MATH 4573: PRACTICE MIDTERM PROBLEMS

INSTRUCTOR: TYLER GENAO

Here is a list of topics we have covered in class or on the homework, up to and including the group theory from §2.11. Any of these topics can appear on the midterm. Note that this list is not necessarily exhaustive.

- §1.2: Divisibility.
  - The Division Algorithm.
  - The greatest common divisor (GCD).
  - The Euclidean Algorithm.
  - Blankinship's Algorithm.
  - The least common multiple (LCM).
- §1.3: Primes.
  - Prime and composite numbers.
  - The Fundamental Theorem of Arithmetic (FTA).
  - Euclid's proof on the infinitude of primes.
- §1.4: The Binomial Theorem.
  - Factorials and binomial coefficients.
  - The Binomial Theorem.
- §2.1: Congruences.
  - Congruences.
  - Residue systems.
  - The Euler phi function.
  - Euler's Theorem, and Fermat's Little Theorem.
  - Multiplicative inverses modulo m.
  - Wilson's Theorem.
  - For odd p, $\exists$ solutions to $x^2 + 1 \mod p \Leftrightarrow p \equiv 1 \pmod 4 \Leftrightarrow \exists a, b \in \mathbb{Z}$ $p = a^2 + b^2$.
- §2.2: Solutions of Congruences.
  - The Linear Congruence Theorem and explicit formulas for solutions.
- §2.3: The Chinese Remainder Theorem (CRT).
  - CRT and explicit formulas for solutions.
  - CRT for residue systems.
  - The factorization formula for $\varphi(n)$.
  - The factorization formula for $\varphi_f(n)$, where $\varphi_f(n)$ counts the number of solutions to $f(x) \mod n$.
- §2.6: Prime Power Moduli (Hensel's Lemma).
  - Hensel's Lemma and explicit formulas for lifting roots.
- §2.10: Number Theory From an Algebraic Viewpoint.
  - Basic group definitions and homomorphisms.

  - The basic group structure of $(\mathbb{Z}/m\mathbb{Z}, +)$ and $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.
- §2.11: Groups, Rings and Fields.
  - The order of a group element.
  - Lagrange's Theorem (for group elements).
  - Cyclic groups and their generators.
  - Formula for the order of a power or multiple of a group element (HW 5 Exercise 4).

Problem 1.

a) Show that for integers $a, b, n \in \mathbb{Z}^+$, if $a \mid n$, $b \mid n$ and $\gcd(a, b) = 1$, then $ab \mid n$.

b) Show that the conclusion to a) is false if $\gcd(a, b) > 1$.

Problem 2. Compute the greatest common divisor of 53 and 173, and express it a $\mathbb{Z}$-linear combination of these two.

Problem 3. Find all integers that give remainders $1, 2$ and 3 when divided by $3, 4$ and 5, respectively.

Problem 4. Determine all integer solutions to the congruence $x^3 + x^2 + 1 \equiv 0 \pmod{27}$, or prove they cannot exist.

Problem 5.

a) What is the additive order of $[6]$ in $\mathbb{Z}/74\mathbb{Z}$?

b) What is the multiplicative order of $[5]$ in $\mathbb{Z}/22\mathbb{Z}$?

Statements

Here are some statements for reference.

1. **(Hensel's lemma)** Let $f(x) \in \mathbb{Z}[x]$. For any $k \geq 1$, if $f(a) \equiv 0 \pmod{p^k}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists an integer $t \in \mathbb{Z}$, unique modulo p, for which $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$.
2. **(Linear congruence)** The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$. In such a case, it has $\gcd(a, m)$ many solutions modulo m.
3. **(Singular roots)** Let $f(x) \in \mathbb{Z}[x]$. If $a \in \mathbb{Z}$ is such that $f(a) \equiv 0 \pmod{p^k}$ and $f'(a) \equiv 0 \pmod{p}$, then there are p lifts of a to a root of $f(x)$ modulo p^{k+1}.
4. **(Chinese remainder theorem)** Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$ be pairwise coprime integers. Then for any integers $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, the system of equations $\{x \equiv a_i \pmod{m_i}\}_{i=1}^r$ has a solution. Furthermore, if x_0 is a solution, then any other solution x_1 satisfies $x_1 \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.
5. **(Wilson's theorem)** For any integer $p > 1$, one has that p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.
6. **(Euler's theorem)** For integers a, m with $m > 0$, if $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.
7. **(Dirichlet's theorem on primes in arithmetic progressions)** If $a, m \in \mathbb{Z}^+$ are coprime, then there exist infinitely many primes $p \in \mathbb{Z}^+$ such that $p \equiv a \pmod{m}$.
8. **(Degree modulo m)** For a polynomial $f(x) \in \mathbb{Z}[x]$, writing $f(x) = a_0 + a_1 x + \ldots + a_r x^r$, for an integer $m > 0$, the degree of f modulo m is the greatest integer n such that $a_n \not\equiv 0 \pmod{m}$ (if it exists).
9. **(Multiplicative inverse)** For integers a and m with $m > 0$, if $\gcd(a, m) = 1$ then there exists $b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{m}$. If $\gcd(a, m) > 1$, then no such b exists.

-Scratch paper-

-Scratch paper-

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).