LECTURE 1: taken from Chapter 1 of Stillwell's "Elements of Number Theory"

§1.1: Natural Numbers

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$ has addition & multiplication

Def^{n}/ <u>a divides n</u> if $n = ab$ for some $a, b \in \mathbb{N}$.
We write a/n if a divides n.
We write $a \nmid n$ if a does not divide n.

Def^{n}/ $p \in \mathbb{N}$ is <u>prime</u> iff only 1 and p divide p.

Examples: 1, 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, ... PRIMES

only even prime in $\mathbb{N}$.

Th^{m}/ $\exists$ ∞ly many primes in $\mathbb{N}$; that is, given $p_1, p_2, \dots, p_k$ primes, we can find <u>another</u> prime p.

PROOF: Consider $N = p_1 p_2 \cdots p_k + 1$. Observe $N > p_1, p_2, \dots, p_k$ hence $p_1, p_2, \dots, p_k \neq N$. Further it is clear that $p_j \nmid N$ for $j = 1, 2, \dots, k$. If N is prime then $p = N$ and we're done. Otherwise N is <u>composite</u> hence $\exists a, b$ s.t. $a, b \neq 1$ and $N = ab$ (also, $a, b \notin \{p_1, p_2, \dots, p_k\}$ as we remarked previously)
If a prime then $p = a$ and we're done. Otherwise $a = a_2 b_2$ and either a_2 is prime and we're done or $a_2 = a_3 b_3$ for some $a_3, b_3 \in \mathbb{N}$.
This cannot continue forever hence eventually we find another prime p. //

descent style proof.

§1.2 INDUCTION

An example, show $3 \mid n^3 + 2n$ for all $n \in \mathbb{N}$.

Base step: $n=1$, note $1^3 + 2(1) = 3$ and $3/3$.

Suppose $3 \mid m^3 + 2m$ for some $m \in \mathbb{N}$. Consider,

$$(m+1)^3 + 2(m+1) = m^3 + 3m^2 + 3m + 1 + 2m + 2 \quad : \text{Binomial Expansion.}$$

$$= m^3 + 2m + 3(m^2 + m + 3)$$

$$= 3(j + m^2 + m + 3) \quad : m^3 + 2m = 3j \text{ for some } j \in \mathbb{N} \text{ by induct. hypo.}$$

Thus $3 \mid (m+1)^3 + 2(m+1)$

and we shown the m^{th} step $\Rightarrow$ the $(m+1)$-th step true. Thus, by PMI $3 \mid n^3 + 2n$ $\forall n \in \mathbb{N}$. //

- Comment: you can build + and × in $\mathbb{N}$ via inductive arguments. If you want to read about that you'll probably need to look up more than Stillwell shows. That said, our focus is not on constructing $\mathbb{N}$ so I go on.

Induction

ascent: show $n \Rightarrow n+1$ and truth at $n=1$. We see this used many places to justify general formulas.

descent: show some process creates strictly decreasing sequence of positive # (in $\mathbb{N}$)

$$a_1 > a_2 > a_3 > \cdots > 0$$

The sequence must terminate before the $|a_1|$-steps (oops a_1-steps will do

Example: Egyptian fractions. Works by descent. Your hwk problem is partly to justify the strict decrease within the method. I show example

Example: write $\frac{43}{24} = 1 + \underbrace{\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}}$ where $n_1, n_2, .., n_k \in \mathbb{N} - \{1\}$. Egyptian fractions for $\frac{43}{24}$

$$\frac{43}{24} = \frac{24+19}{24} = 1 + \frac{19}{24}$$

$$\frac{19}{24} - \frac{1}{2} = \frac{19-12}{24} = \frac{7}{24} \leftarrow$$ subtract largest $\frac{1}{n}$ possible at each stage

$$\underbrace{\frac{7}{24} - \frac{1}{4}} = \frac{7-6}{24} = \frac{1}{24}$$

since $\frac{1}{3} = \frac{8}{24}$ I had to go to $\frac{1}{4}$.

