189-346B/377B: Number Theory

Final Exam

Tuesday, April 17

The 8 *questions in this exam are each worth* 15 *points, and are arranged (in my opinion!) roughly in order of increasing difficulty. Students registered for 346 will be graded out of 100, and students registered for 377 will be graded out of 120. Calculators are not allowed (and would not be useful in any case!)*

1. Let R be the ring of Gaussian integers. State (without proof) what it means to say that R has a Euclidean division algorithm, and give the quotient and remainder for the division of $7 + 5i$ by $3 + i$.

2. State the law of quadratic reciprocity. Give a simple characterisation of the set of primes p for which 3 is a quadratic residue modulo p.

3. a) Define what it means for an integer g to be a *primitive root* modulo a prime p.
b) Let b be an integer not divisible by the prime p. Define the *discrete logarithm mod* p of b to the base g.
c) Show that 2 is a primitive root modulo 13 and calculate the discrete logarithm of 11 modulo 13, $\log_2(11)$.

4. A prime p is called a *Sophie Germain prime* if it is of the form $2q+1$, where q is also a prime. If p is a Sophie Germain prime, and $a \neq 0, 1, -1 \pmod{p}$ is an integer, show that at least one of a or $-a$ is a primitive root mod p.

5. a) Write down the continued fraction expansion of $\sqrt{3}$.
b) Evaluate the infinite continued fraction

$$x = 6 + \frac{1}{6 + \frac{1}{6+\cdots}}.$$

6. a) Show that the Pell equations $x^2 - 2y^2 = -1$ and $x^2 - 2y^2 = 1$ each have infinitely many solutions, and explain how you could write down an infinite set of such solutions.
b) A *triangular number* is an integer of the form $n(n-1)/2$. Show that there are infinitely many triangular numbers which are perfect squares, i.e., that the Diophantine equation $\frac{n(n-1)}{2} = m^2$ has infinitely many integer solutions (m, n). (Hint: you will be using part a)!)

7. Let $f(x) \in \mathbf{Z}[x]$ be a polynomial of degree 3 with integer coefficients, which is not divisible by either 7 or 11.
a) Show that the congruence equation

$$f(x) \equiv 0 \pmod{77}$$

has at most 9 solutions in $\{0, 1, \ldots, 76\}$.
b) Show that the congruence equation

$$f(x) \equiv 0 \pmod{49}$$

has at most 8 solutions in $\{0, 1, \ldots, 48\}$.

8. a) State Dirichlet's Theorem on primes in arithmetic progressions.
b) Give an elementary proof, in the spirit of Euclid's proof of the infinitude of primes, that there are infinitely many primes of the form $2 + 3k$.
c) Explain the argument that Dirichlet used to show that there are infinitely many primes of the form $1 + 3k$ and $2 + 3k$.