Take-Home Midterm
Due Friday October 18 at 11am

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: Do not use any resources on this midterm except **your own brain, course notes, the Math 124 textbooks, and a simple calculator**. You may take as much time as you want, as long as you turn your exam in at 11am on October 18. **There are 6 problems.**

1. (2 points) Let φ denote the Euler φ function. Prove that $\gcd(\varphi(m), \varphi(n)) > 1$ unless either m or n equals 2 or 1.

2. (3 points) Suppose that n is divisible by two distinct primes. Can $(\mathbb{Z}/n)^\times$ be cyclic? Prove or give a counterexample.

3. (2 points) Suppose p is a prime, g is a generator of $(\mathbb{Z}/p)^\times$, and $m \mid p-1$. How many $x \in \mathbb{Z}/p$ satisfy the equation $x^m = g$. (Prove your assertion.)

4. (4 points) Let p be an odd prime and $a \in \mathbb{Z}$. Show that a is a square modulo p if and only if a is a square modulo p^n for any n. Show that this assertion is false if $p = 2$.

5. (a) (2 points) Using the quadratic reciprocity law, show that 5 is a square modulo 211 and 389. (You may assume that both 211 and 389 are prime.)

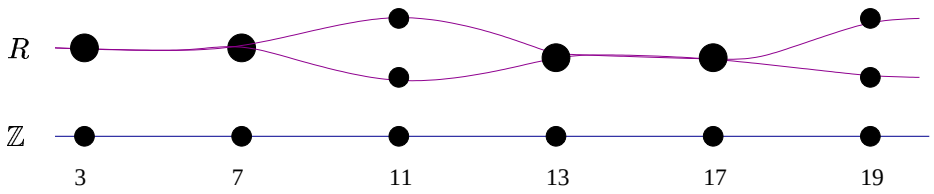
   (b) (5 points) Show how to use the two algorithms from class and the Chinese Remainder Theorem to find **all** square roots of 5 in $\mathbb{Z}/n$, where $n = 211 \cdot 389$.

6. This problem will give you a glimpse into how quadratic reciprocity is central to algebraic number theory. (If you don't know the basic abstract algebra definitions needed to understand this problem, you may consult an abstract algebra textbook. Please state in your solution which book you consult.)

   (a) (2 points) Let
   $$R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}.$$
   Show that R is a ring, but not a field.

   (b) (4 points) Suppose that $p \in \mathbb{Z}$ is a prime with $p \neq 2, 5$. We say that p *splits* in R if $pR = I_1 I_2$ where I_1 and I_2 are non-unit ideals of R (non-unit means neither equals R). Show that 11 splits in R but that 3 doesn't split in R.

   (c) (5 points) Prove that p splits in R if and only if p is a perfect square modulo 5.



Thus quadratic reciprocity gives a simple relationship between whether or not a prime splits in R and the behavior of that prime in $(\mathbb{Z}/5)^\times$. "Class Field Theory" is a vast generalization of this relationship.