Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$3587 = 1819 \cdot 1 + 1768$$

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \end{aligned}$$

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \end{aligned}$$

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \end{aligned}$$

Primjer (1.2)

Odredimo $d = \gcd(3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned}
3587 &= 1819 \cdot 1 + 1768 \\
1819 &= 1768 \cdot 1 + 51 \\
1768 &= 51 \cdot 34 + 34 \\
51 &= 34 \cdot 1 + 17 \\
34 &= 17 \cdot 2
\end{aligned}$$

Sjetimo se rekurzije:

$$\begin{aligned} r_{-1} &= b, \quad r_0 = c; \quad r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} &= 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

Rješenje rekurzijom:

i	-1	0	1	2	3	4
q_i			1	1	34	1
x_i	1	0	1	-1	35	-36
y_i	0	1	-1	2	-69	71

Dakle, $d = 17$, te $3587 \cdot (-36) + 1819 \cdot 71 = 17$.

Definicija

Prirodan broj $p > 1$ *se zove prost ako* p *nema niti jednog djelitelja* d *takvog da je* $1 < d < p$. *Ako prirodan broj* $a > 1$ *nije prost, onda kažemo da je složen.*

Definicija

Prirodan broj $p > 1$ se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.

Teorem

Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).

Definicija

Prirodan broj $p > 1$ *se zove prost ako* p *nema niti jednog djelitelja* d *takvog da je* $1 < d < p$. *Ako prirodan broj* $a > 1$ *nije prost, onda kažemo da je složen.*

Teorem

Svaki prirodan broj $n > 1$ *može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Definicija

Prirodan broj $p > 1$ *se zove prost ako* p *nema niti jednog djelitelja* d *takvog da je* $1 < d < p$. *Ako prirodan broj* $a > 1$ *nije prost, onda kažemo da je složen.*

Teorem

Svaki prirodan broj $n > 1$ *može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$.

Definicija

Prirodan broj $p > 1$ se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.

Teorem

Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$.

Želimo dokazati da se i n može prikazati kao produkt prostih faktora.

Definicija

Prirodan broj $p > 1$ se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.

Teorem

Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).

<u>Dokaz:</u> Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$.

Želimo dokazati da se i n može prikazati kao produkt prostih faktora.

Ako je n prost, nemamo što dokazivati.

Definicija

Prirodan broj $p > 1$ se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.

Teorem

Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$.

Želimo dokazati da se i n može prikazati kao produkt prostih faktora.

Ako je n prost, nemamo što dokazivati.

U protivnom je $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, n_1 i n_2 su produkti prostih brojeva, pa stoga i n ima to svojstvo.

Iz prošlog Teorema slijedi da svaki prirodan broj n možemo prikazati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi.

Iz prošlog Teorema slijedi da svaki prirodan broj n možemo prikazati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi.

Ovakav prikaz broja n zvat ćemo *kanonski rastav* broja n na proste faktore.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1a_2\cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p,a)=1$, pa postoje cijeli brojevi x i y takvi da je $ax+py=1$.

Sada je $abx+pby=b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Sada ako $p|a_1(a_2 \cdots a_n)$, onda $p|a_1$ ili $p|a_2 a_3 \cdots a_n$.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

<u>Dokaz:</u>
Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Sada ako $p|a_1(a_2 \cdots a_n)$, onda $p|a_1$ ili $p|a_2 a_3 \cdots a_n$.

Ako $p|a_2 a_3 \cdots a_n$, onda po induktivnoj pretpostavci $p|a_i$ za neki $i = 2, \ldots, n$.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i, j.

Međutim, to je nemoguće jer iz $p_1 | q_1 q_2 \cdots q_s$, po prethodnoj Propoziciji, slijedi pa p_1 dijeli barem jedan q_j.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j.

Međutim, to je nemoguće jer iz $p_1 | q_1 q_2 \cdots q_s$, po prethodnoj Propoziciji, slijedi pa p_1 dijeli barem jedan q_j.

No, to znači da je $p_1 = q_j$, kontradikcija.