Now, assemble, $\frac{43}{24} = 1 + \frac{19}{24} = 1 + \left(\frac{1}{2} + \frac{7}{24}\right) = 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{24}\right)$

$$\boxed{\frac{43}{24} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{24}}$$

Remark: this can be computationally tedious for nasty examples; $\frac{13}{1728} = \frac{1}{133} + \frac{1}{229\,824}$, yet your hwk shows it's possible always.

§1.3 integers

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \{0, \pm 1, \pm 2, \ldots\}$$

the $\mathbb{Z}$ comes from Zahlen, German for "Numbers"

Abelian Group Properties

$a+(b+c) = (a+b)+c$: associative

$a+0 = a$: additive identity

$a+(-a) = 0$: inverses additively.

$a+b = b+a$: abelian (commutes)

RING PROPERTIES

- multiplication $\times$ with $\underbrace{a(b+c) = ab+ac}_{\text{distributive property.}}$

Comment: terms such as "GROUP" and "RING" have technical meaning, but, these were born from study of $\mathbb{Z}$. The integers are the most important example of a ring. We'll see groups & rings throughout our study (however we don't define them untill later...)

Defn/ $p \in \mathbb{Z}$ is prime if the only integers ~~with~~ which divide p are $-p, p, 1, -1$. The defn of $a|b$ is the same as with $\mathbb{N}$ just replace $\mathbb{N}$ with $\mathbb{Z}$.

Let $a,b \in \mathbb{Z}$, $a|b$ if $\exists j \in \mathbb{Z}$ such that $b = aj$.

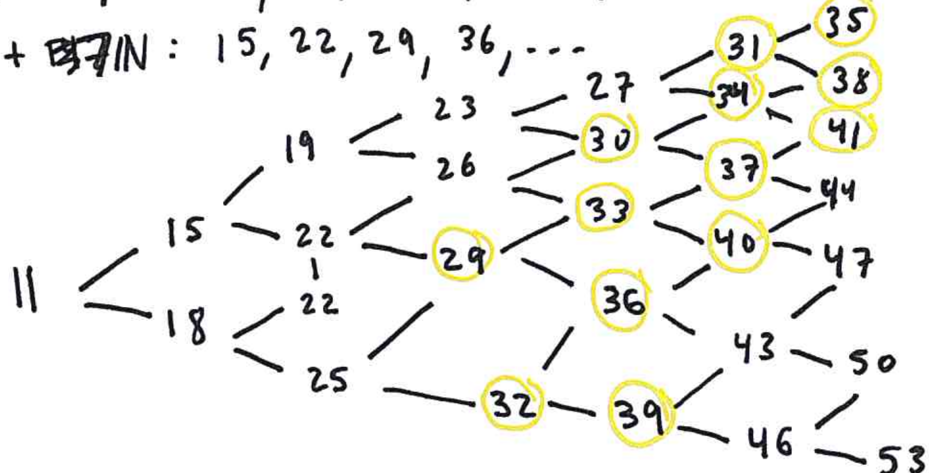
(I'll probably just state the defn for $\mathbb{N}$ & $\mathbb{Z}$ simultaneously in Lecture.)

PROBLEM: Describe numbers $4m + 7n$
① for $m,n \in \mathbb{N}$
② for $m,n \in \mathbb{Z}$ — the next section gives us a tool to solve this with much ease...

① $4 + 7\mathbb{N}$: 11, 18, 25, 32, 39, ...

$4\mathbb{N} + 7$: 11, 15, 19, 23, 27, 31, 35, 39, 43, ...

$8 + 7\mathbb{N}$: 15, 22, 29, 36, ...



You can see all #s from 29 and up are attained.

$29 = (2\times4) + (3\times7) \longrightarrow 33 = (3\times4) + (3\times7)$ etc...

