Teorem 4.7. Prirodan broj n se može prikazati u obliku $n = x^2 + y^2$ $x, y \in \mathbb{Z}$ ako i samo ako se u rastavu na brojeve n na proste faktore svaki prost broj p za koji je $p \equiv 3 (4)$ javlja s parnom potencijom.

Dokaz: Pret. da je $n = x^2 + y^2$, te neka je n djeljiv s prostim brojem $p \equiv 3(4)$. Tada je $x^2 \equiv -y^2 \pmod p$. Ako p ne dijeli x i y onda $\frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2 \equiv -1 \pmod p \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p = 4k+1$ $\Rightarrow\Leftarrow$

Stoga p dijeli x i y pa je n djeljiv s p^2. Sada je

$\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = \frac{n}{p^2}$, pa indukcijom slijedi da se p

u rastavu broja n javlja s parnom potencijom.

Obrat će slijediti iz dvije tvrdnje

Teorem 4.8.:

1) $m_1 = a^2+b^2$ i $m_2 = c^2+d^2 \Rightarrow m_1 m_2 = e^2+f^2$

$\|$ $\|$

$|a+bi|^2$ $|c+di|^2$ $\Rightarrow$ $m_1 \cdot m_2 = |(a+bi)(c+di)|^2 = |e+fi|^2 = e^2+f^2$

2) $2 = 1^2+1^2$ i $p \equiv 1 (4)$, $p = a^2+b^2$ $\rightsquigarrow$ $f(x,y) = x^2+y^2$

$\rightsquigarrow d = -4$

$h(-4) = 1 \dots$

Teorem 4.6. $\rightsquigarrow$ $p = g(a,b)$; $a,b \in \mathbb{Z}$

$\text{disc}(g) = -4$

ako i samo ako

$x^2 \equiv -4 \pmod{4p}$ ima rješenja

$\left(\frac{x}{2}\right)^2 \equiv -1 \pmod p \Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 (4)$

$\Rightarrow$ Budući da je $h(-4) = 1$, $g \sim f \Rightarrow g$ i f reprezentiraju iste brojeve $\Rightarrow$ f reprezentira p tj. $\exists\, c,d \in \mathbb{Z}$ t.d. $c^2+d^2 = p$.

□

Teorem 4.8. Cijeli broj n se može prikazati u obliku x^2-y^2 ako i samo ako $n \not\equiv 2 \pmod 4$.

Dokaz: d.s.

Lagrange

Teorem 4.9. (Teorem o četiri kvadrata) Svaki prirodan broj n može se prikazati u obliku sume kvadrata četiri cijela broja, tj. u obliku $n = x^2+y^2+z^2+w^2$, $x,y,z,w \in \mathbb{Z}$

Dokaz: $(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d) = (ax+by+cz+dw)^2 + (\ )^2 + (\ )^2 + (\ )^2$

Zašto? $\mathbb{Q}(i,j,k) = \{a+bi+cj+dk : a,b,c,d \in \mathbb{Q}\}$

vektorski prostor nad $\mathbb{Q}$ s bazom $\langle 1, i, j, k\rangle$

algebra

$i^2 = j^2 = k^2 = -1$; $ij = -ji$

$z \in \mathbb{Q}(i,j,k)$

$z = a+bi+cj+dk$

$\bar{z} = a-bi-cj-dk$

$|z|^2 = z \cdot \bar{z}$

def: $N(z) = z \cdot \bar{z}$ — norma

d.z. $N(z) = a^2+b^2+c^2+d^2$

preostaje nam dokazati mult. fj. N

$N(z_1 \cdot z_2) = z_1 z_2 \cdot \overline{z_1 z_2}$

$\doteq z_1 \cdot \bar{z}_1 \cdot z_2 \cdot \bar{z}_2$

d.z. z_1 i z_2

$\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$

$z_1 \cdot z_2 \cdot \overline{z_1 z_2} = z_1 z_2 \bar{z}_2 \bar{z}_1$

$= z_1 (z_2 \bar{z}_2) \bar{z}_1$

$= z_1 N(z_2) \bar{z}_1 = N(z_1) z_1 \bar{z}_1 = N(z_1) N(z_2)$ ✓.

$\in \mathbb{Z}$

Dovoljno je tvrdnju iz teorema dokazati za proste brojeve. ($2 = 1^2 + 1^2 + 0^2 + 0^2$)

Promotrimo brojeve $0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$

$x^2+y^2+z^2+w^2 = lp$

$x^2+y^2+1^2+0^2$

Nikoja dva među njima nisu kongruentna modulo p (Teorem 3.1.)

Isto vrijedi i za brojeve $-1-0^2, -1-1^2, -1-2^2, \dots, -1-\left(\frac{p-1}{2}\right)^2$

$\perp \in$

$p < 1$ broj. Po Dirichletovom principu, dva među njima daju isti ostatak modulo p. To znači da postoje x, y (iz $\mathbb{Z}$) t.d. $x^2 \equiv -1 - y^2 \pmod p$

i vrijedi $x^2 + y^2 + 1 < 1 + 2\left(\frac{p}{2}\right)^2 < p^2$. Dakle, dobili smo

da je $x^2 + y^2 + 1 = mp$ za neki cijeli broj $0 < m < p$.

Neka je ℓ najmanji prirodan broj t.d. je $\ell p = x^2+y^2+z^2+w^2$.

Tada je $\ell \leq m < p$. Nadalje, $\underline{\ell \text{ je neparan}}$. Zašto?

Ako bi ℓ bio paran onda bi među brojevima x, y, z i w bilo parno mnogo neparnih brojeva.

$$\frac{1}{2}\ell p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

x y z w — $\frac{x+y}{2}$ $\frac{x-y}{2}$ $\frac{z+w}{2}$ $\frac{z-w}{2}$

par par par par $\rightsquigarrow$ $\in \mathbb{Z}$.

par nep. nep. par

$\Rightarrow \Leftarrow$ s minimalnošću od ℓ.

Da bi dokazali teorem, trebamo pokazati da je $\ell = 1$.

Pretp. $\ell > 1$.

Neka su x', y', z', w' najmanji ostaci po apsolutnoj vrijednosti pri dijeljenju brojeva x, y, z, w s ℓ, te neka je

$$n = x'^2 + y'^2 + z'^2 + w'^2.$$

Tada je $n \equiv 0 \pmod{\ell}$ i $n > 0$. Nadalje, budući da je ℓ neparan, imamo da je $n < 4\left(\frac{\ell}{2}\right)^2 = \ell^2$. Stoga je $n = k \cdot \ell$ za neki $0 < k < \ell$.

$(x^2+y^2+z^2+w^2)(x^2+y^2+z^2+w^2) = \square + \square + \square + \square$

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

$k \cdot \ell$ = $k < \ell$

$\ell \cdot p$

$\ell^2 \cdot k \cdot p$ $\quad k < \ell$

$\Rightarrow k \cdot p = \left(\frac{a}{\ell}\right)^2 + \left(\frac{b}{\ell}\right)^2 + \left(\frac{c}{\ell}\right)^2 + \left(\frac{d}{\ell}\right)^2$

Ako su $\frac{a}{\ell}, \frac{b}{\ell}, \frac{c}{\ell}, \frac{d}{\ell} \in \mathbb{Z}$ onda $\Rightarrow \Leftarrow$ s minimalnošću od ℓ

Zašto su $\in \mathbb{Z}$?

Tvrdnja: Ako x se može prikazati kao suma kvadrata 4 racionalna broja, onda su ti racionalni brojevi cijeli.

Dokaz: d.z.

∎