Math 168: Homework Assignment 3

William Stein

Due: Wednesday, Oct 19, 2005

The problems have equal point value, and multi-part problems are of the same value. You are allowed to use a computer on any problem, as long as you include the exact code used to solve the problem with your solution. Any software systems (e.g., Magma, SAGE, Mathematica, C) are allowed.

You'll need a computer for all but one of these problems.

1 Problems

1. (a) Consider the set of numbers $59 + 1 \pm s$ for $s \leq 15$. How many are B-power smooth for $B = 20$?

   (b) Find the proportion of primes p in the interval from 10^{12} and $10^{12} + 1000$ such that $p - 1$ is $B = 10^5$ power smooth.

2. Illustrate factorization of the integer 154433 using the Pollard $p - 1$ method with parameters of your choosing.

3. Illustrate factorization of the integer 154433 using Lenstra's elliptic curve method with parameters of your choosing.

4. Go the Certicom website:

   `http://www.certicom.com/index.php?action=res,ecc_challenge`

   Copy down the next unsolved elliptic curve cryptography challenge. Write a program (in SAGE, MAGMA, or GP, etc.) that would crack that challenge if allowed to run for a trillion billion years.

5. Let E be the elliptic curve from the notes used in MS-DRM, let B be the point on E (on the top of page 114), and let n be Nikita's private key (right below the definition of B).

   (a) Compute the public key (p, E, B, nB).

   (b) Find a point P on E such that the first 7 digits of the x-coordinate of P are 1234567.

   (c) Encrypt P, i.e., compute the tuple $(rB, P + r(nB))$ for some randomly chosen r.

   (You can paste these numbers out of the pdf file for the notes.)