Lecture 4: chapter 3, §3.3 → in Stillwell.

In $\mathbb{Z}$ only sol^{n} to $ab=1$ is $a, b = \pm 1$.
On the other hand, for p prime, $\mathbb{Z}/p\mathbb{Z}$ has $[a][b] = [1]$ for each $[a] \neq [0]$.

Thm: If $[a] \in \mathbb{Z}/p\mathbb{Z}$ then if $[a] \neq [0]$ then $\exists\ [b] \in \mathbb{Z}/p\mathbb{Z}$ s.t. $[a][b] = [1]$. Equivalently, ~~if $ab \equiv 1 \pmod p$ then~~ if $a \neq 0$ then $ab \equiv 1 \bmod p$ has sol^{n}.

Proof: $\gcd(a, p) = 1 \Rightarrow \exists m, n \in \mathbb{Z}$ s.t. $ma + pn = 1 \Rightarrow ma \equiv 1 \pmod p$. //

Example: $p = 5$, mod 5 we find:

$1 \cdot 1 \equiv 1$, $2 \cdot 3 \equiv 1$, $3 \cdot 2 \equiv 1$, $4 \cdot 4 \equiv 1$

Thus $[1]^{-1} = 1$, $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$

or $(5\mathbb{Z}+1)^{-1} = 5\mathbb{Z}+1$ and $(5\mathbb{Z}+2)^{-1} = 5\mathbb{Z}+3$, etc.

Example: $p = 13$ find $[7]^{-1}$,

Can use gcd techniques to find $[7]^{-1}$ etc...

$(13, 7) \longleftrightarrow (a, b)$

$(7, 6) = (b, a-b)$

$(6, 1) = (a-b, b-(a-b)) = (a-b, 2b-a)$

Hence, $2(7) - 13 = 1 \Rightarrow 2 \cdot 7 \equiv 1 \bmod 13$

$\therefore$ $[7]^{-1} = 2$.

GROUPS:

Each nonzero $[a]$ has $[a]^{-1} = [b]$ for some $b \in \mathbb{Z}$. In fact $\mathbb{Z}/p\mathbb{Z} - \{[0]\}$ forms a group. This has a precise meaning in math.

Def'n A group is a set G together with an operation of multiplication and inversion,

1.) $1 \in G$ s.t. $\underbrace{1 \cdot x = x \cdot 1 = x}_{\text{assuming the group is multiplicative}}$ $\forall x \in G$ [$0 + x = x + 0 = x$ is the needed axiom for additive group]

2.) for each $g \in G$
$\exists\, g^{-1} \in G$ s.t. $g g^{-1} = 1$
and $g^{-1} g = 1$

3.) $x(yz) = (xy)z$ $\forall x, y, z \in G$

4.) to say "operation" means $(a, b) \in G \times G$ is assigned to single element $ab \in G$ for each such pair. (Binary operation)

Th'm $(\mathbb{Z}/p\mathbb{Z})^\times$ is nonzero elements in $\mathbb{Z}/p\mathbb{Z}$. If p prime then $(\mathbb{Z}/p\mathbb{Z})^\times$ forms group w.r.t. the operation $([a], [b]) \longmapsto [ab]$.

Proof: we saw in Episode I the operation $([a], [b]) \mapsto [\bar{ab}]$ is well-defined. ~~[illegible]~~ Moreover, if $[a] \neq [0]$ then we already proved $\exists\, b \in \mathbb{Z}$ for which $[a][b] = [1]$. Thus $(\mathbb{Z}/p\mathbb{Z})^\times$ has inverses for each element ↘

Proof continued

Notice, $[1]$ is the group identity as I assumed in previous page. This is easy to see as:

$$[1][a] = [1 \cdot a] = [a]$$
$$[a][1] = [a \cdot 1] = [a]$$

Hence $[1]$ = "1" in axiom. (some books use e for abstract identity in Group def= would say $[1]=e$)

The fact that $[a][b]=[ab]$ forms binary operation is implicit within discussion of Episode 1.

Associativity? Consider $[a], [b], [c] \in (\mathbb{Z}/p\mathbb{Z})^\times$

$$[a]([b][c]) = [a][bc] = [a(bc)]$$
$$= [(ab)c]$$
$$= [ab][c]$$
$$= ([a][b])[c].$$

Hence all axioms of group hold for $(\mathbb{Z}/p\mathbb{Z})^\times$ or we conclude $(\mathbb{Z}/p\mathbb{Z})^\times$ forms group. //

Remark: sorry this proof is a bit clumsy, hope to clean up in real lecture, probably 4th or 5th meeting..