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Za sada, kao primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \, : \, a, b \in \mathbb{Z}\}$ *navedimo ove dvije faktorizacije broja* 10*:*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Za sada, kao primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ *navedimo ove dvije faktorizacije broja* 10*:*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

U primjenama Osnovnog teorema aritmetike često ćemo prirodan broj a pisati u obliku $a = \prod_p p^{\alpha(p)}$, gdje je $\alpha(p) \geq 0$ i podrazumijevamo da je $\alpha(p) = 0$ za skoro sve proste brojeve p. Ako je $a = 1$, onda je $\alpha(p) = 0$ za sve p.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Obratno, ako je $\alpha(p) \leq \gamma(p)$, onda možemo definirati prirodan broj $b = \prod_p p^{\beta(p)}$ sa $\beta(p) = \gamma(p) - \alpha(p)$. Tada je $ab = c$, pa $a|c$.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Obratno, ako je $\alpha(p) \leq \gamma(p)$, onda možemo definirati prirodan broj $b = \prod_p p^{\beta(p)}$ sa $\beta(p) = \gamma(p) - \alpha(p)$. Tada je $ab = c$, pa $a|c$.

Prema tome, dobili smo da vrijedi

$$a|c \iff \alpha(p) \leq \gamma(p), \quad \forall p. \tag{1}$$

Kao posljedicu formule (1) dobivamo formulu

$$(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}. \tag{2}$$

Definicija

Neka su $a_1, a_2, \ldots, a_n$ *cijeli brojevi različiti od nule. Najmanji prirodan broj* c *za koji vrijedi da* $a_i | c$ *za sve* $i = 1, 2, \ldots, n$ *zove se najmanji zajednički višekratnik i označava s* $[a_1, a_2, \ldots, a_n]$.

Slijedi da je

$$[a, b] = \prod_{p} p^{\max(\alpha(p), \beta(p))}. \tag{3}$$

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p), \beta(p))}. \tag{3}$$

Propozicija

$$(a, b) \cdot [a, b] = |ab|$$

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p), \beta(p))}. \tag{3}$$

Propozicija

$$(a, b) \cdot [a, b] = |ab|$$

Dokaz:
Po Osnovnom teoremu aritmetike i ranije dokazanom, dovoljno je provjeriti da za sve realne brojeve x, y vrijedi:

$$\min(x, y) + \max(x, y) = x + y.$$

Slijedi da je

$$[a,b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Propozicija

$$(a,b)\cdot[a,b] = |ab|$$

Dokaz:

Po Osnovnom teoremu aritmetike i ranije dokazanom, dovoljno je provjeriti da za sve realne brojeve x, y vrijedi:

$$\min(x,y) + \max(x,y) = x + y.$$

Zaista, ako je $x \le y$, onda je $\min(x,y) + \max(x,y) = x + y$, a ako je $x > y$, onda je $\min(x,y) + \max(x,y) = y + x = x + y$. $\square$

Zadatak

Odredite a) $[530, 820]$, *b)* $[720, 125]$.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Reći ćemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je *a kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je *a kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Stoga je a kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je *a kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Stoga je a kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1.

Ako je p prost, onda je $p^k \| a \iff k = \alpha(p)$.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Tada je p očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Tada je p očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$.

Budući da je $m \geq p$, dobivamo da je $n \geq p^2$, pa je $p \leq \sqrt{n}$.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

U svakom koraku, prvi neprekriženi broj je prost, te u idućem koraku križamo njegove prave višekratnike (prvi novoprekriženi broj će biti njegov kvadrat, jer su svi manji višekratnici već ranije prekriženi).

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

U svakom koraku, prvi neprekriženi broj je prost, te u idućem koraku križamo njegove prave višekratnike (prvi novoprekriženi broj će biti njegov kvadrat, jer su svi manji višekratnici već ranije prekriženi).

U našem slučaju, nakon križanja višekratnika od 7, 11 i 13, tablica je gotova (jer je $17 > \sqrt{200}$).

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \dots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, ..., ni sa p_k.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, ..., ni sa p_k.

Dakle, svaki prosti faktor p od n je različit od $p_1, \ldots, p_k$.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, ..., ni sa p_k.

Dakle, svaki prosti faktor p od n je različit od $p_1, \ldots, p_k$.

Budući da je n ili prost ili ima prosti faktor, dobili smo prost broj različit od $p_1, \ldots, p_k$, što je kontradikcija.

Primjer

Dokazati da za svaki prirodan broj n postoji n uzastopnih složenih brojeva.

