HW5 will be due Thurs Apr 30.
There will be no HW6.
Instead of a final exam, I will ask you to prepare a "study sheet," the kind that you might bring to an open book exam. But there is no exam. You will just send me your study sheet.

Study sheet due on Wed May 6 via email.

Topic: Diophantine equation

$$x^2 - ny^2 = z \quad (n \in \mathbb{Z})$$

To study this equation we define a new number system:

$$\mathbb{Z}[\sqrt{n}] = \{ a + b\sqrt{n} : a, b \in \mathbb{Z} \} \subseteq \mathbb{R}.$$

This is a subring of $\mathbb{R}$.

This ring has a "conjugation"

$$(a+b\sqrt{n})^* = (a-b\sqrt{n}).$$

One can check by brute force that

for all $\alpha = a+b\sqrt{n}$

$\beta = c+d\sqrt{n}$

we have

$$(\alpha\beta)^* = \alpha^*\beta^*$$

AMAZING!

"Rationalization" trick from high school:

$$(a+b\sqrt{n})(a+b\sqrt{n})^*$$

$$= (a+b\sqrt{n})(a-b\sqrt{n})$$

$$= a^2 - b^2 n \quad \text{(the square root is gone).}$$

Define the norm function

$$N: \mathbb{Z}[\sqrt{n}] \longrightarrow \mathbb{Z}$$

$$a+b\sqrt{n} \longmapsto a^2 - nb^2$$

In other words, for all $\alpha \in \mathbb{Z}[\sqrt{n}]$
we set $N(\alpha) = \alpha\alpha^*$.

Then it follows from the amazing
fact $(\alpha\beta)^* = \alpha^*\beta^*$ that

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

Proof: $N(\alpha\beta) = (\alpha\beta)(\alpha\beta)^*$

$$= \alpha\beta\alpha^*\beta^*$$
$$= (\alpha\alpha^*)(\beta\beta^*)$$
$$= N(\alpha)N(\beta).$$ ///

In other words, for $\alpha = a + b\sqrt{n}$
$\beta = c + d\sqrt{n}$

we have

$$N(\alpha)N(\beta) = N(\alpha\beta)$$
$$(a^2 - nb^2)(c^2 - nd^2) = N\left((a+b\sqrt{n})(c+d\sqrt{n})\right)$$

$$= N\left((ac+nbd)+(ad+bc)\sqrt{n}\right)$$

$$= (ac+nbd)^2 - n(ad+bc)^2.$$

In other words, for all $a,b,c,d,n \in \mathbb{Z}$:

$$\boxed{(a^2-nb^2)(c^2-nd^2) = (ac+nbd)^2 - n(ad+bc)^2}$$

"Brahmagupta's Identity"
~ 600 AD.

Used to solve so-called Pell's Equation

$$x^2 - ny^2 = 1$$

We will discuss this later. For now we will discuss more general equation $x^2 - ny^2 = z$ $(x,y,z \in \mathbb{Z})$.

First observation:

If $e = a^2 - nb^2$
$f = c^2 - nd^2$

Then from B.I. ef also has this form:

e.f : $(\square)^2 - n(\square)^2$.

Thus our goal is to find prime numbers p such that

$$p = x^2 - ny^2 \quad (x, y \in \mathbb{Z}).$$

"Which primes can be expressed in the form $x^2 - ny^2$?"

Necessary Condition:

Suppose $p = x^2 - ny^2$ $(x, y \in \mathbb{Z})$

Then I claim that $(n/p) = +1$.

Proof: First I claim $p \nmid y$.

If $p \mid y$ then $p \mid x^2 = p + ny^2$

$\Rightarrow p \mid x$

Say $x = px'$ & $y = py'$

$\Rightarrow$ $p = p^2x'^2 - p^2y'^2$

$p = p^2(x'^2 - ny'^2)$. ↯

Since $p \nmid y$, y^{-1} exists mod p.

$$x^2 - ny^2 = p$$
$$x^2 - ny^2 = 0 \mod p$$
$$x^2 = ny^2 \mod p$$
$$\left(\frac{x}{y}\right)^2 = n \mod p.$$

$$\Rightarrow \left(\frac{n}{p}\right) = +1. \qquad ///$$

E.g. If $p = x^2 + y^2$ $\left(x^2 - (-1)y^2\right)$

then must have $\left(\frac{-1}{p}\right) = +1$,

an hence $p = 2$ or $p = 1 \mod 4$.

In other words, primes of the form $x^2 + y^2$ cannot be $= 3 \mod 4$.

Is this condition also sufficient ?

If $\left(\frac{n}{p}\right) = +1$, can we write

$$p = x^2 - ny^2 \quad (x, y \in \mathbb{Z})$$??

Sometimes yes, sometimes no.

Let's try to prove it.

Suppose $\left(\frac{n}{p}\right) = +1$, so that

$$n = m^2 \bmod p$$

$$m^2 - n = 0 \bmod p$$

$$p \mid (m^2 - n) \quad \text{some } m \in \mathbb{Z}.$$

In the ring $\mathbb{Z}[\sqrt{n}]$ we can factor

$$m^2 - n = (m + \sqrt{n})(m - \sqrt{n}).$$

So we have

$$p \mid (m + \sqrt{n})(m - \sqrt{n})$$

"Euclid's Lemma"?

