Teorija brojeva

Filip Najman

7. predavanje

11.5.2023.

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

Reći ćemo da je pozitivno definitna kvadratna forma $f(x, y) = ax^2 + bxy + cy^2$ *reducirana ako je* $-a < b \leq a < c$ *ili* $0 \leq b \leq a = c$.

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

Reći ćemo da je pozitivno definitna kvadratna forma $f(x, y) = ax^2 + bxy + cy^2$ *reducirana ako je* $-a < b \leq a < c$ *ili* $0 \leq b \leq a = c$.

Teorem

Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

Reći ćemo da je pozitivno definitna kvadratna forma $f(x, y) = ax^2 + bxy + cy^2$ *reducirana ako je* $-a < b \leq a < c$ *ili* $0 \leq b \leq a = c$.

Teorem

Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.

Dokaz: Promotrimo supstitucije čije su matrice

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{i} \quad V = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$$

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau F U = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau F U$ imati $a < c$. Nadalje

$$V^\tau F V = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau F U = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau F U$ imati $a < c$. Nadalje

$$V^\tau F V = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Stoga koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$. Ovaj proces mora završiti budući da svaka primjena prve transformacije smanjuje vrijednost od a.

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau FU = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau FU$ imati $a < c$. Nadalje

$$V^\tau FV = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Stoga koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$. Ovaj proces mora završiti budući da svaka primjena prve transformacije smanjuje vrijednost od a.

Ako je sada $b = -a$, onda primjenom supstitucije s matricom V možemo postići da je $b = a$, uz nepromjenjeni c. Ako je $a = c$, onda primjenom supstitucije s matricom U možemo postići da je $b \geq 0$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d.

□

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d.

□

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Primjer

Izračunajmo $h(-4)$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d. □

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Primjer

Izračunajmo $h(-4)$.

Rješenje: Iz $3ac \leq 4$ slijedi $a = c = 1$, pa je $b = 0$. Dakle, $h(-4) = 1$. ♢

Zadatak

Koja je najmanja moguća apsolutna vrijednost diskriminante pozitivno definitne kvadratne forme?

Vrijedi da je $h(d) = 1$ za samo 9 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Nadalje vrijedi da je $\lim_{d \to -\infty} h(d) = \infty$.

Vrijedi da je $h(d) = 1$ za samo 9 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Nadalje vrijedi da je $\lim_{d \to -\infty} h(d) = \infty$.

Sljedeći teorem pokazuje da je $h(d)$ upravo broj neekvivalentnih binarnih kvadratnih formi s diskriminatnom d. Napomenimo da analogna tvrdnja za $d > 0$ ne vrijedi.

Teorem

Ako su f i f' dvije ekvivalentne reducirane forme, onda je $f = f'$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (\pm 1, 0), (0, \pm 1)$, te $(1,1)$ ili $(1,-1)$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (\pm 1, 0), (0, \pm 1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po ranijoj Propoziciji, 2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (\pm 1, 0), (0, \pm 1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po ranijoj Propoziciji, 2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 1) slijedi da f i f' reprezentiraju n isti broj puta.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (\pm 1, 0), (0, \pm 1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po ranijoj Propoziciji, 2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 1) slijedi da f i f' reprezentiraju n isti broj puta.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (\pm 1, 0), (0, \pm 1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po ranijoj Propoziciji, 2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 1) slijedi da f i f' reprezentiraju n isti broj puta.

Stoga je $a < c'$, pa je $c = c'$, pošto je to 2. najveća vrijednost reprezentirana s f, a time onda i f'.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad (1)$$

$$c' = f'(0,1) = f(q,s).$$

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad (1)$$

$$c' = f'(0,1) = f(q,s).$$

Budući da je u našem slučaju $a' = a = f(p,r) = ap^2 + bpr + cr^2$, slijedi da je $p = \pm 1$ i $r = 0$.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad (1)$$

$$c' = f'(0,1) = f(q,s).$$

Budući da je u našem slučaju $a' = a = f(p,r) = ap^2 + bpr + cr^2$, slijedi da je $p = \pm 1$ i $r = 0$.

Sada iz $ps - qr = 1$ slijedi $s = \pm 1$, a iz $c = f(q,s)$ slijedi $q = 0$. To znači da je $b = b'$, pa je $b = 0$.

