Gaussian Integers:

Sums of squares is an elementary question, whos solution requires some descent number theory.

Ex:

$2 = 1+1$, $5 = 1+4$, $13 = 4+9$

$17 = 1+16$, $29 = 4+25$, $37 = 1+36$.

but $3 \neq 1+1$; $7 \neq 1+1, 1+4$;

$11 \neq 1+1, 1+4, 4+4, 1+9$.

Aud: Detect pattern.

Thm 1.1 For all prime numbers $p \neq 2$, one has:

$$p = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}$$

$$\Leftrightarrow p \equiv 1 \pmod 4.$$

Aud: Definition of congruence.

To explain this phenomenon concerning $\mathbb{Z}$, take $\mathbb{Z}[i]$.

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

$$i^2 = -1.$$

<u>Aud</u>: Compute $(x+iy)(x-iy)$.

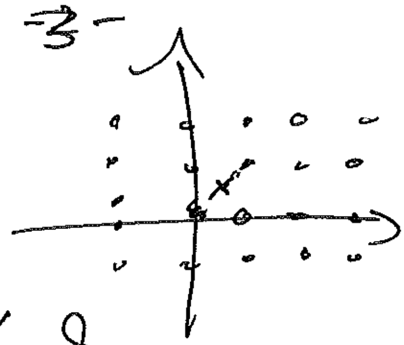
$p = (x+iy)(x-iy)$ yields factorization in $\mathbb{Z}[i]$.

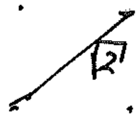
<u>Aud</u>: Recall def. of euclidean rings.
Recall def. of unique factorization ring.

<u>Fact</u>: A ring A commutative and unital that is euclidean is unique factorization.

<u>Prop 1.2</u> and proof.

<u>Illustration</u>:





Norm from book

<u>Aud</u>: Compute factorization of 29 and 11 in $\mathbb{Z}[i]$.

<u>Fact</u> (Wilson's thm): A positive integer n is prime if and only if

$$(n-1)! \equiv -1 \pmod{n}.$$

<u>Aud</u>: Verify non-prime case. ~~Sketch~~ proof.

<u>Proof</u> of Thm 1.1 from book

<u>Aud</u>: Recall def of units, irreducible, and prime.

<u>Fact</u>: If A is an integral domain, then every prime elt is irred.

<u>Ex</u>: $\mathbb{Z}[x]/x^2$ with prime elt $x = (1+x)x$

<u>Aud</u> A number a is a unit iff $N(a) = 1$. (Exc. 1)

<u>Prop 1.3</u> from book (+proof).

Recall associate elts.

<u>Thm 1.4</u> from book incl proof

<u>Aud</u>: Factor 2, 3, 7 in $\mathbb{Z}[i]$.

Prime decomposition from book.

Role of $\mathbb{Z}[i] \subset \mathbb{Q}(i)$:

<u>Prop 1.5</u> from book incl. proof.

For Ex session 1: Ex 2.

Ex — " — 2 : Ex 3.

Ex — " — 3 : Ex 3, 4, 5