MAT-KOL (Banja Luka) **ISSN 0354-6969 (o)**
XXIII (4)(2017), 241-268 **ISSN 1986-5828 (o)**
http://www.imvibl.org/dmbl/dmbl.htm

DOI: 10.7251/MK1704241S

Funkcija eksplicitne kongruencije i njezine primjene

Petar Svirčević

Zagreb, Hrvatska
e-mail: petar.svircevic@zg.t-com.hr

Sažetak. *Dobro je poznato da je specifična grana algebre, unutar teorije brojeva, teorija kongruencija pomoću koje se rješavaju različiti problemi vezani za djeljivost brojeva. Svakako, da ti problemi mogu biti općeniti, a konkretni brojevi mogu biti preveliki, da bi se mogli ispisati i analizirati u razumnom vremenu bez navedene metode. Naime, oni mogu biti toliko veliki, da ih današnja računala, a i buduća, ne mogu u razvijenom obliku ni ispisati. Nadalje znamo, da su kongruencije ustvari relacije ekvivalencije, a to znači da zadovoljavaju uvjete: refleksivnosti, simetrije i tranzitivnosti. Često je operiranje s njima zahtjevno u smislu preglednosti. No, mi ćemo u ovome članku definirati funkciju eksplicitne kongruencije. Jasno je, da je to funkcija diskretne varijable. Nadalje, to je idempotentna funkcija, pa će njezina primjena biti pregledna, dok je sam postupak rješavanja problema kraći, a primijenit ćemo je za rješavanje problema u vezi djeljivosti brojeva i za rješavanje nekih klasa diofantskih jednadžbi. Napomenimo i to, da se za njezinu primjenu ne mora znati dokaz glavnog teorema, odnosno algoritma, dakle ona se može primijeniti za obradu gradiva i u osnovnoj školi. Definicija ove funkcije je uklapa u krilaticu:"Matematika je nauka koju karakterizira težnja, da svoje pojmove i zakone izrazi u oblicima, koji su eksplicitni, generalizirani i primjenljivi u praksi".*

Ključne riječi. *Eksplicitne kongruencije, diskretna idempotentna funkcija, diofantske jednadžbe.*

The Function of Explicit Congruence and its Application

Abstract. *It is well known that the specific branch of algebra, within the theory of numbers, congruence theory, is used to solve various problems related to divisibility of numbers, or to solve some classes of diophantine equations. Of course, these problems may be general, and the actual numbers may be too large to be able to print and analyze in a reasonable time without the above method. Namely, they can be so big that today's computers, and the future, can not even print in a sophisticated way. Furthermore, we know that congruence is in fact the relation of equivalence, which means that it satisfies the conditions: reflexivity, symmetry and transivity. Often the operation with them is demanding in terms of visibility. But in this article we will define the function of explicit congruence. Clearly, it is a discrete variable function. Furthermore, it is a idempotency function, so its application will be clear and the problem solving itself is shorter and we*

will apply it to solve the problem of divisibility of numbers and to solve some diophantine equations. Let us also note that its application does not have to know the proof of the main theorem, ie the algorithm, so it can be applied to the processing of the material and in the elementary school. The definition of this function fits into the vow: "Mathematics is a science characterized by aspiration, to express its terms and laws in forms that are explicit, generalized, and applicable in practice."

Keywords. *Explicit congruences, discrete idempotent function, diophantine equations.*

Napomena 1. Prije nego prijeđemo na gradivo, reproducirat ćemo zadatak iz hvale vrijednog članka, koji je doprineo mojem iniciranju, da se pozabavim definiranjem funkcije eksplicitne kongruencije. Naime, u članku [2] je jasno i elegantno riješen u standardnoj oznaci pomoću kongruencija i ovaj zadatak:

Primjer 1. Dokazati da je broj $2222^{5555}+5555^{2222}$ djeljiv sa 7.

