Lecture V

K. Conrad.

What are the $\mathbb{Z}$-solutions of $x^2 - 11y^2 = 5$?

x	4	7	73	136	1456	...
y	1	2	22	41	439	...

$$(x + y\sqrt{11})(x - y\sqrt{11}) = 5$$

$$(1+2i)(1-2i) = 5 \quad \text{in } \mathbb{Z}[i]$$

Let $d \in \mathbb{Z}$, $d \neq 0$. set

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

If $d = -1$ we get $\mathbb{Z}[i]$

Definition: For $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

set $\bar{\alpha} = a - b\sqrt{d}$ (conjugate) and $N(\alpha) = \alpha\bar{\alpha} = a^2 - db^2 \in \mathbb{Z}$ (norme)

Examples

$d = 2$ $N(a + b\sqrt{2}) = a^2 - 2b^2$ (can be negative!!)

$d = -2$ $N(a + b\sqrt{-2}) = a^2 + 2b^2$

$N(a) = a^2$ $(a \in \mathbb{Z})$

Key property: $N(\alpha\beta) = N(\alpha)N(\beta)$ $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$

Ex $N(4 + \sqrt{11}) = 5$

$N(a+b\sqrt{11}) = 1$? $\quad a^2 - 11b^2 = 1$

For example $\quad N(10+3\sqrt{11}) = 1$

$$N(4+\sqrt{11})(10+3\sqrt{11})^k) = 5 \cdot 1^k = 5 \qquad k \geq 0$$

For any $k \geq 0$

$$x_k + y_k\sqrt{11} = (4+\sqrt{11})(10+3\sqrt{11})^k$$

Satisfies $\quad x_k^2 - 11y_k^2 = 5$ } Infinitely many solutions.

k	x_k	y_k
0	4	1
1	73	22
2	1456	439

Goal now: Use factorization in $\mathbb{Z}[\sqrt{11}]$ to find all $\mathbb{Z}$-solutions of $x^2 - 11y^2 = 5$

Definition: A unit in $\mathbb{Z}[\sqrt{d}]$ is any element with multiplicative inverse.

Examples:

$\mathbb{Z}[\sqrt{2}]$ $\quad (1+\sqrt{2})(\sqrt{2}-1) = 1$

$\mathbb{Z}[\sqrt{3}]$ $\quad (2+\sqrt{3})(2-\sqrt{3}) = 1$

$\mathbb{Z}[\sqrt{11}]$ $\quad (10+3\sqrt{11})(10-3\sqrt{11}) = 1$

Notation: $\mathbb{Z}[\sqrt{d}]^\times$: set of all units in $\mathbb{Z}[\sqrt{d}]$

Example: $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Theorem: A number $u \in \mathbb{Z}[\sqrt{d}]$ is a unit iff $N(u) = \pm 1$.

(Imag) If $uv = 1$ in $\mathbb{Z}[\sqrt{d}]$ $\Rightarrow N(u)N(v) = N(1) = 1$ (in $\mathbb{Z}$)

$\Rightarrow N(u) = \pm 1$

Conversely, if $N(u) = \pm 1$ since $u\bar{u} = \pm 1$

one gets $u^{-1} = \bar{u}$ if $N(u) = 1$

or $u^{-1} = -\bar{u}$ if $N(u) = -1$

In particular, if $d<0$

$$\mathbb{Z}[\sqrt{d}]^\times = \begin{cases} \pm 1, \pm i & d=-1 \\ \pm 1 & d<-1 \end{cases}$$

($d=-2$ $x^2+2y^2=\pm 1$ $\Rightarrow y=0, x=\pm 1$)

If $d>0$

then $\mathbb{Z}[\sqrt{d}]^\times$ is infinite,

[because the Diophantine equation

$$x^2 - dy^2 = 1$$

has a solution $\mathbb{Z}$-solution besides $(\pm 1, 0)$.

i.e. $y \neq 0$.

One can take a solution with $x+y\sqrt{d}$ $x>1, y>1$)

and its infinite powers are solutions too.

(all are differents).

For any unit u, $\alpha \in \mathbb{Z}[\sqrt{d}]$ is divisible by u and $u\alpha$

$$\alpha = u(u^{-1}\alpha) = (u\alpha)u^{-1}$$

Example $31+22\sqrt{2} = (7+5\sqrt{2})(3+\sqrt{2})$ // trivial factorization.

