Math 346/377: Number Theory

Final Exam

Tuesday, April 19

The 8 *questions in this exam are each worth* 15 *points. Students registered for 346 will be graded out of 100, and students registered for 377 will be graded out of 120. (In particular, a student in Math 346 may elect to omit one question in the exam and still get full grades.) Calculators are not allowed – and would not be useful in any case!*

1. Compute a greatest common divisor (gcd) of $11 + i$ and 61 in the ring R of Gaussian integers. (The ring consisting of integer linear combinations of 1 and $i = \sqrt{-1}$). Use your calculation to write 61 as a sum of two integer squares.

2. State the definition of a *Gauss sum*. Use what you know about Gauss sums (which you may state without proof) to express $\sqrt{11}$ as a linear combination of roots of unity with integer coefficients.

3. a) What is the cardinality of $(\mathbf{Z}/69\mathbf{Z})^\times$?
   b) What is the largest order of an element in $(\mathbf{Z}/69\mathbf{Z})^\times$?

4. Recall that an odd prime p is called a *Sophie Germain prime* if $\frac{p-1}{2}$ is also prime. Let p and q be distinct Sophie Germain primes, and let g be an integer which is a primitive root modulo p and modulo q. Given an integer a with $\gcd(a, pq) = 1$, show that the equation

$$g^x \equiv a \pmod{pq}$$

has a solution if and only if $\left(\frac{a}{pq}\right) = 1$, where $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$ is the Jacobi symbol.

5. a) Give the definition of the Riemann zeta-function $\zeta(s)$. For which values of s is $\zeta(s)$ defined?

b) Write down (without proof) Euler's formula for $\zeta(s)$ as a product over the primes.

c) Show that $\sum_p \frac{1}{p}$ diverges, where the sum is taken over all the primes.

6. Compute the continued fraction expansion of $\sqrt{11} \simeq 3.32$, and write down the first three convergents of this continued fraction. Use this to write down a fundamental solution to the Pell equation

$$x^2 - 11y^2 = 1.$$

7. Let r be a real irrational number. Show that there are infinitely many distinct rational numbers p/q such that

$$|p/q - r| < 1/q^2.$$

8. a) Prove Fermat's little theorem that if p is prime, then

$$a^{p-1} \equiv 1 \pmod{p}$$

for all integers a that are relatively prime to p.

b) Show that the converse is false by proving that

$$a^{n-1} \equiv 1 \pmod{n},$$

for all a that are relatively prime to $n = 1105 = 5 \cdot 13 \cdot 17$.