Homework 10: Elliptic Curves II

Due Wednesday, December 5

William Stein

Math 124 Harvard University **Fall 2001**

This is it, the last homework assignment! (There is no homework due December 12.)

1. (5 points) Make up a simple example that illustrates how to use the ElGamal elliptic curve cryptosystem (see Lecture 29). You may mention Nikita and Michael if you wish. Be very clear about what you are illustrating so that the grader can effortlessly understand your example.

2. (5 points) Make up an example that illustrates an interesting aspect of the Pollard $(p-1)$ factorization method.

3. (5 points) Make up an example that illustrates something that you consider an interesting aspect of Lenstra's elliptic curves factorization method.

4. (10 points) Let R be a ring. We say that Fermat's last theorem is false in R if there exists $x, y, z \in R$ and $n \in \mathbb{Z}$ with $n \geq 3$ such that $x^n + y^n = z^n$ and $xyz \neq 0$. For which prime numbers p is Fermat's last theorem false in the ring $\mathbb{Z}/p\mathbb{Z}$?[1]

[1] This problem was on the dreaded Harvard graduate school qualifying examination this year. Every one of the students who took that exam got this problem right.