MetaMath - djeljivost, prosti brojvi i kanonski zapis

Jakov Cigrovski

10. listopada 2022.

1 Primjeri

1. Odredi sve parove prirodnih brojeva (x, y)a koje vrijedi $x^2 - y! = 2016$

   Dokaz. Broj 2016 je djeljiv brojem 32 i nije djeljiv brojem 64.

   Uočimo da ne može vrijediti $y = 1$. Dakle, mora vrijediti $y > 2$ pa je $y!$ paran. Zato x mora biti paran broj. Budući da su onda i x^2 i 2016 djeljivi s 4, i $y!$ mora biti djeljivo s 4, pa je $y \geq 4$. Sada možemo zaključiti da je $y!$ djeljivo sa 8, pa x^2 mora biti djeljivo s 8.

   To znači da x mora biti djeljiv s 4, odnosno da je x^2 djeljivo sa 16. Dakle, $y!$ je djeljivo sa 16, pa je $y \geq 6$.

   Ako je $y \geq 8$ onda je $y!$ djeljivo sa 128, a posebno i s 32 pa x^2 mora biti djeljivo s 32.

   To znači da $x$nmora biti djeljiv barem sa 8, odnosno da je x^2 djeljivo i sa 64.

   Iz toga bi slijedilo da je 2016 djeljivo sa 64, što nije istina. Zato je $y \leq 7$.
   Provjerom vidimo da $2016 + 6!$ nije potpun kvadrat, a $2016 + 7! = 7056 = 84^2$, pa je jedino rješenje $(x, y) = (84, 7)$.

2. Skup prostih brojeva je beskonačan.

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

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

   Uočimo da n nije djeljiv s p_1 (jer p_1 dijeli $p_1 p_2 \ldots p_k$, a ne dijeli 1), isto tako pokažemo da nije djeljiv ni s $p_2, p_3, \ldots, p_k$. Dakle, svaki prosti djelitelj od n je različit od $p_1 p_2 \ldots p_k$. Znamo da je n produkt prostih brojeva, pa postoji p koji dijeli n. Tako smo dobili novi prost broj pa je početna pretpostavka kriva i prostih brojeva ne postoji konačno, već beskonačno.

3. Odredite sve prirodne brojeve n za koje je $n^4 + 4^n$ prost broj.

   Dokaz. Koristiti ćemo poznati identitet Sophie Germain:

   $$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab).$$

   Sada se vratimo na naš problem, ako je n paran broj, $n^4 + 4^n$ je također paran i veći od 2 pa nije prost. Postavimo $n = 2k + 1$.

   $$n^4 + 4^n = n^4 + 4^{2k+1} = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4 = (n^2 + 2^{2k+1} + 2^{k+1}n)(n^2 + 2^{2k+1} - 2^{k+1}n)$$

   Kako bi $n^4 + 4^n$ bio prost broj moralo bi vrijediti $n^2 + 2^{2k+1} - 2^{k+1}n = 1$, prema A-G nejednakosti dobivamo $n^2 + 2^{2k+1} - 2^{k+1}n = n^2 + 2^{2k} + 2^{2k} - 2^{k+1}n \geq 2^{2k}$ što je veće od 1 za $k > 0$ pa je jedina opcija $n = 1,\ k = 0$ i vidimo u tom slučaju $n^4 + 4^n = 5$ jest prost broj.

4. Pokažite da za svaki $n \geq 10$ broj $2^{2^n} + 2^{2^{n-1}} + 1$ ima barem n različitih prostih faktora.

Dokaz. Često kada se traži da se tvrdnja dokaže za svaki prirodan broj koristimo metodu matematičke indukcije. Pokažemo prvo da tvrdnja vrijedi za bazu $n = 1$, $2^{2^n} + 2^{2^{n-1}} + 1 = 6$ te Za $n = 2$, $2^{2^n} + 2^{2^{n-1}} + 1 = 21 = 3 \cdot 7$. Pretpostavimo sada da za neki $n \geq 2$, $2^{2^n} + 2^{2^{n-1}} + 1$ ima barem n različitih prostih faktora. Koristeći identitet $x^4 + x^2 + 1 = (x^2+1)^2 x^2 = (x^2 x + 1)(x^2 + x + 1)$ za $x = 2^{2^{n-1}}$ dobivamo

$$2^{2^{n+1}} + 2^{2^n} + 1 = (2^{2^n} - 2^{2^{n-1}} + 1)(2^{2^n} + 2^{2^{n-1}} + 1).$$

Kako je

$$NZD(2^{2^n} - 2^{2^{n-1}} + 1, 2^{2^n} + 2^{2^{n-1}} + 1) = NZD(2^{2^n} - 2^{2^{n-1}} + 1, 2 \cdot 2^{2^{n-1}}) = 1$$

zaključujemo $2^{2^n} - 2^{2^{n-1}} + 1$ ima prost faktor p koji ne dijeli $2^{2^n} + 2^{2^{n-1}} + 1$ pa slijedi da $2^{2^{n+1}} + 2^{2^n} + 1$ ima barem $n+1$ različitih prostih faktora.