Rješenje: Neka je $a=2222$ i $b=5555$**.** Promatrat ćemo kongruenciju po modulu 7. Imamo $a\equiv 3(mod\ 7)$ i $b\equiv 4(mod\ 7)$. Zbog toga je $a^b\equiv 3^b(mod\ 7)$ i $b^a\equiv 4^a(mod\ 7)$. Dakle, $a^b+b^a\equiv 3^b+4^a(mod 7)$. Promotrit ćemo sada potencije broja 3 modulo 7. Imamo

$$3^1\equiv 3(mod\ 7),\ 3^2\equiv 2(mod 7),\ 3^3\equiv 6(mod\ 7),\ 3^4\equiv 4(mod\ 7),\ 3^5\equiv 5(mod\ 7),\ 3^6\equiv 1(mod\ 7),$$
$$3^7\equiv 3(mod\ 7).$$

Vidimo, da imamo 6 ostataka i to: 3,2,6,4,5 i 1. Mi imamo u eksponentu broja 3 broj 5555. Kako je $5555\equiv 5(mod\ 6)$, to je $3^{5555}\equiv 3^5(mod\ 7)\equiv 5(mod\ 7)$.

Promatrajmo potencije broja 4 modulo 7. Imamo:

$$4^1\equiv 4(mod\ 7),\ 4^2\equiv 2(mod\ 7),\ \ 4^3\equiv 1(mod\ 7),\ 4^4\equiv 4(mod\ 7).$$

Odavde slijedi, da imamo tri ostatka i to: 4,2 i 1. Kako je $2222\equiv 2(mod\ 3)$, to je $4^{2222}\equiv 4^2(mod\ 7)\equiv 2(mod\ 7)$.

Zbog toga je $2222^{5555}+5555^{2222}\equiv 5+2(mod\ 7)\equiv 0(mod\ 7)$. ■

Definicija 1. Funkcija

$$f_m:\mathbb{Z}\to\{0,1,2,...,m-1\};\ \ m\in\mathbb{N}\setminus\{1\},\tag{1}$$

definirana kao

$$f_m(x)=\frac{1+sng\,x}{2}\left(x-\left\lfloor\frac{x}{m}\right\rfloor m\right)+\frac{(1-sng\,x)\,sng\,|x|}{2}\left(m+x+\left\lfloor\frac{|x|}{m}\right\rfloor m\right),\tag{2}$$

se zove *funkcija eksplicitne kongruencije*, gdje ćemo broj *m* zvati *baza eksplicitne kongruencije*. (Možemo umjesto oznake f_m upotrijebiti i oznaku mod_m.)

Rješenje Primjera 1. *pomoću funkcije eksplicitne kongruencije*: (primjena značenja iz Definicije 1. i Teorema 5.):

$$f_7(2222^{5555}+5555^{2222}) = f_7(3^{5\cdot 1111}+4^{2\cdot 1111}) = f_7((f_7(243))^{1111}+(f_7(16))^{1111}) =$$

$$= f_7(5^{1111}+2^{1111}) = f_7((7-2)^{1111}+2^{1111}) = f_7(-2^{1111}+2^{1111}) = 0.$$

Vidimo da se sve može napraviti jednostavno i brzo. Čak smo mogli ispustiti „korak“

$$... = f_7((7-2)^{1111}+2^{1111}) = ...,$$

a to ćemo objasniti u Napomeni 6. No, to ne znači da će rješavanje i drugih zadataka biti baš ovoliko skraćeno.

