Keith Conrad

Quadratic Fields

1

Factorization to solve some diaphantine equations

$$x^2 + y^2 = z^2 \qquad x,y,z \in \mathbb{Z}^+$$

Suppose $\gcd(x,y)=1$

$\Rightarrow \gcd(x,z)=1$ and $\gcd(y,z)=1$

<u>z is odd:</u> squares mod 4 : 0 or 1

If z were even, then

$x^2+y^2 \equiv 0 \mod 4 \Rightarrow x,y$ are even ↯

So z is odd

$x^2+y^2 \equiv 1 \mod 4 \Rightarrow x$ or y is even, other is odd

WLOG, we can assume x odd, y even (and z is odd)

$$x^2 = z^2 - y^2$$

$$= \underbrace{(z+y)}_{\substack{\text{odd}\\ >0}} \underbrace{(z-y)}_{\substack{\text{odd}\\ >0}} \qquad \text{factors are relatively prime}$$

How can $c^2 = a,b$ with $\gcd(a,b)=1$ in $\mathbb{Z}^+$ → because $6^2 \neq (-4)(-9)$ ↘ $\not\square$

$\Rightarrow a,b = \square$

So $z+y = m^2$, $z-y = n^2$, $x^2 = m^2n^2$

for some $m,n \in \mathbb{Z}$ with $\gcd(m,n)=1$

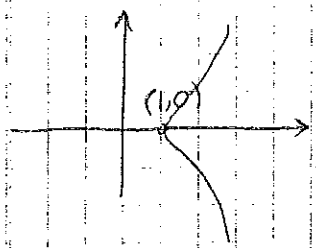
$$x = mn, \quad y = \frac{m^2-n^2}{2}, \quad z = \frac{m^2+n^2}{2}$$

Set $k = \frac{m+n}{2}$, $l = \frac{m-n}{2}$ (in $\mathbb{Z}$) (if m,n both odd)

$$\boxed{x = k^2 - l^2, \quad y = 2kl, \quad z = k^2 + l^2}$$

$y^2 = x^3 - 1$

What are $\mathbb{Z}$-solns?

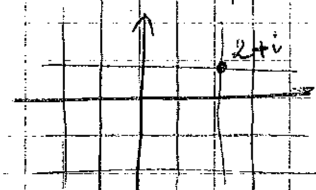


Rewrite as $x^3 = y^2 + 1$
$= (y+i)(y-i)$

In $\mathbb{Z}$: if $c^3 = ab$ and $\gcd(a,b) = 1$
what can we say?
a, b are both cubes (since $-1 = (-1)^3$)

__Question:__ Are $y+i$ and $y-i$ relatively prime in a suitable sense?

__Def__ The Gaussian integers are $\mathbb{Z}[i]$
complex numbers $a+ib$ with $a, b \in \mathbb{Z}$



Factorizations $10 = (3+i)(3-i) = 2 \cdot 5$
in $\mathbb{Z}[i]$ $3+4i = (2+i)^2$

In $\mathbb{Z}$ we have trivial factorizations

$n = n \cdot 1 = (-n)(-1)$

in $\mathbb{Z}[i]$ trivial factorizations are

$\alpha = \alpha \cdot 1 = (-\alpha)(-1)$
$= (i\alpha)(-i) = (-i\alpha)(i)$

We call $\alpha, \beta \in \mathbb{Z}[i]$ relatively primes
if their only common factors are $1, -1, i, -i$

How can we give examples?

Are $1+3i$ and $2+5i$ relatively prime?

Def The norm of $\alpha = a+bi \in \mathbb{Z}[i]$
is $N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$

ex $N(1+3i) = 1^2+3^2 = 10$
$N(2+5i) = 2^2+5^2 = 29$

$* \; N(\alpha\beta) = N(\alpha)N(\beta)$

Observe if δ is a common factor of α and β in $\mathbb{Z}[i]$,
so $\alpha = \delta\lambda$
$\beta = \delta\mu$ in $\mathbb{Z}[i]$

$\Rightarrow N(\alpha) = N(\delta)N(\lambda)$ and $N(\beta) = N(\delta)N(\mu)$
$\Rightarrow N(\delta)$ is common factor
of $N(\alpha)$, $N(\beta)$ in $\mathbb{Z}$

