We're still in $\mathbb{Z}[i]$. We've shown that if p is a (usual) prime, then it is *not* a Gaussian prime if it's a sum of squares; equivalently, it's not a Gaussian prime if it's the norm of some $\alpha \in \mathbb{Z}[i]$ Ended last time with: If $\mathcal{N}(\alpha)$ is prime (in $\mathbb{Z}$), then α is irreducible in $\mathbb{Z}[i]$.

Lemma $1+i$ irreducible, and 2 factors.

Proof $\mathcal{N}(1+i) = 1^2 + 1^2 = 2$ prime in $\mathbb{Z}$; and $2 = (1+i)(1-i)$.

We know: If p odd, and is p is a sum of squares, then $p \equiv 1 \bmod 4$.

Lemma If $p \equiv 1 \bmod 4$, then -1 is a square $\bmod p$.

Proof Use Wilson's lemma $(p-1)!$: Let $p = 4N+1$. Then

$$\begin{aligned} -1 &\equiv (4N)! \bmod p \\ &\equiv (1)(2)(3)\cdots(2N)\cdot((2N+1)\cdot(2N+2)\cdots(4N)) \bmod p \end{aligned}$$

But $2N+1+2N \equiv 0 \bmod p$, $(2N+1) = -2N$. Similarly, $(2N+2) = -(2N-1)$, and so on; $4N = -1$.

$$\begin{aligned} -1 &\equiv (1\cdot 2\cdot 3\cdots 2N)((-2N)(-(2N-1))\cdots(-1)) \bmod p \\ &\equiv (2N)!\cdot(-1)^{2N}\cdot(2N)! \bmod p \end{aligned}$$

So, let $m = (2N)!$. Then $m^2 \equiv -1 \bmod p$, and -1 is a square. $\square$

Lemma If $p = 4N+1$ is a (usual) prime, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof Given p, we can find an m: $p | (m^2+1)$; so $p | (m-i)(m+i)$.

Moreover, $p \nmid m \pm i$. (Check: $\frac{m}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$.)

So p can't be irreducible in $\mathbb{Z}[i]$. ($p | \alpha\beta$, $p \nmid \alpha$, $p \nmid \beta$). From last week, $p = a^2 + b^2$ for some a and b.

Lemma If $p \equiv 3 \bmod 4$, then -1 is *not* a square in $\mathbb{Z}/p$.

Proof Suppose $a^2 \equiv -1 \bmod p$. Write $p = 4N+3$; raise both sides to the $2N+1$ power:

$$\begin{aligned} a^2 &\equiv -1 \bmod p \\ (a^2)^{2N+1} &\equiv (-1)^{2N+1} \bmod p \\ a^{4N+2} &\equiv -1 \bmod p \end{aligned}$$

But this is impossible! $4N+2 = p-1$, so $a^{4N+2} \equiv 1 \bmod p$. $\square$

At this point, we know that $p = \square + \square$ if and only if $p \equiv 1, 2 \bmod 4$.

Theorem Let N be a natural number. Write $N = QM^2$, where Q is square-free. Then N is a sum of squares if and only if all primes dividing Q are 1 or 2 mod 4.

Proof Suppose $N = QM^2 = p_1 p_2 \cdots p_j M^2$, each $p_j \equiv 1, 2 \bmod 4$. From what we've just done, each $p_i = \square + \square$. moreover M^2 is a sum of squares; $M^2 = M^2 + 0^2$. From the first day of class, a product of a sum of (two) squares is again a sum of squares. Thus, $N = \square + \square$.

Conversely, suppose $N = \square + \square$. Write $N = p_1 \cdots p_j M^2$; need to show that each $p_j \equiv 1, 2 \bmod 4$. Suppose some $p_i \not\equiv 1, 2 \bmod 4$. Since $p_i | N$, and N is a sum of squares $N = a^2 + b^2$, we have $p_i | a^2 + b^2$, and $a^2 + b^2 \equiv 0 \bmod p_i$. Suppose $p_i \nmid a$ or $p_i \nmid b$; since if it does, then $p_i^2 | N$. Then

$$\begin{aligned} a^2 + b^2 &\equiv 0 \bmod p_i \\ a^2 &\equiv -b^2 \bmod p_i \\ a^2/b^2 &\equiv -1 \bmod p_i \\ -1 &\equiv \square \bmod p_i \end{aligned}$$

Whoops – no need for proof by contradiction. What we've shown is that for each p_i, the fact that $N = \square + \square$ implies that $-1 \equiv \square \bmod p_i$; which means that $p_i \equiv 1, 2 \bmod 4$. $\square$

1 Pythagorean triples

Suppose (a, b, c) is a primitive Pythagorean triple; $a^2 + b^2 = c^2$, and $\gcd(a, b, c) = 1$. Then $c^2 = (a + bi)(a - bi)$.