Ostaje razmotriti slučaj $a = c$.

Ostaje razmotriti slučaj $a = c$.

Tada broj a ima barem 4 reprezentacije pomoću f (s $(\pm 1, 0)$ i $(0, \pm 1)$), pa mora imati i barem 4 reprezentacije pomoću f', a to povlači da je $c' = a = c$.

Ostaje razmotriti slučaj $a = c$.

Tada broj a ima barem 4 reprezentacije pomoću f (s $(\pm 1, 0)$ i $(0, \pm 1)$), pa mora imati i barem 4 reprezentacije pomoću f', a to povlači da je $c' = a = c$.

Ponovo dobivamo da je $|b| = |b'|$, ali u ovom slučaju iz definicije reduciranosti imamo da je $b \geq 0$, $b' \geq 0$, pa je $b = b'$. □

Zadatak

Odredite $h(-11)$ *i* $h(20)$.

Teorem

Neka su $d < 0$ *i* $n > 0$ *cijeli brojevi. Tada je* n *pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom* d *ako i samo ako kongruencija* $x^2 \equiv d \pmod{4n}$ *ima rješenja.*

Teorem

Neka su $d < 0$ *i* $n > 0$ *cijeli brojevi. Tada je* n *pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom* d *ako i samo ako kongruencija* $x^2 \equiv d \pmod{4n}$ *ima rješenja.*

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Teorem

Neka su $d < 0$ *i* $n > 0$ *cijeli brojevi. Tada je* n *pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom* d *ako i samo ako kongruencija* $x^2 \equiv d \pmod{4n}$ *ima rješenja.*

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Teorem

Neka su $d < 0$ *i* $n > 0$ *cijeli brojevi. Tada je* n *pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom* d *ako i samo ako kongruencija* $x^2 \equiv d \pmod{4n}$ *ima rješenja.*

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Teorem

Neka su $d < 0$ i $n > 0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom d ako i samo ako kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Tada postoje $q, s \in \mathbb{Z}$ takvi da je $ps - rq = 1$. Sada je f ekvivalentna s f' koja je dobivena iz f pomoću matrice prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i vrijedi: $a' = f'(1, 0) = f(p, r) = n$.

Teorem

Neka su $d < 0$ i $n > 0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom d ako i samo ako kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Tada postoje $q, s \in \mathbb{Z}$ takvi da je $ps - rq = 1$. Sada je f ekvivalentna s f' koja je dobivena iz f pomoću matrice prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i vrijedi: $a' = f'(1, 0) = f(p, r) = n$. Ali f i f' imaju istu diskriminantu, pa je

$$b'^2 - 4nc' = d.$$

Dakle, kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenje $x = b'$. $\square$

Teorem

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 broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Teorem

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 broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Teorem

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 broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Ako p ne dijeli x i y, onda odavde dobivamo da je $\left(\frac{-1}{p}\right)$, što je kontradikcija.

Teorem

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 broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Ako p ne dijeli x i y, onda odavde dobivamo da je $\left(\frac{-1}{p}\right)$, što je kontradikcija.

Stoga p dijeli x i y, pa je n djeljiv sa p^2. Sada je $(\frac{x}{p})^2 + (\frac{y}{p})^2 = \frac{n}{p^2}$, pa indukcijom slijedi da se p u rastavu broja n javlja s parnom potencijom.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Promotrimo sada binarnu kvadratnu formu $f(x, y) = x^2 + y^2$. To je reducirana forma s diskriminantom -4. U Primjeru smo ranije pokazali da je $h(-4) = 1$. Stoga je to jedina reducirana forma s diskriminantom -4.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Promotrimo sada binarnu kvadratnu formu $f(x, y) = x^2 + y^2$. To je reducirana forma s diskriminantom -4. U Primjeru smo ranije pokazali da je $h(-4) = 1$. Stoga je to jedina reducirana forma s diskriminantom -4.

Iz ranije dokazanog Teorema slijedi da je n pravo reprezentiran formom $x^2 + y^2$ ako i samo ako kongruencija $x^2 \equiv d = -4 \pmod{4n}$ ima rješenja.

