HW 4 due before Thursday's class.
Submit one pdf file
[CamScanner app. Office Lens.]

Today: • Discuss proofs of Q.R.
• Move on to the next topic:

$$x^2 + ny^2 = z$$

Review Rousseau's Proof of Q.R.

C.R.T. Let $p \neq q$ be odd primes.

$$(\mathbb{Z}/pq\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$
$$x \longmapsto (x, x)$$

Observe:

- $1 \neq -1 \mod pq$
  $2 \neq 0 \mod pq$
  because $2 \nmid pq$

- $x = -x \mod pq$ for all $x \in (\mathbb{Z}/pq)^\times$.
- Elements of $(\mathbb{Z}/pq\mathbb{Z})^\times$ come in pairs $\{x, -x\}$
- Elements of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ come in pairs $\{(x,x), (-x,-x)\}$.

  Alternatively, they come in pairs $\{(a,b), (-a,-b)\}$

Strategy: Pick one element from each pair and multiply. There are two "fairly obvious" choices.

$$M := \prod_{\substack{1 \le x \le \frac{pq-1}{2} \\ \gcd(x, pq) = 1}} (x, x)$$

$$N := \prod_{\substack{1 \le a \le p-1 \\ 1 \le b \le \frac{q-1}{2}}} (a, b)$$

[Reason: $S = \{(a,b) : 1 \le a \le p-1,\ 1 \le b \le \frac{q-1}{2}\}$

Then $(a,b) \in S \iff (a,-b) \notin S$

$\iff (-a,-b) \notin S$ ✓]

Observe that

$$M = \pm N$$

because each elt of $M = \pm$ some element of N.

With some work (involving Wilson's Thm & Euler's Criterion) we showed that

$$M = \left((-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right),\ (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \right)$$

$$N = \left((-1)^{\frac{p-1}{2}},\ (-1)^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \right)$$

Since all entries are ± 1, it doesn't matter if we work mod p, q or just in $\mathbb{Z}$.

QED.

Another nice proof of Q.R. is due to Zolotarev. Given any $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$ we have an invertible function

$$\pi_{a,b} : (\mathbb{Z}/b\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/b\mathbb{Z})^\times$$
$$c \longmapsto ac$$

The inverse is given by

$$\pi_{a,b}^{-1}(c) = a^{-1}c .$$

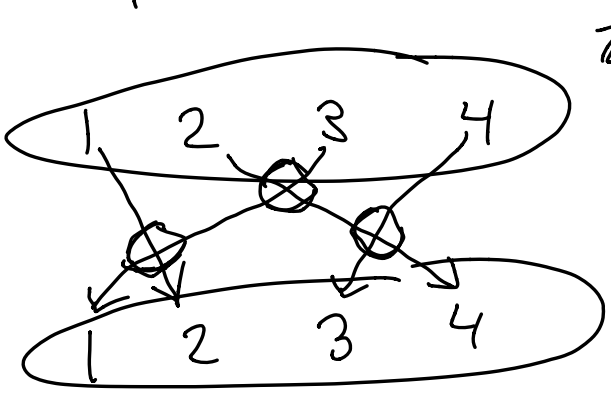
Jargon: $\pi_{a,b}$ is a "permutation" of the set $(\mathbb{Z}/b\mathbb{Z})^\times$.

Zolotarev's Lemma:
Given $a, p \in \mathbb{Z}$ with p prime, $p \nmid a$ we have

$$\left(\frac{a}{p}\right) = \operatorname{sgn}(\pi_{a,p})$$

the "sign of the permutation"

Example: $\pi_{2,5}$



$(-1)^3 = -1$

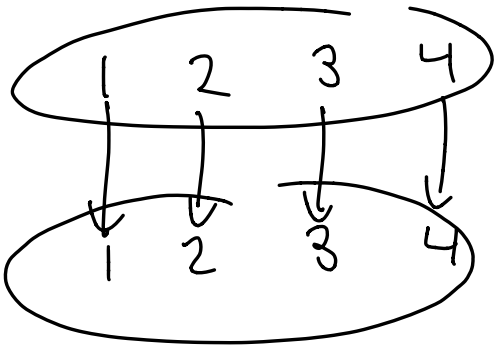
$= \left(\frac{2}{5}\right)$ ✓

Define $\operatorname{sgn}(\pi_{2,5}) = (-1)^{\#\text{crossings}}$

Recall:

a	1	2	3	4
a^2	1	4	4	1

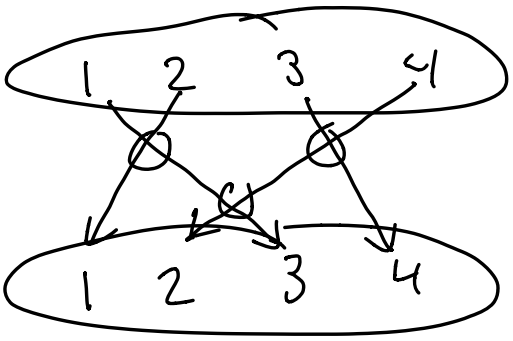
$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = +1$, $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$



