HW5 due Tues May 5.
Exam cheat sheet due Wed May 6.

Last week: Given nonsquare $d \in \mathbb{Z}$,

$$S_d = \{ |x^2 - dy^2| : x, y \in \mathbb{Z} \}.$$

If d is "nice" i.e. if $\mathbb{Z}[\sqrt{d}]$ is "Euclidean" then we proved:

(1) $n \in S_d \iff$ every prime $p \mid n$, $p \notin S_d$ occurs with even mult.

(2) prime $p \in S_d \iff \left(\frac{d}{p}\right) = +1$

$\iff p = (\text{some list}) \bmod 4d.$

Example: Claim $d = 3$ is "nice".

Hence

$$p = |x^2 - 3y^2| \iff \left(\frac{3}{p}\right) = +1$$

$\iff p = 3$ or $p = \pm 1 \bmod 12.$

Issue: It could be tricky to prove that any particular d is nice, i.e. that $\mathbb{Z}[\sqrt{d}]$ is Euclidean.

HW5.1: $\mathbb{Z}[\sqrt{-1}]$ is Euclidean

HW5.2: $\mathbb{Z}[\sqrt{-5}]$ is <u>not</u> Euclidean.

$p = x^2 + 5y^2$ might be hard ...

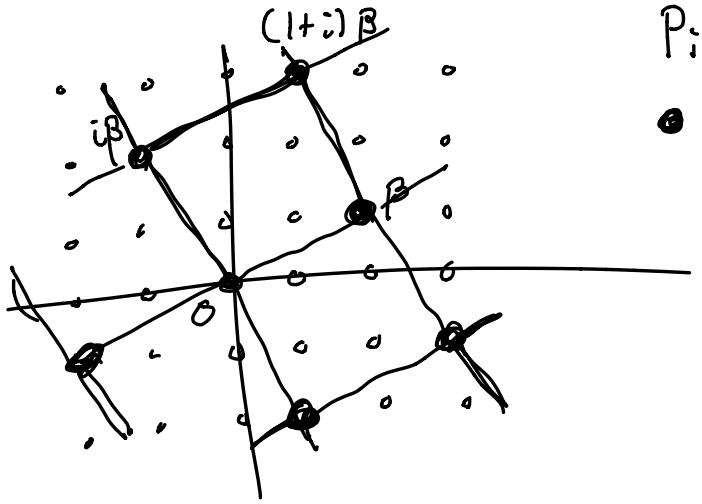
Help for HW5.1

Given $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ with $\beta \neq 0$, want to find some $\chi, \rho \in \mathbb{Z}[\sqrt{-1}]$ such that

$$\begin{cases} \alpha = \chi\beta + \rho \\ N(\rho) < N(\beta) \end{cases}.$$

Geometry: Identify $a + b\sqrt{-1} \leftrightarrow (a,b)$

Gaussian integers form a lattice in the complex plane:



Pick $\beta \neq 0$

● = numbers $x\beta$ for some $x \in \mathbb{Z}[\sqrt{-1}]$.

Numbers of the form βx form a sublattice of squares with side length

$\sqrt{N(\beta)}$

Given α, want to find x such that $\rho = \alpha - x\beta$ is <u>small</u>.

Well: Distance between α & $x\beta$

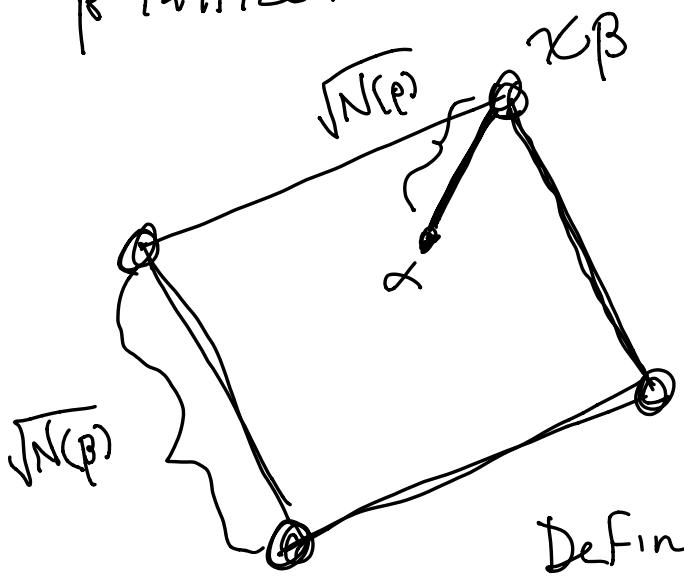
$= \sqrt{N(\alpha - x\beta)} = \sqrt{N(\rho)}$

i.e. want to find x such that

distance$(\alpha, x\beta)$ < distance$(0, \beta)$

$\sqrt{N(\rho)} < \sqrt{N(\beta)}$.