$N=-7 \quad N=-1 \quad N=7$

Definition: An irreducible element α in $\mathbb{Z}[\sqrt{d}]$ is any element not 0 or a unit ($N(\alpha)>1$) such that its only factors are u, $u\alpha$ where $u \in \mathbb{Z}[\sqrt{d}]^\times$.

Theorem: If $N(\alpha) = \pm p$, p prime, then α is irreducible.

Example:

In $\mathbb{Z}[\sqrt{2}]$ $11+\sqrt{2} = (3-\sqrt{2})(5+2\sqrt{2})$

is a irreducible factorization $N=7 \quad N=17$

Theorem: Any $\alpha \in \mathbb{Z}[\sqrt{d}]$ that has $N(\alpha)>1$ is a product of irreducible

(proof)

Induction on $|N\alpha|$

Def: We say that $\mathbb{Z}[\sqrt{d}]$ has a unique factorization if whenever

$$\pi_1 \pi_2 \quad \pi_r = \pi_1' \cdot \pi_s'$$

with irreducible π_i, π_j', one has $\cdot r = s$

$\cdot$ after relabeling $\pi_i = \pi_i'$ up to $\mathbb{Z}[\sqrt{d}]^\times$

Ex: $11+\sqrt{2} = (5+3\sqrt{2})(7-4\sqrt{2})$

$N=7 \qquad N=17$

Set

One had

$$11+\sqrt{2} = (3-\sqrt{2})(5+2\sqrt{2})$$

and $(5+3\sqrt{2}) = (3-\sqrt{2})(1+\sqrt{2})^2$

$(7-4\sqrt{2}) = (5+2\sqrt{2})(1-\sqrt{2})^2$ } unique factorization

Fact: $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{11}]$

have unique factorization.

Return to $x^2-11y^2=5$. Assume (x,y) solution

$$(x+y\sqrt{11})(x-y\sqrt{11}) = (4+\sqrt{11})(4-\sqrt{11})$$

$N=5 \qquad N=5 \qquad N=5 \qquad N=5$

(irreducible)

Fact ⟹ $(x+y\sqrt{11}) = (4\pm\sqrt{11})\cdot u$, $u \in \mathbb{Z}[11]^\times$

what are all the ~~solutions~~ units of $\mathbb{Z}[\sqrt{11}]$?

one $10+3\sqrt{11}$ $\quad (10+3\sqrt{11})^{-1} = 10-3\sqrt{11}$

$$\mathbb{Z}[\sqrt{11}]^\times = \{ \pm(10+3\sqrt{11})^k : k \in \mathbb{Z} \}$$

(see notes)

One says that $10+3\sqrt{11}$ generates the units.

Now: all $\mathbb{Z}$-solutions of $x^2-11y^2=5$

come from $x+y\sqrt{11} = \pm(4\pm\sqrt{11})(10+3\sqrt{11})^k$

$k \in \mathbb{Z}$.

———— o ————

let's go to another equation

$$x^2-10y^2=6$$

Ex: $(x,y)=(4,1)$ one solution.

$$(x+y\sqrt{10})(x-y\sqrt{10}) = 6 = (4+\sqrt{10})(4-\sqrt{10})$$

Th: Any $\alpha \in \mathbb{Z}[\sqrt{10}]$ with norm 6 is irreducible.

(Proof) let α with $N\alpha = 6$

If α were not irreducible it would have a factor β other than u or $u\alpha$

$$\rightsquigarrow \quad \alpha = \beta\gamma$$

then $N\beta > 1$ and $N\gamma > 1$ (if $N\gamma = 1 \Rightarrow \gamma$ unit $\alpha = \beta u \quad \beta = u^{-1}\alpha$)

take Norms $\quad 6 = N\beta\, N\gamma \Rightarrow N\beta = \pm 2$ or ± 3 in $\mathbb{Z}$

set $\beta = a + b\sqrt{10} \quad N\beta = a^2 - 10b^2 = \pm 2$ or ± 3

Consider the equation modulo 5

$$a^2 \equiv 2, 3 \bmod 5 \qquad (2 \equiv -3 \bmod 5)$$

But squares modulo 5 are $0, 1, 4$.