$30 = (4\times4) + (2\times7)$

$31 = (6\times4) + (1\times7)$

$32 = (1\times4) + (4\times7)$

② $1 = 4\times2 - 7 \quad \therefore \quad \boxed{n = 4(2n) - 7n} \quad (\forall n \in \mathbb{Z})$

§1.4 DIVISION WITH REMAINDER

Suppose $b < a$ and $b \nmid a$ then division may be thought of as repeated subtraction. Start with

$$a \longrightarrow a-b \longrightarrow a-2b \longrightarrow \cdots \quad \text{(has to end by descent)}$$

$$23 \xrightarrow[①]{} 23-4=19 \xrightarrow[②]{} 15 \xrightarrow[③]{} 11 \xrightarrow[④]{} 7 \xrightarrow[⑤]{} 3 > 0 \quad \text{(can't go negative)}$$

$$23 - 5(4) = 3 \hookrightarrow 23 = 5(4)+3$$

$$\boxed{a = qb + r \longleftrightarrow \frac{a}{b} = q + \frac{r}{b}}$$

Comment: in practice a calculator can be helpful to find r. Just use $\frac{a}{b} - \underbrace{\left\lfloor \frac{a}{b} \right\rfloor}_{\text{floor function.}} = \frac{r}{b}$

Example: $\frac{45}{7} = 6.\overline{428571}$

$$\lfloor 6.\overline{428571} \rfloor = 6 \hookrightarrow 0.\overline{428571} = \frac{r}{7} \therefore r = 7(0.\overline{428571})$$

$$\boxed{r=3}$$

(Of course, no need for calculator here, it's easy to see $45 = 6(7)+3 \longrightarrow \underline{r=3}$).

§1.5 BINARY NOTATION

$$\boxed{(\text{BASE } 2) \quad a_n a_{n-1} \cdots a_2 a_1 a_0 = a_n \times 2^n + a_{n-1} \times 2^{n-1} + \cdots + a_2 \times 2^2 + a_1 \times 2 + a_0}$$

PROPOSITION: $\frac{m}{2}$ has remainder a_0 if $m = a_n \cdots a_1 a_0$ Base 2.

Example: $\underline{29 = 16+8+4+1} \longrightarrow (29)_{10} = (11101)_2$

$$\left.\begin{aligned} 29 &= 14 \times 2 + 1 \\ 14 &= 7 \times 2 + 0 \\ 7 &= 3 \times 2 + 1 \\ 3 &= 1 \times 2 + 1 \\ 1 &= 0 \times 2 + 1 \end{aligned}\right\} \longrightarrow \underline{(29)_2 = 11101}.$$

(neat technique.)

[my method, look at 2, 4, 8, 16, 32, 64, ... check which 2^n is larger than the given # go from there, always add when can...

16	16
8	24
4	28
~~2~~	~~30~~
1	29

Bingo.

Comment: # of operations to produce n as binary $< 2\log_2(n)$

Allows for fast exponentiation of m^n by

- squaring
- multiplying by m

$\Big\} < 2\log_2(n)$ steps.

Example: $m^{29} = m^{(11101)_2}$

$= m^{2^4+2^3+2^2+1}$

$= m^{16} m^8 m^4 m$

$=$

$$m \longrightarrow m^2 \longrightarrow m^4 \longrightarrow m^{16}$$
$$m^2 \downarrow m^3 \longrightarrow m^9 \longrightarrow m^{10} \longrightarrow m^{20}$$

— just tinkering you can skip this bit —

$$m \xrightarrow[s]{} m^2 \xrightarrow[s]{} m^4 \xrightarrow{m} m^5 \xrightarrow{m} m^6 \xrightarrow{m} m^7 \xrightarrow[s]{} m^{14} \xrightarrow[s]{} m^{28} \xrightarrow{m} m^{29}$$

To obtain m^{29} we squared 4 times & multiplied by m three times, 7 steps. Compare to $2\log_2(29) \approx 2\log_2(32)$
$= 2(5)$
$= 10.$

§1.6 DIOPHANTINE EQUATIONS

Classical goal of algebra: solve equations

Example: $x = \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$ solves $ax^2+bx+c=0$

this is a sol^{n} via radicals. Closed form sol^{n}'s like the above also known for 3rd or even 4th order, But, 5th order it has been proven impossible. Galois Theory gives a answer as to when it is possible to solve via radicals by studying a symmetry which appears between the sol^{n}'s. You can study Stillwell's Elements of Algebra for a nice introduction.

