Reminder

Alg: 0) Find all primes $q_1 < \dots < q_r \le B$ (for a number B to be chosen later) and check that no q_i divides n (otherwise, we're done)

1) Find good $b_1, \dots, b_{r+1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ s.t. $(b_i^2 \bmod n) = q_1^{f_{i1}} \cdots q_r^{f_{ir}}$ by trying $b \in \mathbb{Z}/n\mathbb{Z}$ at random until finding $r+1$ good ones.

2) Compute the kernel of the $r \times (r+1)$-matrix $(f_{ij} \bmod 2)_{j,i}$ over $\mathbb{F}_2$ using Gaussian elimination

3)-5) simple stuff...

Running time: Let $B = n^{1/2t}$ for t to be chosen optimally later... ($\Rightarrow q_r^{2t} \le n$)

$\Rightarrow r \asymp \frac{B}{\log B}$

Step 0 takes time $\tilde{\mathcal{O}}(B + r \log n) \le \tilde{\mathcal{O}}(B \log n)$.

A random $b \in \mathbb{Z}/n\mathbb{Z}$ is good with probability

$$\ge \frac{\frac{r^{2t}}{(2t)!}}{n} \ge \frac{\left(\frac{r}{2t}\right)^{2t}}{n} \asymp \frac{\left(\frac{B}{2t \log B}\right)^{2t}}{n} = \frac{\frac{n}{(\log n)^{2t}}}{n} = \frac{1}{(\log n)^{2t}} \text{ by}$$

Lemma 15.2.3.

$\Rightarrow$ On average, we need to try $\ll (\log n)^{2t}$ random b to find a good one.

$\Rightarrow$ Need to check $\ll r (\log n)^{2t} \le B (\log n)^{2t}$ to find $r+1$ good ones.

Checking whether some $b \in \mathbb{Z}/n\mathbb{Z}$ is good takes time

$$\tilde{O}((r + \log n)\log n) \leq \tilde{O}(r \log n) \leq \tilde{O}(B \log n)$$

($\sum_j f_{ij} \leq \log n$: nr. of trial divisions)

(We'll choose t so that $r \gg \log n$.)

$\Rightarrow$ Step 1 takes time $\tilde{O}(B(\log n)^{2t} \cdot B \log n)$

$= \tilde{O}(B^2 (\log n)^{2t+1})$ on average.

Step 2 takes time $O(r^3) \leq O(B^3)$.

Steps 3-5 take time $\leq \tilde{O}(r^2 \log\log n) \leq \tilde{O}(B^2 \log\log n)$.

$\Rightarrow$ Total time $\leq \tilde{O}(B^2 (\log n)^{2t+1} + B^3)$

$= \tilde{O}(n^{1/t} (\log n)^{2t+1} + n^{3/2t})$

$= \tilde{O}(\exp((\log n) \cdot \frac{1}{t} + (\log\log n) \cdot (2t+1)) + \exp((\log n) \cdot \frac{3}{2t}))$

Choose t to minimise the first summand:

$t = \sqrt{\frac{\log n}{2 \log\log n}} + O(1)$.

$\rightsquigarrow$ Total time

$$\tilde{O}\left(\exp\left((\log n) \cdot \sqrt{\frac{2\log\log n}{\log n}} + (\log\log n) \cdot 2\sqrt{\frac{\log n}{2\log\log n}}\right) + \exp\left((\log n) \cdot \frac{3}{2} \cdot \sqrt{\frac{2\log\log n}{\log n}}\right)\right)$$

$$= \tilde{O}\left(\exp\left(2\sqrt{2} \cdot \sqrt{(\log n)(\log\log n)}\right)\right).$$

⇒ **Thm 15.2.4** We can find a nontrivial divisor of a composite integer n in expected time

$$O\left(\exp\left(C\sqrt{(\log n)(\log\log n)}\right)\right),$$

where $C = 2\sqrt{2}$.

