Math 124 Final Examination

Due Sunday 12 January 2003 by 5pm

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

This is the Fall 2002 Math 124 take-home final examination. *You may not discuss the problems with anyone.* You are allowed to look at books, course notes, web pages, and use a computer (MAGMA, Maple, etc.), but you must acknowledge any sources that you use. If you find the complete solution to one of these problems in a book, then good job—you are allowed to copy it.

For your convenience, the complete course notes are available as a single file at

`http://modular.fas.harvard.edu/edu/Fall2002/124/stein/`.

All problems are worth the same number of points (e.g., problems 2 and 3 are worth the same number of points). Choose and do **EXACTLY 8** of the following 12 problems (e.g., all parts of problems 1, 2, 3, 5, 6, 10, 11, 12). Choose wisely; some problems might be easy, others difficult open problems, and some might ask you to prove something that is false (say what is wrong with the problem for full credit). At least eight are not open problems! Clearly indicate which problem you are attempting and which you are omiting.

If you have trouble getting into the math department to hand in your exam, call my office phone (617-495-1790) or my mobile phone (617-308-0144) so I can open the door.

1. The usual Euler φ function is a map $\mathbb{Z} \to \mathbb{Z}$. Fix a prime number p, and define a polynomial analogue of Euler's function by
$$\Phi(f(x)) = \#(\mathbb{F}_p[x]/(f(x)))$$
(let $\Phi(0) = 0$). Thus, e.g., if $p = 2$ then $\Phi(x^2 + 1) = 4$. Say that polynomials $f(x), g(x) \in \mathbb{F}_p[x]$ are coprime if
$$\gcd(f(x), g(x)) = 1,$$
that is, $f(x)$ and $g(x)$ have no common roots in $\overline{\mathbb{F}}_p$.
   (a) Prove that Φ is multiplicative, in the sense that if $f(x)$ and $g(x)$ are coprime, then
$$\Phi(f(x)g(x)) = \Phi(f(x)) \cdot \Phi(g(x)).$$
   (b) The Euler φ function does not satisfy $\varphi(nm) = \varphi(n)\varphi(m)$ for *all* integers n, m; for example, $6 = \varphi(3 \cdot 3) \neq 4$. Does Φ satisfy $\Phi(f(x)g(x)) = \Phi(f(x)) \cdot \Phi(g(x))$ for *all* polynomials $f(x)$ and $g(x)$? Give a proof or counterexample.
2. Write an insightful review of the book *Uncle Petros and Goldbach's Conjecture*. (Your intended audience is a "typical Harvard undergraduate with greater than usual interest in mathematics", and your review should be at least one page long.)
3. (a) Characterize the positive integers n such that $\mathbb{Z}/n$ is a field.
   (b) Characterize the positive integers n such that $(\mathbb{Z}/n)^\times$ is cyclic.
   (c) Characterize the positive integers n such that n is a sum of two rational squares.
   (d) Characterize the positive integers n such that $1/n$ is a sum of two rational squares.
4. At a conference at the American Institute of Mathematics, Victor Rotger from Barcelona asked me a question about primes. Call a prime number p *Victor* if for every prime $\ell < p/4$ with $\ell \equiv 1 \pmod 8$, we have $\left(\frac{-\ell}{p}\right) = -1$ (that's the quadratic residue symbol). Victor's Question: Are there infinitely many Victor primes? Do numerical computations and formulate an intelligent response to Victor's question. (You don't have to prove anything to get full credit on this problem; just compute and give a reasonably intelligent interpretation of what you find.)

5. (a) Factor the integer
$$n = 10^{100} + 598 \cdot 10^{50} + 67497$$
as a product ab with $a, b > 1$.

(b) Factor the integer
$$n = 10^{90} + 367 \cdot 10^{60} + 38559 \cdot 10^{30} + 1190673$$
as a product pqr with p, q, r integers > 1. You may use that
$$\varphi(n) = 10^{90} + 364 \cdot 10^{60} + 37828 \cdot 10^{30} + 1152480$$
and
$$\sigma(n) = 3 \cdot 10^{30} + 367,$$
where $\sigma(n)$ is the sum of the divisors of n.

6. (a) Find a rational number a/b with $|b| < 10^7$ such that
$$\frac{a}{b} = -1.2547643920645834.$$

(b) Find three distinct solutions to $x^2 - 67y^2 = 1$ with x, y positive integers.

7. (a) Let $f = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ be a quadratic form whose discriminant d is a perfect square, possibly 0. Show that f factors as $(\alpha_1 x + \beta_1 y)(\alpha_2 x + \beta_2 y)$.

(b) Let $f = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ be a quadratic form. Show that there exists x_0, y_0 not both zero such that $f(x_0, y_0) = 0$ if and only if the discriminant of f is a perfect square.

(c) Divide the following set of binary quadratic forms up into equivalence classes modulo the action of $\mathrm{SL}_2(\mathbb{Z})$:
$$S = \{x^2 + y^2,\ -562x^2 + 860xy - 329y^2,\ -x^2 - y^2,\ -x^2 + y^2,$$
$$x^2 + 2yx + 2y^2,\ x^2 + xy - y^2,\ x^2 + xy + 3y^2,\ x^2 - 2y^2\}.$$

(d) Compute the discriminant of the ring of integers of $\mathbb{Q}(\sqrt{25456})$.

8. Consider a right triangle the lengths of whose sides are integers. Prove that the area cannot be a perfect square.

9. Assume the truth of Fermat's last theorem. Deduce that there is no right triangle with rational side lengths and area 1.

10. (a) Does $15x^2 - 7y^2 = 9$ have a solution in the integers?

(b) Does $15x^2 - 7y^2 = 9$ have a solution in the rational numbers?

(c) Does $x^3 + 2y^3 + 4z^3 = 9w^3$ have any nontivial rational solution?

(d) Does $x^3 + 2y^3 = 7(u^3 + 2v^3)$ have any nontrivial rational solutions?

(e) Show that there are no positive integers m and n such that $m^2 + n^2$ and $m^2 - n^2$ are both perfect squares.

11. (a) Suppose $D < -4$ is a square-free integer, let $K = \mathbb{Q}(\sqrt{D})$ and let $\mathcal{O}$ be the ring of integers in K. Prove that the group of units in $\mathcal{O}$ has order 2.

(b) For which squarefree integers D is the prime 2 ramified in $\mathbb{Q}(\sqrt{D})$? (We say that 2 *ramifies* in $\mathbb{Q}(\sqrt{D})$ if $2\mathcal{O}_K = \wp^2$ for some prime $\wp$ of $\mathcal{O}_K$.)

12. Some elliptic curve questions:

(a) Show that the number of pairs (a, b) with $a, b \in \mathbb{F}_p$ such that $4a^3 - 27b^2 \neq 0$ is exactly $p^2 - p$.

(b) Suppose $p > 3$ and $a, b \in \mathbb{F}_p$ are such that $4a^3 + 27b^2 = 0$ with $a \neq 0$. Let r be the unique solution to $-2ar = 3b$. Show that r is a repeated root of the polynomial $x^3 - ax - b$.

(c) Suppose that the polynomial $f(x) = x^3 + ax + b \in \mathbb{F}_p[x]$ has no repeated roots, and let E be the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = f(x)$. Show that
$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x=1}^{p} \left(\frac{f(x)}{p}\right).$$