We will focus on <u>imaginary quadratic number fields</u> K.

(Hafner, McCurley: A rigorous subexponential alg. for computation of class group)

(For general number fields K, see Buchmann: A subexp. alg. for the determination of class groups and regulators of alg. nr. fields)

Rmk $r_1=0$, $r_2=1$, $\mathcal{O}_K^\times = \mu_K$,

$R_K=1$,

$$\omega_K=|\mu_K| = \begin{cases} 2, & \text{otherwise} \\ 4, & K=\mathbb{Q}(i) \\ 6, & K=\mathbb{Q}(\zeta_3) \end{cases}$$

$K=\mathbb{Q}(\sqrt{D_K})$, $D_K<0$.

~~Def An ideal $0\neq\mathfrak{a}\subset\mathcal{O}_K$ is reduced if~~

~~a) it is not divisible by any integer $k\geq 2$ and~~

~~b)~~

(Nonstandard)

Def A fractional ideal $\mathfrak{a}$ is <u>reduced</u> if

$1 \in \mathfrak{a}$ but there is no $x \in \mathfrak{a}$, $x \neq 0$, with $\mathrm{Nm}(x) < 1$.

$\mathrm{Nm}(x) = |\text{compl. emb.}(x)|$

Rmk $1 \in \mathfrak{a} \Leftrightarrow \underset{(1)}{\mathcal{O}_K} \subseteq \mathfrak{a} \Leftrightarrow \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$,

so the inverse of a reduced fractional ideal is an (integral) ideal of $\mathcal{O}_K$.

Lemma 16.3.3 Any ideal class contains at least 1, at most 6 reduced ideals

Pf Let $\mathfrak{b}$ be any fractional ideal

and let $y \in \mathfrak{b}$ be a nonzero element of minimal norm.

Then, $\mathfrak{a} = y^{-1} \cdot \mathfrak{b}$ is reduced. Any reduced ideal in the ideal class $[\mathfrak{b}]$ is of this form. There are at most 6 such y. $\square$

Rmk We can efficiently determine the reduced ideals using Gauß's lattice reduction to find the shortest nonzero vector.

Hence, we can efficiently determine whether two ideals lie in the same ideal class.

Thm 16.3.4 (Minkowski bound)

If $\mathfrak{a}$ is reduced, then $\mathrm{Nm}(\mathfrak{a}^{-1}) \leq \mathcal{O}(\sqrt{|D_K|})$.

Rmk This gives rise to a slow alg. to determine Cl_K:

Find all ideals $\mathfrak{b}$ with $\mathrm{Nm}(\mathfrak{b}) \leq \mathcal{O}(\sqrt{|D_K|})$.

For each, compute the reduced ideals in the same ideal class as $\mathfrak{b}^{-1}$ to determine which $\mathfrak{b}$ are in the same class.

→ Obtain a ideal in each class

Thm 16.3.5 Assume the Extended Riemann Hypothesis (ERH). Then, $\mathcal{C}l_K$ is generated by the (ideal classes of) primes ideals $\mathfrak{p}$ of norm $Nm(\mathfrak{p}) \le 6\,(\log|D_K|)^2$.

Rmk Hence, if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the prime ideals of norm $\le B$ with $B \ge 6\,(\log|D_K|)^2$, then we get a surjective group hom

$$\varphi : \mathbb{Z}^r \twoheadrightarrow \mathcal{C}l_K$$
$$(a_1, \dots, a_r) \mapsto [\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}]$$

To determine $\mathcal{C}l_K$, we need to find its kernel:

$$\mathcal{C}l_K \cong \mathbb{Z}^r / \ker(\varphi)$$

I.e.: Need to find elements generating the rank n lattice $\ker(\varphi)$.

Idea: Find random elements ~~of ker(φ)~~ until they generate $\ker(\varphi)$.

How to tell when we're finished?

Let $\Lambda \subset \ker(\varphi)$, the lattice generated by the elements discovered so far.