α lives in one square of the β lattice:



Let $\chi\beta$ be the <u>closest</u> lattice point.

How close is it?

Define $\rho := \alpha - \chi\beta$.

Argue that $\sqrt{N(\rho)} < \sqrt{N(\beta)}$.

Remark: d is never nice when $d \equiv 1 \bmod 4$, but in this case we can get a partial solution by defining

$$S_d' = \{ |x^2 - dy^2| : 2x, 2y \in \mathbb{Z} \}.$$

$$n \in S_d' \iff 4n \in S_d.$$

Even with this generalization, the

problem of which d are good is unsolved.

Know (Gauss): $d = -163$ is least example of good d.

It is unknown whether $\exists$ greatest good d.

Gauss' "class number problem"

So much for existence of solutions

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

What about uniqueness?

Suppose $x^2 - dy^2 = 1$ $\qquad \alpha = x + y\sqrt{d}$

$$N(x + y\sqrt{d}) = 1.$$

If $u = u + v\sqrt{d}$ is a unit

i.e. $N(u + v\sqrt{d}) = 1$

Then αu is another solution:

$$N(\alpha u) = N(\alpha)\,N(u)$$
$$= N(\alpha) = \pm 1.$$

Multiply any solution by a unit to get another solution.

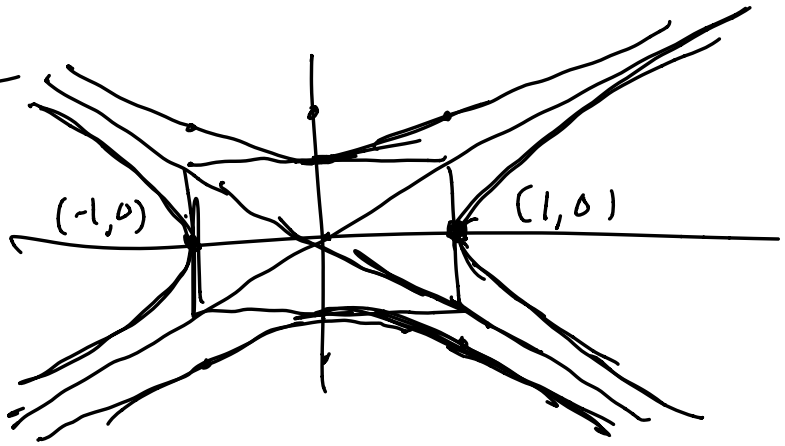
For $d < 0$ this is no big deal because units of $\mathbb{Z}[\sqrt{d}]$ are just ± 1 $d \leq -2$

$\pm 1, \pm i$ $d = -1$.

But when $d > 0$ we will prove that there are <u>infinitely many units</u>.

Example: unit $u = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ satisfies $N(u) = |x^2 - dy^2| = 1$.

$d = 2$



Are there any more integer points, other than just $(\pm 1, 0)$?

Observe: If $\alpha = a + b\sqrt{2}$ are units
$\beta = c + d\sqrt{2}$

$N(\alpha) = N(\beta) = 1$

$|a^2 - 2b^2| = |c^2 - 2d^2| = 1.$

Then $\alpha\beta$ is another unit because

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1 \cdot 1 = 1.$$

i.e. $\alpha\beta = (a + b\sqrt{2})(c + d\sqrt{2})$

$= (ac + 2bd) + (ad + bc)\sqrt{2}$

$N(\alpha\beta) = 1$

$(ac + 2bd)^2 - 2(ad + bc)^2 = 1.$

(a, b) & (c, d) integer points on hyperbolas

$\rightsquigarrow (ac + 2bd, ad + bc)$

is another integer point on hyperbolas.

Jargon: Integer Points $|x^2 - 2y^2| = 1$ form a group.