If δ is factor of $1+3i$ and $2+5i$
then $N(\delta)$ is factor of 10 and 29 in $\mathbb{Z}$

$\Rightarrow N(\delta) = 1$

$\delta = a+bi \Rightarrow a^2+b^2 = 1$
$\Rightarrow \delta = 1 / -1 / i / -i$

So $1+3i$ and $2+5i$ are relatively prime

! If $N(\alpha)$ and $N(\beta)$ are not relatively prime
then it does not mean that α and β
are not relatively prime.

ex $1+2i$ vs $1-2i$

ex $1+2i$ vs $1-2i$

Norms 5

if $\delta \mid 1+2i$ and $\delta \mid 1-2i$

then $N(\delta) = 5$ in $\mathbb{Z}$

$\Rightarrow N(\delta) = 1$ or 5

$\{1+2i;\ 1-2i,\ 2+i,\ 2-i,$
$-1+2i,\ -1-2i,\ -2+i,\ -2-i\}$

take the ratios of this ↑ and $1+2i$ and $1-2i$,

are there non-trivial ratios?

Return to $y^2 = x^3 - 1$

$$\left.\begin{aligned} x^3 &= y^2+1 \\ &= (y-i)(y+i) \end{aligned}\right\} \text{ Assume } x, y \in \mathbb{Z}$$

Thm The Gaussian integers $y+i$ and $y-i$ are relatively prime in $\mathbb{Z}[i]$ for any y fitting the eq. $y^2 = x^3 - 1$

$N(y \pm i) = y^2 + 1$

Proof Let $\delta \in \mathbb{Z}[i]$ be common factor of $y+i$ and $y-i$

$\delta \mid y+i$ in $\mathbb{Z}[i] \Rightarrow N(\delta) \mid \underbrace{N(y+i)}_{y^2+1\,=\,x^3}$

$\delta \mid y-i$ in $\mathbb{Z}[i] \Rightarrow \cancel{N(\delta)}\ \delta \mid 2i$ in $\mathbb{Z}[i]$

$\Rightarrow N(\delta) \mid 4y^2$ and $N(\delta) \mid 4$ in $\mathbb{Z}$

Let's show x odd, y even:

if x were even then $y^2 \equiv -1 \mod 8$
$\equiv 7 \mod 8$ ↯

squares mod 8 $\{0, 1, 4\}$

$\Rightarrow y^2 = x^3 - 1$ even $\Rightarrow y$ even

$\Rightarrow N(\delta)$ is odd $(N(\delta) \mid x^3)$ and $N(\delta) \mid 4$

$\Rightarrow N(\delta) = 1 \Rightarrow \delta = \pm 1$ or $\pm i$

If it were the case in $\mathbb{Z}[i]$ (*)
then $\alpha\beta = y^3$ and α and β
being relatively prime
$\Rightarrow \alpha$ and β are cubes

Then $y + i = (m + ni)^3$ for some $m, n \in \mathbb{Z}$

$$= m^3 + 3m^2 ni - 3mn - n^2 i$$
$$= m^3 - 3mn^2 + (3m^2 n - n^3) i$$
$$= m(m^2 - 3n^2) + n(3m^2 - n^2) i$$

Thus
$$\begin{cases} y = m(m^2 - 3n^2) \\ 1 = n(3m^2 - n^2) \end{cases} \text{ in } \mathbb{Z}$$

$\hookrightarrow n = \pm 1 \Rightarrow 1 = \pm(3m^2 - 1)$

$\cancel{1 = 3m^2 - 1}$ or $1 = -(3m^2 - 1) \Rightarrow m = 0$
$\Rightarrow \boxed{y = 0}$
$\Rightarrow \boxed{x = 1}$

How we can explain (*) ?

This is (in $\mathbb{Z}$) a conseq. of unique fact.

$ab = c^3$ and $\gcd(a, b) = 1$
$\Downarrow$
$a, b = \square$

What does unique factorization look like in $\mathbb{Z}[i]$?

