MATH 304: FINAL EXAM

This exam is open book, open notes, open calculators, etc. – you may consult any resources you wish EXCEPT for other human beings, including your classmates. Please explain your reasoning in complete sentences. The exam is due by Friday 5/11 at noon.

1. Use the Euclidean algorithm to compute $\mathrm{GCD}(1530, 3135)$, then find integers x and y that satisfy the equation

$$1530x + 3135y = \mathrm{GCD}(1530, 3135).$$

2. Compute the values of the following Jacobi symbols: $\left(\frac{374}{945}\right)$ and $\left(\frac{1540}{1773}\right)$.

3. (a) Show that the number of distinct solutions (x, y) (with $0 \leq x \leq p-1$, $0 \leq y \leq p-1$) to the equation $x^2 - y^2 \equiv a \pmod{p}$ is given by:

$$\sum_{y=0}^{p-1} 1 + \left(\frac{y^2 + a}{p}\right).$$

(b) By calculating directly, show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is $p - 1$ if $p \nmid a$ and $2p - 1$ if $p \mid a$. (Hint: use the change of variables $u = x + y$, $v = x - y$.)

(c) Conclude that:

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a, \\ p - 1 & \text{if } p \mid a. \end{cases}$$

4. Let p be an odd prime. Recall the notation (RR), (RN), ... from HW 7, i.e. (RR) is the number of consecutive pairs of quadratic residues in the set $1, \ldots, p-1$, etc.

(a) Show that

$$(RR) + (NN) - (RN) - (NR) = \sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p}\right),$$

then evaluate the sum and show that it is equal to -1 (Hint: use the previous problem).

(b) In HW 7, you showed that:

$$(RR) + (RN) = \frac{p - 2 - \left(\frac{-1}{p}\right)}{2}$$
$$(NN) + (NR) = \frac{p - 2 + \left(\frac{-1}{p}\right)}{2}$$
$$(RR) + (NR) = \frac{p-3}{2}$$
$$(RN) + (NN) = \frac{p-1}{2}.$$

Keeping these facts in mind, prove that:

$$(RR) = \frac{1}{4}\big(p - 4 - (-1)^{(p-1)/2}\big).$$

5. Recall that an integer a is a quadratic residue modulo p if there exists an integer b such that $a \equiv b^2 \pmod{p}$. More generally, we say that a is an nth power residue modulo p if there exists an integer b such that $a \equiv b^n \pmod{p}$ (thus quadratic residues are the same thing as 2nd power residues).

   (a) Find all 7th power residues modulo 13.

   (b) Find all 128th power residues modulo 257.

6. Let p be an odd prime number. Show that 3 is a quadratic residue modulo p if and only if $p \equiv 1$ or $11 \pmod{12}$.

7. Factor the following Gaussian integers into a product of Gaussian primes:

   (a) $11 + 55i$

   (b) $-53 + 583i$

   (c) $6132 - 13140i$

8. Let g be a primitive root modulo m. Prove that g^k is also a primitive root modulo m if and only if k and $\phi(m)$ are relatively prime.

9. Express $\sqrt{11}$ as a continued fraction. What is its periodicity?

10. For each positive integer n, let $F(n)$ be the average value of all positive integers $< n$ that are relatively prime to n. Prove that $F(n) = n/2$. (Hint: first ague that if a is relatively prime to n, then $n - a$ is also relatively prime to n.)

11. Find all solutions x (with $0 \leq x \leq 96$) to the congruence

$$13x^{385} + 73x^{304} + x^{290} + 10x^{193} + 24x^{112} + 70x + 76 \equiv 0 \pmod{97}.$$

12. (Extra Credit) In the final lecture, we discussed the Riemann Zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

In this problem, you will justify the presence of $\zeta(s)$ in a course about number theory by showing that the zeta function knows about the fundamental theorem of arithmetic.

Consider the following infinite product:

$$\prod_{p} \frac{1}{1-p^{-s}}.$$

Here, the product ranges over all prime numbers p, so we can expand the product term by term as:

$$\prod_{p} \frac{1}{1-p^{-s}} = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdots$$

Prove that this product is equal to the Riemann Zeta function:

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}}.$$

(Do not worry about issues of convergence, just present an argument that the two expressions are equal.)