# General Idea of NFS

(1) Find a monic irr. poly $f(x)$ of deg $d$ in $\mathbb{Z}[x]$ & an integer $m$ s.t. $f(m) \equiv 0 \pmod n$

(2) Let $\alpha \in \mathbb{C}$ be an alg. no. that is a root of $f(x)$ & $\mathbb{Z}[\alpha]$ = set of polys in $\alpha$ with integer coffs.

(3) Define $\phi : \mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}_n$ as $\phi(\alpha) = m$ which ensures that for any $f(x) \in \mathbb{Z}[\alpha]$ we have

$$\phi(f(\alpha)) \equiv f(m) \pmod n$$

(4) Find a $< \infty$ set $U$ of coprime integers $(a, b)$ s.t. $\prod_{(a,b) \in U} (a - b\alpha) = \beta^2$, $\prod_{(a,b) \in U} (a - bm) = y^2$

for $\beta \in \mathbb{Z}[\alpha]$ & $y \in \mathbb{Z}$, let $x = \phi(\beta)$

Then $$x^2 \equiv \phi(\beta)\,\phi(\beta) \equiv \phi(\beta^2)$$

$$\equiv \phi\left(\prod_{(a,b) \in U} (a - b\alpha)\right)$$

$$\equiv \prod_{(a,b) \in U} \phi(a - b\alpha)$$

$$\equiv \prod_{(a,b) \in U} (a - bm) \equiv y^2 \pmod n$$

which is required

Many ways this can be implemented — CFRAC and QS/MPQS

— By sieving procs one first tries to find congr(≡) mdn by working over a factor base & then do Gaussian elimination over $\mathbb{Z}_2$ to find a cg $x^2 \equiv y^2 \pmod N$.

**NFS Algo**

Given an odd +ve integer n

**Step ①** (Polynomials selection)

Select 2 irr. polys $f(x)$ & $g(x)$ with small integer coffs for which $\exists$ an integer m s.t.

$$f(m) \equiv g(m) \equiv 0 \pmod N$$

— The polys should not have common factor | ①

**Step ②** (Sieving) $\alpha$ complex root of $f$

$\beta$ " " " $g$

Find pairs $(a, b)$ with $\gcd(a,b) = 1$ s.t. the integral norms of $(a - b\alpha)$ & $(a - b\beta)$:

$$N(a - b\alpha) = b^{\deg(f)} f(a/b)$$

$$N(a - b\beta) = b^{\deg(g)} g(a/b)$$

are smooth w.r.t. to a chosen factor base.

[The principal ideals $a - b\alpha$ & $a - b\beta$ factor into X of prime ideals in the no. field $\mathbb{Q}(\alpha)$ & $\mathbb{Q}(\beta)$.

**Step 3** (Linear Algebra)

Using techniques of linear algebra to find a set $U = \{a_i, b_i\}$ of indices s.t. the two products

$$\prod_U (a_i - b_i\alpha) \quad \& \quad \prod_U (a_i - b_i\beta) \qquad \text{---(*)}$$

are both $\square$s of $\mathbb{Z}$s of prime ideals.

**Step 4** Use the set $S$ in (*) to find an alg. nos $\alpha' \in \mathbb{Q}(\alpha)$ & $\beta' \in \mathbb{Q}(\beta)$ s.t.

$$(\alpha')^2 = \prod_U (a_i - b_i\alpha)$$

$$\& \quad (\beta')^2 = \prod_U (a_i - b_i\beta)$$

Define $\phi_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Z}_n$

$\& \ \phi_\beta : \mathbb{Q}(\beta) \to \mathbb{Z}_n$ via $\phi_\alpha(\alpha) = \phi_\beta(\beta) = m$

where $m$ is a common root of both $f$ & $g$.

Then $x^2 = \phi_\alpha(\alpha')\,\phi_\alpha(\alpha')$

$$= \phi_\alpha((\alpha')^2)$$

$$= \phi_\alpha\left(\prod_{i \in U} (a_i - b_i\alpha)\right)$$

$$= \prod_U \phi_\alpha(a_i - b_i\alpha) = \prod_U (a_i - b_i m)$$

$$= \phi_\beta(\beta')^2 = y^2 \pmod n \qquad (3)$$

→ we can find a factor by computing

$\gcd(x \pm y, n)$.

Ex: NFS factoring example:

$n = 14885 = 5 \cdot 13 \cdot 229 = 122^2 + 1$

∴ put $f(x) = x^2 + 1$ & $m = 122$

s.t. $f(x) \equiv f(m) \equiv 0 \pmod n$

if we choose $|a|, |b| \leq 50$ then we can find by sieving: $a^2 + b^2$

| $(a, b)$ | $\text{Norm}(a+bi)$ | $a+bm$ |
|---|---|---|
| $(-49, 49)$ | $4802 = 2 \cdot 7^4$ ✓ | $5929 = 7^2 \cdot 11^2$ |
| $(-41, 1)$ | $1682 = 2 \cdot 29^2$ ✓ | $81 = 3^4$ |

$(49+49i)(-41+i) = (49-21i)^2$

$f(49-21i) = 49 - 21m$

$= 49 - 21 \cdot 122 = -2513 \to x$

$5929 \cdot 81 = (2^2 \cdot 7 \cdot 11)^2 = 693^2 \to y = 693$

→ $\gcd(x \pm y, n) = \gcd(-2513 \pm 693, 14885)$

$= (65, 229)$