Ova kongruencija je ekvivalentna sa $z^2 \equiv -1 \pmod{n}$. Neka je $n = p_1 p_2 \cdots p_k$. Po pretpostavci je $p_i \equiv 1 \pmod{4}$, pa kongruencija $z^2 \equiv -1 \pmod{p_i}$ ima rješenje; neka je to rješenje $z = z_i$.

Ova kongruencija je ekvivalentna sa $z^2 \equiv -1 \pmod{n}$. Neka je $n = p_1 p_2 \cdots p_k$. Po pretpostavci je $p_i \equiv 1 \pmod{4}$, pa kongruencija $z^2 \equiv -1 \pmod{p_i}$ ima rješenje; neka je to rješenje $z = z_i$.

Po Kineskom teoremu o ostacima, postoji cijeli broj z koji zadovoljava sustav

$$z \equiv z_1 \pmod{p_1}, \ldots, z \equiv z_k \pmod{p_k}.$$

Sada je $z^2 \equiv z_i^2 \equiv -1 \pmod{p_i}$ za svaki i, pa je $z^2 \equiv -1 \pmod{n}$. □

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran.

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Neka je sada $n \not\equiv 2 \pmod 4$. Razlikujemo dva slučaja:

1) $n = 2k + 1$. Tada je $n = (k + 1)^2 - k^2$.

Teorem

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

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Neka je sada $n \not\equiv 2 \pmod 4$. Razlikujemo dva slučaja:

1) $n = 2k + 1$. Tada je $n = (k + 1)^2 - k^2$.

2) $n = 4k$. Tada je $n = (k + 1)^2 - (k - 1)^2$. □

Teorem (Teorem o četiri kvadrata (Lagrange))

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

Teorem (Teorem o četiri kvadrata (Lagrange))

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: Uočimo da vrijedi identitet

$$\begin{aligned}(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d^2) \\ = \quad (ax+by+cz+dw)^2 + (ay-bx+dz-cw)^2 \\ + \quad (az-cx+bw-dy)^2 + (aw-dx+cy-bz)^2. \qquad (2)\end{aligned}$$

Stoga je tvrdnju teorema dovoljno provjeriti za proste brojeve, jer ako vrijedi za njih, tada vrijedi za sve brojeve.

Teorem (Teorem o četiri kvadrata (Lagrange))

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: Uočimo da vrijedi identitet

$$\begin{aligned}(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d^2) \\ = \quad (ax+by+cz+dw)^2 + (ay-bx+dz-cw)^2 \\ + \quad (az-cx+bw-dy)^2 + (aw-dx+cy-bz)^2. \qquad (2)\end{aligned}$$

Stoga je tvrdnju teorema dovoljno provjeriti za proste brojeve, jer ako vrijedi za njih, tada vrijedi za sve brojeve.

Jasno je da je $2 = 1^2 + 1^2 + 0^2 + 0^2$, pa pretpostavimo da je p neparan prost broj.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

To znači da postoje cijeli brojevi x i y takvi da je $x^2 \equiv -1-y^2 \pmod{p}$ i vrijedi $x^2+y^2+1 < 1+2\cdot(\frac{p}{2})^2 < p^2$. Dakle, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj $0 < m < p$.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

To znači da postoje cijeli brojevi x i y takvi da je $x^2 \equiv -1-y^2 \pmod{p}$ i vrijedi $x^2+y^2+1 < 1+2\cdot(\frac{p}{2})^2 < p^2$. Dakle, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj $0 < m < p$.

Neka je sada l najmanji prirodan broj takav da je $lp = x^2+y^2+z^2+w^2$ za neke $x, y, z, w \in \mathbb{Z}$. Tada je $l \leq m < p$, pošto je $mp = x^2+y^2+1^2+0^2 \leq p^2$.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x + y$, $x - y$, $z + w$, $z - w$ parni.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

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

dobili kontradikciju s minimalnošću od l.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

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

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

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

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Neka su x', y', z', w' najmanji ostatci 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 $n \equiv 0 \pmod{l}$ (jer $x \equiv x' \pmod{l}$ itd.) i $n > 0$.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

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

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Neka su x', y', z', w' najmanji ostatci 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 $n \equiv 0 \pmod{l}$ (jer $x \equiv x' \pmod{l}$ itd.) i $n > 0$.