Note: it's enough to assume $\gcd(a, b) = 1$, since if $d|a$ and $d|b$ then $d|c^2$.

Lemma If a and b are relatively prime in $\mathbb{Z}$, they are relatively prime in $\mathbb{Z}[i]$.

Proof Suppose $\gamma \in \mathbb{Z}[i]$, $\gamma | a$, $\gamma | b$. Then

$$\begin{aligned} a &= \gamma \cdot a' \\ \mathcal{N}(a) &= \mathcal{N}(\gamma) \cdot \mathcal{N}(a') \\ b &= \gamma \cdot b' \\ \mathcal{N}(b) &= \mathcal{N}(\gamma) \cdot \mathcal{N}(b') \end{aligned}$$

$\mathcal{N}(a) = a^2$, $\mathcal{N}(b) = b^2$; $\gcd(a,b) = 1$ implies that $\gcd(a^2, b^2) = 1$. So $\mathcal{N}(\gamma)|a^2$, $\mathcal{N}(\gamma)|b^2$, which means that $\mathcal{N}(\gamma) = 1$. Therefore, γ is a unit, and the only common divisors of a and b in $\mathbb{Z}[i]$ are units. $\square$

Lemma Suppose that a and b are relatively prime. Then $a + bi$ and $a - bi$ are relatively prime (as Gaussian integers).

Proof Let $\alpha = a + bi$; $\overline{\alpha} = a - bi$. Suppose $\beta | \alpha$ and $\beta | \overline{\alpha}$. Assume β irreducible, and then derive a contradiction.

Well, $\beta | \alpha$, $\beta | \overline{\alpha}$; $\beta | (\alpha + \overline{\alpha})$; $\beta | 2a$. Similarly, $\beta | (\alpha - \overline{\alpha})$; $\beta | 2b$.

$\beta | 2a$, $\beta | 2b$. Since a and b are relatively prime, this forces $\beta | 2$; so $\beta = \pm 1 \pm i$, and $\beta | alpha$. Then $\overline{\beta} | \overline{\alpha}$; $\beta\overline{\beta} | \alpha\overline{\alpha}$, and $\mathcal{N}(\beta) | \mathcal{N}(\alpha)$. Then $\mathcal{N}(\alpha) = a^2 + b^2$ is even. But, if (a, b, c) is a primitive Pythagorean triple, then c is odd. (Check $\bmod 4$; if both a and b are even, then so is c, and (a,b,c) is not primitive; if both a and b are odd, then $a^2 + b^2 \equiv 2 \bmod 4$; but 2 is not a square mod4, and thus $c^2 \not\equiv 2 \bmod 4$.)

So we can't have an irreducible β dividing α and $\overline{\alpha}$, so α and $\overline{\alpha}$ are relatively prime in $\mathbb{Z}[i]$. $\square$

Lemma In $\mathbb{Z}[i]$, relatively prime factors of a square differ from squares by units.

In other words, if γ is $\square$, and if $\alpha\beta = \gamma$, and $\gcd(\alpha, \beta) = 1$, then α is (almost) a square.

Omitted; use unique factorization. The "differ by a square" part is like the fact that, in $\mathbb{Z}$, $36 = (-2^2) \cdot (-3^2)$; neither factor is a square, but they each differ from a square by a unit.

Back to our primitive pythagorean triple (a, b, c), let $\alpha = a + bi$, $\overline{\alpha} = a - bi$; $\alpha\overline{\alpha} = c^2$. Since $\gcd(\alpha, \overline{\alpha}) = 1$, each of α and $\overline{\alpha}$ is a (unit times) a square.

In particular, $a - bi = \gamma \cdot (u - vi)^2$ for some $\gamma \in \mathbb{Z}[i]^\times$ and $u, v \in \mathbb{Z}$.

So,

$$\begin{aligned} a - bi &\in \{(u - vi)^2, -(u - vi)^2, i(u - vi)^2, -i(u - vi)^2\} \\ (u - vi)^2 &= u^2 + v^2 - 2uvi \end{aligned}$$

So, $a - bi$ is one of $u^2 + v^2 - 2uvi$, $-u^2 - v^2 + 2uvi$, $i(u^2 + v^2) + 2uv$, *etc*.

Equate real and imaginary parts of $a - bi$ and $\gamma(u - vi)^2$, find that

$$\{a, b\} = \{\pm(u^2 + v^2), \pm 2uv\}$$

Which is the same description we'd had in week one of sums of squares! Moreover, any divisor of u and v is a divisor of $u^2 - v^2$ and $2uv$, thus of a and b. So $\gcd(u, v) = 1$.