Def A prime in $\mathbb{Z}[i]$ is any $\pi \in \mathbb{Z}[i]$
that's not 0 or ± 1 or $\pm i$ and
it's only factors are $\pm 1, \pm i, \pm\pi, \pm i\pi$

Thm If $N(\alpha) = p$ is prime in $\mathbb{Z}$ then
α is prime in $\mathbb{Z}[i]$

Proof Write $\alpha = \beta\gamma$, then $p = N(\beta)N(\gamma)$ in $\mathbb{Z}^+$
$\Rightarrow N(\beta)$ or $N(\gamma)$ is $1 \Rightarrow \beta$ or γ is ± 1 or $\pm i$

3 is prime in $\mathbb{Z}[i]$

$N(3) = 9$

Suppose $3 = \beta\gamma$ with $N\beta > 1$, $N\gamma > 1$

$\Rightarrow 9 = N\beta \, N\gamma$ in $\mathbb{Z}^+$

$\Rightarrow N\beta = 3$

$a^2 + \cancel{b^2 = 3}$

<u>Thm</u> ① Every $\alpha \in \mathbb{Z}[i]$ with $N\alpha > 1$

is a product of primes : $\alpha = \pi_1 \dots \pi_r$

② If $\pi_1 \cdots \pi_r = \pi_1' \dots \pi_r'$ (π_j, π_k' prime)

then $r = s$ and after relabelling

we can say $\pi_j = u_j \pi_j'$ where $u_j = \pm 1$ or $\pm i$

<u>Ex</u> $5 = (2+i)(2-i) = (1+2i)(1-2i)$

$\cdot i$

$\cdot -i$

<u>Cor</u> If $\alpha\beta = \gamma^n$ in $\mathbb{Z}[i]$ and

α, β are rel. prime then

$\alpha = u\mu^n$ and $\beta = v\lambda^n$ with $u, v \in \{\pm 1, \pm i\}$

<u>Ex</u> $(4+3i)\,2 = (3+i)^2$

$4+3i = i(2-i)^2$ $\quad 2 = -i(1+i)^2$

if $n = 3$, then v, u are cubes $(1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i = i^3)$

$\rightarrow$ suck in

12/07/11 What are the $\mathbb{Z}$-solutions of $x^2 - 11y^2 = 5$?

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

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

Let $d \in \mathbb{Z}$, $d \neq \square$,

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

e.g. $d = -1$: we get $\mathbb{Z}[i]$.

<u>Def</u> For $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

set $\overline{\alpha} = a - b\sqrt{d}$ conjugate and

$N(\alpha) = \alpha\overline{\alpha}$

Norm: $= a^2 - db^2 \in \mathbb{Z}$

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

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

$N(a) = a^2$

$*$ $N(\alpha\beta) = N\alpha \cdot N\beta$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$

<u>Ex</u> $N(4 + \sqrt{11}) = 5$

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

$a^2 = 11b^2 + 1$

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

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

For any $k \geq 0$

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

satisfies $x_k^2 - 11y_k^2 = 5$

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

we missed some solutions?

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

Def A unit in $\mathbb{Z}[\sqrt{d}]$ is any element with a multiplicative inverse

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

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

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

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

$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Thm A number u in $\mathbb{Z}[\sqrt{d}]$ is a unit $\iff Nu = \pm 1$

Pf If $uv = 1$ in $\mathbb{Z}[\sqrt{d}]$

then $N(uv) = N(1) \Rightarrow N(u)N(v) = 1$ in $\mathbb{Z}$

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

And if $N(u) = \pm 1$ then $u\bar{u} = \pm 1$

so $u^{-1} = \bar{u}$ or $u^{-1} = -\bar{u}$

If $d < 0$,

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

e.g. $d = -2$: $x^2 + 2y^2 = \pm 1 \Rightarrow x = \pm 1, y = 0$

If $d > 0$ then $\mathbb{Z}[\sqrt{d}]^\times$ is infinite

because the Diophantine equation

$x^2 - dy^2 = 1$ (drawing lines, see B. Conrad)