Nadalje, budući da je l neparan, imamo da je $n < 4 \cdot (\frac{l}{2})^2 = l^2$. Stoga je $n = kl$ za neki cijeli broj k takav da je $0 < k < l$.

Pošto se n i lp mogu zapisati kao sume 4 kvadrata, Iz

$$\begin{aligned}(kl)(lp) &= (x^2+y^2+z^2+w^2)((x')^2+(y')^2+(z')^2+(w')^2) \\ &= (xx'+yy'+zz'+ww')^2+(x'y-y'x+w'z-z'w)^2 \\ &+ (x'z-z'x+y'w-w'y)^2+(x'w-w'x+z'y-y'z)^2 \quad (5)\end{aligned}$$

slijedi da se broj $(kl)(lp)$ može prikazati kao suma kvadrata četiri cijela broja, i štoviše, svaki od tih kvadrata djeljiv je sa l^2.

Pošto se n i lp mogu zapisati kao sume 4 kvadrata, Iz

$$\begin{aligned}(kl)(lp) &= (x^2+y^2+z^2+w^2)((x')^2+(y')^2+(z')^2+(w')^2) \\ &= (xx'+yy'+zz'+ww')^2+(x'y-y'x+w'z-z'w)^2 \\ &+ (x'z-z'x+y'w-w'y)^2+(x'w-w'x+z'y-y'z)^2 \quad (5)\end{aligned}$$

slijedi da se broj $(kl)(lp)$ može prikazati kao suma kvadrata četiri cijela broja, i štoviše, svaki od tih kvadrata djeljiv je sa l^2.

Odavde dijeljenjem s l^2 slijedi da se broj kp može prikazati kao suma četiri kvadrata, no to je u kontradikciji s minimalnošću od l. □

Metoda koju smo upotrijebili u posljednjem dijelu dokaza prethodnog Teorema naziva se *Fermatova metoda beskonačnog spusta*.

Aritmetičke funkcije

Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$.

Aritmetičke funkcije

Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$.

Jedan primjer multiplikativne funkcije je Eulerova funkcija za koju je ranije dokazano da zadovoljava ovo svojstvo.

Aritmetičke funkcije

Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$.

Jedan primjer multiplikativne funkcije je Eulerova funkcija za koju je ranije dokazano da zadovoljava ovo svojstvo.

Često uz multiplikativnu funkciju f vežemo funkciju $g(n) = \sum_{d|n} f(d)$.

Aritmetičke funkcije

Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$.

Jedan primjer multiplikativne funkcije je Eulerova funkcija za koju je ranije dokazano da zadovoljava ovo svojstvo.

Često uz multiplikativnu funkciju f vežemo funkciju $g(n) = \sum_{d|n} f(d)$.

Pokažimo da je g također multiplikativna. Neka je $(m, n) = 1$. Tada je

$$\begin{aligned} g(mn) &= \sum_{d|m} \sum_{d'|n} f(dd') = \sum_{d|m} \sum_{d'|n} f(d)f(d') \\ &= \left(\sum_{d|m} f(d) \right) \left(\sum_{d'|n} f(d') \right) = g(m)g(n). \end{aligned}$$

Često ćemo koristiti i da za proizvoljnu funkciju f vrijedi

$$\sum_{d|n} f(n) = \sum_{d|n} f(n/d).$$

Često ćemo koristiti i da za proizvoljnu funkciju f vrijedi

$$\sum_{d|n} f(n) = \sum_{d|n} f(n/d).$$

Na primjer za $n = 6$ vrijedi

$$f(1) + f(2) + f(3) + f(6) = f(6/1) + f(6/2) + f(6/3) + f(6/6).$$

Često ćemo koristiti i da za proizvoljnu funkciju f vrijedi

$$\sum_{d|n} f(n) = \sum_{d|n} f(n/d).$$

Na primjer za $n = 6$ vrijedi

$$f(1) + f(2) + f(3) + f(6) = f(6/1) + f(6/2) + f(6/3) + f(6/6).$$

Također često mijenjamo redoslijed sumacije, pa imamo

$$\sum_{d} \sum_{d'} f(d, d') = \sum_{d'} \sum_{d} f(d, d'),$$

s tim da moramo paziti po čemu idu d i d' tako da se s obje strane pojavljuju isti $f(d, d')$.