Napomena 2. Npr. iz Definicije 1. slijedi $f_3(7) = \frac{1+sng\,7}{2}\left(7-\left\lfloor\frac{7}{3}\right\rfloor 3\right) = 7-2\cdot 3 = 1,$ a to odgovara kongruenciji $7 \equiv 1(mod\,3)$ ili $7 \equiv -2(mod\,3)$. Analognim postupkom dobivamo, da je npr.

$$f_3(-7) = \frac{(1-sng\,(-7))sng|-7|}{2}\left(3+(-7)+\left\lfloor\frac{|-7|}{3}\right\rfloor 3\right) = 3-7+2\cdot 3 = 2,$$

a to odgovara ovim kongruencijama $(-7) \equiv (-1)(mod\,3)$ ili $(-7) \equiv 2(mod\,3)$. Ovi ishodi su i bili za očekivati, jer se u prvom slučaju radi o funkciji a u drugom o relaciji ekvivalencije. Nadalje, vidljivo je, da je Definicijom 1. ustvari definirana diskretna i surjektivna funkcija. No, još ćemo dokazati, da je ona i idempotentna, a to je njezino temeljno svojstvo, koje ćemo često koristiti pri dokazu teorema i u primjeni. Inače, u matematici, često koristimo i druge idempotentne funkcije, kao npr.: $|\ |: \mathbb{R} \to \{0\} \cup \mathbb{R}^+;\ \lfloor\ \rfloor: \mathbb{R} \to \mathbb{Z};\ \lceil\ \rceil: \mathbb{R} \to \mathbb{Z};\ sng: \mathbb{R} \to \{-1, 0, 1\};$ ...

Znamo, da je funkcija $f: D \to K$ idempotentna, ako je $f(f(x)) = f(x)$ ili u oznaci $f^{(2)}(x) \equiv (f \circ f)(x) = f(x), \forall x \in D$. To je ustvari idempotentnost s obzirom na kompozicijsko potenciranje.

Teorem 1. Funkcija eksplicitne kongruencije, dana s (2), je idempotentna.

Dokaz: Neka je $f_m(x_0) = y_0 \in \{0,1,2,...,m-1\}$, za proizvoljno $x_0 \in \mathbb{Z}$. Neka je još i $f_m(x) = f_m^{(1)}(x)$. Tada je

$$f_m^{(2)}(x_0) = f_m(f_m(x_0)) = f_m(y_0) = y_0 = f_m(x_0).$$

Tada iz pretpostavke $f_m^{(n-1)}(x_0) = y_0$ slijedi da je

$$f_m^{(n)}(x_0) = f_m^{(1)}(f_m^{(n-1)}(x_0)) = f_m(x_0),$$

pa je time teorem dokazan. ■

Definicija 2. Ako je

$$\frac{a}{m}=b+\frac{r}{m};\ \ 0\le r<m-1;\ \ a,b\in\mathbb{Z};\tag{3}$$

tada se *r* zove *pravi ostatak* ili samo *ostatak* . Kada je

$$\frac{a}{m}=(b-1)+\frac{m+r}{m}=(b-2)+\frac{2m+r}{m}=(b-3)+\frac{3m+r}{m}=\ldots,\tag{4}$$

tada se $m+r$ zove *minimalni hiperostatak*, i konačno kažemo, kada je

$$\frac{a}{m}=(b+1)+\frac{-m+r}{m}=(b+2)+\frac{-2m+r}{m}=(b+3)+\frac{-3m+r}{m}=\ldots,\tag{5}$$

tada se $-m+r$ zove *maksimalni hipoostatak*.

Lema 1. Ako je $a_n, k_n, n, m\in\mathbb{N},\ m>1, a_n=mk_n+r_n$ i $0\le r_n<m-1$; tada je

$$\left\lfloor\frac{a_1}{m}\right\rfloor+\ldots+\left\lfloor\frac{a_n}{m}\right\rfloor+\left\lfloor\frac{a_1+\ldots+a_n}{m}-\left\lfloor\frac{a_1}{m}\right\rfloor-\ldots-\left\lfloor\frac{a_n}{m}\right\rfloor\right\rfloor=\left\lfloor\frac{a_1+\ldots+a_n}{m}\right\rfloor.\tag{6}$$