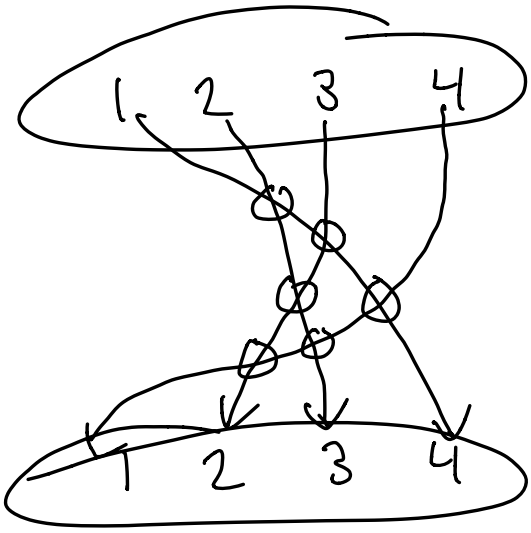
$\operatorname{sgn}(\pi_{1,5}) = (-1)^{\#\text{crossings}}$

$= (-1)^0$

$= -1 = \left(\frac{1}{5}\right)$ ✓



$$\operatorname{sgn}(\pi_{3,5}) = (-1)^3$$
$$= -1 = \left(\frac{3}{5}\right) \checkmark$$

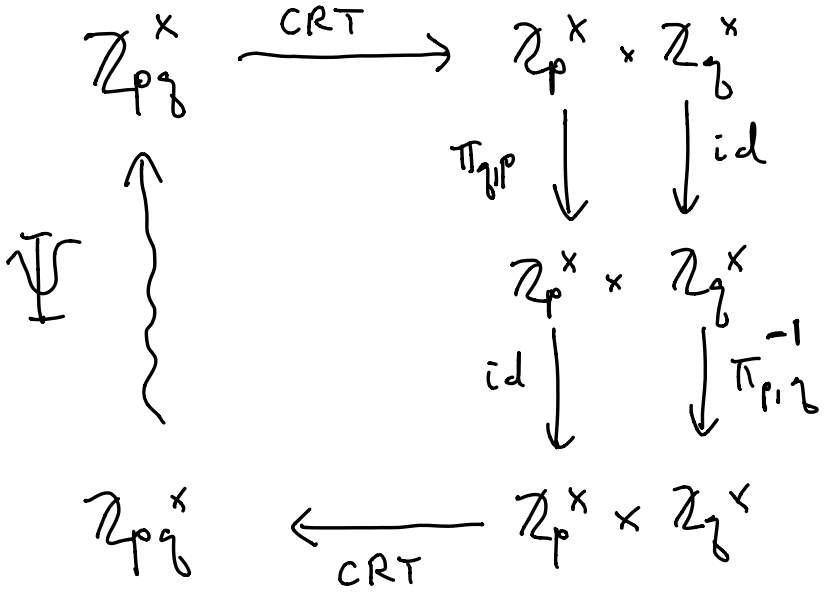


$$\operatorname{sgn}(\pi_{4,5}) = (-1)^6$$
$$= +1 = \left(\frac{4}{5}\right) \checkmark$$

For any permutations $\pi, \mu : S \to S$ we have

- $\operatorname{sgn}(\pi \circ \mu) = \operatorname{sgn}(\pi)\operatorname{sgn}(\mu)$
- $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$

Zolotarev's Proof of QR.



On one hand

$$\begin{aligned}\operatorname{sgn}(\Psi) &= \operatorname{sgn}(\cancel{CRT}^{-1} \circ \pi_{p,q}^{-1} \circ \pi_{q,p} \circ \cancel{CRT}) \\ &= \operatorname{sgn}(\pi_{p,q}) \operatorname{sgn}(\pi_{q,p}) \\ &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\end{aligned}$$

On the other hand, a combinatorial argument ("card shuffling") shows that $\operatorname{sgn}(\Psi) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

QED.