[Def^{n}/ An equation is Diophantine if you only seek integer sol^{n}'s.

For example, the Diophantine quadratic eq^{n} is to find $x \in \mathbb{Z}$ for which $ax^2+bx+c=0$.

- One might think of ax^2+bx+c as an object independent of where x is taken, that is an interesting pursuit... see more on "varieties" In particular, read Chapter 6 of <u>FEARLESS SYMMETRY</u> by ASH and GROSS. That popular book is great for seeing way past this course...

<u>Definitions of Our Main Examples</u>

1.) Pythagorean Eq^{n}: $x^2+y^2=z^2$, whose $\mathbb{N}$-sol^{n}'s (x,y,z) are known as <u>Pythagorean Triples</u>

2.) The Pell Eq^{n} $x^2-ny^2=1$ for any nonsquare $n \in \mathbb{N}$.

3.) The Butchet Eq^{n} $y^3=x^2+n$ for any $n \in \mathbb{N}$

4.) The Fermat Eq^{n} $x^n+y^n=z^n$ for any $n \in \mathbb{N}$, $n>2$.

One of our goals is to understand the structure of $\mathbb{Z}$-sol^{n}'s to the eq^{n}'s above. Of course, the PYTHAGOREAN Eq^{n} is ancient. See the table of values known to Babylonians circa 1800 BC, the "Plimpton 322 tablet"

y	z	x^2
119	169	14,400
3367	4825	$(3456)^2$
4601	6649	$(4800)^2$
12709	18541	$(13,500)^2$
65	97	$(72)^2$

etc

⋮

$$x^2+y^2=z^2$$

$$x^2 = z^2-y^2 \longrightarrow \underline{x=120}.$$

$$\underbrace{(120, 119, 169)}_{\text{Pythagorean Triple}}$$

in case you're wondering, I used a calculator (wolframalpha)

these "Pythagorean Triples" predate the Pythagoreans by $\approx$ 1300 years. Anyway, the story gets more interesting when $\approx$ 300 BC <u>Euclid</u> showed all $\mathbb{N}$ - sol$^{\underline{n}}$'s of $x^2+y^2=z^2$ can be produced <u>parametrically</u> as follows,

$$\boxed{\begin{aligned} x &= (u^2-v^2)w \\ y &= 2uvw \\ z &= (u^2+v^2)w \end{aligned}}$$

$\longleftarrow$ Euclid's Parametrization of Pythag. Triples.

for $u, v, w \in \mathbb{N}$.

<u>Exercise 1.6.3</u>

Proof that $(\underbrace{(u^2-v^2)w}_{x}, \underbrace{2uvw}_{y}, \underbrace{(u^2+v^2)w}_{z})$ is Pythag. Trip $\forall (u,v,w) \in \mathbb{N}^3$,

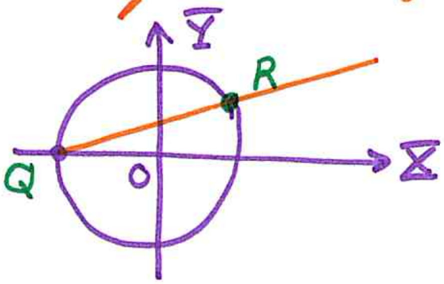
$$\begin{aligned} x^2+y^2 &= [(u^2-v^2)w]^2 + [2uvw]^2 = (u^4-2u^2v^2+v^4)w^2 + 4u^2v^2w^2 \\ &= (u^4+2u^2v^2+v^4)w^2 \\ &= (u^2+v^2)^2w^2 \\ &= ((u^2+v^2)w)^2 \\ &= z^2. \end{aligned}$$

§1.7 THE DIOPHANTUS CHORD METHOD

- what is described here comes ≈ 500 years after Euclid's parametric presentation. Despite the namesake "Diophantine" we actually see how Diophantus found rational ($\mathbb{Q}$) sol$^{\underline{n}}$'s to a given eq$^{\underline{n}}$ close to $x^2+y^2=z^2$...

