Math 571-01, Cryptography Project 02
Quadratic Sieve
University of Massachusetts, Amherst

Matthew Gramigna
Wei Xie
Barry Greengus

April 3, 2017

1 Introduction

Put introduction here.

2 Motivation via Difference of Squares Factoring

Why we care about QSieve. It's the most important step of dif sqaures factoring, etc.

3 Overview of Quadratic Sieve

Explain how quadratic sieve works TODO more info +equations + fix "=" to congruent
Setup Step: Given number N and set of primes P, where all elemenet in P ¿= B, set a=floor of the sqrt(N), set a quadratic polynomial. we will use F(T) = T$\hat{2}$ - 221.

Step 1: build a list of F(a) to F(L(a)). TODO define L(), explain why we use it. explain why we start at a.

Step 2: For i=2 to B, where i=some p in P or is prime factor of some p in P:

Step 3: Predict where division of elem in list by i CAN happen.
if p — F(T), then T$\hat{2}$ = N mod p has a solution, else no solution so you cant divide by p.
So, if p odd and T$\hat{2}$ = N mod p has two solutions, a and b. all mulitples of those solutions can also be divided by the p

Step 4: Divide all multiples of the solutions a and b in the list by p

Step 5: Whenever the quotient of a list element is 1, it's prime factors are clearly only primes ¡= B and is thus B-smooth

4 Implementation

We used GP, TODO more info