

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

FINAL EXAM SAMPLE

The Final Exam is scheduled for Wednesday Dec. 20, 4-6 pm. Don't be late!!

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).

What's on the exam? Everything we learned this term . But, there will be a heavy emphasis on the material from the second half of the course.

1. DEFINITIONS

Review all the definitions from Sample Exams 1,2 and Exams 1,2, as well as:

- If $m \geq 1$ is an integer, we say an integer g is a primitive root mod m if
- We say a is a d th power modulo m if
- The Order Lemma states that
- Euler's theorem states that
- Lagrange's theorem on polynomials states that
- What is an open encryption-key cryptosystem?
- Give a short description of the RSA encryption/decryption scheme.
- State Bertrand's Postulate (=Theorem of Chebyshev).

2. TRUE/FALSE

- If m is not a prime, then there is no primitive root modulo m .
- For every odd prime p , there are $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$.
- For $m > 1$, $(\mathbb{Z}/m\mathbb{Z})$ has zero divisors if and only if m is composite.
- An integer $n \in \mathbb{Z}$ is of the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$ if and only if there exists an element $\alpha \in \mathbb{G}$ with norm $N(\alpha) = n$.
- Farshid is an intellectual snob. [This question asks for your opinion, so your answer is, by definition, correct.]

f. If a is an integer not divisible by the prime p , then $x = a^{p-2}b$ is always a solution of $ax \equiv b \pmod{p}$.

g. Whenever m, n are coprime, we have $x \equiv y \pmod{mn}$ if and only if the two congruences $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$ hold.

h. If p is a prime and k is an integer in the range $1 \leq k \leq p-1$, then

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

i. If x, y are integers, and p is a prime, then $(x+y)^p \equiv x^p + y^p \pmod{p}$.

j. If $\gcd(a, m) = 1$ and $\text{order}(\{a\}_m) = k$, then for all integers $t|k$, $\text{order}(\{a^t\}_m) = k/t$.

3. SHORT ANSWER

a. How many elements in $(\mathbb{Z}/137\mathbb{Z})^\times$ have order 17?

b. Find the remainder when $s = 2 + 2^2 + 2^3 + 2^4 + \cdots + 2^{96}$ is divided by 17.

c. I have fewer than 1000 mathematics books. When I count them all in groups of 25, 24 books get left out. When I count them all in groups of 24, 23 books are left out. Based on this information alone, is it possible to determine how many mathematics books I have? If so, do it; if not, explain why not.

d. It is a fact that $2^{36} \equiv -1 \pmod{433}$. Use this fact to find **all** elements of order 3 in $(\mathbb{Z}/433\mathbb{Z})^\times$. Hint: 433 is a prime number.

e. Find integers a, b such that $a^2 + b^2 = 1717$. Hint: $1717 = 101 \cdot 17$.

f. For the RSA system with $(n, e) = (3233, 37)$, what is the decryption key d ? Hint: $3233 = 53 \cdot 61$. If the coded message is $C = 77$, what is the plaintext message M ?

4. PROOFS

a. Use the existence of primitive roots to prove Wilson's theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

b. Prove that if p is a prime satisfying $p \equiv 1 \pmod{4}$, and g is a primitive root mod p , then $-g$ is also a primitive root mod p .

c. Show that if $\gcd(a, b) = 1$, then $\gcd(a+b, ab) = 1$.

d. Suppose $n \geq 2$ is an integer. Prove that if for some $a \in \mathbb{Z}$ satisfying $\gcd(a, n) = 1$, $\text{order}(\{a\}_n) = n - 1$, then n is a prime number.

e. Suppose p is an odd prime. Prove that if there exist **coprime** integers a, b (i.e. $\gcd(a, b) = 1$) such that $p|n$ where $n = a^2 + b^2$, then $p \equiv 1 \pmod{4}$.

f. Suppose a, x, b, y are integers satisfying $ax + by = \gcd(a, b)$. Show that $\gcd(x, y) = 1$.

g. Show that if p, q are odd primes such that $p = 2q + 1$, then -4 is a primitive root modulo p . Hint: use problem 5 from HW8.

h. Show that if g is a primitive root mod p , and $gh \equiv 1 \pmod{p}$, then h is a primitive root mod p also.

5. EXTRA CREDIT

1. The Liouville λ -function is defined by $\lambda(1) = 1$ and for $n > 1$ having prime factorization $n = p_1^{e_1} \dots p_r^{e_r}$, $\lambda(n) = (-1)^{e_1 + e_2 + \dots + e_r}$.

(a) Prove that λ is a multiplicative function.

(b) For $n \geq 1$, show that $\sum_{d|n} \lambda(d)$ is 1 if n is a perfect square and 0 otherwise.

(c) Show that for $n \geq 1$, $\sum_{d|n} \mu(d)\lambda(d) = 2^{\omega(n)}$ where $\omega(n)$ is the number of distinct prime divisors of n .

2. Let p be a prime number. Writing positive integers a, b in base p as $a = a_0 + a_1p + a_2p^2 + \dots + a_r p^r$ and $b = b_0 + b_1p + b_2p^2 + \dots + b_s p^s$, we have the usual notion of what it means to have a “carry” when we add a and b by adding their base p digits. Recalling the formula

$$v_p(a!) = \frac{a - (a_0 + a_1 + \dots + a_r)}{p - 1},$$

prove that

$$v_p \binom{a+b}{a}$$

is simply the number of carries that occur in adding a and b in base p .