Najveći zajednički djelitelj i Euklidov algoritam

Adian Anibal Santos Sepčić

14.1.2024.

1. Najveći zajednički djelitelj

Znati kako brzo i jednostavno pronaći najveći zajednički djelitelj dva broja ili dva izraza je matematički alat kojim bi svaki malo ozbiljniji natjecatelj iz matematike trebao znati dobro baratati. Srećom, ovo je nešto što svakako možete postići poznavanjem i primjenom samo tri vrlo jednostavna svojstva najvećeg zajedničkog djelitelja (**leme 1.2, 1.3, 1.4**), koja su u kombinaciji dovoljno moćna da gotovo svaki izraz s najvećim zajedničkim djeliteljem svedu na najjednostavniji mogući oblik.

Definicija 1.1

Najveći zajednički djelitelj dva cijela broja a i b označava se kao $D(a,b)$ i definiran je kao najveći prirodan broj koji dijeli i jedan i drugi, osim za $D(0,0)$. Definiramo $D(0,0)=0$, iz razloga koji će možda biti jasniji iz dokaza idućih lema.

Lema 1.2

Za sve cijele brojeve a, b, c vrijedi da $D(ac,bc) = c \cdot D(a,b)$.

Dokaz.
Ako $\mathbf{c \neq 0}, \mathbf{(a,b) \neq (0,0)}$
Vrijedi ekvivalencija tvrdnji :
$d|a$ i $d|b \iff dc|ac$ i $dc|bc$
Znači, najveći prirodan broj d koji zadovoljava lijevu stranu (postoji, jer $(a,b) \neq (0,0)$) isti je kao najveći broj d koji zadovoljava desnu stranu. Po definiciji najvećeg zajedničkog djelitelja tu jednakost možemo izraziti na idući način:

$$D(a,b) = \frac{D(ac,bc)}{c} \implies D(ac,bc) = c \cdot D(a,b)$$

Ako $\mathbf{c = 0}$, tada $D(ac,bc) = c \cdot D(a,b) = 0$
Ako $\mathbf{a = b = 0}$, tada $D(ac,bc) = D(a,b) = D(0,0) = 0$, pa $D(ac,bc) = c \cdot D(a,b) = 0$ □

Lema 1.3

Elementarni oblik:
Za sve cijele brojeve a, b i k vrijedi $D(a,b) = D(a, b+ka)$.

Modularni oblik:
Ako su a, b_1 i b_2 cijeli brojevi takvi da $b_1 \equiv b_2 \pmod{a}$, tada $D(a,b_1) = D(a,b_2)$.

Dokaz.
Ako $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{0}, \mathbf{0})$
$D(a,b) \mid a,\ D(a,b) \mid b \implies D(a,b) \mid b + ka$
$\implies$ Najveći zajednički djelitelj a i b je zajednički djelitelj a i $b+ka$, pa $D(a,b) \leq D(a, b+ka)$.

$D(a, b+ka) \mid a,\ D(a, b+ka) \mid b+ka \implies D(a, b+ka) \mid (b+ka) - ka \implies D(a, b+ka) \mid b$
$\implies$ Najveći zajednički djelitelj a i $b+ka$ je zajednički djelitelj a i b, pa $D(a, b+ka) \leq D(a,b)$.

Znači, dobivamo $D(a,b) \leq D(a, b+ka)$ i $D(a, b+ka) \leq D(a,b)$, pa mora vrijediti
$D(a,b) = D(a, b+ka)$.

Ako $\mathbf{a = b = 0}$, tada tvrdnja vrijedi, jer $D(0,0) = D(0, 0 + k \cdot 0) = 0$ □

Lema 1.4

Ako su cijeli brojevi a i b relativno prosti, to jest $D(a,b) = 1$, tada za sve cijele brojeve c vrijedi

$$D(a, bc) = D(a, c)$$

Dokaz.
Ako $(\mathbf{a}, \mathbf{c}) \neq (\mathbf{0}, \mathbf{0})$
Neka $d = D(a,c)$.
Neka $a = da_1$ i $c = dc_1$, pa su a_1 i c_1 relativno prosti cijeli brojevi.
$D(a, bc) = D(da_1, bdc_1) = d \cdot D(a_1, b_1 c_1)$
No, kako su a_1 i b relativno prosti (jer su a i b relativno prosti) te su a_1 i c_1 relativno prosti, a_1 nema zajednički prosti faktor niti sa b_1, niti sa c_1, pa tako nema niti zajednički prosti faktor sa $b_1 c_1$. Stoga, a_1 i $b_1 c_1$ su relativno prosti, pa $D(a_1, b_1 c_1) = 1$.
$\implies D(a, bc) = d \cdot D(a_1, b_1 c_1) = d = D(a, c)$

