Lecture 5

Theorem: There are no $\mathbb{Z}$-solns to $y^2 = x^3 - 51$.

Pf: $x^3 = y^2 + 51 = (y+\sqrt{-51})(y-\sqrt{-51})$

Now $\mathbb{Q}[\sqrt{-51}] \supset \underbrace{\mathbb{Z}\left[\frac{1+\sqrt{-51}}{2}\right]}_{h = \text{classnumber} = 2} \supset \mathbb{Z}[\sqrt{-51}]$

$\Rightarrow (x)^3 = (y+\sqrt{-51})(y-\sqrt{-51})$ as ideals

Claim: The ideals $(y+\sqrt{-51})$ and $(y-\sqrt{51})$ in $\mathbb{Z}\left[\frac{1+\sqrt{-51}}{2}\right]$ have no common factor except (1).

Well, let $\mathfrak{a} \mid (y+\sqrt{-51})$, $\mathfrak{a} \mid (y-\sqrt{-51})$

Recall $\mathfrak{a} \mid \mathfrak{b} \Rightarrow \mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$ $\quad (2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z} \subset 2\mathbb{Z}$

So $(y+\sqrt{-51}) \subset \mathfrak{a}$, $(y-\sqrt{-51}) \subset \mathfrak{a}$

So $y+\sqrt{-51}$, $y-\sqrt{-51} \in \mathfrak{a}$

$\Rightarrow 2\sqrt{-51} \in \mathfrak{a} \Rightarrow (2\sqrt{-51}) \subset \mathfrak{a} \Rightarrow (2)(\sqrt{-51}) \subset \mathfrak{a}$

* In $\mathcal{O}_K$, $\mathfrak{b} \subset \mathfrak{a} \Rightarrow \mathfrak{a} \mid \mathfrak{b}$ Note: Not true for all rings in general

$\Rightarrow \mathfrak{a} \mid \overset{\text{prime}}{(2)}(\sqrt{-51}) = \mathfrak{p}_3 \cdot \mathfrak{p}_{17}$ ie $\mathfrak{a} \mid (2)\mathfrak{p}_3 \cdot \mathfrak{p}_{17}$

We saw yesterday that (2) is prime in $\mathbb{Z}\left[\frac{1+\sqrt{-51}}{2}\right] \rightarrow x^2 - x + 13$ irred. mod 2

If $\mathfrak{a} \neq (1)$, it would have to be divisible by (2), $\mathfrak{p}_3$, or $\mathfrak{p}_{17}$

$\Rightarrow (2)$, $\mathfrak{p}_3$, or $\mathfrak{p}_{17}$ is a factor of $(y+\sqrt{-51})$, hence a factor of $(x)^3$ $\Rightarrow (2)$, $\mathfrak{p}_3$, or $\mathfrak{p}_{17}$ are factors of (x).

Could $(2) \mid (x)$?

Could $(2)|(x)$, $\mathfrak{p}_3|(x)$, or $\mathfrak{p}_{17}(x)$ in $\mathbb{Z}[\frac{1+\sqrt{-51}}{2}]$?

Take norms

$\Rightarrow 4|x^2$ in $\mathbb{Z}^+$.
$\Rightarrow 2|x \Rightarrow y^2 \equiv -51 (8)$
$\equiv 5(8)$

Can't happen

$3|x^2 \Rightarrow 3|x$
$\Rightarrow 3|y$
$\Rightarrow 51 = x^3 - y^2$
$\equiv 0 \bmod 9$

Can't happen.

$17|x^2$
$\vdots$
$51 \equiv 0 (\bmod 17^2)$

Can't happen

$\therefore \mathfrak{a} = (1)$

Now in $(x)^3 = (y+\sqrt{-51})(y-\sqrt{-51})$ we can see that

$(y+\sqrt{-51}) = \mathfrak{c}^3$. In $Cl(\mathbb{Q}[\sqrt{-51}])$, this becomes

$$[(y+\sqrt{-51})] = [\mathfrak{c}^3]$$
$$[1] = [\mathfrak{c}^2][\mathfrak{c}]$$
$$= \underline{[\mathfrak{c}]^2}[\mathfrak{c}]$$

$h=2$

$$= [1][\mathfrak{c}]$$
$$= [\mathfrak{c}] \Rightarrow [\mathfrak{c}] \text{ is principal}$$

$$(y+\sqrt{-51}) = \left(a+b\cdot\frac{1+\sqrt{-51}}{2}\right)^3$$
$$= \left(\left(a+b\,\frac{1+\sqrt{-51}}{2}\right)^3\right)$$

$y+\sqrt{-51} = \left(a+b\,\frac{1+\sqrt{51}}{2}\right)^3$ as elements in $\mathbb{Z}[\frac{1+\sqrt{-51}}{2}]$

$$\Rightarrow 8y + 8\sqrt{-51} = (2a+b)^3 + 3(2a+b)(\cancel{-51ab}\ -51b^2)$$
$$+ (3(2a+b)^2 b - 51b^3)\sqrt{-51}$$

but $3|8$, $\#$

Comments on Class numbers of quadratic fields

1) There are analytic methods to derive formulas for $h(\mathbb{Q}[\sqrt{d}])$, complex-analytic and p-adic analytic.
   - The formula for $d>0$ involves a nontrivial unit in O_K

2) It seems that $h=1$ infinitely often for $d>0$. Still unproved.

