

Thm Let n be an integer. Then $n = a^2 + b^2$ iff in the decomposition

$$n = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta_p} \prod_{p \equiv 3(4)} p^{\gamma_p} \quad \text{all the } \gamma_p \text{'s are even.}$$

Proof: By 4 lemmas.

Lemma 1: p prime. Then $x^2 \equiv -1 \pmod{p}$ has a sol'n iff $p \equiv 1(4)$, or $p=2$.

Pf: If $p=2$, okay. $1^2 \equiv -1 \pmod{2}$.

Wilson's thm: $(p-1)! \equiv -1 \pmod{p}$.

$$\text{Assume } p \text{ odd. } (p-1)! = (1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}) \left(\frac{p+1}{2} \cdot \dots \cdot (p-j) \cdot \dots \cdot (p-1) \right) = \prod_{j=1}^{\frac{p-1}{2}} j(p-j)$$

$$\text{So } -1 \equiv (p-1)! \equiv \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \pmod{p}$$

$$\equiv \prod_{j=1}^{\frac{p-1}{2}} -j^2 \pmod{p} \equiv (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j^2 \right)$$

If $p \equiv 1(4)$, $4 | p-1 \Rightarrow \frac{p-1}{2}$ even.

$$\text{So in this case, } -1 \equiv \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 \pmod{p}.$$

Conversely, if we have x with $x^2 \equiv -1 \pmod{p}$, then $(x, p) = 1$.

Then raise both sides to the $\frac{p-1}{2}$ power.

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

By Fermat's little thm: $x^{p-1} \equiv 1 \pmod{p}$, so

$$(-1)^{\frac{p-1}{2}} = 1 \Rightarrow \frac{p-1}{2} \text{ even so } 2 | \frac{p-1}{2} \Rightarrow 4 | p-1 \Rightarrow p \equiv 1(4)$$

Lemma 2: Let q be a prime factor of $a^2 + b^2$. Then if $q \equiv 3(4)$, then $q | a$ and $q | b$.

Pf: By contradiction.

Suppose $(a, q) = 1$ (since q has no proper divisors)

$$a^2 \equiv -b^2 \pmod{q} \quad (a, q) = 1 \Rightarrow \exists c \text{ s.t. } ac \equiv 1 \pmod{q}$$

$$\Rightarrow 1 \equiv -b^2 c^2 \pmod{q} \Rightarrow 1 \equiv -(bc)^2 \pmod{q} \Rightarrow -1 \equiv (bc)^2 \pmod{q}$$

\therefore By Lemma 1, $q \equiv 1(4)$, which is a contradiction.

Lemma 2 implies $n = a^2 + b^2 \Rightarrow \gamma_p$'s even.

By induction on n .

$n=1$ ok

$$n = a^2 + b^2 = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta_p} \prod_{p \equiv 3(4)} p^{\gamma_p}$$

Suppose some $\gamma_{p_0} > 0$. (otherwise, done)

By Lemma 2, $p_0 | a$ and $p_0 | b$, so apply to

$$\left(\frac{a}{p_0} \right)^2 + \left(\frac{b}{p_0} \right)^2 \quad (\text{this is decreasing } \gamma_{p_0} \text{ by } 2).$$

This is the sum of 2 squares, and less than n ,

so by induction hypothesis, γ'_{p_0} (the power of p_0

in expansion of $\left(\frac{a}{p_0} \right)^2 + \left(\frac{b}{p_0} \right)^2$ is even $\Rightarrow \gamma_{p_0} = \gamma'_{p_0} + 2$ even

Lemma 3: If n_1 and n_2 are sums of two squares, then so is $n_1 \cdot n_2$.

Pf: $n_1 = a^2 + b^2$ $n_2 = c^2 + d^2$

Show $(a^2 + b^2)(c^2 + d^2)$ is sum of squares.

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

We want to show that if $n = 2^\alpha \prod_{p \equiv 1(4)} p^{\beta_p} \prod_{p \equiv 3(4)} p^{\gamma_p}$, $n = a^2 + b^2$.

Lemma 3 \Rightarrow enough to check that if $p \equiv 1(4)$, then

$p = a^2 + b^2$ (p prime). Since 2 is a sum of squares, and $\prod_{p \equiv 3(4)} p^{\gamma_p}$ is a square (since γ_p even).

Lemma 4: If p prime, $p \equiv 1(4)$, then $p = a^2 + b^2$.

Pf: $p \equiv 1(4) \Rightarrow \exists x$ s.t. $x^2 \equiv -1(p)$

$$\left[\begin{array}{l} \text{Aside: } (a^2 + b^2) = (a + bi)(a - bi) \\ (a + bx)(a - bx) \equiv a^2 + b^2 (p) \end{array} \right]$$

Define $K =$ biggest integer $< \sqrt{p}$ s.t. $K < \sqrt{p} < K + 1$.

$$f(u, v) = v + xv$$

Look at $f(u, v)$ for $0 \leq u, v \leq K$.

This gives $(K+1)^2$ numbers, which is more than p numbers $\Rightarrow \exists (u_1, v_1)$ and (u_2, v_2) s.t.

$$u_1 + xv_1 \equiv u_2 + xv_2 \pmod{p}$$

Let $a = u_1 - u_2$ and $b = v_1 - v_2$ $|a| < \sqrt{p}$ $|b| < \sqrt{p}$

Then $a \equiv -xb \pmod{p} \Rightarrow a^2 \equiv -1 \cdot b^2 \pmod{p}$

$$\Rightarrow p \mid a^2 + b^2$$

on the other hand, $|a^2 + b^2| \leq |a^2| + |b^2| < 2p$

$$\Rightarrow a^2 + b^2 = p$$

Ex: Find the integer t s.t. $t^9 = 76023109865456217 \approx 7.6 \times 10^{17}$

Point: Reduce mod 20.

$$\phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$$t^9 \equiv t \pmod{20} = 17 \pmod{20} \quad (\text{since } 17 + 100(\dots))$$

$$\text{Thus } p = \{17, 37, 57, 77, 97, 117, \dots\}$$

$$100^9 = 10^{18} \text{ too big}$$

$$80^9 \approx 1.3 \times 10^{17} \text{ (too small)}$$

\therefore answer is 97.