Ako $\mathbf{a = c = 0}$, tada $D(a, bc) = D(a, c) = D(0,0) = 0$ □

2. Euklidov algoritam

Euklidov algoritam je na osnovnoj razini samo način za određivanje najvećeg zajedničkog djelitelja dva prirodna broja. Ono što nam omogućuje ovo je svojstvo algoritma da uvijek završava na najvećem zajedničkom djelitelju dva početna broja (lema 2.2). Za ovu svrhu je najučinkovitije koristiti ubrzani Euklidov algoritam (definicija 2.3). No, Euklidov algoritam također može biti ključno sredstvo dokazivanja i otkrivanja nekih vrlo zanimljivih formula koje ćete dokazivati u zadacima nakon uvoda. Također, Euklidov algoritam izvan domene prirodnih brojeva ima još neka zanimljiva svojstva (zadaci 9,12,13).

Definicija 2.1

Euklidov algoritam definiramo kao opetovano primjenjivanje funkcije E na par nenegativnih realnih brojva (x, y) dok drugi ne bude jednak 0, tada kažemo da algoritam **završava**.

$$E(x, y) = (max(x, y) - min(x, y), min(x, y))$$

Primjer: $(24, 10) \xrightarrow{E} (14, 10) \xrightarrow{E} (4, 10) \xrightarrow{E} (6, 4) \xrightarrow{E} (2, 4) \xrightarrow{E} (2, 2) \xrightarrow{E} (0, 2) \xrightarrow{E} (2, 0)$ (kraj)

Napomena: Postoji mnogo pomalo različitih definicija Euklidovog algoritma i ovako definirana funkcija E nije iz opće literature, pa **nemojte na natjecanju pisati $\mathbf{E(x, y)}$ bez da objasnite što je funkcija $\mathbf{E}$**, kako biste recimo učinili za $D(x, y)$.

Lema 2.2

Euklidov algoritam počevši od para prirodnih brojeva (a, b) uvijek će završiti u paru $(D(a, b), 0)$.

Dokaz.

Dokažimo da će Euklidov algoritam u ovom slučaju završiti

Ako je (a, b) par prirodnih brojeva, neka $E(a, b) = (a_1, b_1)$. Tada vrijedi

$a_1 + b_1 = (max(a, b) - min(a, b)) + min(a, b) = max(a, b) < a + b$

Znači, korak $(a, b) \xrightarrow{E} (a_1, b_1)$ smanjit će zbroj brojeva u paru sve dok su početni brojevi prirodni. Znači, u nekom trenutku će neki od brojeva u paru postati 0, jer će inače nakon nekog broja koraka zbroj brojeva u paru postati negativan, što je nemoguće jer će brojevi u paru uvijek ostati nenegativni. Ako je drugi broj u ovom paru 0, tada algoritam završava, a ako je prvi broj u paru 0, tada će idući par imati 0 na drugom mjestu:

$(a, b) \xrightarrow{E} (a_1, b_1) \xrightarrow{E} \ldots \xrightarrow{E} (d, 0)$ (kraj) ILI $(a, b) \xrightarrow{E} (a_1, b_1) \xrightarrow{E} \ldots \xrightarrow{E} (0, d) \xrightarrow{E} (d, 0)$ (kraj)

Sada kada znamo da će algoritam završiti, recimo da završava u paru $(d, 0)$. Primjetimo sada da po lemi 1.3 najveći zajednički djelitelj ostaje isti nakon svakog koraka Euklidovog algoritma, pa vrijedi:

$d = D(d, 0) = D(a, b) \implies$ Algoritam završava u $(D(a, b), 0)$ □

Definicija 2.3

Ubrzani Euklidov algoritam definiramo kao opetovano primjenjivanje funkcije E^+ na par nenegativnih cijelih brojeva dok neki ne bude jednak 0, tada kažemo da algoritam **završava**.

$$E^+(x, y) = (max(x, y)\%min(x, y), min(x, y))$$

Ovdje definiramo $a\%b$ kao ostatak pri dijeljenju a brojem b.