Consequence: If we can find one nontrivial solution say $|x^2 - 2y^2| = 1$ $(y \neq 0)$ then we obtain infinitely many solutions:

$$\alpha = (x + y\sqrt{2})$$

$$\alpha^k = x_k + y_k\sqrt{2}.$$

infinitely many solutions

Theorem: Every solution $|x^2 - 2y^2| = 1$ has the form $(\pm x, \pm y)$ where

$$x + y\sqrt{2} = (1 + \sqrt{2})^k$$

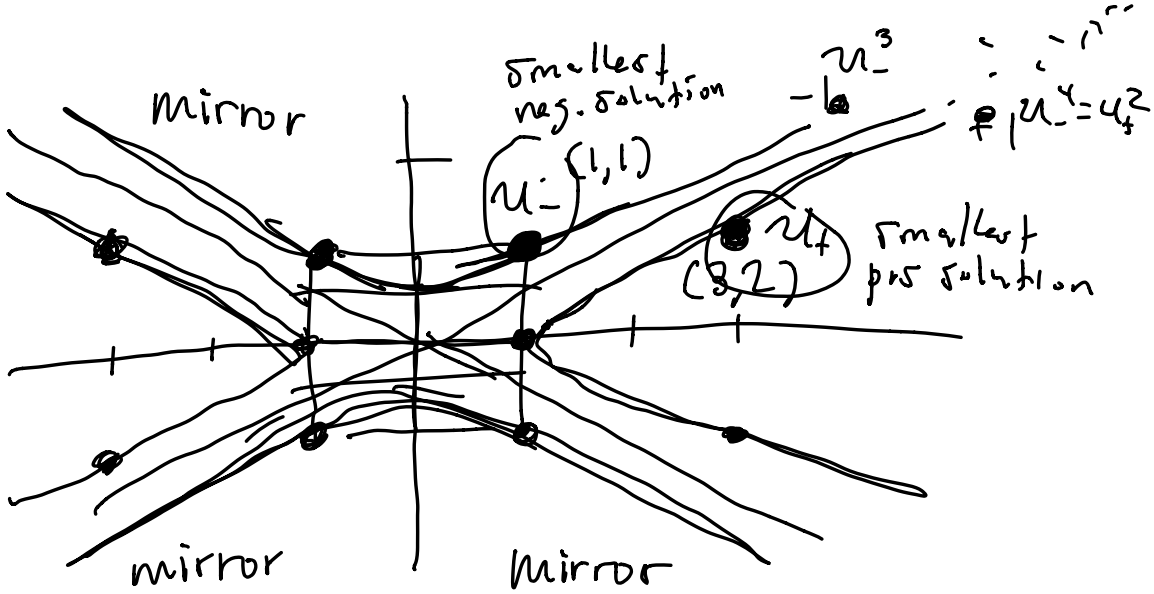
for some $k \in \mathbb{Z}$. ///

Smallest Solution $1 + \sqrt{2}$.

$N(1+\sqrt{2}) = |1^2 - 2\cdot 1^2| = +1$ ✓

$N((1+\sqrt{2})^k) = (+1)^k = +1$ ✓

Claim: Every solution is $(\pm)$ some power of the smallest solution.



Fact $u_+ = u_-^2$

smallest soln of $x^2 - 2y^2 = +1$ = (smallest soln of $x^2 - 2y^2 = -1$)^2

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

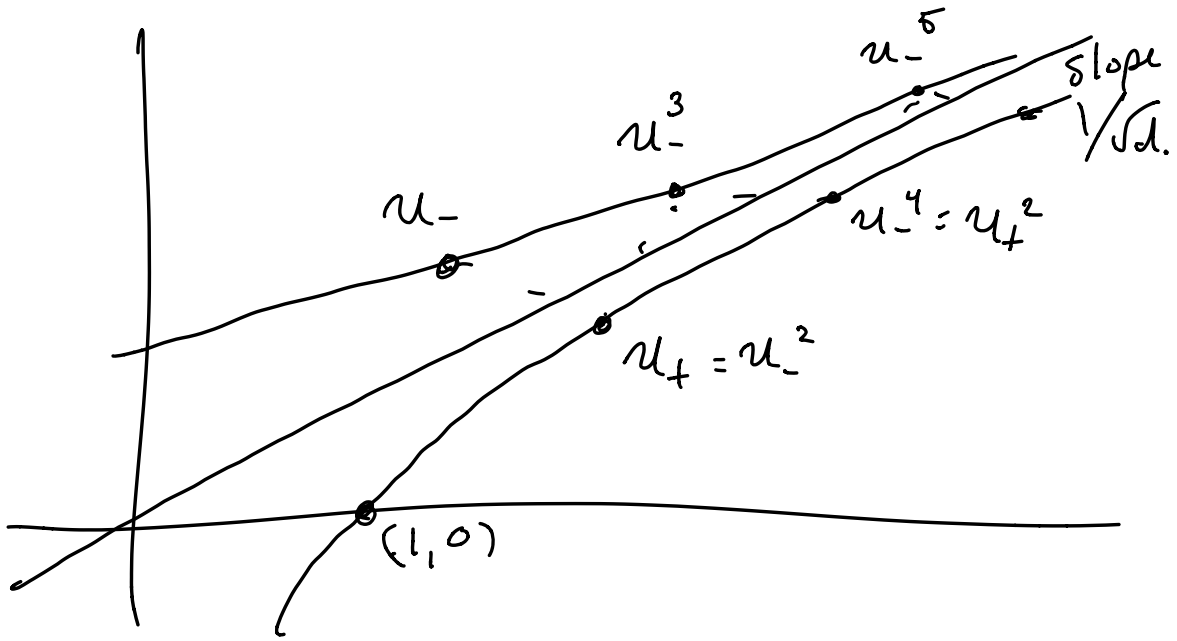
Theorem: Always exists a smallest positive solution $u_+ = x + y\sqrt{d}$. nontrivial. $(x^2 - dy^2 = +1)$

