

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

EXAM 2 SAMPLE

Exam 2 will take place Wednesday Nov. 16 in class. Don't be late. The format of the exam will be pretty close to what you get here (approximately the same number of questions, etc.)

For the true/false and short answer sections, you do not need to justify your answer, just GET the answer. For the "proofs" part, you do need to justify your steps.

Don't spend too much time on the short answer/definitions/TF. You want to leave enough time to think about the proofs which carry half the points roughly. I have included MANY more problems in this sample exam than there will be on the actual exam (in order to give you more practice).

1. Define the following terms. Throughout the exam, m denotes a positive integer, and a, b, x, y denote elements of \mathbb{Z} .
 - a. $x \equiv y \pmod{m}$ means
 - b. We define the congruence class $\{a\}_m$ as
 - c. We say that a congruence class $\{a\}_m$ is invertible if
 - d. The set $\mathbb{Z}/m\mathbb{Z}$ is defined to be
 - e. The set $(\mathbb{Z}/m\mathbb{Z})^\times$ is defined to be
 - f. The Bézout Theorem states that
 - g. The Euclidean theorem for \mathbb{Z} states that
 - h. We say that $\{a\}_m$ is a zero-divisor if
 - i. The Euler phi function φ is defined by $\varphi(m) =$
 - j. The binomial theorem states that
 - k. The binomial coefficient $\binom{n}{m}$ is defined by
 - l. State (any form of) the Chinese Remainder Theorem.
 - m. If $\gcd(a, m) = 1$, $\text{order}(\{a\}_m) =$
 - n. The Riemann Zeta function is defined by

- o. The Euler product formula for the Riemann Zeta function is
- p. The prime-counting function $\pi(x)$ is defined by
- q. State Wilson's theorem.

2. True/False

- a. If $\gcd(a, b) = d$, then for all integers c , there exist integers x, y such that $ax + by = dc$.
- b. For all positive integers m, n and for $x, y \in \mathbb{Z}$, $x \equiv y \pmod{mn}$ holds if and only if $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$.
- c. If p is a prime, $(\mathbb{Z}/p^k\mathbb{Z})$ has zero divisors if and only if $k > 1$.

3. Short Answer

- a. Use the Euclidean algorithm to determine $\gcd(247, 47)$ and to find integers x, y such that $247x + 47y = \gcd(247, 47)$.
- b. Determine the multiplicative inverse of $\{247\}_47$ or explain why no such inverse exists.
- c. Compute $\text{order}(\{2\}_{17})$. Hint: $2^4 = 16$.
- d. Find an integer x such that $3x \equiv 17 \pmod{47}$ and $5x \equiv 13 \pmod{37}$.

4. Proofs

- a. Prove that if $\gcd(m, n) = d$, then the equation $mx + ny = e$ is solvable with $x, y \in \mathbb{Z}$ if and only if $d|e$.
- b. Prove that if p is a prime, then for $1 \leq a \leq p-1$, and $e = \text{order}(\{a\}_p)$, we have $e|p-1$.
- c. Show that there are infinitely many primes p satisfying $p \equiv 3 \pmod{4}$.
- d. Prove that if 7 does not divide a , then either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.
- e. Suppose a, b are integers not divisible by the prime p . Show that
 - (a) If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.
 - (b) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

Hint for (b): Use (a) to write $b = a + pj$. Now use the binomial theorem and analyze the binomial coefficients involved.

f. Find all the solutions in $\mathbb{Z}/29\mathbb{Z}$ of the congruence

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}.$$

Hint: multiply by $x - 1$.

g. Suppose $m = a_0 + a_1 11 + a_2 11^2 + a_3 11^3 + \dots + a_n 11^n$ where the integers a_0 satisfy $0 \leq a_0 \leq 10$. (This is called the base-11 expansion of m). Let $s = a_0 + a_1 + \dots + a_n$. Show that $10|m$ if and only if $10|s$.

h. Let p be an odd prime. Suppose an integer a not divisible by p has order 3 modulo p , i.e. $\text{order}(\{a\}_p) = 3$. Show that $\text{order}(\{1+a\}_p) = 6$.

Extra Credit.

a. Prove that $v_p(n!) = (n - \sigma_p(n))/(p-1)$ where $\sigma_p(n) = a_0 + a_1 + \dots + a_r$, the a_i being the base- p digits of n i.e. $n = a_0 + a_1 p + a_2 p^2 + \dots + a_r p^r$ and $0 \leq a_i \leq p-1$ for $i = 0, 1, \dots, r$.

b. Suppose $f(x) = a_0 + a_1 x + \dots + a_r x^r$ is a polynomial with integer coefficients. Let m, n be coprime integers. Prove that if N_q is the number of solutions of $f(x) \equiv 0 \pmod{m}$ in $\mathbb{Z}/q\mathbb{Z}$, then $N_{mn} = N_m N_n$.

c. Show that if we write the rational number

$$h_n - 1 = \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

in lowest terms as $h_n - 1 = a/b$ with coprime positive integers a, b , then $p|a$.