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

Any $x + y\sqrt{d}$ with $x \geq 1$ and $y \geq 1$ has

inf. many different many powers

For any unit u,

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

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

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

e.g. in $\mathbb{Z}[\sqrt{2}]$

$31 + 22\sqrt{2} = (7+5\sqrt{2})(3+\sqrt{2})$

$N = -7 \quad N = -1 \quad N = 7$ → trivial factorization

Def 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 $u \in \mathbb{Z}[\sqrt{d}]^{\times}$

Thm If $N\alpha = \pm p$ for p prime in $\mathbb{Z}^{+}$
then α is irreducible

Ex $11 + \sqrt{2} = (\underset{N=7}{3-\sqrt{2}})(\underset{N=17}{5+2\sqrt{2}})$ In $\mathbb{Z}[\sqrt{2}]$
→ irreducible factorization → both prime

Thm Any $\alpha \in \mathbb{Z}[\sqrt{d}]$ that has $|N\alpha| > 1$
is a product of irreducibles

proof induct on $|N\alpha|$

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

$\pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s'$

with irred π_j, π_k'

- $r = s$
- after relabeling: $\pi_j = u_j \pi_j'$ $\quad u_j \in \mathbb{Z}[\sqrt{d}]^{\times}$

For any unit u,

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

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

e.g. in $\mathbb{Z}[\sqrt{2}]$

$$31 + 22\sqrt{2} = (7+5\sqrt{2})(3+\sqrt{2})$$

$N = -7$ $\quad N = -1$ $\quad N = 7$ $\rightarrow$ trivial factorization

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

<u>Thm</u> If $N\alpha = \pm p$ for p prime in $\mathbb{Z}^+$
then α is irreducible

<u>Ex</u> $11 + \sqrt{2} = (\underset{N=7}{3-\sqrt{2}})(\underset{N=17}{5+2\sqrt{2}})$ In $\mathbb{Z}[\sqrt{2}]$
$\rightarrow$ irreducible factorization $\rightarrow$ both prime

<u>Thm</u> Any $\alpha \in \mathbb{Z}[\sqrt{d}]$ that has $|N\alpha| > 1$
is a product of irreducibles

<u>proof</u> induct on $|N\alpha|$

We say $\mathbb{Z}[\sqrt{d}]$ has <u>unique</u> factorization
if whenever

$$\pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s'$$

with irred π_j, π_k'

- $r = s$
- after relabeling: $\pi_j = u_j \pi_j'$ $\quad u_j \in \mathbb{Z}[\sqrt{d}]^\times$

ex $11 + \sqrt{2} = \underset{N=7}{(5+3\sqrt{2})}\underset{N=17}{(7-4\sqrt{2})}$

$= \underset{N=7}{(3-\sqrt{2})}\underset{N=17}{(5+2\sqrt{2})}$

$$(5+3\sqrt{2}) = (3-\sqrt{2})(1+\sqrt{2})^2$$
$$(7-4\sqrt{2}) = (5+2\sqrt{2})(1-\sqrt{2})^2$$

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

have unique factorization

Return to $x^2 - 11y^2 = 5$ $(x, y \in \mathbb{Z})$

$$\underset{N=5}{(x+y\sqrt{11})}\underset{N=5}{(x-y\sqrt{11})} = \underset{N=5}{(4+\sqrt{11})}\underset{N=5}{(4-\sqrt{11})}$$

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

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

one $10 + 3\sqrt{11}$

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

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

"$10 + 3\sqrt{11}$ generates the units"

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

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

Other example:

What are the $\mathbb{Z}$-solns of

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

Ex $(x, y) = (4, 1)$

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

$$= \underset{N=6}{(4+\sqrt{10})}\underset{N=6}{(4-\sqrt{10})}$$

Thm Any $\alpha \in \mathbb{Z}[\sqrt{10}]$ with norm 6 are irreducible

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

$\rightsquigarrow \alpha = \beta\gamma$ $\quad |N\beta| > 1$, $|N\gamma| > 1$

$[\alpha = \beta u \Rightarrow \beta = u^{-1}\alpha]$

Take norm $6 = N\beta \cdot N\gamma$ in $\mathbb{Z}$

$\Rightarrow N\beta = \pm 2$ or ± 3

$\beta = a + b\sqrt{10}$: $a^2 - 10b^2 = \pm 2$ or ± 3
$a, b \in \mathbb{Z}$

$\underset{\text{mod } 5}{\Longrightarrow}$ $a^2 \equiv \pm 2$ or ± 3 mod 5

$a^2 \equiv 2, 3$ mod 5

contradiction because $\square$ mod 5: 0, 1, 4 !