Every pos. solution has the form u_+^k for some k.

If a smallest neg soln exists $u_- = x' + y'\sqrt{d}$ $(x'^2 - dy'^2 = -1)$

then $u_-^2 = u_+$,

hence every solution (pos or neg) has the form u_-^k for some k.



Remark: The (-1)-hyperbola $x^2 - dy^2 = -1$ may have no integer points.

OPEN QUESTION for which d this happens.

Two issues:

(1) Prove that u_+ (smallest pos sol) always exists.

(2) Give an algorithm to compute u_+ (and also u_-, when it exists.)

Idea for both (1) & (2):

$$p^2 - dq^2 = \pm 1$$

$$p^2 = \pm 1 + dq^2$$

$$\frac{p^2}{q^2} = \frac{\pm 1}{q^2} + d \approx d \quad (q \text{ large})$$

$$\frac{p}{q} \approx \sqrt{d} \quad (q \text{ large}).$$

Idea: Find rational approximations to the irrational $\sqrt{d}$.

Solutions to $x^2 - dy^2 = \pm 1$ $\overset{\checkmark}{\Longrightarrow}$ rational approximations to $\sqrt{d}$.

Good Idea:

rational approx. to $\sqrt{d}$ $\overset{?}{\Longrightarrow}$ solutions to $x^2 - dy^2 = \pm 1$.

Problem was solved by Euler - Lagrange.

By the way: $x^2 - dy^2 = \pm 1$ is called "Pell's Equation"

Today I will sketch an abstract proof that nontrivial solution of $x^2 - dy^2 = +1$ always exists.

Next time I'll show an algorithm. "continued fractions."

Lemma (Dirichlet Approximation):

For all $d, n \in \mathbb{Z}$ with $\sqrt{d} \in \mathbb{R} - \mathbb{Q}$, $n \geq 2$, there exist some $p, q \in \mathbb{Z}$

$$\begin{cases} |p - q\sqrt{d}| < 1/n \\ 0 < q < n. \quad \text{(hence } 0 < |p - q\sqrt{d}| \text{)} \end{cases}$$

Proof: For all $1 \leq k \leq n-1$, since $\sqrt{d} \notin \mathbb{Q}$ there is $a_k \in \mathbb{Z}$ such that

$$0 < a_k - k\sqrt{d} < 1$$

Furthermore, $k \neq l \Rightarrow a_k - k\sqrt{d} \neq a_l - l\sqrt{d}$.

Consider the numbers

$0 = 0 - 0\sqrt{d}$, $a_1 - \sqrt{d}$, $a_2 - 2\sqrt{d}$, $\cdots$, $a_{n-1} - (n-1)\sqrt{d}$, $1 = 1 - 0\sqrt{d}$.

$n+1$ of these.

Divide $[0,1]$ into intervals length $\frac{1}{n}$.

Pigeonhole $\Rightarrow$ One such interval contains two of the numbers.