2 Lakši lanac

1. Neka je $a = 123456789$ te $N = a^3 - 2a^2 - 3a$. Dokažite da je N djeljiv s 540.

Dokaz. Kako je $540 = 2^2 \cdot 3^3 \cdot 5$, dovoljno je pokazati da je N djeljiv s 4, 5 i 27. Faktorizacijom dobivamo $N = a(a-3)(a+1)$.

(a) a je neparan pa su $a+1$ i $a-3$ parni što znači da 4 dijeli N.

(b) $a + 1 = 123456790$ što je djeljivo s 5 pa 5 dijeli N.

(c) Zbroj znamenaka od a je 45 pa $9 \mid a$ pa lagano vidimo da onda $3 \mid a - 3$ te zaključujemo da 27 dijeli N

Pokazali smo za 4, 5 i 27 da dijele N pa i 540 dijeli N.

2. Dokažite da je najveća zajednička mjera brojeva $2n^2 + 3$ i $n^2 + n + 1$, 1 ili 7.

Dokaz. Korištenjem Euklidovog algoritma imamo:

$$\begin{aligned} M\left(2n^2+3, n^2+n+1\right) &= M\left(2n^2+3-2\left(n^2+n+1\right), n^2+n+1\right) = M\left(-2n+1, n^2+n+1\right) = \\ &= M\left(2n-1, 2n^2+2n+2\right) = M\left(2n-1, 2n^2+2n+2-n\left(2n-1\right)\right) = \\ &= M\left(2n-1, 3n+2\right) = M\left(2n-1, 3n+2-(2n-1)\right) = M\left(2n-1, n+3\right) = \\ &= M\left(2n-1-2(n+3), n+3\right) = M\left(-7, n+3\right) \in \{1, 7\} \end{aligned}$$

3. Postoji li n takav da je $n^2 + n + 1$ kvadrat prirodnog broja?

Dokaz. Vrijedi

$$(n+1)^2 = n^2 + 2n + 1 > n^2 + n + 1 > n^2.$$

Pa smo izraz smjestili između dva uzastopna kvadrata što znači da $n^2 + n + 1$ ne može biti kvadrat.

4. Pokažite da za svaki n možemo pronaći n uzastopnih složenih brojeva.

Dokaz. Uzmemo brojeve $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1$ koji su redom djeljivi s 2, 3, $\ldots$, $n+1$ i jasno vrijedi $(n+1)! + k > k$ za sve $k, n \in \mathbf{N}$.

5. Pokažite da prostih brojeva oblika $4k+3$ ima beskonačno mnogo.

Dokaz. Prvo primjetimo da množenjem dva broja oblika $4k+1$ i $4l+1$ dobivamo opet broj istog oblika $(4k+1)(4l+1) = 4(4kl+k+l)+1$.

Pretpostavimo da su $p_1, p_2, \dots, p_m$ svi takvi prosti brojevi. Promotrimo broj

$$n = 4p_1p_2 \dots p_k - 1.$$

Uočimo da n nije djeljiv s p_1 (jer p_1 dijeli $4p_1p_2 \dots p_k$, a ne dijeli 1), isto tako pokažemo da nije djeljiv ni s $p_2, p_3, \dots, p_k$. Dakle, svaki prosti djelitelj od n je različit od $p_1p_2 \dots p_k$. Primjetimo da n daje ostatak 3 pri dijeljenju s 4, pa postoji p prost broj, oblika $4k+3$ koji dijeli n. Tako smo dobili novi prost broj pa je početna pretpostavka kriva i prostih brojeva oblika $4k+3$ ne postoji konačno, već beskonačno.

3 Teži lanac

1. Neka je 2^k+1 prost broj, za $k \geq 0$. Pokažite da je tada $k=0$ ili $k=2^n$ za neki $n \geq 0$.

Dokaz. Pretpostavimo da je $k > 0$ i da ima neparnog djelitelja p tako da je $k = ap$. Zapišimo

$$2^k + 1 = (2^a)^p + 1^p = (2^a+1)(2^{a(p-1)} - 2^{a(p-2)} + \cdots + 1).$$

Stoga vidimo da 2^a dijeli 2^k+1 pa nije prost. Zaključujemo da $k=0$ ili k nema neparnih djelitelja, to jest $k=2^n$.