Primjer: $(24, 10) \xrightarrow{E^+} (4, 10) \xrightarrow{E^+} (2, 4) \xrightarrow{E^+} (0, 2)$ (kraj)

Napomena: Postoji mnogo pomalo različitih definicija Euklidovog algoritma i ovako definirana funkcija E^+ nije iz opće literature, pa **nemojte na natjecanju pisati $\mathbf{E^+(x, y)}$ bez da objasnite što je funkcija $\mathbf{E^+}$**, kako biste recimo učinili za $D(x, y)$.

Lema 2.4

Ubrzani Euklidov algoritam s početkom u paru prirodnih brojeva (a, b) završava u paru $(0, D(a, b))$.

Dokaz.
Ako su x i y nenegativni cijeli brojevi takvi da $x <= y$, tada postoje $k \in \mathbb{N}$ i $d \in \mathbb{N}_0$ takvi da $y = kx + d$. Znači, primjenjivanje E^+ na (x, y) isto je kao primjenjivanje E na (x, y) k puta :
$(x, y) \xrightarrow{E^+} (d, y)$
$(x, y) \xrightarrow{E} ((k-1)y + d, y) \xrightarrow{E} \ldots \xrightarrow{E} (d, y)$
Zbog ovoga ubrzani Euklidov algoritam poprima iste vrijednosti kao običan Euklidov algoritam, s time da neke preskače i s time da prestaje prvi put kada je neki broj u dobivenom paru jednak 0. To će se dogoditi kada manji broj u paru dijeli veći i tada će prvi broj biti 0 te će tako algoritam završiti:
$(x, kx) \xrightarrow{E^+} (0, x)$ (kraj)
Kako Euklidov algoritam ne mijenja najveći zajednički djelitelj, u ubrzanom Euklidovom algoritmu će konačan najveći zajednički djelitelj također biti $D(a, b)$, pa nužno završava u paru $(0, D(a, b))$. □

Lakši zadaci

1. Odredi najveći zajednički djelitelj 1649 i 816.
2. Dokaži da su dva uzastopna prirodna broja uvijek relativno prosta.
3. Ako su a i b relativno prosti prirodni brojevi, dokaži da su za sve prirodne brojeve n brojevi a^n i $a + b$ također relativno prosti.
4. Ako su a i b relativno prosti prirodni brojevi, dokaži da $D(a + b, a^2 - ab + b^2) \mid 3$.

Umjereni zadaci

5. Neka su $\frac{a}{b}$ i $\frac{c}{d}$ potpuno skraćeni pozitivni razlomci.

   (a) Dokaži da će Euklidov algoritam s početkom u $(\frac{a}{b}, \frac{c}{d})$ završiti nakon konačno mnogo koraka

   (b) Odredi u kojem paru brojeva Euklidov algoritam s početkom u $\left(\frac{a}{b}, \frac{c}{d}\right)$ završava.

   Napomena: Pogledaj definiciju Euklidovog algoritma u uvodu i lemu 2.2

6. Neka je a neka znamenka od 1 do 9 i neka je x_k općenito k-teroznamenkasti broj oblika $x_k = \overline{aa \ldots a}$. Dokaži da $D(x_n, x_m) = x_{D(n,m)}$ za sve prirodne brojeve n i m.
   (**Primjer:** $D(222222, 222222222) = 222$ jer $D(6, 9) = 3$).

7. Definiramo Fibonaccijev niz $F_0, F_1, F_2 \ldots$ tako da je 0-ti član $F_0 = 0$, prvi član $F_1 = 1$ i svaki idući član je zbroj prethodna dva ($F_{n+1} = F_n + F_{n-1}$ za sve prirodne brojeve n). Dokaži da su svaka dva uzastopna Fibonaccijeva broja relativno prosta, to jest da za sve prirodne brojeve n vrijedi:

$$D(F_{n-1}, F_n) = 1$$

8. Neka su a i b relativno prosti prirodni brojevi. Dokaži da izraz $D(a^n + b^n, a^{n+1} + b^{n+1})$ gdje je n prirodan broj može jedino poprimiti vrijednosti 1 i 2.