An integer sol$^{\underline{n}}$ $(x,y,z)=(a,b,c)$ of $x^2+y^2=z^2$ gives $a^2+b^2=c^2$ hence $\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$ so, we may seek $X, Y \in \mathbb{Q}$ for which $X^2+Y^2=1$. Geometrically, a rational pt. on the unit-circle

- Diophantus did this with algebra, the geometry here came later, I'm not sure the precise history here.



$Q=(-1,0)$

$R=(X,Y)$

slope $= t = \dfrac{Y}{X+1} \in \mathbb{Q}$

$Y = t(X+1)$

- any line with rational slope t from Q to pt. (X,Y) on circle gives a rational pt ($X \in \mathbb{Q}$ & $Y \in \mathbb{Q}$)
- Find intersection of $Y=t(X+1)$ & $X^2+Y^2=1$ in usual way:

$$X^2+Y^2 = X^2+t^2(X+1)^2 = 1$$

$$\hookrightarrow X^2+t^2(X^2+2X+1)=1$$

$$\boxed{(t^2+1)X^2+2t^2X+t^2-1=0}$$

This, we know how to solve!

Continuing,

$$(t^2+1)X^2 + 2t^2X + t^2-1 = 0$$

$t^2+1 \neq 0$ nothing lost.

$$X^2 + \frac{2t^2}{1+t^2}X + \frac{t^2-1}{t^2+1} = 0$$

$$\longrightarrow \left(X + \frac{t^2}{1+t^2}\right)^2 = \frac{1-t^2}{t^2+1} + \left[\frac{t^2}{1+t^2}\right]^2$$

$$= \frac{(1-t^2)(1+t^2)+t^4}{(1+t^2)^2}$$

$$= \frac{1-t^2+t^2-t^4+t^4}{(1+t^2)^2}$$

$$= \frac{1}{(1+t^2)^2} \rightarrow (X+\alpha)^2 = \beta^2$$

$$\hookrightarrow X = -\alpha \pm \beta$$

$$\therefore \quad X = \frac{-t^2}{1+t^2} \pm \frac{1}{1+t^2}$$

$$\underbrace{X = \frac{1-t^2}{1+t^2}}_{\text{interesting sol}^{\text{n}}} \quad \text{or} \quad \frac{-t^2-1}{1+t^2} = \underbrace{\frac{-(1+t^2)}{1+t^2} = -1}_{\text{from } (-1,0) \text{ pt.}}.$$

Thus, $Y = t(X+1) = t\left(\frac{1-t^2}{1+t^2} + \frac{1+t^2}{1+t^2}\right) = \frac{2t}{1+t^2}$

and $\boxed{\text{we find rational pt. } \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \text{ for}}$ any $t \in \mathbb{Q}$.

(we derive Euclid's f-la's next ↗

We found for $t \in \mathbb{Q}$, the point

$$R = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

is on the unit-circle $X^2 + Y^2 = 1$. Now,
$t \in \mathbb{Q} \Rightarrow \exists u, v \in \mathbb{Z}$ s.t. $t = v/u$ hence,

$$R = \left(\frac{1 - v^2/u^2}{1 + v^2/u^2}, \frac{2v/u}{1+v^2/u^2} \right)$$

$$= \left(\frac{u^2 - v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2} \right)$$

But, $X = \frac{x}{z}$ and $Y = \frac{y}{z}$ hence from this we find,

$$\frac{x}{z} = \frac{(u^2-v^2)w}{(u^2+v^2)w} \quad \& \quad \frac{y}{z} = \left(\frac{2uv}{u^2+v^2}\right)\frac{w}{w}$$

