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 $\{x_1, x_2, \ldots, x_k\}$ 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 $y^2 \equiv Q \equiv \displaystyle\prod_{i=1}^{k} p_i^{a_i} \pmod n$ 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 $\vec{v} = \{a_1, a_2, \ldots, a_k\}$ 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 $\vec{v} \in \mathit{Null\ Space}$, 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 $x^2 = \prod_{i}^{k} Q_i$, the factor of n is $gcd(y \pm x, n)$

1.2 Math and Algorithm in Quadratic Sieve

1.2.1 Legendre Symbol & Laws of Quadratic Reciprocity

From now, we know two ways to test whether n is a quadratic residue mod p, one is Euler Criterion, and the other is Legendre symbol. In practice, probably because we factor base is not insanely large, we did not noticed how much faster does Legendre symbol than the Euler criterion (since Euler criterion is an $\mathcal{O}(\log n)$ algorithm).

1.2.2 Shanks Tonelli's Algorithm

Shanks Tonelli's Algorithm is a faster algorithm to find the root of a quadratic residue. In class, we only learn the simple case, which is when $p \equiv 3 \pmod 4$. Since this algorithm is very important for quadratic sieve, we are going to prove the algorithm.

Given $x^2 \equiv n \pmod p$, we want to find x.

let $p - 1 = 2^e S,\ x \equiv n^{\frac{S+1}{2}} \pmod p,\ t \equiv n^S \pmod p$.

we have, $x^2 \equiv n^{S+1} \equiv n^S n \equiv tn \pmod p$, notice that,

if $t \equiv 1 \pmod p$, our $x = \pm n^{\frac{S+1}{2}} \pmod p$

if $t \not\equiv 1 \pmod p$, then find a quadratic non-residue a and let $b \equiv a^S \pmod p$, then, $b^{2^e} \equiv (a^S)^{2^e} \equiv a^{2^e S} \equiv a^{p-1} \equiv 1 \pmod p$, Since we know a is a quadratic non-residue, By Euler Criterion, $a^{\frac{p-1}{2}} \equiv b^{2^{e-1}} \equiv -1 \pmod p \to 2^e$ is the order of b.

we have $t^{2^e} \equiv 1 \pmod p$, and we let $2^{e'}$ be the order of $t \pmod p$, since n is a quadratic residue, $e' \leq e - 1$

let $c \equiv b^{2^{e-e'-1}} \pmod p$, $b' \equiv c^2$, $t' = tb'$, $x' = cx$, after this construction, $x'^2 \equiv t'n \pmod p$ still holds, since $x'^2 \equiv b^{2^{e-e'}} x^2 \equiv tnb^{2^{e-e'}} \equiv tnb' \equiv t'n \pmod p$. And we can repeat this process until $e' = 0$ we can find a $t' = 1$, and our final solution is $\pm x' \pmod p$

1.2.3 Logarithm Approximation

Logarithm approximation plays a very import role in implementing the sieving process. Since we use the polynomial $Q(x) = (x)^2 - n$, and we want to sieving in the interval $[\lfloor\sqrt{n}\rfloor - M, \lfloor\sqrt{n}\rfloor + M]$, therefore, $\log{(Q(x))} \approx \log{(Q(\lfloor\sqrt{n}\rfloor + M))} = \log{(2M\sqrt{n} + M^2)}$, because of M^2 is trivial if $\sqrt{n}$ is huge, $\log{(Q(x))} \approx 0.5 \log n + logM$. We also know $Q(x) = \prod_{i=1}^{k} p_i^{a_i}$ where $p_i \in S_{fb}, k = |S_{fb}|$ if $Q(x)$ has a smooth relationship in our factor base, then we have, $\log{(Q(x))} = \log \prod_{i=1}^{k} p_i^{a_i} = \sum_{i=1}^{k} a_i \log p_i$. This formula tell us if we can find a $\log Q(x) = \sum_{i=1}^{k} a_i \log p_i \approx 0.5 \log n + logM$ it probably a candidates of smooth number.

1.3 Sieving In Quadratic Sieve

1.3.1 Pre-Sieving

1.3.2 Sieving

1.3.3 Saving the result

1.3.4 Our optimization

1.4 Linear Algebra (Finding Null Space)

1.5 Problems we met, and solutions