Lagrange's Th^m

To understand this theorem we need to know a little about cosets.

Def^n/ If G a group and $H \subseteq G$ which is also a group via the (multiplication) operation of G restricted to H then H is a subgroup of G and we denote $H \leq G$.

Example: $(\mathbb{Z}, +)$ forms group & $2\mathbb{Z} \leq \mathbb{Z}$ since sum of even #'s is even. In contrast, $2\mathbb{Z}+1 \not\leq \mathbb{Z}$ as $3+3=6$.

Next we define coset (left & right)

Def^n/ If $H \leq G$ then the left cosets of H in G are $gH = \{gh \mid h \in H\}$. Likewise, the right cosets are $Hg = \{hg \mid g \in G\}$.

In additive notation, $g+H$ is left coset and $H+g$ is right coset. The choice of g to represent the coset is not unique (as discussed in Episode 1)

Th^m/ LAGRANGE'S THEOREM: If H is subgroup of finite group G then $|H|$ divides $|G|$

$|H|$ = # of elements in H (order of H)

$|G|$ = # of elements in G (order of G)

Th^{m}/ (LAGRANGE'S Th^{m}) The order of any subgroup of a finite group divides the order of the group. That is, if $|G| < \infty$ then $H \leq G \Rightarrow |H| \mid |G|$.

Proof ① We begin by arguing $|H| = |gH| \ \forall g \in G$. It suffices to give a bijective correspondence between H and gH. Consider $\psi : H \to gH$ by $\psi(x) = gx$. Clearly ψ is into. In addition, ψ is onto as is seen from noting $y \in gH \Rightarrow \exists h \in H$ s.t. $y = gh$. Observe $\psi(h) = gh = y$. Thus ψ onto.

Next, $\psi(x) = \psi(y) \Rightarrow gx = gy \Rightarrow g^{-1}gx = g^{-1}gy$
$\Rightarrow x = y$
$\Rightarrow \psi$ is 1-1.

② Cosets are disjoint. If $g_1H \neq g_2H$ then $g_1H \cap g_2H = \emptyset$. Equivalently, if $g_1 \in g_2H$ then $g_1H = g_2H$. I'll keep it positive and go with the 2nd statement, suppose $g_1 \in g_2H$ then $\exists h \in H$ s.t. $g_1 = g_2h \Rightarrow g_2 = g_1h^{-1}$. Let $x \in g_1H \Rightarrow \exists h_1 \in H$ s.t. $x = g_1h_1 = g_2hh_1$ and as $hh_1 \in H$ (since $H \leq G$ it's closed under multiplication) we see $x = g_2hh_1 \in g_2H \therefore g_1H \subseteq g_2H$. Conversely if $y \in g_2H \Rightarrow \exists h_2 \in H$ s.t. $y = g_2h_2 = g_1h^{-1}h_2$ and $h^{-1}h_2 \in H$ as $H \leq G$ thus $y = g_1h^{-1}h_2 \in g_1H$ Hence $g_2H \subseteq g_1H \therefore g_1H = g_2H$.

Proof conclusion:

We've shown ① all cosets $|gH| = |H|$.
and ② the cosets partition G into disjoint subsets. Therefore, as # of distinct cosets must be finite ($|G| < \infty$) we find

$$|G| = |H| + |g_2 H| + |g_3 H| + \cdots + |g_k H|$$
$$= \underbrace{|H| + |H| + \cdots + |H|}_{\text{\# of coset times}}$$
$$= k\,|H|$$

Therefore, $|H| \,/\, |G|$ as claimed. //

We use Lagrange's Th^{m} to prove Fermat's little Th^{m} in §3.4. However, I thought you might appreciate a short digression into its direct application

Example: $(\mathbb{Z}/7\mathbb{Z})^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ ← yet another notation for $[\,]$ etc.

6 elements ⇒ only have subgroups with 2, 3 or just 1 or all (silly subgroups)

$H_1 = \{\bar{1}, \bar{2}, \bar{4}\}$ $\qquad$ $H_2 = \{\bar{1}, \bar{6}\}$

H_1	$\bar{1}$	$\bar{2}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{2}$

all modulo 7.

