Math 124: Final Examination

Due at 5pm on Sunday, January 13th, 2001

William Stein

Math 124 Harvard University **Fall 2001**

Instructions. *Thoroughly justify all answers. While taking the exam, please do not discuss these problems with anyone else, and consult only those references that are explicitly mentioned on the Math 124 web page. (If you inadvertently stumble upon a solution while reading or studying for another class, e.g., Math 122, please make that clear in your solution.)*

If you wish to use the result of a homework problem in the solution of one of the problems below, include your solution of that homework problem (a photocopy is acceptable). You may use any result that was proved in the lecture notes or the course textbooks, but please give a precise reference.

There are 10 problems, each worth 10 points, and problem n was "inspired" by homework assignment n. Problems 3, 5(ii), 6, 7, and 10 would be difficult to do without a computer; for these problems, you do not have to use PARI, though I recommend that you do.

Turning in the exam. *The exam is due on Sunday, January 13th at 5pm. Some of you don't have a key to the math department, so you might not be able to go to my office (SC 515) and give me your exam. If this is the case, call me at (617)495-1790 or (617)308-0144, and I'll come downstairs and meet you at the elevator, and if that doesn't work just slide it under my door on Monday morning (but no later!!).*

1. The Fibonnaci numbers F_n are defined as follows: $F_1 = F_2 = 1$ and for $n \geq 3$, $F_n = F_{n-2} + F_{n-1}$. Prove that for every integer n, the greatest common divisor of F_n and F_{n+1} is 1.

2. Let n be an *odd* positive integer, and let $f(n) = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$, where $(\mathbb{Z}/n\mathbb{Z})^*$ is the group of integers modulo n that are coprime to n.

   (i) (5 points) Prove that $f(n) \in \{\pm 1\}$.

   (ii) (5 points) Find a formula for $f(n)$ in terms of the number of prime factors of n. [Hint: You might find the result of Problem 4 on this exam useful.]

3. Consider the RSA cryptosystem with public key

   $$(n, e) = (409333777761339043060441442265769, 254815086050320391994953910098867).$$

   (i) (3 points) A secret message has been encoded as the number $m = 12939458$. Encrypt the number m using the above RSA cryptosystem.

   (ii) (4 points) Find the decoding key d; i.e., "break" this RSA cryptosystem.

   (iii) (3 points) Decrypt 32057244346049879915981853097024 6. [Hint: The answer won't look like total nonsense.]

4. Let p be an odd prime. Prove that $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic for all $n \geq 1$. (I.e., prove that there is an element of $(\mathbb{Z}/p^n\mathbb{Z})^*$ of order $\#(\mathbb{Z}/p^n\mathbb{Z})^*$.)

5. (i) (5 points) Evaluate the infinite continued fraction $[3, \overline{1, 4}]$.
   (ii) (5 points) Determine the infinite continued fraction of $(1 + \sqrt{23})/5$.

6. Write $m = 1062155618907279051761554 73$ as a sum of two positive integer squares.

7. Determine the structure of the group C_D of equivalence classes of primitive positive definite binary quadratic forms of discriminant $D = -888$. Your answer should consist of C_D expressed as a product of cyclic groups. [Hint: Use the functions in `forms.gp` from Lecture 24.]

8. This problem describes a special case of a theorem that was originally proven by Eichler and Shimura. The modularity theorem says that a similar statement is true for every elliptic curve over $\mathbb{Q}$.

   (i) (3 points) Let E be the elliptic curve given by the equation

   $$y^2 = x^3 - 4x^2 + 16.$$

   Let $M_p = \#E(\mathbb{Z}/p\mathbb{Z})$ be the number of points on E over $\mathbb{Z}/p\mathbb{Z}$ (don't forget the point at infinity). Calculate M_p for $p = 3, 5, 7, 13, 17, 19, 23, 29$.

   (ii) (3 points) Let $f(q)$ be the (formal) power series given by the infinite product

   $$f(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + \cdots$$

   Let N_n be the coefficient of q^n in $f(q)$,

   $$f(q) = \sum_{n=1}^{\infty} N_n q^n.$$

   Calculate N_n for $n < 30$.

   (iii) (4 points) For each $p = 3, 5, 7, 13, 17, 19, 23, 29$, compute the sum $M_p + N_p$ of the quantities calculated in (i) and (ii), then formulate a conjecture as to what this value should be for any prime $p > 29$.

9. Let E be the elliptic curve defined by the equation $y^2 = x^3 + x$. For each odd prime p, let N_p be the number of points in the group $E(\mathbb{Z}/p\mathbb{Z})$ of points on E with coordinates in $\mathbb{Z}/p\mathbb{Z}$.

   (i) (5 points) For each odd prime $p < 30$, find N_p.
   (ii) (5 points) Make a general conjecture for the value of N_p when $p \equiv 3 \pmod 4$, and prove your conjecture.

10. Demonstrate how to use the elliptic curve factorization method to completely factor the integer 124531325385603661726997. (You may use the `isprime` function of PARI to verify primality of numbers.)

11. (Extra credit: automatic A in course, plus fame and glory) Let E be the elliptic curve $y^2 + xy = x^3 - x^2 - 79x + 289$. Prove that $L^{(2)}(E, 1) = 0$, where $L^{(2)}(E, s)$ is the second derivative of the L-series associated to E.