Dokaz: Ako uvažimo dane uvjete, tada lijeva strana od (6) prima oblik

$$k_1+\ldots+k_n+\left\lfloor k_1+\ldots+k_n+\frac{r_1+\ldots+r_n}{m}-k_1-\ldots-k_n\right\rfloor=k_1+\ldots+k_n+\left\lfloor\frac{r_1+\ldots+r_n}{m}\right\rfloor=$$

$$=\frac{mk_1+\ldots+mk_n}{m}+\left\lfloor\frac{r_1+\ldots+r_n}{m}\right\rfloor=\left\lfloor\frac{(mk_1+r_1)+\ldots+(mk_n+r_n)}{m}\right\rfloor=\left\lfloor\frac{a_1+\ldots+a_n}{m}\right\rfloor\ .$$

Dakle dobili samo desnu stranu od (6), pa je time lema u potpunosti dokazana (vidite [1]). ■

Lema 2. Ako je $a_1, a_2\in\mathbb{N},$ tada je

$$f_m(a_1+a_2)=f_m(f_m(a_1)+f_m(a_2)).\tag{7}$$

Dokaz: Neka je

$$a_1=k_1m+r_1,\ \ a_2=k_2m+r_2;\tag{8}$$

gdje su r_1 i r_2 pravi ostaci, dakle $0\le r_1, r_2<m-1$, koje smo definirali u Definiciji 2. Uvažimo li Definiciju 1. i (8), tada imamo da je lijeva strana od (7)

$$f_m(a_1+a_2)=r_1+r_2-\left\lfloor\frac{r_1+r_2}{m}\right\rfloor m.\tag{9}$$

Analogno, desna strana od (7) je

$$f_m\left(k_1m+r_1-\left\lfloor\frac{k_1m+r_1}{m}\right\rfloor m+k_2m+r_2-\left\lfloor\frac{k_2m+r_2}{m}\right\rfloor m\right)=f_m\left(r_1+r_2-\left\lfloor\frac{r_1+r_2}{m}\right\rfloor m\right),$$

a to je identično s relacijom (9), ako na istu primjenimo svojstvo idempotentnosti, čime je ova lema dokazana. ■

Pomoću matematičke indukcije lako možemo dokazati i lemu 3.

Lema 3. Ako je $a_1,\dots,a_n,n\in\mathbb{N}$, tada je

$$f_m(a_1+\dots+a_n)=f_m(f_m(a_1)+\dots+f_m(a_n)).$$ ■

Zapravo, mi se pripremamo da dokažemo da ta jednakost vrijedi za sve $a_1,\dots,a_n\in\mathbb{Z}$.

Lema 4. Ako je $a\in\mathbb{N}$, tada je

$$f_m(-a)=m-f_m(a)=f_m(m-f_m(a)).$$

Dokaz: Iz (2) slijedi

$$f_m(-a)=m-a+\left\lfloor\frac{a}{m}\right\rfloor m=m-f_m(a)=f_m(m-f_m(a)),$$

pa je time tvrdnja dokazana. ■

Primjer 2. Važi da je $f_3(-7)=f_3(3-f_3(7))=2$, što je pravi ostatak.

Lema 5. Ako je $a_1,a_2\in\mathbb{N}$, tada je

$$f_m(a_1-a_2)=f_m(f_m(a_1)-f_m(a_2)).$$

Dokaz: Jasno je da postoji $k\in\mathbb{N}$, takav da je $km-a_2>0$, pa dobivamo, da je

$$f_m(a_1-a_2)=f_m(f_m(a_1)+f_m(km-a_2))=f_m\left(f_m(a_1)+km-a_2-\left\lfloor\frac{km-a_2}{m}\right\rfloor m\right)=$$

$$=f_m\left(f_m(a_1)+km-a_2-km+\left\lfloor\frac{a_2}{m}\right\rfloor m\right)=f_m\left(f_m(a_1)-a_2+\left\lfloor\frac{a_2}{m}\right\rfloor m\right)=$$

$$=f_m\left(f_m(a_1)-\left(a_2-\left\lfloor\frac{a_2}{m}\right\rfloor m\right)\right)=f_m(f_m(a_1)-f_m(a_2)).$$ ■

Ako uvažimo zadnje tri leme, zaključujemo da važi navedeni teorem.