H_2	$\bar{1}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{6}$
$\bar{6}$	$\bar{6}$	$\bar{1}$

§3.4 Fermat's little theorem:

Consider $a, a^2, a^3, a^4, \ldots$ modulo p we must eventually repeat; $\exists m, n \in \mathbb{N}$ s.t. $a^{m+n} \equiv a^m \bmod p$
hence $a^n \equiv 1 \pmod p$ for some n.

Example: consider $p = 7$ and $a = 2$,

$\{2, 4, 8, 16, \ldots\} \equiv \{2, 4, 1, 2, \ldots\}$ here $2^3 \equiv 1 \bmod 7$

Example: $p = 7$ and $a = 3$,

$\{3^1, 3^2, 3^3, 3^4, 3^5, \ldots\} = \{3, 9, 27, 81, \ldots\}$ ← modulo 7

$\equiv \{3, 2, 6, 3\cdot 6, \ldots\}$

$\equiv \{3, 2, 6, 4, 4\cdot 3, 4\cdot 9, \ldots\}$

$\equiv \{3, 2, 6, 4, 5, 1\}$

Here we find $3^6 \equiv 1 \bmod 7$.

Example: $p = 7$ and $a = 6$

Notice $a^2 = 36 \equiv 1 \bmod 7$

Claim: $H = \{[a^m] \mid m \in \mathbb{N}\}$ forms a subgroup of $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$.

Proof: $[a^m][a^n] = [a^m a^n] = [a^{m+n}]$ so H is closed under multiplication. Further, associative inherited from $\mathbb{Z}$. Finally, as $\exists r$ s.t $a^r \equiv 1 \bmod p$ we note $a^m a^{m-m} = a^r \equiv 1$ hence each element in H has inverse, and, $a^r \equiv 1 \in H$.
(I built H_1 and H_2 via this claim, $H_1 = \{[2], [2]^2, [2]^3 \equiv 1\}$)

Th^m (Fermat's little theorem)
If p is prime and $a \not\equiv 0 \pmod p$, then $a^{p-1} \equiv 1 \pmod p$.

Proof: Notice $\mathbb{Z}/p\mathbb{Z}$ has p-elements $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ has $p-1$.
If $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ then by Lagrange's Th^m $|H| \mid p-1$.
Consider $H = \{a, a^2, .., a^n \equiv 1\}$ for $a \not\equiv 0 \pmod p$ and n is the least power for which $a^n \equiv 1 \bmod p$. Note, $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ as we argued on last page(s) and so $|H| = n$ must divide $p-1$ $\therefore$ $p-1 = mn$ for some $m \in \mathbb{N}$. Thus, $a^{p-1} = a^{mn} = (a^n)^m \equiv 1^m = 1 \pmod p$. ///

Corollary: If p is prime and $a \not\equiv 0 \pmod p$ then $a^{p-2} \cdot a \equiv 1 \bmod p$.

Example: $p = 13$, $a = 7$ then $a^{p-2} = 7^{11}$ well, compare to pg. ①, we found $[7]^{-1} = 2$. I'd have to work a bit to see that from 7^{11},

$$7^{11} = 7^{10} \cdot 7 = (7^2)^5 7 = (49)^5 \cdot 7 \quad \searrow\ 49 = 39 + 10$$
$$\equiv 10^5 \cdot 7$$
$$= 70 \cdot 10^4 \quad \searrow\ 70 = 65 + 5$$
$$\equiv 5 \cdot 10^4 \quad \searrow\ -3 = 10 - 13$$
$$\equiv 5 \cdot (-3)^4 \quad \searrow\ 9 = +13 - 4$$
$$= 5 \cdot 9 \cdot 9$$
$$= 5 \cdot (-4)^2$$
$$= 5 \cdot 16$$
$$\equiv 5 \cdot 3 \equiv 2.$$

Remark: you can probably improve on my calculation here →

Example: $p = 7$, $a = 5$

$$a^{p-2} = 5^5 = (5^2)^2 \cdot 5 \equiv (25)^2 \cdot (-2)$$
$$\equiv (4)^2 \cdot (-2)$$
$$= 4(-8)$$
$$\equiv 4(-1)$$
$$\equiv -4$$
$$\equiv 3. \quad \hookrightarrow [5]^{-1} = [3] \text{ in } \mathbb{Z}/7\mathbb{Z}.$$

Example: the other way to calculate,

$$(7, 5) = (a, b)$$
$$(5, 2) = (b, a-b)$$
$$(2, 1) = (a-b,\ b - 2(a-b)) = (a-b,\ -2a+3b)$$

$$\therefore \quad -2(7) + 3(5) = 1 \quad \therefore \quad \underline{[5]^{-1} = [3]}.$$

Primitive roots:

> **Def^{n}/** The minimum positive $n \in \mathbb{N}$ such that $a^n \equiv 1 \pmod{p}$ is called the <u>order</u> of a in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Notice $\{a, a^2, \ldots, a^n \equiv 1\}$ is a subgroup of <u>order</u> n so the terminology is consistent. Further the order of a must divide $p-1$.

