- The norm to consider is $N: \mathbb{Z}[\alpha] \to \mathbb{Z}$ mapping $a_0 + a_1\alpha + \dots + a_d\alpha^d \mapsto \prod_{\beta \in Z(f) \cap \mathbb{C}} (a_0 + a_1\beta + \dots + a_d\beta^d)$

- Eg. $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/\langle x^3 - 2\rangle =: \mathbb{Q}(\alpha)$, where α is of deg $= 3$.

  The norm maps $a_0 + a_1 2^{1/3} + a_2 \cdot 2^{2/3}$

  $\mapsto (a_0 + a_1 \cdot \alpha + a_2\alpha^2) \cdot (a_0 + a_1\alpha w + a_2\alpha^2 w^2) \cdot (a_0 + a_1\alpha w^2 + a_2\alpha^2 w)$

  where $w = \sqrt[3]{1} \in \mathbb{C}$.

- Hope to find two squares in $\mathbb{Z}[\alpha]$ that are "congruent" mod n.

<u>Input</u>: Large n.
<u>Output</u>: Factoring n.
<u>Algo</u>:

1) Fix a degree d, $m = \lfloor n^{1/d} \rfloor$.

   Express n in <u>base m</u>, say

   $n = m^d + c_{d-1}m^{d-1} + \dots + c_1 m + c_0$. Consider

   $f(x) := x^d + c_{d-1}x^{d-1} + \dots + c_1 x + c_0 \in \mathbb{Z}[x]$.

2) Factor $f(x)$ by L^3.

If it factors then we factor n OR pick an irred. factor as f.

3) Now f is irreducible: Consider the number field $\mathbb{Q}[X]/\langle f(X)\rangle =: \mathbb{Q}(\alpha)$.

- $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.
- We have a homomorphism φ from the "integers"

$$\varphi : \begin{array}{ccc} \mathbb{Z}[\alpha] & \longrightarrow & \mathbb{Z}/n\mathbb{Z}, \\ \alpha & \longmapsto & m \end{array}$$

- We have a norm in $\mathbb{Q}(\alpha)$,

$$\mathcal{N} : \begin{array}{ccc} \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q} \\ a_0 + \cdots + a_{d-1}\alpha^{d-1} & \longmapsto & \prod\limits_{\beta \in \mathbb{C},\, f(\beta)=0} (a_0 + a_1\beta + \cdots + a_{d-1}\beta^{d-1}) \end{array}$$

4) Sieving: For a carefully chosen (x, y), find $U \subseteq \{(a,b) \in \mathbb{Z}^2 \mid a, b \leq x\}$ s.t. both $(a - bm)$ & $\mathcal{N}(a - b\alpha)$ are y-smooth.

(for a sq. in $\mathbb{Z}$) (for a sq. in $\mathbb{Z}[\alpha]$)

[$\triangleright$ $\mathcal{N}(a - b\alpha) = b^d \cdot f\left(\frac{a}{b}\right) = \sum\limits_{i=0}^{d} c_i a^i b^{d-i}$.]

[▷ $a-b\alpha$ factors, in the ring of integers O_k of k, into prime ideals $\mathfrak{q}_i \triangleleft O_k$.
▷ Further, $N(a-b\alpha) = \prod_i q_i^{e_i}$ if $\mathfrak{q}_i \triangleleft \mathbb{Z}[\alpha]$, in which case each $\mathfrak{q}_i$ corresponds to a prime q_i.
In fact, every prime ideal $\mathfrak{q} \mid (a-b\alpha)$ is in 1-1 correspondence with a prime q & $r \in \mathbb{F}_q$ s.t. $a-br = f(r) = 0$ in $\mathbb{F}_q$.]

5) Matrix reduction: Find $U' \subseteq U$ s.t.

- $\prod_{a,b \in U'} (a-bm) = v^2$ in $\mathbb{Z}$, &

- $\prod_{a,b \in U'} (a-b\alpha) = \gamma^2$ in $\mathbb{Z}[\alpha]$.

6) OUTPUT $\gcd(v - \phi(\gamma), n)$.

Analysis:

- NFS needs all the algorithms that we have seen in the course – fast integer/matrix mult., polynomial fact. over $\mathbb{F}_p$ or $\mathbb{Q}$, gcd, primality!

- The time complexity of NFS is dominated by $u^{2+o(1)} + y^{2+o(1)}$.

Sieving   Matrix reduction

- So, we intend $\log u \approx \log y$.

- The integer $(a-bm)\cdot N(a-b\alpha) \approx$

$$(a-bm)\cdot \sum_{0\le i\le d} c_i a^i b^{d-i} \approx u n^{1/d}\cdot n^{1/d} u^d \approx u^{d+1}\cdot n^{2/d}.$$

▷ A number $\le u^{d+1}\cdot n^{2/d}$ is y-smooth with probability r^{-r}, where $r = \log_y(u^{d+1} n^{2/d}) \approx \log(u^{d+1} n^{2/d})/\log u$.

- To maximize the probability we minimize

$$r = d+1 + (2/d)\cdot \log_u n .$$

$$\Rightarrow d \approx \sqrt{2\log_u n} \Rightarrow r \approx 2\cdot\sqrt{2\log_u n}.$$

- To get the squares, via matrix reduction, we need $\#U \approx y \Rightarrow u^2\cdot r^{-r} \approx y$

$\Rightarrow \log u \approx r\log r \Rightarrow r \approx \log u/\log\log u$.

$$\Rightarrow \sqrt{8 \log_u n} \approx \log u / \log\log u$$

$$\Rightarrow 2\cdot(\log n)^{1/3} \approx (\log u)\cdot(\log\log u)^{-2/3}$$

$$\Rightarrow \quad \log u \approx 2\cdot(\log n)^{1/3}\cdot(\log\log u)^{2/3}$$

$$\approx 2\cdot(\log n)^{1/3}\cdot\left(\tfrac{1}{3}\cdot\log\log n\right)^{2/3}$$

$$\Rightarrow \quad y \approx u \approx L_n\left(1/3, \sqrt[3]{8/9}\right).$$

▷ The time complexity is $L_n\left(\frac{1}{3}, \sqrt[3]{64/9}\right)$.
The degree $d = (3 \log n / \log\log n)^{1/3}$.

The algebraic obstructions

(i) $\mathbb{Z}[\alpha]$ is possibly not $\mathcal{O}_K$.
Thus, γ may not exist in $\mathbb{Z}[\alpha]$, and then $\phi(\gamma)$ does not make sense.

▷ $\forall a \in \mathcal{O}_K$, $f'(\alpha)\cdot a \in \mathbb{Z}[\alpha]$.

(ii) For $a \in \mathcal{O}_K$, the exponent of a wrt every prime $\mathfrak{q} \triangleleft \mathbb{Z}[\alpha]$ may be even, without a being a square.

▷ If $a - b\alpha \pmod{P}$ is a <u>square</u> for <u>random</u> $O(\lg n)$ primes $P \trianglelefteq \mathbb{Z}[\alpha]$, then whp $(a - b\alpha)$ is a square in $\mathcal{O}_K$ (up to a unit).

(iii) $\mathcal{O}_K$ has <u>infinitely</u> many <u>units</u> unlike $\mathbb{Z}$.
We need to identify them.

▷ $|\mathcal{O}_K^* / \mathcal{O}_K^{*2}| \leq 2^d$.

- Thus, algebraic number theory takes care of all the obstructions (heuristically).

<u>Success</u>: Largest numbers factored are by NFS.
Eg. $2^{1157} + 1$ (347-digit number).