Definicija

Möbiusova funkcija $\mu(n)$, $n \in \mathbb{N}$ *je definirana sa*

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan} \\ (-1)^k, & \text{ako je } n = p_1 p_2 \cdots p_k,\ p_i \text{ različiti prosti brojevi.} \end{cases}$$

Očito je funkcija μ multiplikativna, pa je i funkcija $\nu(n) = \sum_{d|n} \mu(d)$ također multiplikativna.

Definicija

Möbiusova funkcija $\mu(n)$, $n \in \mathbb{N}$ *je definirana sa*

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan} \\ (-1)^k, & \text{ako je } n = p_1 p_2 \cdots p_k,\ p_i \text{ različiti prosti brojevi.} \end{cases}$$

Očito je funkcija μ multiplikativna, pa je i funkcija $\nu(n) = \sum_{d|n} \mu(d)$ također multiplikativna.

Dakle, $\nu(1) = 1$, dok za $n > 1$ vrijedi

$$\nu(n) = \nu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1}) \cdots \nu(p_k^{\alpha_k})$$

$$= (\mu(1) + \mu(p_1) + \mu(p_1^2) + \cdots) \cdots (\mu(1) + \mu(p_k) + \mu(p_k^2) + \cdots)$$

$$= (1 - 1 + 0 + \cdots) \cdots (1 - 1 + 0 + \cdots) = 0.$$

Teorem (Möbiusova formula inverzije)

Neka je $f : \mathbb{N} \to \mathbb{C}$ *proizvoljna funkcija, te neka je* $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. *Tada je* $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$.

Teorem (Möbiusova formula inverzije)

Neka je $f : \mathbb{N} \to \mathbb{C}$ *proizvoljna funkcija, te neka je* $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. *Tada je* $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$. *Obrnuto, ako je* $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ *za svaki* $n \in \mathbb{Z}$, *onda je* $F(n) = \sum_{d|n} f(d)$.

Teorem (Möbiusova formula inverzije)

Neka je $f : \mathbb{N} \to \mathbb{C}$ *proizvoljna funkcija, te neka je* $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. *Tada je* $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$. *Obrnuto, ako je* $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ *za svaki* $n \in \mathbb{Z}$, *onda je* $F(n) = \sum_{d|n} f(d)$.

Dokaz: Dokažeimo prvu tvrdnju. Imamo:

$$\begin{aligned} \sum_{d|n} \mu(d) F(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} f(d') \nu(\frac{n}{d'}) = f(n). \end{aligned}$$

Da bi dokazali obrat, zapišimo jednakost $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ u obliku $f(n) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$.

Da bi dokazali obrat, zapišimo jednakost $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ u obliku $f(n) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$. Sada je

$$\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d}) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(\frac{n}{dd'}) F(d') = \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(\frac{n}{dd'}) F(d')$$

Da bi dokazali obrat, zapišimo jednakost $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ u obliku $f(n) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$. Sada je

$$\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d}) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(\frac{n}{dd'}) F(d') = \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(\frac{n}{dd'}) F(d')$$

$$= \sum_{d'|n} F(d') \sum_{d|\frac{n}{d'}} \mu(\frac{n}{dd'}) = \sum_{d'|n} F(d') \nu(\frac{n}{d'}) = F(n).$$

□

Primjenimo li Möbiusovu formulu inverzije na relaciju $\sum_{d|n} \varphi(d) = n = id(n)$, dobivamo

$$\varphi(n) = \sum_{d|n} \mu(d) id\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{6}$$

Primjenimo li Möbiusovu formulu inverzije na relaciju $\sum_{d|n} \varphi(d) = n = id(n)$, dobivamo

$$\varphi(n) = \sum_{d|n} \mu(d) id\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{6}$$

Definicija

Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.

Primjenimo li Möbiusovu formulu inverzije na relaciju $\sum_{d|n} \varphi(d) = n = id(n)$, dobivamo

$$\varphi(n) = \sum_{d|n} \mu(d) id\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{6}$$

Definicija

Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.

Jasno je da vrijedi $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$.

Primjenimo li Möbiusovu formulu inverzije na relaciju $\sum_{d|n} \varphi(d) = n = id(n)$, dobivamo

$$\varphi(n) = \sum_{d|n} \mu(d) id\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{6}$$

Definicija

Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.