Teorem 2. Ako je $a_1, \dots, a_n \in \mathbb{Z}$; $n \in \mathbb{N}$, tada je

$$f_m(a_1 + \dots + a_n) = f_m(f_m(a_1) + \dots + f_m(a_n)) \text{ . } \blacksquare$$

Sada ćemo se pozabaviti problemima, kako se eksplicitno kongruiraju produkti, odnosno potencije cijelih brojeva.

Lema 6. Ako je $a_1, a_2 \in \mathbb{N}$, tada je

$$f_m(a_1 \cdot a_2) = f_m(f_m(a_1) \cdot f_m(a_2)). \tag{10}$$

Dokaz: $f_m(a_1 \cdot a_2) = f_m(\underbrace{a_2 + \dots + a_2}_{a_1}) = f_m(\underbrace{f_m(a_2) + \dots + f_m(a_2)}_{a_1}) =$

$$= f_m(a_1 f_m(a_2)) = f_m(\underbrace{a_1 + \dots + a_1}_{f_m(a_2)}) = f_m(\underbrace{f_m(a_1) + \dots + f_m(a_1)}_{f_m(a_2)}) = f_m(f_m(a_1) \cdot f_m(a_2)) \text{ . } \blacksquare$$

Lema 7. Ako je $a_1, a_2 \in \mathbb{N}$, tada je

$$f_m(-a_1 \cdot a_2) = f_m(f_m(-a_1) \cdot f_m(a_2)).$$

Dokaz: $f_m(-a_1 \cdot a_2) = f_m((-a_1) \cdot a_2)) = f_m(-\underbrace{a_1 - \dots - a_1}_{a_2}) =$

$$= f_m(\underbrace{f_m(-a_1) + \dots + f_m(-a_1)}_{a_2}) = f_m(f_m(-a_1) \cdot a_2) = f_m(f_m(-a_1) \cdot f_m(a_2)) \text{ . } \blacksquare$$

Očigledno je da iz Leme 6. i Leme 7. slijedi naredna lema.

Lema 8. Ako je $a_1, a_2 \in \mathbb{Z}$, tada je

$$f_m(a_1 \cdot a_2) = f_m(f_m(a_1) \cdot f_m(a_2)). \tag{11}$$

Sada ćemo, koristeći Lemu 8 – matematičkom indukcijom – dokazati naredni teorem.

Teorem 3. Ako je $a_1, \dots, a_n \in \mathbb{Z}$; $n \in \mathbb{N}$, tada je

$$f_m(a_1 \cdot \dots \cdot a_n) = f_m(f_m(a_1) \cdot \dots \cdot f_m(a_n)). \tag{12}$$

Dokaz: Iz (11) slijedi, da je (12) točno za $n = 1$ i $n = 2$. Pretpostavimo sada, da je $n > 2$, tada je

$$f_m(a_1 \cdot \dots \cdot a_{n-1} a_n) = f_m((a_1 \cdot \dots \cdot a_{n-1}) a_n) = f_m(f_m((a_1) \cdot \dots \cdot f_m(a_{n-1})) \cdot f_m(a_n)) =$$

$$= f_m(f_m(a_1) \cdot \dots \cdot f_m(a_{n-1}) f_m(a_n)),$$

pa je time (12) dokazano. ■

Korolar 1. Ako je $a \in \mathbb{Z}$; $n \in \mathbb{N}$, tada je

$$f_m(a^n) = f_m((f_m(a))^n).$$

Dokaz: Dokaz ovoga teorema, odnosno korolara, izravno slijedi iz T3, ako se izvrši specijalizacija $a = a_1 = ... = a_n \in \mathbb{Z}$. ■