Or, as we may find familar,

$$\boxed{\begin{aligned} x &= (u^2-v^2)w \\ y &= 2uvw \\ z &= (u^2+v^2)w \end{aligned}}$$

use imaginati to see the $\frac{w}{w}$ factor ☺

Comment: there is a nice connection between $\mathbb{Q}$ & $\mathbb{Z}$ sol^{n}'s of $x^2+y^2 = z^2$ since the eq^{n} has summands of same degree (homogeneous) ~~For contrast~~, If $\left(\frac{v_1}{u_1}\right)^2 + \left(\frac{v_2}{u_2}\right)^2 = \left(\frac{v_3}{u_3}\right)^2$ we can multiply by $(u_1u_2u_3)^2$ to obtain $v_1^2 + v_2^2 = v_3^2$ ($\mathbb{Z}$-sol^{n})

In nonhomogeneous case not so easy... Exercises on pg 16 explore this a bit, but I did not assign since not our focus.

§1.8 GAUSSIAN INTEGERS

We saw a neat derivation of Euclid's f-las via Diophantus Chord technique, here we find yet another way by introducing COMPLEX NUMBERS

$$x^2 + y^2 = (x - yi)(x + yi) \quad \text{where } \underbrace{i = \sqrt{-1}}_{i^2 = -1}.$$

Given $x, y \in \mathbb{Z}$ the numbers

$$x + yi \quad \text{and} \quad x - yi$$

are complex integers. We define,

$$\boxed{\text{Def}^{n}/ \ \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}}$$ ← GAUSSIAN INTEGERS

Digression: $\mathbb{Z}[i]$ is a RING.

$(a + ib) + (x + iy) = a + x + i(b + y)$: good concept of +

$$(a + ib)(x + iy) = ax + iay + ibx + i^2 by$$
$$= ax - by + i(ay + bx)$$: good multiplication

"good" in a sense we define carefully later but essentially, this means the numbers $a + ib \in \mathbb{Z}[i]$ behave the same as those in $\mathbb{Z}$. Bottom line we may manipulate Gaussian integers just like integers.

Two Square Identity: a sum of two squares times a sum of two squares is a sum of two squares.

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2$$

Proof: we use Gaussian Integers to guide the algebra,

$$\begin{aligned}(a_1^2 + b_1^2)(a_2^2 + b_2^2) &= (a_1 + i b_1)(a_1 - i b_1)(a_2 + i b_2)(a_2 - i b_2) \\ &= [a_1 a_2 - b_1 b_2 - i(b_1 a_2 + a_1 b_2)] \cdot \\ &\quad\ [a_1 a_2 - b_1 b_2 + i(b_1 a_2 + a_1 b_2)] \\ &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2 . \quad //\end{aligned}$$

(so simple this is) cool.

Corollary: If the triples (a_1, b_1, c_1) and (a_2, b_2, c_2) are Pythagorean then so is the triple $\underbrace{(a_1 a_2 - b_1 b_2,\ a_1 b_2 + b_1 a_2,\ c_1 c_2)}_{*}$

Proof: If (a_1, b_1, c_1) & (a_2, b_2, c_2) are Pythag. triples then

$$a_1^2 + b_1^2 = c_1^2 \quad \text{and} \quad a_2^2 + b_2^2 = c_2^2 .$$

Then, by the two-square identity,

$$\begin{aligned}(c_1 c_2)^2 = c_1^2 c_2^2 &= (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\ &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2\end{aligned}$$

Hence $*$ is indeed a Pythagorean triple. //

In complex analysis we study $z = x+iy$ for $x, y \in \mathbb{R}$ the complex conjugate is $\bar{z} = x - iy$ then

$$z\bar{z} = (x+iy)(x-iy) = x^2+y^2$$

We define the modulus $|z|$ by $|z| = \sqrt{z\bar{z}}$ and the beautiful fact is that $|zw| = |z||w|$. The square of the modulus is $z\bar{z} = x^2+y^2 = \text{norm}(z)$

Hence,

$$\boxed{\text{norm}(z_1)\,\text{norm}(z_2) = \text{norm}(z_1 z_2)}$$

[this is the 2-square identity as we may note ↴

$$z_1 z_2 = (a_1+ib_1)(a_2+ib_2) = a_1a_2 - b_1b_2 + i(a_2b_1 + a_1b_2)$$]

DIGRESSION [Comment: in other coursework I almost always use "norm" as a function $\|\cdot\| : V \to \mathbb{R}$ where $\|cv\| = |c|\,\|v\|$. Its the length of a vector in V. However, here the norm is the square of what I would usually term a norm. This appears a custom of #-theory.]