Jasno je da vrijedi $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$.

Pošto su konstantna funkcija i identita multiplikativna, slijedi da su funkcije τ i σ također multiplikativne.

Budući da je $\tau(p^j) = j + 1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} (\alpha_i + 1),$$

Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\begin{aligned} \tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} (\alpha_i + 1), \\ \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \end{aligned}$$

Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\begin{aligned} \tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} (\alpha_i + 1), \\ \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \end{aligned}$$

Često ćemo aproksimirati sumu integralima. Za rastuću integrabilnu funkciju f vrijedi

$$\int_{a-1}^{b} f(x)dx \leq \sum_{k=a}^{b} f(k) \leq \int_{a}^{b+1} f(x)dx.$$

Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\begin{aligned} \tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} (\alpha_i + 1), \\ \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \end{aligned}$$

Često ćemo aproksimirati sumu integralima. Za rastuću integrabilnu funkciju f vrijedi

$$\int_{a-1}^{b} f(x)dx \leq \sum_{k=a}^{b} f(k) \leq \int_{a}^{b+1} f(x)dx.$$

Posebno

$$\int_{k-1}^{k} f(x)dx \leq f(k) \leq \int_{k}^{k+1} f(x)dx.$$

Propozicija

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

Propozicija

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Propozicija

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} = n(\frac{1}{n} + \sum_{d=1}^{n-1} \frac{1}{d})$$

Propozicija

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} = n(\frac{1}{n} + \sum_{d=1}^{n-1} \frac{1}{d})$$

$$< n \left(1 + \sum_{d=1}^{n-1} \frac{1}{d}\right) \leq n \cdot \left(1 + \int_1^n \frac{1}{x}\, dx\right) = n(1 + \ln n).$$

Propozicija

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} = n(\frac{1}{n} + \sum_{d=1}^{n-1} \frac{1}{d})$$

$$< n \left(1 + \sum_{d=1}^{n-1} \frac{1}{d}\right) \leq n \cdot \left(1 + \int_1^n \frac{1}{x}\, dx\right) = n(1 + \ln n).$$

2) Funkcija $f(n) = \frac{\sigma(n)\varphi(n)}{n^2}$ je multiplikativna.

Propozicija

1) $\sigma(n) < n(1+\ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} = n\left(\frac{1}{n} + \sum_{d=1}^{n-1} \frac{1}{d}\right)$$

$$< n\left(1 + \sum_{d=1}^{n-1} \frac{1}{d}\right) \leq n \cdot \left(1 + \int_1^n \frac{1}{x}\, dx\right) = n(1+\ln n).$$

2) Funkcija $f(n) = \frac{\sigma(n)\varphi(n)}{n^2}$ je multiplikativna. Nadalje,

$$f(p^j) = \frac{(p^{j+1}-1)p^{j-1}(p-1)}{(p-1)p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2},$$

pa je

$$f(n) \geq \prod_{p|n}\left(1 - \frac{1}{p^2}\right) \geq \prod_{m=2}^{\infty}\left(1 - \frac{1}{m^2}\right) = \frac{1\cdot 3}{2\cdot 2} \cdot \frac{2\cdot 4}{3\cdot 3} \cdot \frac{3\cdot 5}{4\cdot 4} \cdot \frac{4\cdot 6}{5\cdot 5} \cdots = \frac{1}{2}.$$

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ eksplicitno provjerimo. □

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ ekplicitno provjerimo. □

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj.

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ ekplicitno provjerimo. □

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj.

Mi ćemo to učiniti za funkcije τ, σ i φ. Pritom ćemo rabiti sljedeću oznaku: $f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x.

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ ekplicitno provjerimo. □

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj.

Mi ćemo to učiniti za funkcije τ, σ i φ. Pritom ćemo rabiti sljedeću oznaku: $f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x.

Na primjer, budući da je $\lfloor x \rfloor = x - \{x\}$, a $\{x\}$ je omeđena funkcija, možemo pisati: $\lfloor x \rfloor = x + O(1)$.

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ ekplicitno provjerimo. □

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj.

Mi ćemo to učiniti za funkcije τ, σ i φ. Pritom ćemo rabiti sljedeću oznaku: $f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x.