Dokaz: To su npr. brojevi

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n,\ (n+1)!+n+1,$$

jer je $(n+1)!+j$ djeljivo sa j za $j=2,3,\ldots,n+1$.

Primjer

Dokazati da ne postoji polinom $f(x)$ *s cjelobrojnim koeficijentima, stupnja* ≥ 1*, takav da je* $f(n)$ *prost za sve* $n \in \mathbb{N}$*.*

Dokaz: Pretpostavimo suprotno. Neka je $f(1) = p$, gdje je p prost broj.

Primjer

Dokazati da ne postoji polinom $f(x)$ s cjelobrojnim koeficijentima, stupnja ≥ 1, takav da je $f(n)$ prost za sve $n \in \mathbb{N}$.

Dokaz: Pretpostavimo suprotno. Neka je $f(1) = p$, gdje je p prost broj.

Primjetimo da je $f(1 + kp) - f(1)$ djeljivo sa $(1 + kp) - 1 = kp$. To vrijedi jer $x - y$ dijeli $x^m - y^m$ pa onda $x - y$ dijeli svaki monom od $f(x) - f(y)$, a time i sam $f(x) - f(y)$. Uvrštavanjem $x = 1 + kp$ i $y = 1$ dobivamo tvrdnju.

Primjer

Dokazati da ne postoji polinom $f(x)$ s cjelobrojnim koeficijentima, stupnja ≥ 1, takav da je $f(n)$ prost za sve $n \in \mathbb{N}$.

Dokaz: Pretpostavimo suprotno. Neka je $f(1) = p$, gdje je p prost broj.

Primjetimo da je $f(1 + kp) - f(1)$ djeljivo sa $(1 + kp) - 1 = kp$. To vrijedi jer $x - y$ dijeli $x^m - y^m$ pa onda $x - y$ dijeli svaki monom od $f(x) - f(y)$, a time i sam $f(x) - f(y)$. Uvrštavanjem $x = 1 + kp$ i $y = 1$ dobivamo tvrdnju.

Slijedi da $p | f(1 + kp)$, za svaki $k \in \mathbb{N}$.

Primjer

Dokazati da ne postoji polinom $f(x)$ s cjelobrojnim koeficijentima, stupnja ≥ 1, takav da je $f(n)$ prost za sve $n \in \mathbb{N}$.

Dokaz: Pretpostavimo suprotno. Neka je $f(1) = p$, gdje je p prost broj.

Primjetimo da je $f(1 + kp) - f(1)$ djeljivo sa $(1 + kp) - 1 = kp$. To vrijedi jer $x - y$ dijeli $x^m - y^m$ pa onda $x - y$ dijeli svaki monom od $f(x) - f(y)$, a time i sam $f(x) - f(y)$. Uvrštavanjem $x = 1 + kp$ i $y = 1$ dobivamo tvrdnju.

Slijedi da $p|f(1 + kp)$, za svaki $k \in \mathbb{N}$.

Međutim, po pretpostavci $f(1 + kp)$je prost, pa mora biti $f(1 + kp) = p$, $\forall k \in \mathbb{N}$.

Primjer

Dokazati da ne postoji polinom $f(x)$ s cjelobrojnim koeficijentima, stupnja ≥ 1, takav da je $f(n)$ prost za sve $n \in \mathbb{N}$.

Dokaz: Pretpostavimo suprotno. Neka je $f(1) = p$, gdje je p prost broj.

Primjetimo da je $f(1+kp) - f(1)$ djeljivo sa $(1+kp) - 1 = kp$. To vrijedi jer $x - y$ dijeli $x^m - y^m$ pa onda $x - y$ dijeli svaki monom od $f(x) - f(y)$, a time i sam $f(x) - f(y)$. Uvrštavanjem $x = 1 + kp$ i $y = 1$ dobivamo tvrdnju.

Slijedi da $p | f(1+kp)$, za svaki $k \in \mathbb{N}$.

Međutim, po pretpostavci $f(1+kp)$je prost, pa mora biti $f(1+kp) = p$, $\forall k \in \mathbb{N}$.

