

RSA Project paper

RSA Group

Li Qiu

Yiwei

Leester Mei

Akeem

November 27, 2016

1 Quadratic Sieve

Quadratic Sieve method is actually discovered step by step. It is a optimization of Dixon's Factorization Method. So, to learn what is Quadratic Sieve, we have to understand Dixon's Method. And Dixon's Method is also related to Fermat's Factorization and Kraitchik's Factorization Method. Here, I will briefly introduce these three factorization methods.

1.1 Brief Hierarchies Of Quadratic Sieve

1.1.1 Fermat's Factorization

Fermat factorization method is very straight forward, if we are going to factor n , since:

$$n = ab \Rightarrow \left[\frac{1}{2}(a+b) \right]^2 - \left[\frac{1}{2}(a-b) \right]^2$$

let

$$x = \frac{1}{2}(a+b), y = \frac{1}{2}(a-b) \Rightarrow n = x^2 - y^2$$

Therefore, we just need to find a x satisfy:

$$Q(x) = y^2 = x^2 - n$$

and obviously, the smallest x is $\lceil \sqrt[2]{n} \rceil$ and if we can find a $Q(x)$ is a square root, then we can find the factors of n which is $a = x + y, b = x - y$

1.1.2 Kraitchik's Factorization

Kraitchik's method is instead of checking $x^2 - n$ is a square, he suggests to check $x^2 - kn$ a square number, which is equivalent to find $y^2 \equiv x^2 \pmod{n}$. And the only interesting solution is $x \not\equiv \pm y \pmod{n}$. Besides this, instead of seeking one $x^2 - n$ is square, he was

looking for a set of number $\{x_1, x_2, \dots, x_k\}$ such that $y^2 \equiv \prod_{i=1}^k (x_i^2 - n) \equiv \prod_{i=1}^k x_i^2 \equiv \left(\prod_{i=1}^k x_i \right)^2$

\pmod{n} is square. if he can find a relation like this, then, the factors of n is $\gcd(|y \pm \prod_{i=1}^k x_i|, n)$

1.1.3 Dixon's Factorization

One of the great improvement of Dixon's method comparing to the method before is that he replace the requirement from "is a square of an integer" to "has only small prime factors". To explain this we need introduce 2 concepts which are **Factor Base** and **Smooth Number**.

Factor Base is a set of prime factors $S_{fb} = \{p|p \leq B\}$ where B is some integer.

Smooth Number is a integer that all its prime factor within the **Factor Base** which means if we choose integer B and Q , $Q = \prod_{i=1}^k p_i^{a_i}$ where $a_i, k \in \mathbb{Z}, p_i \in S_{fb}$. We called Q is a **B-Smooth** Number.

Recall Kraitchik's Method, he suggests to find a relation $y^2 \equiv \left(\prod_{i=1}^k x_i\right)^2 \pmod{n}$. But

Dixon's idea is different, he is looking for the relation of $y^2 \equiv Q \equiv \prod_{i=1}^k p_i^{a_i} \pmod{n}$ where

$a_i \in \mathbb{Z}$, $k = |S_{fb}|$, $p_i \in S_{fb}$. For each relation is found, it can represent as a exponent vector $\vec{v} = \{a_1, a_2, \dots, a_k\}$ over \mathbb{F}_2 , and after finding k relations, we have a matrix $m = \{\vec{v}_i | i \leq k\}$. And searching the null space of this matrix, could help us to find the square integer. Since $M\vec{v} = 0$ where $\vec{v} \in \text{Null Space}$, we know which rows sum together are equal to 0, which also implies the products of corresponding Q to that row is a square integer. After found the relation, let $x^2 = \prod_i Q_i$, the factor of n is $\gcd(y \pm x, n)$

1.2 Math and Algorithm in Quadratic Sieve

1.2.1 Legendre Symbol & Quadratic Reciprocity

1.2.2 Shanks Tonelli's Algorithm

1.2.3 Logarithm Approximation

1.3 Sieving In Quadratic Sieve

1.3.1 How we do it

1.4 16 mins to less than 1s