 12, 21–23.
§6.1 10, 18–22, 28.
§6.3 7–10, 13, 22.
§7.1 2, 5–7, 20–23.
§7.2 1–3, 8–10, 34.
HW 5: 4–6.
HW 6: 4, 6.
HW 7: 5, 6.
HW 8: 9.

Concentrate on the following concepts.

- Fundamental theorem of arithmetic.
- Least common multiple.
- Linear diophantine equations.
- Congruences modulo m and properties.
- Inverse modulo m.
- Chinese remainder theorem.
- Wilson's theorem.
- Fermat's Little Theorem.
- Euler's $\phi-$function.
- Euler's Theorem.
- Properties of Euler's $\phi-$function.
- Multiplicative functions.
- Sum of divisors $\sigma-$function.
- Number of divisors $\tau-$function.

Do the following practice questions.

1) Prove that any prime $p > 3$ is of the form $6k + 1$ or $6k - 1$, for some $k \in \mathbb{N}$.

2) Let N be an integer such that $N > 1$. Let $p_1, ..., p_n$ be all the different prime numbers that divide N. Prove the following.

a) If all primes $p_1, ..., p_n$ are of the form $6k + 1$ then the $N \bmod 6 = 1$.

b) If N satisfies that $N \bmod 6 = 5$, then $2 \nmid N$, $3 \nmid N$ and there exists a prime of the form $p = 6k - 1$ that divides N.

3) §3.5 # 56. (*Hint:* Use the previous problem.)

4) Let n be an odd natural number. Prove that $n \mid 2^{(n-1)!} - 1$.

5) Show that $a^{40} - 1$ is divisible by 440 whenever $(a, 110) = 1$.

6) Let $x, y, n \in \mathbb{N}$. Let $a \in \mathbb{Z}$ be an integer such that $(a, n) = 1$. Prove that, if $x \equiv y \pmod{\phi(n)}$ then

$$a^x \equiv a^y \pmod{n}.$$

7) Let p be an odd prime. Assume that there exists x_0 such that $x_0^2 \equiv -1 \pmod{p}$. Show the following.

a) $x_0^k \not\equiv 1 \pmod{p}$, for $k = 1, 2, 3$.

b) If we define $r = \phi(p) \,\mathbf{mod}\, 4$ then $x_0^r \equiv 1 \pmod{p}$.

c) $r = 0$ and hence $p \equiv 1 \pmod{4}$.

8) Let p be an odd prime such that $p \equiv 3 \pmod{4}$. Let a be an integer such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We will show that the equation $x^2 \equiv a \pmod{p}$ has no solution. By way of contradiction, suppose that there exists x_1 such that $x_1^2 \equiv a \pmod{p}$. Let $\ell = \frac{3p-5}{4}$. Show the following.

a) $\ell \in \mathbb{N}$.

b) If we define $x_0 = x_1 a^\ell$, then $x_0^2 \equiv -1 \pmod{p}$.

c) $p \equiv 1 \pmod{4}$. This is a contradiction and hence $x^2 \equiv a \pmod{p}$ has no solution.

9) Let z be an integer. Define

$$x = z \,\mathbf{mod}\, 8, \qquad y = z \,\mathbf{mod}\, 125.$$

This is, x, y are the remainders that result when we divide z by 8 and 125, respectively. Prove that

$$z^n \equiv 376y^n - 375\, x^n \pmod{1000},$$

for all $n \in \mathbb{N}$.
(*Hint:* prove first that $z^n \equiv x^n \pmod{8}$ and $z^n \equiv y^n \pmod{125}$.)

10) §7.2 #40. (*Hint:* You can use that $\phi(p^i) = p^{i-1}(p-1)$, if p is prime and $i \in \mathbb{N}$.

11) Let $m_1, m_2 \in \mathbb{N}$ be two integers such that $(m_1, m_2) = 1$. Let $x_1, x_2 \in \mathbb{Z}$. Prove that the following two statements are equivalent.

a) $(x_1, m_1) \cdot (x_2, m_2) = 1$.

b) $(x_1 \cdot m_2 + x_2 \cdot m_1,\ m_1 m_2) = 1$.

12) Let $m_1, m_2 \in \mathbb{N}$ be two integers such that $(m_1, m_2) = 1$. Let $x_1, x_2 \in \mathbb{Z}$ such that $(x_1, m_1) \cdot (x_2, m_2) = 1$. Bezout's theorem implies that there exists $y_1, y_2 \in \mathbb{Z}$ such that $m_2 y_1 + m_1 y_2 = 1$. Show the following.

a) There exists integers $\overline{x_1}$ and $\overline{x_2}$ such that

$$x_1\, \overline{x_1} \equiv 1 \pmod{m_1}, \qquad x_2\, \overline{x_2} \equiv 1 \pmod{m_2}.$$

b) If we define $z = x_1 \cdot m_2 + x_2 \cdot m_1$, then there exists $\overline{z} \in \mathbb{Z}$ such that

$$z\, \overline{z} \equiv 1 \pmod{m_1 m_2}.$$

c) Write $\overline{z}$ in terms of $\overline{x_1}$, $\overline{x_2}, m_1, m_2, y_1, y_2$. (*Hint:* Use the CRT.)