Ex: $p = 7$, $p-1 = 6 \longrightarrow$ orders $1, 2, 3, 6$ possible for a. an element of order 6 would be <u>primitive root</u> for p. On page 7 we saw $n = 6$ for $a = 3$ relative $p = 7$.

> **Def^{2}/** If p is prime then a of order $p-1$ is called a primitive root

§3.5 CONGRUENCE THEOREMS OF WILSON & LAGRANGE

Later we need to calculate $(p-1)!$ for quad. reciprocity. Fortunately ∃ nice way in view of Th^{m}s in §3.4. Recall $(p-1)! = (p-1)(p-2)\cdots 3\cdot 2\cdot 1$, but,

Th^{m} (WILSON'S TH^{m}) If p is prime then $(p-1)! \equiv -1 \pmod p$.

Proof: Note $1, 2, 3, \ldots, p-1$ have inverses mod p. As we consider $(p-1)! = (p-1)(p-2)\cdots 3\cdot 2\cdot 1$ note all factors, which are order 2 all that's left, we must study these self-inverse factors. Consider $x^2 \equiv 1 \bmod p$

$\Rightarrow x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \bmod p$

$\Rightarrow (x-1)(x+1)$ divided by p

But $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Hence $p \mid x-1$ or $p \mid x+1$.

That is, $x \equiv 1$ or $x \equiv -1 \bmod p$.

Example: $30! \equiv -1 \pmod{31}$.

Th^{m} (Lagrange's polynomial congruence theorem)
If $P(x)$ is polynomial of degree n with $\mathbb{Z}$-coeff. and p is prime, then the congruence $P(x) \equiv 0 \pmod p$ has at most n incongruent sol^{n}s $\pmod p$.

(there may be no sol^{n}s to $P(x) \equiv 0$, or $1, 2, 3, \ldots$ up to n.)

Proof: let $P(x) = a_n x^n + \cdots + a_1 x + a_0$. If $\nexists$ a sol^n then we're done. Otherwise, $\exists r \in \mathbb{Z}$ s.t. $P(r) \equiv 0 \pmod{p}$. Therefore,

$$\begin{aligned} P(x) &\equiv P(x) - P(r), \mod p \\ &= (a_n x^n + \cdots + a_1 x + a_0) - (a_n r^n + \cdots + a_1 r + a_0) \\ &= a_n (x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \cdots + a_1 (x - r) \\ &= (x - r) Q(x) \end{aligned}$$

where $Q(x)$ is of degree $(n-1)$. Thus $(x-r)Q(x) \equiv 0 \pmod{p}$ $\Rightarrow p \mid (x-r)Q(x)$ hence $p \mid x-r$ or $p \mid Q(x)$ by prime divisor property. Thus $x \equiv r$ or $Q(x) \equiv 0 \mod (p)$. ~~Suppose inductively~~ Next, repeat the argument on $Q(x)$ to either conclude $x = r$ is only sol^n or $Q(r_2) \equiv 0$ $\Rightarrow P(x) \equiv (x-r)(x-r_2)Q_2(x)$. But this can only continue to $P(x) = (x-r)(x-r_2)\cdots(x-r_n)$ as degree $P(x)$ is n. //

Remark: you're free to use induction like Stillwell on p. 54.

§3.6 Inverses mod n

For $[a] \in \mathbb{Z}/n\mathbb{Z}$ (where n not prime) it is not always possible to solve $[a][b] = [1]$.

Example: in $\mathbb{Z}/6\mathbb{Z}$ we have $[2][3] = [0]$

if $[2][b] = [1]$ then $[b][2][3] = [1][3] = [3]$

$[0]$

$\Rightarrow [b] = 0$

$\Rightarrow [2][b] = [0] = [1]$.

absurd!