Say $a-b\sqrt{d}$ & $a'-b'\sqrt{d}$ are two such numbers in the same subinterval, then

$$|(a-b\sqrt{d})-(a'-b'\sqrt{d})| < \frac{1}{n}$$

$$|(a-a')-(b-b')\sqrt{d}| < \frac{1}{n}$$

Note that $b-b' \neq 0$ since otherwise the inequality $|a-a'| < \frac{1}{n}$ implies $a \neq a'$ which contradicts the fact that

$$a-b\sqrt{d} \neq a'-b'\sqrt{d}.$$

Finally, since $0 \leq b < n$ & $0 \leq b' < n$ we have $0 < |b-b'| < n$, as desired. ///

Theorem (Existence of Nontrivial Positive Pell Solutions):
Given $d \in \mathbb{Z}$, $\sqrt{d} \in \mathbb{R} - \mathbb{Q}$, there exist some $x, y \in \mathbb{Z}$, $y \neq 0$, such that

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

↖ positive

The first proof was given by Lagrange in 1768. We will give a slicker proof due to Dirichlet (1840).

Proof: Suppose we can find some $a_1, a_2, b_1, b_2, M \in \mathbb{Z}$ satisfying

$$(*)\begin{cases} (a_1, b_1) \neq (a_2, b_2), & \text{(i)} \\ a_1^2 - d b_1^2 = a_2^2 - d b_2^2 = M \ (\neq 0) & \text{(ii)} \\ a_1 = a_2 \bmod M \ \ \& \ \ b_1 = b_2 \bmod M. & \text{(iii)} \end{cases}$$

[Remark: If $|M| = 1$ then we're done already.]

Then I claim that

$$x = \frac{a_1 a_2 - d b_1 b_2}{M}, \quad y = \frac{a_1 b_2 - a_2 b_1}{M}$$

is a solution. To see this, first note that (ii) & (iii) imply

$$a_1 a_2 - d b_1 b_2 \equiv a_1^2 - d b_1^2 = M \equiv 0 \bmod M$$
$$a_1 b_2 - a_2 b_1 \equiv a_1 b_2 - a_1 b_2 = 0 \bmod M,$$

hence $x, y \in \mathbb{Z}$. Next observe that (i) & (ii) imply $a_1 b_2 - a_2 b_1 \neq 0$,

hence $y \neq 0$. Finally, note that

$$\frac{a_1 - b_1\sqrt{d}}{a_2 - b_2\sqrt{d}} = \frac{a_1 - b_1\sqrt{d}}{a_2 - b_2\sqrt{2}} \cdot \frac{a_2 + b_2\sqrt{d}}{a_2 + b_2\sqrt{d}} = x - y\sqrt{d},$$

hence by multiplicativity of norm we have

$$\begin{aligned} x^2 - dy^2 &= N(x - y\sqrt{d}) \\ &= N\left((a_1 - b_1\sqrt{d})/(a_2 - b_2\sqrt{d})\right) \\ &= N(a_1 - b_1\sqrt{d}) / N(a_2 - b_2\sqrt{d}) \\ &= M/M = +1. \end{aligned}$$

It only remains to prove (*) and for this we use Dirichlet approximation:

" $\forall n \geq 1$, $\exists a, b \in \mathbb{Z}$ with $|a - b\sqrt{d}| < 1/n$ and $0 < b < n$." (hence $0 < |a - b\sqrt{d}|$)

In particular, we have $|a - b\sqrt{d}| < 1/n < 1/b$.

Now pick some $n' > n$ with $1/n' < |a - b\sqrt{d}|$ and repeat the argument to find $a', b' \in \mathbb{Z}$ such that $0 < |a' - b'\sqrt{d}| < 1/n' < 1/b'$.

Repeat to obtain ∞ many pairs $a, b \in \mathbb{Z}$ such that $0 < |a - b\sqrt{d}| \leq \frac{1}{b}$. $(b > 0)$

But this implies

$$a = a - b\sqrt{d} + b\sqrt{d} \leq |a - b\sqrt{d}| + b\sqrt{d}$$
$$< \frac{1}{b} + b\sqrt{d} \leq 1 + b\sqrt{d}$$

and hence

$$|a^2 - db^2| = (a + b\sqrt{d})\,|a - b\sqrt{d}|$$
$$\leq (1 + b\sqrt{d} + b\sqrt{d})\,\frac{1}{b}$$
$$= \frac{1}{b} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Thus $\exists$ ∞ many pairs $a, b \in \mathbb{Z}$ $(b > 0)$ with $|a^2 - db^2| \leq 1 + 2\sqrt{d}$.

$\Rightarrow$ $\exists$ some $-(1 + 2\sqrt{d}) \leq M \leq 1 + 2\sqrt{d}$

$\exists$ ∞ many a, b with $a^2 - db^2 = M$ $(\neq 0$ because $b \neq 0)$

Among these, one of the finitely many congruence classes $(a \bmod M, b \bmod M)$ must repeat.

Q.E.D.