Budući da polinom $f(x) - p$ ima beskonačno mnogo nultočaka, on mora biti nulpolinom, pa je $f(x) = p$, što je u suprotnosti s pretpostavkom da je $\operatorname{st} f \geq 1$. $\square$

Kongruencije

Teoriju kongruencija uveo je u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Kongruencije

Teoriju kongruencija uveo je u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Definicija

Ako cijeli broj $m \neq 0$ *dijeli razliku* $a - b$, *onda kažemo da je* a *kongruentan* b *modulo* m *i pišemo* $a \equiv b \pmod{m}$. *U protivnom, kažemo da* a *nije kongruentan* b *modulo* m *i pišemo* $a \not\equiv b \pmod{m}$.

Kongruencije

Teoriju kongruencija uveo je u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Definicija

Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a kongruentan b modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.

Budući da je $a - b$ djeljivo s m ako i samo ako je djeljivo s $-m$, bez smanjenja općenitosti možemo se usredotočiti na pozitivne module i kod nas će ubuduće modul m biti prirodan broj. Kongruencije imaju mnoga svojstva zajednička s jednakostima.

Propozicija

Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Propozicija

Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Dokaz: Treba provjeriti refleksivnost, simetričnost i tranzitivnost.

Propozicija

Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Dokaz: Treba provjeriti refleksivnost, simetričnost i tranzitivnost.
(1) Iz $m|0$ slijedi $a \equiv a \pmod{m}$.

Propozicija

Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Dokaz: Treba provjeriti refleksivnost, simetričnost i tranzitivnost.
(1) Iz $m|0$ slijedi $a \equiv a \pmod{m}$.

(2) Ako je $a \equiv b \pmod{m}$, onda postoji $k \in \mathbb{Z}$ takav $a - b = mk$. Sada je $b - a = m \cdot (-k)$, pa je $b \equiv a \pmod{m}$.

Propozicija

Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.

Dokaz: Treba provjeriti refleksivnost, simetričnost i tranzitivnost.
(1) Iz $m|0$ slijedi $a \equiv a \pmod{m}$.

(2) Ako je $a \equiv b \pmod{m}$, onda postoji $k \in \mathbb{Z}$ takav $a - b = mk$. Sada je $b - a = m \cdot (-k)$, pa je $b \equiv a \pmod{m}$.

(3) Iz $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ slijedi da postoje $k, l \in \mathbb{Z}$ takvi da je $a - b = mk$ i $b - c = ml$. Zbrajanjem dobivamo $a - c = m(k + l)$, što povlači $a \equiv c \pmod{m}$. $\square$

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$*, onda je* $a + c \equiv b + d \pmod{m}$*,* $a - c \equiv b - d \pmod{m}$*,* $ac \equiv bd \pmod{m}$*.*
(2) Ako je $a \equiv b \pmod{m}$ *i* $d|m$*, onda je* $a \equiv b \pmod{d}$*.*

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$*, onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ *i* $d|m$*, onda je* $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$*, onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$.

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ *i* $d|m$, *onda je* $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$, *onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$.

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ *i* $d|m$, *onda je* $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$, *onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$.

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ *i* $d | m$, *onda je* $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$, *onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$.

Propozicija

Neka su a, b, c, d *cijeli brojevi.*
(1) Ako je $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$*, onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ *i* $d|m$*, onda je* $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$*, onda je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$. Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$.

Propozicija

Neka su a, b, c, d cijeli brojevi.
(1) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ i $d|m$, onda je $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$ za svaki $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$. Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$.

(2) Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ek)$, pa je $a \equiv b \pmod{d}$.

Propozicija

Neka su a, b, c, d cijeli brojevi.
(1) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
(2) Ako je $a \equiv b \pmod{m}$ i $d|m$, onda je $a \equiv b \pmod{d}$.
(3) Ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$ za svaki $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$. Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$.

(2) Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ek)$, pa je $a \equiv b \pmod{d}$.

(3) Iz $a - b = mk$ slijedi $ac - bc = (mc) \cdot k$, pa je $ac \equiv bc \pmod{mc}$. $\square$

Propozicija

Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.

Propozicija

Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.

Dokaz: Neka je $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$, gdje su $c_i \in \mathbb{Z}$.

Propozicija

Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.

Dokaz: Neka je $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$, gdje su $c_i \in \mathbb{Z}$.

Budući da je $a \equiv b \pmod{m}$, uzastopnom primjenom prethodne Propozicije dobivamo: $a^2 \equiv b^2 \pmod{m}$, $a^3 \equiv b^3 \pmod{m}$, $\ldots$, $a^n \equiv b^n \pmod{m}$.