~~If~~ $\mathbb{Z}[\sqrt{10}]$ has unique fact^{n}

then $x + y\sqrt{10} = (4 \pm \sqrt{10})u$, $u \in \mathbb{Z}[\sqrt{10}]^{\times}$ with $Nu = 1$

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

if $Nu = 1$, then $u = \pm(3 + \sqrt{10})^{2l}$
$= \pm(19 + 6\sqrt{10})^{l}$

so $x + y\sqrt{10} = \pm(4 \pm \sqrt{10})(19 + 6\sqrt{10})^{l}$ for some $l \in \mathbb{Z}$

! $\mathbb{Z}[\sqrt{10}]$ does <u>not</u> have unique factorization

$$\underbrace{\underset{N=4}{2} \cdot \underset{N=9}{3}}_{\text{irred}} = \underset{\substack{\text{irred} \\ N=6}}{(4 + \sqrt{10})} \underset{\substack{\text{irred} \\ N=6}}{(4 - \sqrt{10})}$$

$\underset{N=6}{4 + \sqrt{10}} \neq \underset{N=\pm 4}{2u}$ or $\underset{N=\pm 9}{3u}$ $\quad u \in \mathbb{Z}[\sqrt{10}]^{*}$

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

$\mathbb{Q}$ $\qquad$ $\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\}$

ratios $\qquad$ ratios

$\mathbb{Z}$ $\qquad$ $\mathbb{Z}[\sqrt{d}]$

Eg $\quad \frac{1}{3+\sqrt{2}} = \frac{3-\sqrt{2}}{9-2} = \frac{3}{7} - \frac{1}{7}\sqrt{2}$

Quadratic field = any $\mathbb{Q}[\sqrt{d}]$ $\quad d \in \mathbb{Z}$, $d \neq \square$

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

$$f_\alpha(x) = (x - \alpha)(x - \bar{\alpha})$$
$$= x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$$
$$= x^2 \underbrace{- 2r}_{\in \mathbb{Q}} x + \underbrace{(r^2 - ds^2)}_{\in \mathbb{Q}}$$

α is root

We call α an <u>integer</u> 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 $f_\alpha(x) = x^2 - \underbrace{2a}_{\in \mathbb{Z}} x + \underbrace{a^2 - db^2}_{\in \mathbb{Z}}$

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

Ex $\mathbb{Q}[\sqrt{18}] = \{r + s\sqrt{18} \mid r, s \in \mathbb{Q}\}$
$= \{r + 3s\sqrt{2} \mid r, s \in \mathbb{Q}\}$
$= \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$
$= \mathbb{Q}[\sqrt{2}]$

BUT $\mathbb{Z}[\sqrt{8}] = \{a + 3b\sqrt{2}\}$
$\subsetneq \mathbb{Z}[\sqrt{2}]$

THM For a quadratic field $\mathbb{Q}[\sqrt{d}]$
Where d is squarefree,
its integers are

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

Quadfield		integers	
$\mathbb{Q}[i]$	$d=-1$	$\mathbb{Z}[i]$	
$\mathbb{Q}[\sqrt{2}]$		$\mathbb{Z}[\sqrt{2}]$	
$\mathbb{Q}[\sqrt{3}]$		$\mathbb{Z}[\sqrt{3}]$	
$\mathbb{Q}[\sqrt{-3}]$		$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$	
$\mathbb{Q}[\sqrt{5}]$		$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$	$5 \equiv 1 \ (4)$
$\mathbb{Q}[\sqrt{-5}]$		$\mathbb{Z}[\sqrt{-5}]$	$-5 \equiv 3 \ (4)$
$\mathbb{Q}[\sqrt{-39}]$		$\mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$	$-39 \equiv 1 \ (4)$