Na primjer, budući da je $\lfloor x \rfloor = x - \{x\}$, a $\{x\}$ je omeđena funkcija, možemo pisati: $\lfloor x \rfloor = x + O(1)$.

Također, zbog

$$\int_1^{\lfloor x \rfloor} \frac{1}{t}\, dt \leq \sum_{n \leq x} \frac{1}{n} < 1 + \int_1^x \frac{1}{t} dt,$$

tj. $\ln \lfloor x \rfloor \leq \sum_{n \leq x} \frac{1}{n} < 1 + \ln x$, možemo pisati:

$$\sum_{n \leq x} \frac{1}{n} = \ln x + O(1).$$

Sljedeću lemu ostavljamo bez dokaza.

Lema

Vrijedi: $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\,.$

Sljedeću lemu ostavljamo bez dokaza.

Lema

Vrijedi: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Propozicija

1) $\sum_{n\leq x} \tau(n) = x \ln x + O(x)$
2) $\sum_{n\leq x} \sigma(n) = \frac{1}{12}\pi^2 x^2 + O(x \ln x)$
3) $\sum_{n\leq x} \varphi(n) = \frac{3}{\pi^2} \cdot x^2 + O(x \ln x)$

Dokaz:

1)

$$\begin{aligned}\sum_{n\leq x} \tau(n) &= \sum_{n\leq x}\sum_{d|n} 1 = \sum_{d\leq x}\sum_{m\leq \frac{x}{d}} 1 = \sum_{d\leq x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d\leq x} \left(\frac{x}{d} + O(1)\right) \\ &= x \sum_{d\leq x} \left(\frac{1}{d} + O(1)\right) = x \ln x + O(x)\end{aligned}$$

2) Primijetimo da je

$$\sum_{n\leq x}\sigma(n)=\sum_{n\leq x}\sum_{d|n}d=\sum_{n\leq x}\sum_{d|n}\frac{n}{d}=\sum_{d\leq x}\sum_{n=md\leq x}\frac{md}{d}=\sum_{d\leq x}\sum_{m\leq\frac{x}{d}}m.$$

2) Primijetimo da je

$$\sum_{n\le x}\sigma(n)=\sum_{n\le x}\sum_{d\mid n}d=\sum_{n\le x}\sum_{d\mid n}\frac{n}{d}=\sum_{d\le x}\sum_{n=md\le x}\frac{md}{d}=\sum_{d\le x}\sum_{m\le\frac{x}{d}}m.$$

Nadalje je

$$\sum_{m\le\frac{x}{d}}m=\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)=\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right).$$

2) Primijetimo da je

$$\sum_{n\le x}\sigma(n)=\sum_{n\le x}\sum_{d\mid n}d=\sum_{n\le x}\sum_{d\mid n}\frac{n}{d}=\sum_{d\le x}\sum_{n=md\le x}\frac{md}{d}=\sum_{d\le x}\sum_{m\le\frac{x}{d}}m.$$

Nadalje je

$$\sum_{m\le\frac{x}{d}}m=\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)=\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right).$$

Sada je

$$\sum_{d\le x}\frac{1}{d^2}-\sum_{d=1}^{\infty}\frac{1}{d^2}=O\left(\int_x^{\infty}\frac{1}{t^2}\,dt\right)=O\left(\frac{1}{x}\right).$$

Konačno je, po Lemi koju nismo dokazivali $\sum_{d=1}^{\infty}\frac{1}{d^2}=\frac{\pi^2}{6}$. Slijedi

2) Primijetimo da je

$$\sum_{n\le x}\sigma(n)=\sum_{n\le x}\sum_{d\mid n}d=\sum_{n\le x}\sum_{d\mid n}\frac{n}{d}=\sum_{d\le x}\sum_{n=md\le x}\frac{md}{d}=\sum_{d\le x}\sum_{m\le\frac{x}{d}}m.$$

Nadalje je

$$\sum_{m\le\frac{x}{d}}m=\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)=\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right).$$

Sada je

$$\sum_{d\le x}\frac{1}{d^2}-\sum_{d=1}^{\infty}\frac{1}{d^2}=O\left(\int_x^{\infty}\frac{1}{t^2}\,dt\right)=O\left(\frac{1}{x}\right).$$