Propozicija

Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.

Dokaz: Neka je $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$, gdje su $c_i \in \mathbb{Z}$.

Budući da je $a \equiv b \pmod{m}$, uzastopnom primjenom prethodne Propozicije dobivamo: $a^2 \equiv b^2 \pmod{m}$, $a^3 \equiv b^3 \pmod{m}$, $\ldots$, $a^n \equiv b^n \pmod{m}$.

Tada je $c_i a^i \equiv c_i b^i \pmod{m}$ i konačno:

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \cdots + c_0 \pmod{m}.$$

$\square$

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$*.*
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$*, onda je* $x \equiv y \pmod{m}$*.*

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$.
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$, *onda je* $x \equiv y \pmod{m}$.

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$.

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$.
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$, *onda je* $x \equiv y \pmod{m}$.

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$.

Sada imamo: $\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z$, tj. $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y - x)$.

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$*.*
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$*, onda je* $x \equiv y \pmod{m}$*.*

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$.

Sada imamo: $\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z$, tj. $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y - x)$.

No, brojevi $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ su relativno prosti, pa zaključujemo da $\frac{m}{(a,m)}$ dijeli $y - x$, tj. da je $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$.
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$*, onda je* $x \equiv y \pmod{m}$.

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$.

Sada imamo: $\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z$, tj. $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y - x)$.

No, brojevi $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ su relativno prosti, pa zaključujemo da $\frac{m}{(a,m)}$ dijeli $y - x$, tj. da je $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Obrnuto, ako je $x \equiv y \pmod{\frac{m}{(a,m)}}$, onda po prethodno dokazanoj Propoziciji dobivamo $ax \equiv ay \pmod{\frac{am}{(a,m)}}$.

Teorem

Vrijedi: $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$*.*
Specijalno, ako je $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$*, onda je* $x \equiv y \pmod{m}$*.*

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$.

Sada imamo: $\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z$, tj. $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y - x)$.

No, brojevi $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ su relativno prosti, pa zaključujemo da $\frac{m}{(a,m)}$ dijeli $y - x$, tj. da je $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Obrnuto, ako je $x \equiv y \pmod{\frac{m}{(a,m)}}$, onda po prethodno dokazanoj Propoziciji dobivamo $ax \equiv ay \pmod{\frac{am}{(a,m)}}$.

No, (a, m) je djelitelj od a, pa dobivamo $ax \equiv ay \pmod{m}$. $\square$

Definicija

Skup $\{x_1, \cdots, x_m\}$ *se zove potpuni sustav ostataka modulo m ako za svaki* $y \in \mathbb{Z}$ *postoji točno jedan* x_j *takav da je* $y \equiv x_j \pmod{m}$. *Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Definicija

Skup $\{x_1, \cdots, x_m\}$ *se zove potpuni sustav ostataka modulo m ako za svaki* $y \in \mathbb{Z}$ *postoji točno jedan* x_j *takav da je* $y \equiv x_j \pmod{m}$. *Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Očito je da postoji beskonačno mnogo potpunih sustava ostataka modulo m. Jedan od njih je tzv. sustav najmanjih nenegativnih ostataka:

$$\{0, 1, \ldots, m-1\}.$$

Definicija

Skup $\{x_1, \cdots, x_m\}$ *se zove potpuni sustav ostataka modulo* m *ako za svaki* $y \in \mathbb{Z}$ *postoji točno jedan* x_j *takav da je* $y \equiv x_j \pmod{m}$*. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo* m *uzmemo po jedan član.*

Očito je da postoji beskonačno mnogo potpunih sustava ostataka modulo m. Jedan od njih je tzv. sustav najmanjih nenegativnih ostataka:

$$\{0, 1, \dots, m-1\}.$$

Pored njega, često se koristi i sustav apsolutno najmanjih ostataka. Ako je m neparan broj, apsolutno najmanji ostatci su

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2},$$

a ako je m paran, onda su to

$$-\frac{m-2}{2}, -\frac{m-4}{2}, \dots, -1, 0, 1, \dots, \frac{m-2}{2}, \frac{m}{2}.$$

Teorem

Neka je $\{x_1, \ldots, x_m\}$ *potpuni sustav ostataka modulo* m, *te neka je* $(a, m) = 1$. *Tada je* $\{ax_1, \ldots, ax_m\}$ *također potpuni sustav ostataka modulo* m.