Teži zadaci

9. Kakvi moraju biti pozitivni realni brojevi x i y da bi Euklidov algoritam s početkom u (x, y) završio nakon konačno mnogo koraka?

10. Za sve prirodne brojeve a, dokaži da $D(a^a + (a+1)^{a+1}, a^{a+1} + (a+1)^a) \mid a^2 + a - 1$.

11. Neka su a i b relativno prosti prirodni brojevi takvi da $a > b$. Dokaži da za sve prirodne brojeve n i m vrijedi iduća formula:

$$D(a^n - b^n, a^m - b^m) = a^{D(n,m)} - b^{D(n,m)}$$

12. Neka je φ pozitivno realno rješenje jednadžbe $\varphi^2 - \varphi - 1 = 0$ ($\varphi \approx 1.618$). Dokaži da za sve prirodne brojeve n vrijedi $E^n(1, \varphi) = (\frac{1}{\varphi^n}, \frac{1}{\varphi^{n-1}})$, gdje $E^n(x, y)$ označava funkciju E primijenjenu n puta na par pozitivnih realnih brojeva (x, y).

(**Primjer:** $E^3(10, 24) = E^2(14, 10) = E(4, 10) = (6, 4)$)
Napomena: Pogledaj definiciju funkcije E u uvodu.

Za najhrabrije

13. Koristeći rezultat iz prethodnog zadatka, dokaži iduću formulu za sve prirodne brojeve n:

$$E^n(1, \varphi) = ((-1)^n(F_{n+1} - F_n\varphi), (-1)^{n-1}(F_n - F_{n-1}\varphi)))$$

Napomena: $F_0, F_1, F_2 \ldots$ je Fibonaccijev niz, počevši od $F_0 = 0, F_1 = 1$.
Napomena: Pogledaj definiciju funkcije E u uvodu.

14. Za sve nenegativne cijele brojeve n i m dokaži da $D(F_n, F_m) = F_{D(n,m)}$.
Napomena: $F_0, F_1, F_2 \ldots$ je Fibonaccijev niz, počevši od $F_0 = 0, F_1 = 1$.
Napomena: $D(0, 0)$ je definiran kao 0.

3. Rješenja

1. *Odredi najveći zajednički djelitelj 1649 i 816.*
$D(1649, 816) = D(1649 - 2 \cdot 816) = D(17, 816) = 17$, jer $17 \mid 816$

2. *Dokaži da su dva uzastopna prirodna broja uvijek relativno prosta.*

Za sve $a \in \mathbb{N}$ vrijedi $D(a, a+1) = D(a, (a+1) - a) = D(a, 1) = 1$, jer $D(a, 1) \mid 1$.

3. *Ako su a i b relativno prosti prirodni brojevi, dokaži da su za sve prirodne brojeve n brojevi a^n i $a + b$ također relativno prosti.*

Brojevi a i $a + b$ su relativno prosti, jer $D(a, a+b) = D(a, (a+b) - a) = D(a, b) = 1$.
$\implies a^n$ i $a + b$ nemaju zajednički prosti faktor, jer a i $a + b$ nemaju, pa su relativno prosti.

4. *Ako su a i b relativno prosti prirodni brojevi, dokaži da $D(a + b, a^2 - ab + b^2) \mid 3$.*
$D(a + b, a^2 - ab + b^2) = D(a + b, a^2 - ab + b^2 - (a + b)^2) = D(a + b, -3ab) = D(a + b, 3ab)$
Primjetimo da $D(a + b, b) = D((a + b) - b, b) = D(a, b) = 1$ i da analogno $D(a + b, a) = 1$.
$\implies D(a + b, 3ab) = D(a + b, 3a) = D(a + b, 3)$, $D(a + b, 3) \mid 3$
$\implies D(a + b, a^2 - ab + b^2) \mid 3$

5. *Neka su $\frac{a}{b}$ i $\frac{c}{d}$ potpuno skraćeni pozitivni razlomci.*

(a) *Dokaži da će Euklidov algoritam s početkom u $(\frac{a}{b}, \frac{c}{d})$ završiti nakon konačno mnogo koraka.*

(b) *Odredi u kojem paru brojeva Euklidov algoritam s početkom u $\left(\frac{a}{b}, \frac{c}{d}\right)$ završava.*