Napomena 3. Ovo što ćemo sada napomenuti, zapravo slijedi iz predhondih teorema. Ako bi npr. rekli da je $f_7(5^{1111}) = f_7(-2^{1111})$, tada bi se to moglo učiniti, da je to kontradiktorno s Definicijom 1, pa da se sada ne radi o eksplicitnoj kongruenciji, koju smo dali s (1) i (2). Sada ćemo to pojasniti. Naime, ako $a \in \{0, 1, 2, ..., m-1\}$ i $n > a$, tada je

$$f_n((n-a)^{2k-1}) = f_n\left(\binom{2k-1}{0}n^{2k-1} - \binom{2k-1}{1}n^{2k-2}a^1 + ... - \binom{2k-1}{2k-1}a^{2k-1}\right) = f_n(-a^{2k-1})$$

i

$$f_n((n-a)^{2k}) = f_n\left(\binom{2k}{0}n^{2k} - \binom{2k}{1}n^{2k-1}a^1 + ... + \binom{2k}{2k}a^{2k}\right) = f_n(a^{2k}) \text{ za } k \in \mathbb{N}.$$

Prema tome možemo reći, da je npr. $f_7(5^{2k-1}) = f_7(-2^{2k-1})$ i $f_7(5^{2k}) = f_7(2^{2k})$, i ta svojstva slijede iz definirane *funkcije eksplicitne kongruencije*. To ćemo svojstvo često koristiti kod rješavanja problema.

Primjer 2. Provjerimo obrađeno gradivo na jednom jednostavnom primjeru. Jasno je, da je $f_3(7) = 1$. No, to smo mogli i „zakomplicirati“, pa reći $7 = 5 - 11 + 13$. Tada bi dobili

$$f_3(7) = f_3(5 - 11 + 13) = f_3(f_3(5) - f_3(11) + f_3(13)) = f_3(2 - 2 + 1) = 1,$$

što smo i očekivali.

Sada ćemo sve predhodno dokazane tvrdnje sintetizirati u Teorem 5, koji vrijedi onda i samo onda ako vrijede sve predhodne tvrdnje. Ta ekvivalencija se može jednostavno dokazati. Dakle, tu se radi o sumi produkata potencija cijelih brojeva.

Teorem 5. Ako je $n, i, j, k_j \in \mathbb{N}$; $\alpha_{ij} \in \mathbb{N}$; $a_{ij} \in \mathbb{Z}$; tada je

$$f_m\left(\sum_{i=1}^{n}\prod_{j=1}^{k_j} a_{ij}^{\alpha_{ij}}\right) = f_m\left(\sum_{i=1}^{n}\prod_{j=1}^{k_j} f_m(a_{ij}^{\alpha_{ij}})\right). \quad ■ \qquad (13)$$

Primjer 3. Primjenimo (13) na jednom jednostavnom zadatku. Naime, dokažimo da je broj $11^{22}\cdot 12^3+7^5\cdot 6^7-13^2-2016^{2017}$ djeljiv s 5. Ako primijenimo Teorem5, tada imamo

$$f_5(11^{22}\cdot 12^3+7^5\cdot 6^7-13^2-2016^{2017})=f_5(1^{22}\cdot 2^3+2^5\cdot 1^7-3^2-1^{2017})=f_5(30)=0,$$

dakle tvrdnja je točna. Inače, taj tretirani broj u razvijemom obliku bi imao 6666 znamenaka.

Sada ćemo izneseno gradivo primijenjivati riješavajući probleme, a za neke ćemo dati samo uputu. Što se tiče slaganja zadataka po težini, ili postizanja pune metodičnosti, tu bi moglo biti primjedbi, jer je gradivo isprepleteno, tako da to nije baš bilo jednostavno postići.

Zadatak 1. Broj $1^{2016}+2^{2016}+3^{2016}+4^{2016}$ u diobi s 5 daje ostatak 4.