$\therefore \alpha$ is irreducible

So, If $\mathbb{Z}[\sqrt{10}]$ has a unique factorization then

$$\underset{N=6}{x + y\sqrt{10}} = \underset{N=6}{(4 \pm \sqrt{10})}\, u \qquad \text{with } Nu = 1$$

Units in $\mathbb{Z}[\sqrt{10}]$

$$\mathbb{Z}[\sqrt{10}]^{+} = \{ \pm (3 + \sqrt{10})^k : k \in \mathbb{Z} \}$$

so one needs $u = \pm (3 + \sqrt{10})^{2k}$

and $\quad x + y\sqrt{10} = \pm (4 \pm \sqrt{10})(3 + \sqrt{10})^{2k}$.

Unfortunately $\mathbb{Z}[\sqrt{10}]$ has NOT unique factorization.

$$2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$$
$$N=4 \quad N=9 \qquad \text{irred.} \quad \text{irred.}$$

If 2 or 3 were not irreducible, then have factor of norm 2 or norm 3 (not possible).

$\therefore$ 2 and 3 are irreducible and

$$2 \neq u(4 \pm \sqrt{10})$$
$$N=4 \qquad N=6$$

} NO unique factorization.

However, the result is correct!!

How do fix the possibility of non unique factorization in $\mathbb{Z}[\sqrt{d}]$?

$\mathbb{Q}$ / ratio / $\mathbb{Z}$

$\mathbb{Q}[\sqrt{d}] = \{r+s\sqrt{d} : r,s \in \mathbb{Q}\}$ / ratio / $\mathbb{Z}[\sqrt{d}]$

$$\frac{1}{3+\sqrt{2}} \cdot \frac{3-\sqrt{2}}{3-\sqrt{2}} = \frac{3}{7} - \frac{1}{7}\sqrt{2}$$

Def: A quadratic field : any $\mathbb{Q}[\sqrt{d}]$ $\quad d \in \mathbb{Z}, d \neq 0$

$\mathbb{Q}[\sqrt{d}]$ / ? / $\mathbb{Z}[\sqrt{d}]$

Def: For any $\alpha = r+s\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ set

$\bar{\alpha} = r-s\sqrt{d}$

$$f_\alpha(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha}$$

$$= x^2 - 2rx + (r^2 - ds^2)$$

Any α is a root of f_α.

We call α an integer of $\mathbb{Q}[\sqrt{d}]$ if $f_\alpha(x)$ has coefficients in $\mathbb{Z}$.

Ex. If $a,b \in \mathbb{Z}$ then $\alpha = a+b\sqrt{d}$ is an integer of $\mathbb{Q}[\sqrt{d}]$. since

$$f_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$$

Ex $\alpha = \frac{1+\sqrt{5}}{2}$

has $f_\alpha(x) = x^2 - x - 1$ so $\frac{1+\sqrt{5}}{2}$ is an integer of $\mathbb{Q}[\sqrt{5}]$

Ex: $\mathbb{Q}[\sqrt{12}] = \{r+s\sqrt{12} : r,s \in \mathbb{Q}\}$

$= \{r+3s\sqrt{2} : r,s \in \mathbb{Q}\}$

$= \mathbb{Q}[\sqrt{2}]$

However $\mathbb{Z}[\sqrt{12}] = \{a+b3\sqrt{2}\} \subsetneq \mathbb{Z}[\sqrt{2}]$

Remark

~~We quadratic fields, we always assume~~

Thm: For a quadratic field $\mathbb{Q}[\sqrt{d}]$ where d is square-free, its integers are

$$\begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \equiv 2,3 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \end{cases}$$

Quadratic field	Integers
$\mathbb{Q}[i]$	$\mathbb{Z}[i]$
$\mathbb{Q}[\sqrt{2}]$	$\mathbb{Z}[\sqrt{2}]$
$\mathbb{Q}[\sqrt{3}]$	$\mathbb{Z}[\sqrt{3}]$
$\mathbb{Q}[\sqrt{-3}]$	$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$
$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
$\mathbb{Q}[\sqrt{-5}]$	$\mathbb{Z}[\sqrt{-5}]$
$\mathbb{Q}(\sqrt{-39})$	$\mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$
$\mathbb{Q}(\sqrt{10})$	$\mathbb{Z}[\sqrt{10}]$