2. Dokaži da je za svaki prirodan broj n, broj

$$\frac{n^4}{24} + \frac{n^3}{4} + \frac{11n^2}{24} + \frac{n}{4}$$

također prirodan.

Dokaz. Izraz možemo faktorizirati:

$$\frac{n^4}{24} + \frac{n^3}{4} + \frac{11n^2}{24} + \frac{n}{4} = \frac{n(n+1)(n+2)(n+3)}{24}$$

Među 4 uzastopna broja imamo 2 parna od kojih je 1 djeljiv s barem 4 te barem 1 broj je djeljiv s 3 pa zaključujemo da je izraz djeljiv s $2 \cdot 4 \cdot 3 = 24$ što smo i htjeli pokazati.

3. Odredite sve pozitivne cijele brojeve n za koje jednadžba

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

ima točno pet rješenja $(x,\, y)$ u skupu pozitivnih cijelih brojeva.

Dokaz. Množenjem s nxy jednadžba postaje

$$\begin{aligned} yn + xn &= xy \\ xy - xn - yn + n^2 &= n^2 \\ (x-n)(y-n) &= n^2 \end{aligned}$$

Promatrajmo rastav na proste faktore od n, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Broj rješenja jednadžbe jednak je broju rastava broja n^2 na dva faktora, tj.

$$(2\alpha_1+1)(2\alpha_2+1)\dots(2\alpha_k+1).$$

Taj broj je 5 samo u slučaju $k=1$ i $\alpha_1 = 2$. Svi traženi n-ovi su oblika p^2 gdje je p prost broj.

4. Neka su p, q prosti brojevi takvi da je p^2+pq+q^2 kvadrat. Pokažite da je p^2-pq+q^2 prost broj.

Dokaz. Promotrimo slučaj $p = q$. Tada je $p^2 + pq + q^2 = 3p^2$ što nije kvadrat pa odbacujemo ovaj slučaj. Nadalje, bez smanjenja općenitosti možemo pretpostaviti da je $p < q$. Označimo, $p^2 + pq + q^2 = k^2 \geq 1$. Ekvivalentna jednadžba glasi $(p + q - k)(p + q + k) = pq$ pa imamo 2 slučaja:

(a) $p+q-k=1$ i $p+q+k=pq$
Slijedi, $k = p+q-1$ iz čega dobivamo $p+q+(p+q-1) = pq \iff (p-2)(q-2) = 3 \iff p = 3, q = 5$ što u konačnici daje $p^2 - pq + q^2 = 9 - 15 + 25 = 19$ prost broj.

(b) $p+q-k=p$ i $p+q+k=q$
Ovaj slučaj je jasno nemoguć jer je $p+q+k > q$.

Slijedi tvrdnja zadatka.

4 Najteži lanac

1. Pronađite sve proste brojeve p, q, r takve da vrijedi jednakost $p^q = r - 1$.

Dokaz. U ovom zadatku još ključno je gledati parnosti i ostatke pri cjelobrojnom dijeljenju. Pogledajmo prvo može li r biti paran. Ako je $r = 2$ onda $p^q = 1$ što ne može biti jer su p i q prosti, a 1 nije. Zaključujemo r je neparan pa ga možemo zapisati u obliku $2k + 1$. Tada je $p^q = 2k + 1 - 1 = 2k$. S obzirom na to da je p prost, a jedini paran prost broj je 2 zaključujemo da $p = 2$. Sada imamo jednadžbu $2^q = 2k$. Pogledajmo slučaj kad je q paran, odnosno $q = 2$. Tada je $2^q = 2^2 = 4 = r - 1$ što bi značilo da je $r = 5$ i to je jedno zadovoljavajuće rješenje. Još moramo pogledati slučaj kad je q neparan. Tada ga možemo zapisati kao $q = 2l + 1$. Jednadžba sada glasi $2^{2l+1} = 2k$. odnosno $2 \cdot 4^l = 2k$ odnosno $4^l = k$. Sada gledajmo ostatak pri dijeljenju s 3. 4 i sve njegove potencije daju ostatak 1 pri dijeljenju s 3 pa i k mora davati ostatak jedan pri dijeljenju s 3. S obzirom na to da je $r = 2k + 1$ značilo bi da r daje ostatak 0 pri dijeljenju s 3 pa kako je r prost jedina opcija je da je on upravo 3. Ako je $r = 3$ onda bi moralo vrijediti da je $q = 1$, a q je prost. Zaključujemo jedino rješenje je $p = 2, q = 2, r = 5$.