Unknowns:

- Is p a prime element of the ring $\mathbb{Z}[\sqrt{n}]$?
- Does Euclid's Lemma hold in the ring $\mathbb{Z}[\sqrt{n}]$?

From now on, let's assume that $\sqrt{n} \notin \mathbb{Z}$, and hence $\sqrt{n} \notin \mathbb{Q}$.

Then for all $a, b, c, d \in \mathbb{Z}$ we have

$$a + b\sqrt{n} = c + d\sqrt{n} \iff a = c \ \& \ b = d.$$

Proof: Suppose $b \neq d$. Then

$$a + b\sqrt{n} = c + d\sqrt{n}$$

$$(b-d)\sqrt{n} = c - a$$

$$\sqrt{n} = \frac{c-a}{b-d} \notin \mathbb{Q}. \ \lightning$$

Hence $b = d$ and

$$c - a = (b-d)\sqrt{n}$$
$$= 0$$

$\Rightarrow a = c.$ ///

I also claim that for $\alpha \in \mathbb{Z}[\sqrt{n}]$,

$$N(\alpha) = 0 \iff \alpha = 0 + 0\sqrt{n}.$$

Proof: $\alpha = 0 + 0\sqrt{n}$

$\Rightarrow N(\alpha) = 0^2 - n0^2 = 0.$

Conversely, let $\alpha = a + b\sqrt{n}$ and suppose $N(\alpha) = 0$

$$a^2 - nb^2 = 0$$

If $b \neq 0$ then

$$n = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$$ ↯

Therefore $b = 0$. Hence $a = 0$, and

$$\alpha = 0 + 0\sqrt{n}.$$ ///

Corollary: $\mathbb{Z}[\sqrt{n}]$ is an "integral domain":

$$\alpha\beta = 0 \Rightarrow \alpha = 0 \text{ or } \beta = 0.$$

Proof: $\alpha\beta = 0$

$$N(\alpha\beta) = 0$$

$$N(\alpha)N(\beta) = 0$$

$$\Rightarrow N(\alpha) = 0 \text{ or } N(\beta) = 0.$$

$$\Rightarrow \alpha = 0 \text{ or } \beta = 0.$$ ///

Another useful fact:

If $\alpha \in \mathbb{Z}[\sqrt{n}]$ is a unit (i.e. is invertible), then $\exists\ \beta \in \mathbb{Z}[\sqrt{n}]$

such that $\alpha\beta = 1 + 0\sqrt{n}$

Taking norms gives

$$N(\alpha\beta) = 1^2 - n0^2 = 1$$

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

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

///

Definition: Say $\pi \in \mathbb{Z}[\sqrt{n}]$ is prime if

- π is not a unit.
- $\pi = \alpha\beta$ then α or β (or both) is a unit.

Theorem (Rational Primes of $\mathbb{Z}[\sqrt{n}]$):

Let $\pm p \in \mathbb{Z}$ be a prime integer.

Then $\pm p$ is prime in the ring $\mathbb{Z}[\sqrt{n}]$

$\Leftrightarrow \pm p$ is <u>not</u> of the form $x^2 - ny^2$

Proof: If $\pm p = x^2 - ny^2$ $(x, y \in \mathbb{Z})$

then $\pm p = (x + y\sqrt{n})(x - y\sqrt{n})$

$(p + 0\sqrt{n})$

could either of these be a unit?

Take norms:

$$N(\pm p) = N(x + y\sqrt{n})\, N(x - y\sqrt{n})$$

[Recall: $N(a + b\sqrt{n}) = (a + b\sqrt{n})(a - b\sqrt{n})$
$= a^2 - nb^2$.]

$$p^2 = (x^2 - ny^2)(x^2 - n(-y)^2).$$

$$p^2 = (x^2 - ny^2)^2$$

$$\Rightarrow N(x + y\sqrt{n}) = x^2 - ny^2 = \pm p \neq \pm 1$$

$\Rightarrow x \pm y\sqrt{n}$ are not units.

Hence $\pm p$ not prime in $\mathbb{Z}[\sqrt{n}]$.

Conversely, suppose $\pm p$ not prime in $\mathbb{Z}[\sqrt{n}]$. We will show $\pm p = x^2 - ny^2$ for some $x, y \in \mathbb{Z}$.

Not prime in $\mathbb{Z}[\sqrt{n}]$

$\Rightarrow \quad \pm p = (x + y\sqrt{n})\,\gamma$

$(p + 0\sqrt{n})$ — both non-units in $\mathbb{Z}[\sqrt{n}]$

Take norms:

$$N(\pm p) = N(x + y\sqrt{n})\,N(\gamma)$$

$$p^2 = (x^2 - ny^2)\,N(\gamma) \quad \text{in } \mathbb{Z}.$$

where $x^2 - ny^2 \neq \pm 1$ because $x + y\sqrt{n}$ & γ are non-units

$N(\gamma) \neq \pm 1$

By unique factorization in $\mathbb{Z}$, we must have

$$x^2 - ny^2 = \pm p \quad \checkmark$$

$$N(\gamma) = \pm p$$

QED

Recall the unknowns:

- is p prime in $\mathbb{Z}[\sqrt{n}]$?
- does Euclid's Lemma hold in $\mathbb{Z}[\sqrt{n}]$?

First question is answered. ✓

Second question...

NEXT TIME.