Dokaz: Dovoljno je dokazati da je $ax_i \not\equiv ax_j \pmod{m}$ za $i \neq j$.

Teorem

Neka je $\{x_1, \ldots, x_m\}$ *potpuni sustav ostataka modulo* m*, te neka je* $(a, m) = 1$*. Tada je* $\{ax_1, \ldots, ax_m\}$ *također potpuni sustav ostataka modulo* m*.*

Dokaz: Dovoljno je dokazati da je $ax_i \not\equiv ax_j \pmod{m}$ za $i \neq j$.

Pretpostavimo da je $ax_i \equiv ax_j \pmod{m}$. Tada ranije dokazani Teorem povlači da je $x_i \equiv x_j \pmod{m}$, tj. $i = j$. $\square$

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je svaki cijeli broj x koji je zadovoljava.

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je svaki cijeli broj x koji je zadovoljava.

Ako je x_1 neko rješenje ove kongruencije, a $x_2 \equiv x_1 \pmod{m}$, onda je x_2 također rješenje.

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je svaki cijeli broj x koji je zadovoljava.

Ako je x_1 neko rješenje ove kongruencije, a $x_2 \equiv x_1 \pmod{m}$, onda je x_2 također rješenje.

Dva rješenja x i x' smatramo ekvivalentnim ako je $x \equiv x' \pmod{m}$. Broj rješenja kongruencije je broj neekvivalentnih rješenja.

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$.

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$.

Odavde je očito da $(a, m)|b$.

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$.

Odavde je očito da $(a, m)|b$.

Pretpostavimo sada da $d = (a, m)$ dijeli b.

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$.

Odavde je očito da $(a, m)|b$.

Pretpostavimo sada da $d = (a, m)$ dijeli b.

Stavimo $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$. Sada trebamo riješiti kongruenciju $a'x \equiv b' \pmod{m'}$.

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ *ima rješenja ako i samo ako* $d = (a, m)$ *dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$.

Odavde je očito da $(a, m)|b$.

Pretpostavimo sada da $d = (a, m)$ dijeli b.

Stavimo $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$. Sada trebamo riješiti kongruenciju $a'x \equiv b' \pmod{m'}$.

No, ona ima točno jedno rješenje modulo m'. Zaista, budući da je $(a', m') = 1$ kad x prolazi potpunim sustavom ostataka modulo m' i $a'x$ prolazi tim istim sustavom, tj. svaki ostatak modulo m' (pa tako i b') se dobiva točno za jedan x iz potpunog sustava ostataka modulo m'.

Jasno je da ako je x' neko rješenje od $a'x' \equiv b' \pmod{m'}$, onda su sva rješenja od $ax \equiv b \pmod{m}$ u cijelim brojevima dana sa $x = x' + nm'$, za $n \in \mathbb{Z}$, a sva međusobno neekvivalentna rješenja sa $x = x' + nm'$, gdje je $n = 0, 1, \ldots, d - 1$.

Jasno je da ako je x' neko rješenje od $a'x' \equiv b' \pmod{m'}$, onda su sva rješenja od $ax \equiv b \pmod{m}$ u cijelim brojevima dana sa $x = x' + nm'$, za $n \in \mathbb{Z}$, a sva međusobno neekvivalentna rješenja sa $x = x' + nm'$, gdje je $n = 0, 1, \ldots, d-1$.

Dakle, ako d dijeli b, onda kongruencija $ax \equiv b \pmod{m}$ ima točno d rješenja modulo m. $\square$

Iz prethodnog Teorema slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno.

Iz prethodnog Teorema slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno.

Ovo pak povlači da skup ostataka $\{0, 1, \ldots, p-1\}$ pri dijeljenju sa p, uz zbrajanje i množenje $\pmod{p}$, čini polje.

Iz prethodnog Teorema slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno.

Ovo pak povlači da skup ostataka $\{0, 1, \ldots, p-1\}$ pri dijeljenju sa p, uz zbrajanje i množenje $\pmod{p}$, čini polje.

To polje se obično označava sa $\mathbb{Z}_p$ ili $\mathbb{F}_p$.