Neka $E^n(x, y)$ označava funkciju E primijenjenu n puta na par pozitivnih realnih brojeva (x, y) (znači $E^n(x, y) = E(E(\ldots(x, y))\ldots)$) i neka $z \cdot (x, y)$ označava (xz, yz) za sve realne brojeve z. Sada primijetimo da ako je $z > 0$ vrijedi:
$E(xz, yz) = (max(xz, yz) - min(xz, yz), min(xz, yz))$
$E(xz, yz) = (z \cdot max(x, y) - z \cdot min(x, y), z \cdot min(x, y))$
$E(xz, yz) = z \cdot E(x, y)$

Znači, općenito vrijedi :
$E^n(xz, yz) = E^{n-1}(z \cdot E(x, y)) = E^{n-2}(z \cdot E^2(x, y)\ldots) = z \cdot E^n(x, y)$

$$E^n(xz, yz) = z \cdot E^n(x, y)$$

Koristeći ovo pravilo, možemo lako riješiti zadatak:
Neka je k broj koraka nakon kojeg Euklidov algoritam s početkom u (ad, bc) završava, znači $E^k(ad, bc) = (D(ad, bc), 0)$. Tada vrijedi:
$E^k(\frac{a}{b}, \frac{c}{d}) = \frac{1}{bd} E^k(ad, bc) = \frac{1}{bd}(D(ad, bc), 0) = (\frac{D(ad, bc)}{bd}, 0)$

Znači, nakon k koraka će Euklidov algoritam s početkom u $(\frac{a}{b}, \frac{c}{d})$ završiti u paru $(\frac{D(ad, bc)}{bd}, 0)$.

6. *Neka je a neka znamenka od 1 do 9 i neka je x_k općenito k-teroznamenkasti broj oblika $x_k = \overline{aa\ldots a}$. Dokaži da $D(x_n, x_m) = x_{D(n,m)}$ za sve prirodne brojeve n i m.*

***Za svrhu rješavanja zadatka, definirajmo $\mathbf{x_0 = 0}$**
Primijetimo da za sve nenegativne cijele brojeve a i b takve da $a \geq b$ vrijedi:
$x_a = x_{a-b} + 10^{a-b}x_b$ (*ovo možemo reći samo zato što smo definirali $x_0 = 0$)
$\implies D(x_a, x_b) = D(x_{a-b}, x_b)$
Ovo znači da vršenjem Euklidovog algoritma na indekse n i m možemo svesti izraz $D(x_n, x_m)$ na izraz $D(x_{D(n,m)}, x_0)$
$\implies D(x_n, x_m) = D(x_{D(n,m)}, x_0) = x_{D(n,m)}$

7. *Definiramo Fibonaccijev niz $F_0, F_1, F_2 \ldots$ tako da je 0-ti član $F_0 = 0$, prvi član $F_1 = 1$ i svaki idući član je zbroj prethodna dva ($F_{n+1} = F_n + F_{n-1}$ za sve prirodne brojeve n). Dokaži da su svaka dva uzastopna Fibonaccijeva broja relativno prosta, to jest da za sve prirodne brojeve n vrijedi:*

$$D(F_{n-1}, F_n) = 1$$

$D(F_{n-1}, F_n) = D(F_{n-1}, F_n - F_{n-1}) = D(F_{n-1}, F_{n-2}) = D(F_{n-3}, F_{n-2}) \ldots = D(F_0, F_1)$
$\implies D(F_{n-1}, F_n) = D(F_0, F_1) = D(0, 1) = 1$

8. *Neka su a i b relativno prosti prirodni brojevi. Dokaži da izraz $D(a^n + b^n, a^{n+1} + b^{n+1})$ gdje je n prirodan broj može jedino poprimiti vrijednosti 1 i 2.*

$D(a^n + b^n, a^{n+1} + b^{n+1}) = D(a^n + b^n, a^{n+1} + b^{n+1} - a(a^n + b^n))$
$D(a^n + b^n, a^{n+1} + b^{n+1}) = D(a^n + b^n, b^{n+1} - ab^n)$
$D(a^n + b^n, a^{n+1} + b^{n+1}) = D(a^n + b^n, b^n(b - a))$