Th^m/ The eq^n $ab \equiv 1 \bmod n$ has a sol^n iff $\gcd(a,n) = 1$

Proof: If $\gcd(a,n) = 1$ then by Bezout's Th^m $\exists m, k \in \mathbb{Z}$ s.t. $am + nk = 1 \Rightarrow am \equiv 1 \bmod(n)$.

Conversely, if $ab \equiv 1 \bmod n$ has a sol^n. Thus $ab - 1 = nk$ for some $k \in \mathbb{Z}$. Hence $\underbrace{ab + nk}_{*} = 1$

Thus $\gcd(a,n) = 1$. ($*$ $\Rightarrow$ a common divisor of a & n also divides 1.)

Example: $\mathbb{Z}/6\mathbb{Z}$ has $[1], [5]$ with $\gcd(1,6) = 1$, and $\gcd(5,6) = 1$. However, $2, 3, 4$ have common divisors larger than 1 w.r.t. 6. $\Rightarrow \varphi(6) = 2$.

↙ Euler-φ-function

Def^n/ $\varphi(n) = \#$ of $a < n$ for which $\gcd(a,n) = 1$

Properties of φ $<$ $\varphi(p^i) = p^{i-1}(p-1)$ for p prime

$\varphi(mn) = \varphi(m)\varphi(n)$ if $\gcd(m,n) = 1$.

Example: $\varphi(30) = \varphi(5)\varphi(6) = 4 \cdot 2 = 8$.

Def'n $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$

Observe $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

Example: $(\mathbb{Z}/30\mathbb{Z})^\times$ has $\varphi(30) = \varphi(6)\varphi(5) = 2 \cdot 4 = 8$ elements.

Th'm (Euler's Th'm) If $[a]^{-1}$ exists for $\mathbb{Z}/n\mathbb{Z}$ then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Proof: note $|\mathbb{Z}/n\mathbb{Z}|$ = # of elements $= \varphi(n) = |G|$ ($G = (\mathbb{Z}/n\mathbb{Z})^\times$)

Also $H = \{a, a^2, a^3, \dots\} \leq G$ must be finite group, hence by Lagrange's Th'm $|H| \mid |G| \Rightarrow$ least n s.t. $a^n \equiv 1 \mod n$ divides $\varphi(n)$

Thus $\varphi(n) = mn \Rightarrow a^{\varphi(n)} = (a^n)^m = 1 \mod n$ //

Corollary: $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ has $[a]^{-1} = [a^{\varphi(n)-1}]$.

Proof: $[a][a^{\varphi(n)-1}] = [a a^{\varphi(n)-1}] = [a^{\varphi(n)}] = [1]$. //

(used Euler's Th'm)

Remark: for general n ∄ nice way to compute φ... unless we know prime factorization of n. But, this is hard to compute for large $n \Rightarrow$ RSA not too easy to crack.. (well, this is part of it see Chapter 4 for more.)

§3.7 Quadratic Diophantine Eq^n's.

Linear case $ax+by=c$ was not too hard to solve, we ~~gave~~ saw complete algorithm in §2.6. The problem of finding integer sol^n's of $ax^2+bxy+cy^2=d$ will require most of this course. We begin here by showing certain quadratic forms cannot attain certain values.

Example 1. $x^2+y^2=p$ has no sol^n for $p \in 4\mathbb{Z}+3$.

Proof: it suffices to show $x^2+y^2 \not\equiv 3 \pmod 4$. $\exists < \infty$ cases to check; $x, y \equiv 0, 1, 2, -1$ ← nice to use -1 rather than 3.

$0^2+0^2 \equiv 0$
$0^2+(\pm 1)^2 \equiv 1$
$0^2+(2)^2 = 4 \equiv 0$

$(\pm 1)^2+0^2 = 1$
$(2)^2+0^2 = 4$ etc...
$(\pm 1)^2+(\pm 1)^2 = 2$
$(\pm 1)^2+(2)^2 = 5 \equiv 1$

Clearly by explicit computation of cases $x^2+y^2 \not\equiv 3$
Hence a prime of form $4\mathbb{Z}+3$ is not attained by x^2+y^2 for $x, y \in \mathbb{Z}$. //

Example 2: $x^2+2y^2=p$ has no sol^n of the form $8n+5$ or $8n+7$ for $n\in\mathbb{Z}$.

