FINAL EXAM REVIEW
MATH 115: NUMBER THEORY

Problem 1.

(a) Show that if p is an odd prime of the form $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$, then $p \equiv 1 \pmod 4$.

(b) Let p be a prime of the form $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and a an odd prime. Prove that

$$\left(\frac{a}{p}\right) = 1.$$

Problem 2. Evaluate the Legendre symbol

$$\left(\frac{103}{229}\right).$$

Problem 3. Let $p \in \mathbb{Z}_{>0}$ be an odd prime and $n = 3^p + 1$. Let q be an odd prime divisor of n.

(a) What is the order of 3 modulo n?

(b) Show that q is of the form $q = 2kp+1$ for some integer $k \in \mathbb{Z}_{>0}$.

Problem 4. Find all positive integers n such that $\phi(n) \mid 3n$.

Problem 5.

(a) Use the fact that 3 is a primitive root modulo the prime 79 to find all $x \in \mathbb{Z}/79\mathbb{Z}$ satisfying

$$x^{40} \equiv 2 \pmod{79}.$$

(b) Is 2 a primitive root modulo 79?

Problem 6. Let N be a perfect number. Show that

$$\prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) < \frac{1}{2}.$$

Problem 7. A bank encodes a 3 digit PIN number using RSA encryption with key $e = 835$ and $n = pq = 1411 = 17 \cdot 83$. If Alice's PIN number is encoded as the ciphertext 002, what is her three-digit PIN number?

Problem 8. Let p be the prime

$$p = 131 = 2 \cdot 5 \cdot 13 + 1.$$

Use the fact that 53 has order 5 modulo p and that 39 has order 13 to find a primitive root r modulo p.

Problem 9. Let p be an odd prime with primitive root r.

(a) Let a be an integer with $\gcd(a, p) = 1$. Show that a is a quadratic residue modulo p if and only if $\log_r a$ is even.

(b) Show that if a is a quadratic residue modulo p, then a is not a primitive root modulo p.

(c) Amongst the quadratic nonresidues modulo p, how many are primitive roots?

Problem 10. Let σ_k be the arithmetic function

$$\sigma_k(n) = \sum_{d|n} d^k.$$

(a) Simplify

$$\sum_{d|n} \mu(d)\sigma_k(n/d).$$

(b) Prove that the function

$$S_k(n) = \sum_{d|n} \mu(d)\sigma_k(d)$$

is multiplicative.