$D(a^n + b^n, b^n) = D((a^n + b^n) - b^n, b^n) = D(a^n, b^n) = 1$, jer su a i b relativno prosti
$\implies D(a^n + b^n, b^n(b - a)) = D(a^n + b^n, b - a)$

$a^n + b^n \equiv 2a^n \pmod{b - a}$
$\implies D(a^n + b^n, b - a) = D(2a^n, b - a)$

$D(a, b - a) = D(a, (b - a) + a) = D(a, b) = 1$
$D(2a^n, b - a) = D(2, b - a)$, jer kako je a relativno prost sa $b - a$, a^n također jest
$\implies D(a^n + b^n, a^{n+1} + b^{n+1}) = D(2, b - a) \mid 2$
$\implies D(a^n + b^n, a^{n+1} + b^{n+1}) \in \{1, 2\}$

9. *Kakvi moraju biti pozitivni realni brojevi x i y da bi Euklidov algoritam s početkom u (x, y) završio nakon konačno mnogo koraka?*

Neka su a i b pozitivni realni brojevi takvi da $a > b$ i $a : b \notin \mathbb{Q}$.
Neka tada $(a_1, b_1) = E(a, b) = E(a - b, b)$.
$\implies a_1 : b_1 = \dfrac{a - b}{b} = a : b - 1 \notin \mathbb{Q}$

Znači, ako provodimo Euklidov algoritam počevši od dva broja kojima je omjer iracionalan, omjer dobivenih parova će uvijek biti iracionalan, pa nikada ne može biti jednak 0, što znači da algoritam nikada neće završiti.
$\implies$ Ako $x : y \notin \mathbb{Q}$, tada Euklidov algoritam s početkom u (x, y) ne završava.

Pretpostavimo sada suprotno
$\implies$ Neka $x : y = n : m$ gdje $n, m \in \mathbb{N}$ i neka $x = cn$, $y = cm$
Neka su n_k i m_k brojevi dobiveni provođenjem k koraka Euklidovog algoritma na n i m. Tada provođenjem tih k koraka na x i y dobivamo cn_k i cm_k. Znači, ako Euklidov algoritam s početkom u (n, m) završi nakon nekog broja koraka (a mora, jer $a, b \in \mathbb{N}$), nakon istog broja koraka će završiti i algoritam s početkom u (x, y).
$\implies$ Ako $x : y \in \mathbb{Q}$, tada Euklidov algoritam s početkom u (x, y) završava nakon konačno mnogo koraka. Stoga je rješenje zadatka:

$$x : y \in \mathbb{Q}$$

10. *Za sve prirodne brojeve a, dokaži da $D(a^a + (a+1)^{a+1}, a^{a+1} + (a+1)^a) \mid a^2 + a - 1$.*

$D(a^a + (a+1)^{a+1}, a^{a+1} + (a+1)^a)$
$= D(a^a + (a+1)^{a+1} - (a+1)(a^{a+1} + (a+1)^a), a^{a+1} + (a+1)^a)$
$= D(a^a - (a+1)a^{a+1}, a^{a+1} + (a+1)^a)$
$= D(a^a(a^2 + a - 1), a^{a+1} + (a+1)^a)$

$D(a, a^{a+1} + (a+1)^a) = D(a, (a+1)^a) = 1$ (jer $D(a, a+1) = D(a, 1) = 1$)
$\implies D(a^a(a^2 + a - 1), a^{a+1} + (a+1)^a) = D(a^2 + a - 1, a^{a+1} + (a+1)^a) \mid a^2 + a - 1$
$\implies D(a^a + (a+1)^{a+1}, a^{a+1} + (a+1)^a) \mid a^2 + a - 1$

11. *Neka su a i b relativno prosti prirodni brojevi takvi da $a > b$. Dokaži da za sve prirodne brojeve n i m vrijedi iduća formula:*

$$D(a^n - b^n, a^m - b^m) = a^{D(n,m)} - b^{D(n,m)}$$

Ako su x i y neki prirodni brojevi takvi da $x > y$, tada:
$D(a^x - b^x, a^y - b^y)$
$= D(a^x - b^x - a^{x-y}(a^y - b^y), a^y - b^y)$
$= D(a^{x-y}b^y - b^x, a^y - b^y)$
$= D(b^y(a^{x-y} - b^{x-y}), a^y - b^y)$