Rmk $\exp(C(\log n)^\delta) \underset{\delta,\varepsilon}{<<} n^\varepsilon \quad \forall\, \delta < 1,\ \varepsilon > 0$

(subexponential in $\log n$)

$$\exp(C(\log n)^\delta) >> (\log n)^k \quad \forall\, \delta > 0,\ k > 0$$

(superpolynomial in $\log n$)

Improvements (finding good $(b_i^2 \bmod n)$)

1) Make step 1 faster (cf. HW).

2) Make step 2 (Gaussian elimination) faster:

Since $(b_i^2 \bmod n) = q_1^{f_{i1}} \cdots q_r^{f_{ir}}$, we have $\sum_j f_{ij} \leq \mathcal{O}(\log n)$, which is way smaller than r.

$\Rightarrow$ The matrix $(f_{ij})_{i,j}$ is sparse.

Can find the kernel more quickly using Wiedemann's alg

3) Improve the estimate in Lemma 15.2.3.

4) Heuristic improvement:

Instead of using $(b^2 \bmod n)$ for arbitrary b, use $(b^2 \bmod n)$ for $b = \lceil \sqrt{n} \rceil + c$, where

$0 \leq c \ll n^{\varepsilon}$. $\Rightarrow b^2 = \lceil \sqrt{n} \rceil^2 + 2\lceil \sqrt{n} \rceil c + c^2 \approx n$

$\Rightarrow (b^2 \bmod n) = (\lceil \sqrt{n} \rceil^2 - n) + 2\lceil \sqrt{n} \rceil c + c^2$ / for suff. small c

$\ll n^{\frac{1}{2}+\varepsilon}$.

~~It is more likely that a~~ random number $\ll n^{\frac{1}{2}+\varepsilon}$ is more likely only divisible by small primes than a random number $\leq n$.

$\Rightarrow$ heuristic running time $\mathcal{O}_\varepsilon(\exp((1+\varepsilon)\sqrt{(\log n)(\log\log n)})) \quad \forall \varepsilon > 0$

Q Why not simply use $(b^2 \bmod n) = b^2$ for $0 \leq b \ll n^{\frac{1}{2}}$?

A If nothing is actually reduced mod n, the alg. always returns the trivial result 1.

Pomerance (useless) proved in 1992 that another alg. has expected running time $\mathcal{O}_\varepsilon(\exp((1+\varepsilon)\sqrt{(\log n)(\log\log n)}))$ $\forall \varepsilon$

Lenstra

That's the best proven running time.

But:
Rmk The general number field sieve has a heuristic

running time

$$\mathcal{O}_\delta\left(\exp\left(\left(C+o(1)\right)(\log n)^{1/3}(\log\log n)^{2/3}\right)\right)$$

with $C = (64/9)^{1/3}$.

16. Number fields

several ways of specifying a field ext. $L|K$:

a) $L = K[X]/f(X)$, $f(X) \in K(X)$

L is a field if and only if $f(X)$ is irreducible.

L is a product of fields if and only if $f(X)$ is squarefree.

$[L:K] = \deg(f) =: n$.

$\| \dim_K(L)$

b) Give the multiplication table:

For a basis $w_1, \dots, w_n$ of L as a K-vector space, specify the numbers $a_{ijk} \in K$ such that

$$w_i w_j = \sum_k a_{ijk} w_k .$$

With respect to this basis, the mult. by w_i is given by the matrix $M_i = (a_{jk})_{k,j}$.

Rmk In a), a basis of $L|K$ is $1, X, \dots, X^{n-1}$, so el. of L corr. to pol. $g(X) \in K[X]$ of degree $< n$.

W.r.t. the basis $1, \dots, X^{n-1}$, the coeff. in the mult. table are given by

$$\left(X^{(i-1)+(j-1)} \bmod f\right) = \sum_k a_{ijk} X^{k-1}$$

(a_{ijk} only depends on $i+j$)

If $i-1+j-1 \le n$, then $a_{ijk} = \begin{cases} 1, & k-1 = i-1+j-1 \\ 0, & \text{otherwise.} \end{cases}$