Where next ?

Previously we solved the homogeneous Q.D.E. (quadratic Diophantine eq.)

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

Now we consider the nonhomogeneous

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

This problem is harder.

Preview of main ideas:

There is a "multiplication rule!"

Suppose $a_1^2 + b_1^2 = c_1$ & $a_2^2 + b_2^2 = c_2^2$ with $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}$. Then we get another solution

$$(a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 = c_1 c_2$$

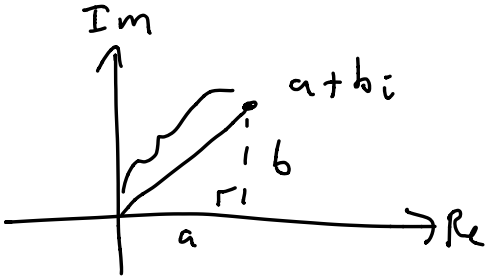
Where does this come from ?!

Rule was known to Diophantus.

but it makes more sense in terms of complex numbers. Let $i = \sqrt{-1}$.

Define absolute value:

$$|a+bi| := \sqrt{a^2+b^2}$$



Miracle: Absolute value of complex numbers is multiplicative:

$$|(a+bi)(c+di)| = |a+bi|\,|c+di|$$

$$|(ac-bd)+(ad+bc)i|^2 = |a+bi|^2\,|c+di|^2$$

$$(ac-bd)^2+(ad+bc)^2 = (a^2+b^2)(c^2+d^2)$$

"The two square identity"

(a,b,c) & (a',b',c') solve $x^2+y^2=z$

then so does

$$(aa'-bb',\ ab'+a'b,\ cc').$$

This recipe gives ∞ many solutions.

where the 3rd coordinates just multiply in the usual way.

Question: Can we also factor the 3rd coordinate?

Suppose $c_1 c_2 = a^2 + b^2$.

Can we find some a_1, b_1, a_2, b_2 such that $c_1 = a_1^2 + b_1^2$?

$c_2 = a_2^2 + b_2^2$.

No, not always. There are some restrictions. For example, if

$$a^2 + b^2 = c$$

then I claim that $c = 0, 1, 2 \bmod 4$.

Indeed:

x	0	1	2	3	mod 4.
x^2	0	1	0	1	

So $a^2 + b^2 = 0 + 0 = 0, 1, 2 \bmod 4$.

$0 + 1$

$1 + 0$

$1 + 1$

If $c \equiv 3 \bmod 4$ then

$$c \neq a^2 + b^2 .$$

But $c \cdot c = c^2 + 0^2$ ✓

The problem of which numbers are sums of two squares was solved by Fermat, but his proof was complicated. We will follow a much cleaner proof due to Gauss.

Gauss' Idea:
Consider the set of "complex integers"

$$\mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \}.$$

Gauss showed that this number system has a unique prime factorization theorem, similar to $\mathbb{Z}$.

Consequence:

$$a + bi = \pi_1 \pi_2 \cdots \pi_k$$ Gaussian prime factorization

Take absolute value^2 of each side:

$$a^2+b^2 = \underbrace{|\pi_1|^2\,|\pi_2|^2 \cdots |\pi_k|^2}_{\text{what kind of integers?}}.$$

We will see later, if π is a Gaussian prime then

$$|\pi|^2 = \begin{cases} p & \text{for integer prime } p \neq 3 \bmod 4 \\ p^2 & \text{for integer prime } p = 3 \bmod 4 \end{cases}$$

It follows that any number $a^2+b^2 \in \mathbb{Z}$ has the following kind of prime factorization:

$$a^2+b^2 = 2^k p_1^{d_1} \cdots p_k^{d_k} q_1^{2e_1} \cdots q_l^{2e_l}$$

where $p_i = 1 \bmod 4$

$q_i = 3 \bmod 4$

In other words, primes of the form $3 \bmod 4$ occur with <u>even multiplicity</u>.

Conversely, we will show that any number where prime factors $\equiv 3 \bmod 4$ occur with even multiplicity is a sum of two squares.

Summary (Fermat's Theorem)

An integer is a sum of two squares

$\Longleftrightarrow$ its prime factors $\equiv 3 \bmod 4$ occur with even multiplicity.

More generally, the Diophantine equation

$$x^2 + ny^2 = z$$

is closely related to the algebraic structure of the ring

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

Next time, we will prove that the ring $\mathbb{Z}$ has unique prime factorization & will try to extend the proof to the rings $\mathbb{Z}[\sqrt{-n}]$.