~~We either have $\Lambda \subsetneq \ker(\varphi)$,~~

If $\Lambda \subsetneq \ker(\varphi)$, then $[\ker(\varphi) : \Lambda] \ge 2$, so

$$\left|\mathbb{Z}^r/\Lambda\right| \ge 2 \cdot \left|\mathbb{Z}^r/\ker(\varphi)\right| = 2\,|\mathcal{C}l_K|.$$

Hence, it suffices to know $|\mathcal{C}l_K|$ within a factor of 2, which (assuming ERH) can be computed using the class number formula.

How to "quickly" find random elements of $\ker(\varphi)$?

Pick a random vector $a = (a_1, \dots, a_r) \in \mathbb{Z}^r$.

~~The ideal $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ is~~

[This only lies in $\ker(\varphi)$ with (very small) prob. $\approx \frac{1}{\# Cl_K}$!]

Compute a reduced (fractional) ideal $\mathfrak{a}$ in the ideal class $[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}] = [\mathfrak{p}_1]^{a_1} \cdots [\mathfrak{p}_r^{a_r}]$ using fast exponentiation, reducing at every step to ensure that we only need to work with ideals of norm $\leq |D_K|$ at any time.

If $\mathfrak{a}^{-1} = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ with integers $b_1, \dots, b_r \geq 0$,

then $[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}] = [\mathfrak{a}\mathfrak{a}^{-1}] = [1]$,

so $\boxed{a+b} = (a_1 + b_1, \dots, a_r + b_r) \in \ker(\varphi)$.

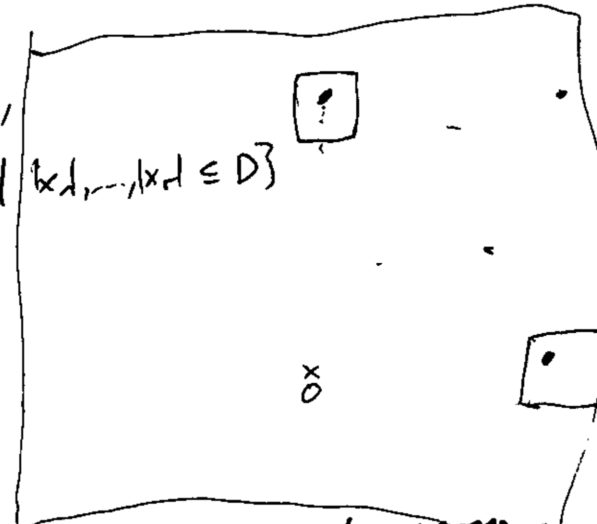
(Note that $b_1, \dots, b_r \leq O(\log |D_K|)$
because $\mathrm{Nm}(\mathfrak{a}^{-1}) \leq O(\sqrt{|D_K|})$.)

Otherwise try again, with a new random vector $a \in \mathbb{Z}^r$.

~~First, to obtain r linearly independent~~

We pick the first r vectors a (uniformly) from

$$(2r|D|, 0, \dots, 0) + \underbrace{\mathcal{B}(D)}_{\{x\in\mathbb{Z}^r \,\mid\, |x_1|,\dots,|x_r| \le D\}},$$



$$(0, 2r|D|, \dots, 0) + \mathcal{B}(D),$$

$$\vdots$$

$$(0, \dots, 0, 2r|D|) + \mathcal{B}(D)$$

so the first r elements of $\ker(\varphi)$ we construct span a random lattice $\Lambda \subset \mathbb{Z}^r$ of random and covolume $\le O((r|D|)^r)$.

Afterwards, we pick vectors a from $\mathcal{B}(|D|^2)$ until $|\mathbb{Z}^r/\Lambda|$ is small enough.

Analyzing the expected running time and choosing $\mathcal{B}$ (bound on norm of ℓ_i we consider) optimally, we get:

Thm 16.3.6 (McCurley) Assuming GRH, we can determine Cl_K in expected time $\tilde{O}\left(\exp\left(\underbrace{\sqrt{2}}_{\text{can presumably be improved...}} \cdot \sqrt{\log|D_K| \log\log|D_K|}\right)\right)$.