Proof: the claim is equivalent to the incongruence $x^2+2y^2 \not\equiv 5, 7 \pmod 8$. There are finitely many cases; $x, y \equiv 0, \pm1, \pm2, \pm3, 4$. Mod 8,

$$(\pm1)^2 + 2(0)^2 \equiv 1 \qquad 0^2+2(\pm1)^2 \equiv 2$$
$$(\pm2)^2 + 2(0)^2 \equiv 4 \qquad 0^2+2(\pm2)^2 \equiv 0$$
$$(\pm3)^2 + 2(0)^2 \equiv 1 \qquad 0^2+2(\pm3)^2 \equiv 3$$
$$4^2+2(0)^2 \equiv 0 \qquad 0^2+2(4)^2 \equiv 0$$

etc.... ~~$(\pm3)^2+2^2 = 13 + 8 = 25 \equiv 1$~~

$$(\pm3)^2 + 2\cdot4^2 = 9+32 \equiv 1$$
$$4^2 + 2\cdot(\pm3)^2 = 16+18 \equiv 3$$

are you bored of this? I am. I'll trust the claim, it is clear how to finish casewise. //

Example 3: $x^2+3y^2=p$ has no sol^n for $p\in 3\mathbb{Z}+2$

Proof: check $x, y \equiv 0, \pm1$, mod (3).

$$0^2+3(0)^2=0, \quad 0^2+3\cdot(1)^2=3\equiv 0$$
$$1^2+3(0)^2=1\equiv 1, \quad 1^2+3(\pm1)^2=4\equiv 1$$

Oh, that's it. Hence x^2+3y^2 does not attain any value in $3\mathbb{Z}+2$.

The results discussed on (15) were claimed by Fermat by a method called "method of descent", that technique is more sophisticated than our easy congruence... later Stillwell uses descent to show $x^3+y^3 \neq z^3$ over $\mathbb{Z}$. nontrivially. Fermat also showed x^2+y^2 takes every prime value of the form $4n+1$.

Fermat also studied primes of the form x^2+y^2, x^2+2y^2, x^2+3y^2 as a response to reading Diophantus who said:

"65 is naturally divided into squares in two ways, namely into 7^2+4^2 and 8^2+1^2, which is due to the fact that 65 is the product of 13 and 5, each of which is the sum of two squares."

This suggests Diophantus was aware of:

$$\boxed{(a_1^2+b_1^2)(a_2^2+b_2^2) = (a_1a_2 \pm b_1b_2)^2 + (b_1a_2 \mp a_1b_2)^2}$$

Let's see $13 = 4+9 = 2^2+3^2$ and $5 = 4+1 = 2^2+1^2$

$$(2^2+3^2)(2^2+1^2) = (4 \pm 3)^2 + (6 \mp 2)^2$$
$$= \underline{7^2+4^2} \text{ and } \underline{1^2+64^2}.$$

- Knowing which $n \in \mathbb{N}$ are sums of squares depends on knowing which primes are sums of two squares.
  - Ex. 1: primes of form $4n+3$ are not sums of two squares
  - Much harder: show all primes of form $4n+1$ are sums of squares
    Showcase problem for Lagrange, Gauss, we give Dedekinds $\mathbb{Z}[i]$-based argument.
- We have more to say about x^2+2y^2 & x^2+3y^2 later.

—(we skip §3.8 and §3.9)—

§3.10 Discussion

- congruence concept due to Gauss 1801
  - ▶ trades statements about remainders for near equalities $a \equiv b \bmod n$ etc..
  - ▶ Congruence class converts $\equiv$ to $=$ of sets Dedekind (1857) (as discussed in Episode I)
    - ◀ $n\mathbb{Z} + a = n\mathbb{Z} + b$

- Fermat's little theorem $a^{p-1} \equiv 1 \bmod p$ grew from $a = 2$ case by Fermat, induction extends to other a (see pg. 64)

- 1750 Euler essentially proved Lagrange's Th^{m} (20 yrs. before Lagrange and 80 yrs before formal group concept given by Galois)

  $\{1, a, a^2, \ldots, a^{n-1}\}$

  $\{b, ba, ba^2, \ldots, ba^{n-1}\}$ ← partition

  $\Rightarrow$ size of coset must divide $n-1$.

- primes of the form $x^2 + ny^2$

  $n=1$ Babylonians or Diophantus mastered by Fermat ~1640 proved by Euler ~1755 (Fermat didn't show his proofs always)

  $n=2,3$ again Fermat

  ▷ Hasse-Minkowski explains why impossibility of certain values for $ax^2 + bxy + cy^2$ seen via congruences or quadratic