Stillwell argues, $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ is reduced to $\mathbb{Z}$ by the norm: $\mathbb{Z}[i] \to \mathbb{Z}$ hence properties of $\mathbb{Z}$ are lifted to $\mathbb{Z}[i]$... anyway, that doesn't happen until a later chapter so relax, what follows next is very insightful ↴

$\mathbb{Z}[i]$ HOLDS SECRET OF PYTHAGOREAN EQ^n

$$z^2 = x^2+y^2 = \underbrace{(x-yi)}_{\text{square}}\underbrace{(x+iy)}_{\text{square}}$$

Why? Because for x, y to have no common divisor it must also follow $x-yi$ & $x+iy$ have no common divisor (we prove this sort of thing for $\mathbb{Z}$ in next chapter) thus each factor of z must either show up in $x-yi$ or $x+iy$ as a square since z^2 has all squares $z = p_1p_2 \cdots p_k \rightarrow z^2 = p_1^2p_2^2 \cdots p_k^2$.

for example

$(12)^2 = 3^2 \cdot 4^2$
$(100)^2 = 25 \cdot 4 \cdot 5 \cdot 20$
$= (125)(80)$

have common divisor

Thus,

$$x - yi = (u-iv)^2$$

$$\therefore \ x - yi = u^2 - v^2 - 2iuv$$

$$x = u^2 - v^2$$
$$y = 2uv$$
$$z^2 = x^2+y^2 = (u^4 - 2u^2v^2 + v^4) + (4u^2v^2)$$
$$\Rightarrow \ z^2 = u^4 + 2u^2v^2 + v^4 = (u^2+v^2)^2$$
$$\therefore \ \underline{z = u^2+v^2}$$

We find the primitive pythagorean triple

$$(u^2-v^2,\ 2uv,\ u^2+v^2)$$

for $u, v \in \mathbb{Z}$. This would be Euclid's f-las with $w = 1$. You can multiply these to get new triples.

Example: $u = 2$, $v = 1 \rightsquigarrow (3, 4, 5) : 3^2+4^2 = 5^2$
multiply by 3: $(9, 12, 15) : 9^2 + 12^2 = 15^2$
$81 + 144 = 225$ cool.

§1.9 DISCUSSION

Note: these are my favorite sections in ~~each~~ the book.

$\boxed{\text{Question: what values does } x^2+y^2 \text{ attain as } x,y \text{ run through } \mathbb{Z}}$

Fermat ~ 1640 x^2+2y^2, x^2+3y^2
(read Diophantus)

↓

[Euler, Lagrange, Legendre, Gauss] studied $ax^2+bxy+cy^2$
late 18^{th} century

↓

Gauss' Disquisitiones Arithmeticae
finished study by brute algebra
(1801), Gauss did not use
algebraic # theory, just
algebraic might... worked
directly with quadratic forms
with $\mathbb{Z}$-coefficients.

algebraic # theory used $\sqrt{2}$ or i to see things about $\mathbb{Z}$
≈ 1770 Euler & Lagrange saw through $y^3 = x^2+2$
by $(x+\sqrt{-2})(x-\sqrt{-2})$ etc..
assumption $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-2}]$ behave like $\mathbb{Z}$.

1832, $\mathbb{Z}[i]$
justified by Gauss
(Chapter 6 in Stillwell)

↓

invented "ideal" #'s ← Kummer & Dedekind → 1871 demystified Kummer's ideal #, made concrete.

found correct technique
to deal with algebraic #'s which
don't behave like $\mathbb{Z}$ ---> enter Rings, Ideals etc...