MATH 4573: PRACTICE MIDTERM PROBLEMS

INSTRUCTOR: TYLER GENAO

Here's the topics we've covered that can be addressed on the exam (not a comprehensive list!).

- §1.2, divisibility:
  - the division algorithm;
  - the GCD;
  - the Euclidean algorithm;
  - Blankinship's algorithm;
  - the LCM.
- §1.3: Primes:
  - prime and composite numbers;
  - the fundamental theorem of arithmetic;
  - the infinitude of primes.
- §1.4: the binomial theorem:
  - factorials;
  - the binomial theorem.
- §2.1: congruences:
  - Euler's totient function;
  - Euler's theorem;
  - multiplicative inverses;
  - Wilson's theorem;
  - solutions to $x^2 + 1 \bmod p$, and sums of squares.
- §2.2: solutions of congruences:
  - linear congruence theorem.
- §2.3: the Chinese remainder theorem:
  - the CRT and explicit formula for solutions;
  - factorization formula for $\phi(n)$;
  - factorization formula for $\phi_f(n)$ (solutions to $f \bmod m$).
- §2.6: prime power moduli:
  - Hensel's lemma and the formula for lifting roots.
- §2.7: prime modulus:
  - number of roots of $f \bmod p$ is at most $\deg(f)$ (if $f \not\equiv 0 \pmod p$).
- §2.10: number theory from an algebraic viewpoint:
  - group definition and homomorphisms;
  - group structure of $(\mathbb{Z}/m\mathbb{Z}, +)$ and $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.
- §2.11: groups, rings and fields:
  - group elements of finite order;
  - formula for order of powers/multiples of group elements (from HW 5);

– cyclic groups and their generators;
– Lagrange's theorem;
– rings and their homomorphisms;
– products of groups and rings;
– the CRT for the ring $\mathbb{Z}/m\mathbb{Z}$;
– fields.

Problem 1.

a) Show that if $a \mid n$, $b \mid n$ and $\gcd(a, b) = 1$, then one has $ab \mid n$.

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

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

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

Problem 4. If they exist, determine all integer solutions to the congruence $x^3 + x^2 + 1 \equiv 0 \pmod{27}$.

Problem 5. Find all integers which satisfy the equation $\phi(x) = 4$.

Problem 6.

a) What is the additive order of $[6]$ in $\mathbb{Z}/14\mathbb{Z}$?

b) What is the multiplicative order of $[5]$ in $\mathbb{Z}/11\mathbb{Z}$?

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).