2. Odredite sve proste brojeve p, q i r takve da je $p^{2q} + q^{2p} = r$.

Dokaz. Uvrštavanjem vidimo da $p = q = 2$ nije rješenje i da je $r > 4$. Pretpostavimo da su i p i q neparni: tada je $p^{2q} + q^{2p}$ parno, odnosno r je paran prost broj veći od 4 - kontradikcija. Znači da je ili p ili q paran, ali s obzirom da su oba broja prosta i znamo da $p = q = 2$ nije rješenje, točno jedan od ta dva broja je jednak 2. Bez smanjenja općenitosti, neka je $p = 2$ jer je jednadžba simetrična po pitanju p i q (ako je (p, q) rješenje onda je i (q, p)). Početna jednadžba onda postaje

$$2^{2q} + q^4 = r \Rightarrow 4^q + q^4 = r.$$

Zadatku možemo dalje pristupiti na dva načina:

1. način.
Možemo koristiti tzv. *Sophie Germain identity*, koji nam daje faktorizaciju $a^4 + 4b^4 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$. Znamo da je q neparan i veći ili jednak 3, pa ga možemo zapisati kao $q = 2k + 1$, $k \in \mathbb{N}$. Dalje, ako promotrimo 4^q, možemo ga raspisati kao:

$$4^q = 4^{2k+1} = 4 \cdot 4^{2k} = 4 \cdot 2^{4k} = 4 \cdot (2^k)^4.$$

Sada je naš početni izraz postao $(2k + 1)^4 + 4 \cdot (2^k)^4$, na što možemo primijeniti prije spomenut identitet:

$$(2k + 1)^4 + 4 \cdot (2^k)^4 =$$

$$= ((2k+1)^2 + 2\cdot(2^k)^2 - 2\cdot(2k+1)2^k)((2k+1)^2 + 2\cdot(2^k)^2 + 2\cdot(2k+1)2^k) =$$
$$= ((2k+1)^2 + 2^{2k+1} - 2^{k+1}(2k+1))((2k+1)^2 + 2^{2k+1} + 2^{k+1}(2k+1)).$$

Preostaje dokazati da je svaka od ovih zagrada veća od 1. Za $(2k+1)^2 + 2^{2k+1} + 2^{k+1}(2k+1)$ je to očito jer su svi članovi pozitivni i veći od 1. S druge strane, za $k \geq 3$ vrijedi $2^{2k+1} \geq 2^{k+1}(2k+1)$ (dokaz ostavljamo vama za vježbu - indukcija ili nešto drugo...) pa je $(2k+1)^2 + 2^{2k+1} - 2^{k+1}(2k+1) \geq (2k+1)^2 > 1$. Preostaje još provjera za $k = 1$ i $k = 2$ (isto ostavljamo vama - samo uvrštavanje...)
Dobili smo da je $4^q + q^4$ uvijek složen broj pa ova jednadžba nema rješenja za p, q, r proste.

2. način.
Promotrimo ovaj izraz modulo 5. 4^q daje ostatak 1 ili -1 pri djeljenju s 5, ovisno o parnosti broja q (-1 ako je q neparan, a 1 ako je q paran). Kako smo zaključili da je q neparan, znači da 4^q daje ostatak -1 pri dijeljenju s 5. S druge strane, q^4 daje ostatak 1 ili 0 pri dijeljenju s 5. Sada razlikujemo dva slučaja:

1. slučaj: q^4 je djeljiv s 5. Kako je q prost broj, a q^4 je djeljivo s 5 ako i samo ako je q djeljiv s 5, jedina mogućnost je $q = 5$. Preostaje provjeriti je li $4^5 + 5^4 = 1649$ prost broj. Kako je $1649 = 17 \cdot 97$, ovaj slučaj nema rješenja.
2. slučaj: q^4 daje ostatak 1 pri djeljenju s 5. Kako 4^q daje ostatak -1 pri djeljenju s 5, $4^q + q^4 \equiv -1 + 1 \equiv 0 \pmod 5$, odnosno r je djeljiv s 5. Kako je r prost broj, $r = 5$ je jedina mogućnost. Međutim, jednadžba $4^q + q^4 = 5$ nema rješenje u prostim brojevima jer $q = 1$ nije prost broj.
Zaključujemo da ne postoje prosti brojevi p, q, r takvi da je $p^{2q} + q^{2p} = r$.