Math 124 Final Exam

Deadline: The exam is due in my office (SciCen 334) by noon on Monday, May 8. If you come by early before I'm there, you can slip it under my door.

Disclaimer, Terms, and Conditions:

You may not discuss the exam with anyone except myself. You may *only* consult the following:

- The beloved text (Davenport).
- Your class notes.
- Old HW sets and Lionel's solution handouts.

You may also use a calculator or computer to ease your labors.

If you have any questions, you can contact me by the following methods.

- email: nathand@math.harvard.edu
- phone: 5-5340 (Office) 576-3043 (Home 9am-10pm only please, but other than that...)
- office: SciCen 334, stop by anytime.

While I've checked the exam carefully, there could still be a mistake somewhere. Please contact me if you think something is fishy.

Good luck and have fun!

Actual exam:

All questions are weighted equally. On problems that ask you to do one of the following, you can do both (if you want) and I'll give you the highest score earned on that problem.

1. Let $p \geq 5$ be a prime with $p \equiv 3 \mod 4$. Suppose that $q = 2p + 1$ is also prime. Prove that $2^p - 1$ is not prime.
2. When is a rational prime p in $\mathbb{Z}$ a prime in the Gaussian integers $\mathbb{Z}[i]$?
3. **Do ONE of the following:**
   (a) Prove that there are infinitely many $n \in \mathbb{N}$ such that $3|n$ and $n + 1$ and $n/3 + 1$ are both perfect squares.
   (b) A number $n \in \mathbb{N}$ is called k-abundant if $\sigma(n) > kn$. Prove that there are infinitely many k-abundant numbers for any k.
4. Prove that there are infinitely many primes of the form $8k + 7$.

5. **Do ONE of the following:**

   (a) If p is an odd prime such that $q = 2p + 1$ also prime, show that there are no integral solutions to $x^p + y^p + z^p = 0$ with $p \not| xyz$. Hint: Look at

   $$-x^p = (y + z)(z^{p-1} - z^{p-2}y + \cdots + y^{p-1})...$$

   (b) Give a formula (similar to what we had for Pythagorean Triples) for all solutions to

   $$x^2 + y^2 = z^3$$

   with x and y relatively prime integers.

6. **Do ONE of the following:**

   (a) Let $k \in \mathbb{N}$. Let $D_k = (3^k + 1)^2 + 3$. Show that the continued fraction expansion of $\sqrt{D_k}$ has period of length $6k$.

   (b) Prove or Disprove: If $x^2 - dy^2 = -1$ has a solution with $x, y \in \mathbb{N}$ then so does $x^2 - d^n y^2 = -1$ for all *odd* $n \geq 1$.

7. Let π be a prime in the Gaussian integers $\mathbb{Z}[i]$. Let $\alpha \in \mathbb{Z}[i]$ with α not divisible by π. Prove that

   $$\alpha^{N(\pi)-1} \equiv 1 \mod \pi.$$

8. Let

   $$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

   define an elliptic curve over $\mathbb{F}_p$, for p an odd prime.

   (a) For any $n \in \mathbb{N}$, show that there are most n^2 points on $C(\mathbb{F}_p)$ of order dividing n, that is, such that $nP = \mathcal{O}$.

   (b) Use (a) to show that $C(\mathbb{F}_p)$ is either cyclic or a product of 2 cyclic groups.

9. Let $p \equiv 3 \mod 4$ be a prime, and let $b \in \mathbb{F}_p$ be non-zero.

   (a) Show that the equation

   $$v^2 = u^4 - 4b$$

   has $p - 1$ solutions (u, v) with $u, v \in \mathbb{F}_p$.

   (b) Show that if (u, v) is a solution of the equation in (a), then

   $$\phi(u, v) = \left(\frac{1}{2}(u^2 + v), \frac{1}{2}u(u^2 + v)\right)$$

   is a point on the elliptic curve:

   $$C : y^2 = x^3 + bx.$$

   (c) Prove that the curve C defined in (b) satisfies $\#C(\mathbb{F}_p) = p + 1$.