due-02-19.sagews

February 17, 2014

Contents

1 Homework 5 Due Feb 19, 2014

1.1 Instructions

- Put your solutions in the empty space below the problem.
- When youre done, open the worksheet, and copy/paste the URL to this worksheet into an email to wstein@gmail.com with the subject math 480: homework 02-12.

1.2 Problems

1.2.1 Problem 1: Computing the cardinality of an elliptic curve modulo p.

a. Let E be the elliptic curve $y^2 = x^3 + 2x + 3$ over the finite field $\mathbf{F}_p$, where $p = 2^{107} - 1$. Compute the cardinality of the group $E(\mathbf{F}_p)$ using Sage. (Hint: this is a one-liner in Sage see the worksheet for 2014-02-07.)

b. Give an estimate for how long you think it would take a single Sage command (one processor) to compute the cardinality of the group of rational points on $y^2 = x^3 + 14x + 2$ over the finite field $\mathbf{F}_p$, where $p = 2^{44,497} - 1$. Your estimate should be at least as precise as a few seconds, a few minutes, a couple of days, a couple of months, a couple of years, etc. (Dont worry about RAM requirements.) Your estimate should be supported by actual computations. The idea is to compute the cardinality of several other similar groups, but for various size primes, and come up with a mathematical model for how the time grows as a function of the prime.

1.2.2 Problem 2: The ABC Conjecture

An abc triple is a triple of positive integers a, b, c such that $a + b = c$ and $\gcd(a, b) = 1$.

The quality of an abc triple is

$$q(a, b, c) = \frac{\log(c)}{\log(\prod_{p|abc} p)}.$$

(Here $\prod_{p|abc} p$ means the product of the prime divisors of abc. Thus if $abc = 6 \cdot 3^2 \cdot 5$, then $\prod_{p|abc} p = 2 \cdot 3 \cdot 5 = 30$.)

Conjecture (The abc conjecture) For every $\epsilon > 0$, there are only finitely many abc triples such that $q(a, b, c) > \epsilon$.

Exercises:

- Prove that if a, b, c is an a, b, c triple then $\gcd(b, c) = 1$ and $\gcd(a, c) = 1$.
- Prove that for any triple a, b, c, we have $q(a, b, c) > \frac{1}{3}$.
- Give an example of a triple a, b, c with $q(a, b, c) > 1$.

1.2.3 Problem 3: Your project

a. Make changes to your project based on the feedback from somebody else in class. (To get credit, include their feedback below so I can check that you addressed it.)

b. Write more until your project has at least 5 solid pages of content. (I will grade based on quantity, not quality this time.) Im making the overall homework shorter this time so you can spend morime working on your project.