1 Motivation

Finding factorization of natural numbers is one of the oldest and most difficult problems in mathematics. In this talk, we discuss the **Number Field Sieve**, which is computationally one of the fastest algorithms to give a prime decomposition of an integer.
The main idea of the Number Field sieve is the following lemma:-

Lemma. *Let n be a natural number. If $a, b \in [0, n-1]$ s.t. $a \pm b$ is not divisible by n and $a^2 \equiv b^2 (\mod n)$. Then $g.c.d(n, a-b), g.c.d(n, a+b) > 1$ and $n = g.c.d(n, a-b) g.c.d(n, a+b)$.*

There are possibly two ways to find a, b as in the lemma above - the first one is called the ***Quadratic Sieve***; and the other one is the ***Number Field Sieve***. The procedure that both these sieve's employ is very similar but the Number Field sieve is the better algorithm for large numbers.

2 Strategy

The strategy of the ***Number Field Sieve*** to obtain factorization of a positve integer n by finding a, b as above, is as follows:- ***Choose the ring of integers $\mathcal{O}$ of a number field s.t. there are $\theta_1, ..., \theta_n \in \mathcal{O}$ and a ring homomorphism $\phi : \mathcal{O} \to \mathbb{Z}/n\mathbb{Z}$ satisfying the property that $\theta_1 ... \theta_n$ is a square, $u^2 \in \mathcal{O}$, and $\phi(\theta_1)...\phi(\theta_n)$ is a square, $v^2 \in \mathbb{Z}/n\mathbb{Z}$.***

3 Exponent vectors

We will try to choose our θ_i's as above, from the list $\{a - b\alpha\}$, where α is a suitably chosen ***algebraic integer*** and a, b are co-prime numbers. We also choose a B s.t. $N(a - b\alpha)$ is ***B-smooth***. If $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of α, then we will define the ***exponent vector***

$$\vec{v}(a - b\alpha) := (exp_p(N(a - b\alpha)))_{p,r}$$

where (p, r) runs over primes p and $r \in [0, p-1]$ s.t. $p | f(r)$. Following is the crucial theorem:-

Theorem. *If $\mathcal{S}$ is a set of pairs of co-prime numbers (a,b) s.t. $N(a - b\alpha)$ is $B-$**smooth**. Then if $\prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is a square in $\mathcal{O}$, then*

$$\sum_{(a,b)\in\mathcal{S}} \vec{v}(a - b\alpha) \equiv 0 (\mod 2)$$

4 Obstructions

The above theorem provides us a necessary condition for a product of algebraic integers to be a square but there are some strong theoretical obstructions to the converse. We will discuss them and prove two important results which helps us evade these obstructions, *atleast computationally.*

5 Complexity analysis

From the discussion on obstructions, it is clear that the algorithm we are presenting is ***heuristic***. So rather than finding time complexity of the algorithm, which depends on many parametrs being used so far (like the B for the $B-$**smooth numbers**, the algebraic integer chosen etc.), we will find these parameters so that the time complexity of the heuristic algorithm we present is, ***the minimal one.***

6 Square roots

Even after obtaining the θ_i's and the homomorphism ϕ as above, we are not done yet!! We still need to find the square roots of the $\prod \theta_i$ and $\prod \phi(\theta_i)$. We will use the ***Hensel's lemma*** to resolve this issue quite efficiently.

7 Summary algorithm

We will finally present the algorithm and go through an example using the **https://github.com/radii/msieve.git**.