3) Gauss conjectured for $d \to -\infty$ $(d<0)$ that $h \to \infty$
Thm: (Baker, Heegner, Stark). There are 9 imag quad fields with $h=1$ (conjecture of Gauss)

$$d = -1, -2, -3, -7, -11, -19, -47, -67, -163.$$

Thm: (Goldfeld; Gross, Zagier)
there's an effective lower bound on $h(\mathbb{Q}[\sqrt{d}])$ for $d<0$
which $\to \infty$ as $d \to -\infty$
} ideas related to BSD

Now there are complete tables of $h = 1, 2, \ldots, 100$ for $d<0$. (Watkins)

Usual way one sees proof that $\mathbb{Z}$ or $\mathbb{Z}[i]$ have unique factorization is by first showing there's a division algorithm.

Division algorithm in R: There's $d: R-\{0\} \to \mathbb{N}$ (Euclidean)
s.t. for all $a, b \in R$ with $b \neq 0$ we can write
$a = bq + r$ for some $q, r \in R$ where $r=0$ or $d(r) < d(b)$

Ex: $R = \mathbb{Z}$, $d(n) = |n|$
$R = \mathbb{Z}[i]$, $d(\alpha) = N(\alpha)$
$R = \mathbb{Z}[\sqrt{2}]$, $d(\alpha) = |N(\alpha)|$
$R = \mathbb{Q}[x]$, $d(f) = \deg f$.

* To say that O_K is Euclidean does not require $d(\alpha) = |N(\alpha)|$ (norm-Euclidean).

Thm: Only 5 imag. quadratic O_k are Euclidean
($d = \underbrace{-1, -2, -3, -7, -11}_{\text{norm works}}$)

So $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ has unique fact^n but it's not Euclidean.

Thm: There are only 16 norm-Euclidean O_k where $d>0$.
Last one is $\mathbb{Q}[\sqrt{73}]$

Now $\mathbb{Q}[\sqrt{14}]$ has $h=1$
So $\mathbb{Z}[\sqrt{14}]$ is known not to be norm-Euclidean.

Thm: (Harper, 2004) $\mathbb{Z}[\sqrt{14}]$ is Euclidean

Beyond quadratics

- Number field: $k = \mathbb{Q}[\alpha]$ → root of some irred. poly in $\mathbb{Q}[x]$

Ex. Cubic field

$\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q} + \mathbb{Q}\sqrt[3]{2} + \mathbb{Q}\sqrt[3]{4}$

An integer in k is the root of a monic $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in \mathbb{Z}[x]$

The set of all integers in k is a ring, denoted O_k

Ex. $k = \mathbb{Q}[\sqrt[3]{2}] \Rightarrow O_k = \mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$

$\frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$ is an integer in $\mathbb{Q}[\sqrt[3]{10}]$, root of $x^3 - x^2 - 3x - 3$

What can be said
- O_k have unique fact^n of ideals.
  (No simple analogues of $\alpha\bar{\alpha} = (d)$ in quad case)

- The group $Cl(K)$ is finite
- $O_K^\times$ = units is infinite except when $K = \mathbb{Q}$ or ~~these~~ imag. quad.
  - but always finitely generated.

Open Question: Show there are infinitely many number fields ~~with~~ with $h=1$

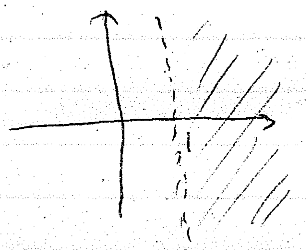
Conjecture (Weber): The field $\overset{K_n}{\overset{\shortparallel}{\mathbb{Q}}}[2\cos(\frac{2\pi}{2^n})]$ have class number 1.

As of 2009, least prime factor of any $h(K_n)$ is $> 10^8$.

Generalized Riemann Hypothesis.

For $Re(s) > 1$

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s}$$



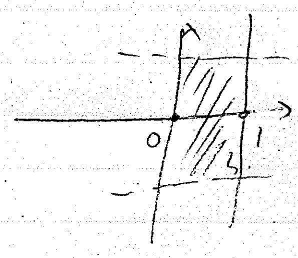
For any K = # field

$$\zeta_K(s) = \sum_{\substack{a \subset O_K \\ a \neq (0)}} \frac{1}{(N(a))^s} = \prod_p \frac{1}{1 - \frac{1}{(N p)^s}}$$

- It's possible to extend the meaning of $\zeta_K(s)$ to all of $\mathbb{C}$. There's a relation b/w $\zeta_K(s)$ and $\zeta_K(1-s)$

- GRH

If $\zeta_K(s)$ and $0 < Re(s) < 1$ then $Re(s) = 1/2$



~~Thm~~ Thm (Weinberger, 1973)

If GRH is true then any number field ~~except~~ $\mathbb{Q}$ and imag quad fields (i.e., $O_K^\times$ = is finite) which have $h=1$ is Euclidean.

Look up "$\mathbb{Q}[\sqrt{69}]$ is Euclidean.