Homework Assignment 4
Due Wednesday October 23

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others,* and acknowledge who you work with. There are **7 problems**.

1. In this exercise (which is taken from Andrew's *Number Theory*), we extend the definition of $\left(\frac{a}{m}\right)$ to include the case where m is any odd number. If $m = p_1 p_2 \cdots p_r$ where the p_i are odd primes (not necessarily distinct), then

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right).$$

This extended symbol is called the *Jacobi symbol.* In each of the following problems, assume what we've proved in class and what is in the notes.

   (a) (2 points) Compute $\left(\frac{7}{5!}\right)$.

   (b) (2 points) Prove that if c is odd, then $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$.

   (c) (3 points) Prove that if b and c are odd, then $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$.

   (d) (2 points) Prove that if $a \equiv b \pmod{c}$, where c is odd, then $\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right)$.

   (e) (3 points) Prove that if c is odd, then $\left(\frac{-1}{c}\right) = (-1)^{(c-1)/2}$.

   (f) (4 points) Prove that if a and c are odd and relatively prime, then

$$\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) = (-1)^{\frac{1}{4}(a-1)(c-1)}.$$

   (g) (3 points) Is it possible that $\left(\frac{n}{m}\right) = 1$ while the congruence $x^2 \equiv n \pmod{m}$ has no solution? Prove your answer.

2. (2 points each) Show how to solve each of the following problems by making intelligent use of MAGMA and the MAGMA documentation. Include the MAGMA code you write in your solution.

   (a) Find all pairs $(x, y) \in \mathbb{Z}/17 \times \mathbb{Z}/17$ such that $y^2 + y = x^3 + x$.

   (b) How many positive integers $n < 100$ have the property that $(\mathbb{Z}/n)^\times$ is **not** cyclic?

   (c) The equation $x^2 + 3x + 5 = 0$ has two solutions in the ring $\mathbb{Z}_5$ of 5-adic integers. Find each of them to precision $O(5^{21})$, so your answers should be of the form $a_0 + a_1 5 + a_2 5^2 + \cdots + a_{20} 5^{20} + O(5^{21})$. [Hint: If `R:=pAdicRing(5)`, then the command `R`SeriesPrinting:=true;` switches to printing 5-adics in the form $a_0 + a_1 5 + a_2 5^2 + \cdots$.]

(d) Find an integer x such that $x^2 + 3x + 5 \equiv 0 \pmod{5^{30}}$.

(e) Find the coefficient of q^{289} in the product

$$q \cdot \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2.$$

3. (3 points) Find a prime p such that the equation

$$x^2 + y^2 + z^2 - 7 = 0$$

has no solution in $\mathbb{Z}_p$. (Prove your assertion.)

4. (2 points each) Compute the first 5 digits of the 10-adic expansions of the following rational numbers:

$$\frac{13}{2}, \quad \frac{1}{389}, \quad \frac{17}{19}, \quad \text{the 4 square roots of 41.}$$

5. (3 points) Let $N > 1$ be an integer. Prove that the series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots.$$

converges in $\mathbb{Q}_N$.

6. Prove that 9 has a cube root in $\mathbb{Q}_{10}$ using the following strategy (this is a special case of "Hensel's Lemma".)

   (a) (2 points) Show that there is $\alpha \in \mathbb{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

   (b) (6 points) Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbb{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbb{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

   (c) (2 points) Conclude that 9 has a cube root in $\mathbb{Q}_{10}$.

7. (2 points each)

   (a) Let p and q be distinct primes. Prove that $\mathbb{Q}_{pq} \cong \mathbb{Q}_p \times \mathbb{Q}_q$.

   (b) Is $\mathbb{Q}_{p^2}$ ismorphic to $\mathbb{Q}_p \times \mathbb{Q}_p$ or $\mathbb{Q}_p$?