Konačno je, po Lemi koju nismo dokazivali $\sum_{d=1}^{\infty}\frac{1}{d^2}=\frac{\pi^2}{6}$. Slijedi

$$\begin{aligned}\sum_{n\le x}\sigma(n)&=\sum_{d\le x}\left[\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right)\right]=\frac{x^2}{2}\sum_{d\le x}\left(\frac{1}{d}\right)^2+x\sum_{d\le x}O\left(\frac{1}{d}\right)\\&=\left[\frac{\pi^2}{12}x^2+O(x)\right]+xO(\ln x)=\frac{\pi^2}{12}x^2+O(x\ln x).\end{aligned}$$

3) Prema (6), imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{n\leq x}\sum_{d|n}\mu(d)\cdot\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m.$$

3) Prema (6), imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{n\leq x}\sum_{d|n}\mu(d)\cdot\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m.$$

Već smo vidjeli da je zadnja suma jednaka $\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d})$.

3) Prema (6), imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{n\leq x}\sum_{d|n}\mu(d)\cdot\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m.$$

Već smo vidjeli da je zadnja suma jednaka $\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d})$. Nadalje

$$\sum_{d\leq x}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\Big(\frac{1}{x}\Big).$$

3) Prema (6), imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{n\leq x}\sum_{d|n}\mu(d)\cdot\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m.$$

Već smo vidjeli da je zadnja suma jednaka $\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d})$. Nadalje

$$\sum_{d\leq x}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\Big(\frac{1}{x}\Big).$$

Da bi izračunali $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$, pomnožimo je s $\sum_{d=1}^{\infty}\frac{1}{d^2}$.

3) Prema (6), imamo:

$$\sum_{n\le x}\varphi(n)=\sum_{n\le x}\sum_{d\mid n}\mu(d)\cdot\frac{n}{d}=\sum_{d\le x}\mu(d)\sum_{m\le\frac{x}{d}}m.$$

Već smo vidjeli da je zadnja suma jednaka $\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d})$. Nadalje

$$\sum_{d\le x}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\Big(\frac{1}{x}\Big).$$

Da bi izračunali $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$, pomnožimo je s $\sum_{d=1}^{\infty}\frac{1}{d^2}$. Dobivamo:

$$\Big(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\Big)\Big(\sum_{d=1}^{\infty}\frac{1}{d^2}\Big)=\sum_{m=1}^{\infty}\frac{1}{m^2}\sum_{dd'=m}1\cdot\mu(d)=\sum_{m=1}^{\infty}\frac{1}{m^2}\sum_{d\mid m}\mu(d)$$

$$=\sum_{m=1}^{\infty}\frac{\nu(m)}{m^2}=1.$$

Prema tome, dobili smo da je $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}$, pa konačno imamo:

$$\sum_{n\le x}\varphi(n)=\sum_{d\le x}\mu(d)\Big[\frac{1}{2}\Big(\frac{x}{d}\Big)^2+O\Big(\frac{x}{d}\Big)\Big]=\frac{x^2}{2}\sum_{d\le x}\Big(\frac{\mu(d)}{d^2}\Big)+\sum_{d\le x}O\Big(\frac{x}{d}\Big)$$

$$= \frac{3}{\pi^2} x^2 + O(x \ln x).$$

□

Budući da je $\sum_{n \leq x} \varphi(n) \sim \frac{3}{\pi^2} x^2$, $\sum_{n \leq x} n \sim \frac{1}{2} x^2$, rezultat iz Propozicije 3) može se interpretirati i tako da kažemo da je vjerojatnost da su dva nasumce izabrana cijela broja relativno prosta jednaka $\frac{6}{\pi^2} \approx 0.6079$.

$$= \frac{3}{\pi^2} x^2 + O(x \ln x).$$

□

Budući da je $\sum_{n \leq x} \varphi(n) \sim \frac{3}{\pi^2} x^2$, $\sum_{n \leq x} n \sim \frac{1}{2} x^2$, rezultat iz Propozicije 3) može se interpretirati i tako da kažemo da je vjerojatnost da su dva nasumce izabrana cijela broja relativno prosta jednaka $\frac{6}{\pi^2} \approx 0.6079$.

Godine 1896. Hadamard i de la Vallée Poussin su dokazali da je $\pi(x) \sim \frac{x}{\ln x}$ kad $x \to \infty$.