No, $D(b^y, a^y - b^y) = D(b^y, a^y) = 1$, jer su a i b relativno prosti.
$\implies D(b^y(a^{x-y} - b^{x-y}), a^y - b^y) = D(a^{x-y} - b^{x-y}, a^y - b^y)$
$\implies D(a^x - b^x, a^y - b^y) = D(a^{x-y} - b^{x-y}, a^y - b^y)$

Ovo znači da provođenjem Euklidovog algoritma na eksponente n i m možemo svesti izraz $D(a^n - b^n, a^m - b^m)$ na izraz $D(a^{D(n,m)} - b^{D(n,m)}, a^0 - b^0)$
$\implies D(a^n - b^n, a^m - b^m) = D(a^{D(n,m)} - b^{D(n,m)}, 0) = a^{D(n,m)} - b^{D(n,m)}$

12. *Neka je φ pozitivno realno rješenje jednadžbe $\varphi^2 - \varphi - 1 = 0$ ($\varphi \approx 1.618$). Dokaži da za sve prirodne brojeve n vrijedi $E^n(1, \varphi) = (\frac{1}{\varphi^n}, \frac{1}{\varphi^{n-1}})$, gdje $E^n(x, y)$ označava funkciju E primijenjenu n puta na par pozitivnih realnih brojeva (x, y).*

Malim manipulacijama formule $\varphi^2 - \varphi - 1 = 0$ možemo doći do idućeg rezultata:
$\varphi^2 - \varphi - 1 = 0$
$\varphi^2 - \varphi = 1$
$\varphi - 1 = \frac{1}{\varphi}$

Uz ovaj rezultat možemo riješiti zadatak indukcijom:

Baza ($\mathbf{n = 1}$):

Kako $\varphi > 1$, vrijedi $E(1, \varphi) = (\varphi - 1, 1) = (\frac{1}{\varphi}, 1)$

Korak ($\mathbf{n \to n + 1}$):

Pretpostavimo da $E^n(1, \varphi) = (\frac{1}{\varphi^n}, \frac{1}{\varphi^{n-1}})$ za neki $n \in \mathbb{N}$.

Kako $\varphi > 1$, vrijedi $\frac{1}{\varphi^n} < \frac{1}{\varphi^{n-1}}$, pa onda:

$$E^{n+1}(1, \varphi) = E(\frac{1}{\varphi^n}, \frac{1}{\varphi^{n-1}}) = (\frac{1}{\varphi^{n-1}} - \frac{1}{\varphi^n}, \frac{1}{\varphi^n}) = (\frac{\varphi - 1}{\varphi^n}, \frac{1}{\varphi^n}) = (\frac{1}{\varphi^{n+1}}, \frac{1}{\varphi^n})$$

Kako su baza i korak indukcije sigurno zadovoljeni, tvrdnja zadatka je dokazana.

13. *Koristeći rezultat iz prethodnog zadatka, dokaži iduću formulu za sve prirodne brojeve n:*

$$E^n(1, \varphi) = ((-1)^n(F_{n+1} - F_n\varphi), (-1)^{n-1}(F_n - F_{n-1}\varphi)))$$

Pazi:
Ovaj zadatak rješava se indukcijom, ali valja napomenuti da je vrlo jednostavno previdjeti najbitniji detalj čitavog dokaza (podcrtani dio dokaza), znači rješenje nije *"samo indukcija"*. Ako bismo ovaj dio dokaza izostavili i zanemarili kao da je *samo detalj*, lako bismo mogli dokazati razne besmilice, poput iduće **netočne** formule, koja ne radi niti za $n = 2$:

$$E^n(1, \pi) = ((-1)^n(F_{n+1} - F_n\pi), (-1)^{n-1}(F_n - F_{n-1}\pi)))$$

Dokaz:
Neka $E^n(1, \varphi) = (a_n, b_n)$.
Tada iz rezultata prethodnog zadatka znamo da za sve $n \in \mathbb{N}$ vrijedi $a_n < b_n$, znači:

$$(a_{n+1}, b_{n+1}) = E(a_n, b_n) = (b_n - a_n, a_n)$$

Ostatak zadatka rješavamo indukcijom:

Baza ($\mathbf{n = 1}$):
$E(1, \varphi) = (\varphi - 1, 1) = ((-1)(1 - 1\varphi), 1 - 0\varphi)))$

