FINAL EXAM
MATH 115: NUMBER THEORY

Answer each question completely, and give sufficient justification and proof. Write neatly and in complete sentences!

Name	
Student ID	

Problem 1	/10
Problem 2	/10
Problem 3	/15
Problem 4	/15
Problem 5	/15
Problem 6	/10
Problem 7	/15
Problem 8 (Bonus)	/10
Total Score	/90

Date: August 12, 2004.

Problem 1. Let p be an odd prime and $k \in \mathbb{Z}_{>0}$. Show that the congruence

$$x^2 \equiv 1 \pmod{p^k}$$

has only the solutions $x \equiv \pm 1 \pmod{p^k}$.

Problem 2. For which primes p does the congruence

$$x^2 + x + 1 \equiv 0 \pmod{p}$$

have a solution?

Problem 3. The integer $n = pq = 51809$ (with p and q prime) is used in an RSA cryptosystem. Through espionage, you find out that

$$\sigma(n) = 52416.$$

Find p and q.

Problem 4.

(a) Show that the arithmetic function $f(n) = (-1)^{n-1}$ is multiplicative.

(b) Let g be the arithmetic function
$$g(n) = \sum_{d|n} \mu(d) f(d).$$
Prove that $g(n) = 0$ if n is not a power of 2.

Problem 5. Let a be an odd prime, $b \in \mathbb{Z}_{>0}$, and suppose that $p = a^2 + 5b^2$ is prime. Prove that a is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 5$.

Problem 6. Let $n \in \mathbb{Z}_{>1}$ be an integer with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

with p_i prime and $e_i \in \mathbb{Z}_{>0}$. Let

$$m = \operatorname{lcm}\big(\phi(p_1^{e_1}), \phi(p_2^{e_2}), \dots, \phi(p_r^{e_r})\big).$$

(a) Show that for every $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, the order of a modulo n divides m.

(b) Is it true that for every $n \in \mathbb{Z}_{>0}$, there exists an element of order m modulo n?

Problem 7. Let p, q be odd primes for which $p = 2q + 1$. Let $a \in \mathbb{Z}$ be an integer satisfying

$$a \not\equiv -1, 0, 1 \pmod{p}.$$

Show that $-a^2 \bmod p$ is a primitive root modulo p.

Problem 8 (Bonus). Let $n \in \mathbb{Z}$ be an integer with $n > 6$. Show that

$$\phi(n) > \sqrt{n}.$$