

12/7/06

Number Theory Problem: When is a positive integer expressible as a sum of two squares, and if so in how many ways?

Recall \mathcal{O} is a quadratic integer ring, so $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ with norm inherited from $\mathbb{Q}(\sqrt{D})$, $N(a+b\sqrt{D}) = a^2 - b^2D$.

Lemma $\alpha \in \mathcal{O}$ is a unit if & only if $N(\alpha) = \pm 1$.

Finding units equivalent to Diophantine Eq. $a^2 - b^2D = \pm 1$

Question What are the primes in \mathcal{O} ?

Lemma If $N(\alpha) = \pm p \in \mathbb{Z}$ then α is irreducible.

Prop Let $\pi \in \mathcal{O}$ be prime. Then $(\pi) \cap \mathbb{Z} = (p)$, p prime.
Thus $p \in (\pi)$ so $p = \pi \gamma$.

Proof Observe that $(\pi) \cap \mathbb{Z}$ is prime. Let $\pi = a + b\sqrt{D}$.
Then $N(\pi) = \pi(a - b\sqrt{D}) \in (\pi)$ so $p \in (\pi)$. \square

Now suppose $p = \pi \pi'$, π irred. Then $p^2 = N(p) = N(\pi)N(\pi')$
So $N(\pi') = p$ also. Thus:

Prop Let $p \in \mathbb{Z}$ be prime. Either p is still prime in \mathcal{O} or p factors into two irreducibles in \mathcal{O} .

Special Case: $D = -1$, Primes in Gaussian integers $\mathbb{Z}[i]$.

PID so $\text{irred} \leftrightarrow \text{prim}$.

Prop p factors in $\mathbb{Z}[i]$ if & only if $p = a^2 + b^2$ $a, b \in \mathbb{Z}$

Proof If $p = a^2 + b^2$ then $p = (a+bi)(a-bi)$.

Conversely if $p = (a+bi)(c+di)$ then $a=c$ $b=-d$ //

Example $2 = 1^2 + 1^2 = (1+i)(1-i)$
 $5 = 1^2 + 2^2 = (1+2i)(1-2i)$

Lemma If p odd, $p = a^2 + b^2$ then $p \equiv 1 \pmod{4}$

Proof $c^2 \equiv 0 \text{ or } 1 \pmod{4}$

Corollary Primes $\equiv 3 \pmod{4}$ remain irreducible in $\mathbb{Z}[i]$.

Prop Let $p \in \mathbb{Z}$. Then p divides some $n^2 + 1$
if & only if $p \equiv 1 \pmod{4}$

Proof $2 \mid 1^2 + 1^2$ ✓

Now $p \mid n^2 + 1 \iff n^2 \equiv -1 \pmod{p}$

So $p \mid n^2 + 1 \implies n$ has order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$

$\implies 4 \mid p-1$

$p \equiv 1 \pmod{4}$

Conversely suppose $p \equiv 1 \pmod 4$.

Lemma $(\mathbb{Z}/p\mathbb{Z})^*$ has a unique element of order 2

Proof $m^2 \equiv 1 \pmod p \Rightarrow p \mid (m^2 - 1) = (m-1)(m+1)$
 $\Rightarrow p \mid m-1$ or $p \mid m+1$ //

So $4 \mid p-1$ so $(\mathbb{Z}/p\mathbb{Z})^*$ has subgroup of order 4 which, by Lemma, is cyclic.

Thus $\exists n$ s.t. $n^2 \equiv -1 \pmod p$
so $p \mid n^2 + 1$ //

Cor $p \equiv 1 \pmod 4$ is not irreducible in $\mathbb{Z}[i]$

Proof We know $p \mid n^2 + 1 = (n+i)(n-i)$

If p is irred then $p \mid n+i$ or $p \mid n-i$.

But p is real so $p \mid n+i$ or $p \mid n-i$ \nexists

Theorem

1. (Fermat's Thm on sum of squares)

$p \in \mathbb{Z}$ is a sum of two squares if & only if

$p \equiv 1 \pmod 4$. Also $p = a^2 + b^2$ uniquely up to \pm, a, b .

2. Irreducibles in $\mathbb{Z}[i]$ are

- a. $1+i$, $\sqrt{2}$
- b. primes $\equiv 3 \pmod 4$
- c. $a+bi$ as above.

Back to our original question:

Prop $n \in \mathbb{Z}$ is a sum of two squares iff only if it is the norm of some $a+bi$.

Let $A+Bi \in \mathbb{Z}[i]$, factor it into irreducibles

$$A+Bi = \pi_1 \pi_2 \cdots \pi_r$$

$$N(\pi_i) = 2$$

$$(*) \quad N(p \equiv 3) \text{ is } p^2$$

$$N(a+bi) \text{ is } a^2 + b^2$$

COR Let $n = 2^k p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$

$$p_i \equiv 1 \pmod{4}$$

$$q_j \equiv 3 \pmod{4}$$

Then

1. n is a sum of two squares iff each b_j is even

2. # ways to write it is

$$4 \cdot (a_1+1)(a_2+1) \cdots (a_r+1)$$

Proof 1 is clear from *

$$n = 2^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s} \quad \begin{matrix} p_i \equiv 1 \\ q_j \equiv 3 \end{matrix}$$

Assume all b_j even.

Let $p_i = \pi_i \overline{\pi_i}$ with π_i irreducible.

Thus $N(A+Bi) = n$ where

$$A+Bi = (1+i)^k (\pi_1^{a_{i1}} \overline{\pi_1}^{a_{i2}}) \dots (\pi_r^{a_{r1}} \overline{\pi_r}^{a_{r2}}) q_1^{b_1/2} \dots q_s^{b_s/2}$$

$$a_{i,1} + a_{i,2} = a_i$$

$$a_{i,1} = 0, 1, 2, \dots, a_i$$

so $(a_i+1)(a_i+1) \dots (a_i+1)$ distinct elements $A+Bi$ of norm n , upto units

But 4 units! //

Example $493 = 17 \cdot 29 \quad a_1 = a_2 = 1 \quad 16 \text{ ways}$

$$17 = (4+i)(4-i) \quad 29 = (5+2i)(5-2i)$$

$$\begin{aligned} (4+i)(5+2i) &= 18+13i \\ (4+i)(5-2i) &= 22-3i \\ (4-i)(5+2i) &= 22+3i \\ (4-i)(5-2i) &= 18-13i \end{aligned} \quad \begin{aligned} 493 &= \pm 18^2 \pm 13^2 \\ &= \pm 22^2 \pm 3^2 \end{aligned}$$

finds 2