Korak $(\mathbf{n \to n+1})$
Pretpostavimo da formula vrijedi za neki $n \in \mathbb{N}$.
Tada će vrijediti:
$b_{n+1} = a_n = (-1)^n(F_{n+1} - F_n\varphi)$

$a_{n+1} = b_n - a_n$
$a_{n+1} = (-1)^{n-1}(F_n - F_{n-1}\varphi) - ((-1)^n(F_{n+1} - F_n\varphi))$
$a_{n+1} = (-1)^{n+1}(F_n - F_{n-1}\varphi + F_{n+1} - F_n\varphi)$
$a_{n+1} = (-1)^{n+1}((F_n + F_{n+1}) - (F_{n-1} + F_n)\varphi)$
$a_{n+1} = (-1)^{n+1}(F_{n+2} - F_{n+1}\varphi)$

Ako samo uvrstimo dobivene formule za a_{n+1} i b_{n+1} u formulu $E^{n+1}(1, \varphi) = (a_{n+1}, b_{n+1})$, dobivamo dokaz koraka indukcije, koji uz bazu čini potpun dokaz tvrdnje zadatka:

$$E^{n+1}(1, \varphi) = ((-1)^{n+1}(F_{n+2} - F_{n+1}\varphi), (-1)^n(F_{n+1} - F_n\varphi)))$$

14. *Za sve nenegativne cijele brojeve n i m dokaži da $D(F_n, F_m) = F_{D(n,m)}$.*

Čarobna formula koja će nam omogućiti da zadatak svedemo na primjenu Euklidovog algoritma je iduća:

$$\forall n \in \mathbb{N}_0, m \in \mathbb{N} : \ F_{n+m} \equiv F_{m+1}F_n \pmod{F_m}$$

Ova tvrdnja vrijedi, jer ako promatramo Fibonaccijev niz modulo F_m do $(m+1)$-vog člana, dobivamo iduću situaciju:
$0 \to 1 \to 1 \to 2 \to 3 \to 5 \ldots F_{m-1} \to 0 \to F_{m+1} \to F_{m+1} \to 2F_{m+1} \to 3F_{m+1} \to 5F_{m+1} \ldots$
Znači, kada ponovno zapisujemo Fibonaccijev niz, sada krećući od m-tog člana, ne krećemo od $F_0 \equiv 0 \pmod{F_m}$, $F_1 \equiv 1 \pmod{F_m}$, nego od F_{m+1} puta većeg početnog stanja:
$F_m \equiv 0 \pmod{F_m}$, $F_{m+1} \equiv F_{m+1} \pmod{F_m}$

Znači, cijeli ostatak niza biti će pomnožen sa F_{m+1} modulo F_m. Zato mora vrijediti
$F_{n+m} \equiv F_{m+1}F_n \pmod{F_m}$.

Uz ovo, još dokazujemo tvrdnju 7. zadatka:
$D(F_m, F_{m+1}) = D(F_m, F_{m+1} - F_m) = D(F_m, F_{m-1}) = D(F_{m-2}, F_{m-1}) \ldots = D(F_0, F_1)$
$\implies D(F_m, F_{m+1}) = D(F_0, F_1) = D(0, 1) = 1$
$\implies F_m$ i F_{m+1} su relativno prosti

Sada imamo dovoljno informacija da dovršimo dokaz na klasičan način:
Ako su n i m prirodni brojevi takvi da vrijedi $n \geq m$, tada vrijedi:
$D(F_n, F_m) = D(F_{n-m}F_{m+1}, F_m)$ (jer $F_n \equiv F_{n-m}F_{m+1} \pmod{F_m}$)
$D(F_{n-m}F_{m+1}, F_m) = D(F_{n-m}, F_m)$ (jer $D(F_m, F_{m+1}) = 1$)

$$\implies D(F_n, F_m) = D(F_{n-m}, F_m)$$

Ova formula znači da možemo primjenjivanjem Euklidovog algoritma na indekse n i m svesti izraz $D(F_n, F_m)$ na izraz $D(F_{D(n,m)}, 0)$.
$\implies D(F_n, F_m) = D(F_{D(n,m)}, 0) = F_{D(n,m)}$
$\implies D(F_n, F_m) = F_{D(n,m)}$