Rješenje: $f_5(1+2^{4\cdot 504}+3^{4\cdot 504}+4^{4\cdot 504})=f_5(1+16^{504}+81^{504}+256^{504})=$

$$=f_5(1+(f_5(16))^{504}+(f_5(81))^{504}+(f_5(256))^{504})$$

$$=f_5(1+1^{504}+1^{504}+1^{504})=f_5(4)=4.$$

Dakle, tvrdnja je točna. Svakako, da smo proceduru mogli skratiti, jer već nakon prvog koraka vidimo koliki je rezultat.

Zadatak 2. Broj $2^{1000}+5^{1000}+6^{1000}+9^{1000}$ je djeljiv sa 7.

Rješenje: $f_7(2^{1000}+(-2)^{1000}+(-1)^{1000}+2^{1000})=f_7(3\cdot 2^{1000}+1)=$

$$=f_7(3\cdot 8^{333}\cdot 2+1)=f_7(3\cdot 1\cdot 2+1)=f_7(7)=0.$$

Tvrdnja je točna.

Zadatak 3. Odredimo zadnju znamenku, znamenku jedinica, broja 3^{2017}.

Rješenje: Zadnja znamenka, ili znamenka jedinica, broja 3^{2017} je

$$f_{10}(3^{2017})=f_{10}(3^{4\cdot 504}\cdot 3)=f_{10}(81^{504}\cdot 3)=f_{10}(1^{504}\cdot 3)=3.$$

Zadatak 4. Naći znamenku desetica broja $101^{100}+102^{100}$.

Rješenje: Ako taj broj podijelimo sa 100 dobit ćemo dvoznamenkasti ostatak iz kojeg vidimo znamenke desetica. Dakle

$$f_{100}\,(1+2^{100}) = f_{100}\,(1+(2^{10})^{10}) = f_{100}\,(1+(24)^{10}) = = f_{100}\,(1+(76^2)^5) = f_{100}\,(1+76) = 77.$$

Znamenka desetica je 7.

Zadatak 5. Neka je $\alpha \in \mathbb{N}$ $n-$znamenkasti broj u bazi 10 ($n \in \mathbb{N}$), čiji zapis u skraćenom i punom zapisu glasi

$$\alpha = (a_n a_{n-1}..a_2 a_1)_{(10)} = 10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10^1 a_2 + a_1,$$

gdje je $a_1, a_2, \ldots, a_n \in \{0,1,\ldots,9\}$ i $a_n \neq 0$. Treba naći znamenku, koja je na k-om mjestu počev sa znamenkom jedinica a_1 ($k = 1, 2, \ldots, n$).

Rješenje: Jasno je, da je

$$a_1 = f_{10^1}(\alpha) = f_{10^1}(\alpha) - f_{10^0}(\alpha),\ (f_{10^0}(\alpha) = 0),$$

$$a_2 = f_{10^2}(\alpha) - f_{10^1}(\alpha),\ a_3 = f_{10^3}(\alpha) - f_{10^2}(\alpha), \ldots,\ a_n = f_{10^n}(\alpha) - f_{10^{n-1}}(\alpha),$$

a iz toga slijedi da je k-ta znamenka od α dana s relacijom $a_k = f_{10^k}(\alpha) - f_{10^{k-1}}(\alpha).$

Zadatak 6. Bilo koji prirodni broj je djeljiv s 9, onda i samo onda, ako mu je suma znamenaka djeljiva s 9.

Rješenje: Ako je $\alpha \in \mathbb{N}$ n-znamenkasti broj u bazi 10 zapisan u obliku

$$\alpha = (a_n a_{n-1}\ldots a_2 a_1)_{(10),} \text{ gdje je } a_1, a_2, \ldots, a_n \in \{0,1,\ldots,9\} \text{ i } a_n \neq 0,$$

tada je

$$f_9(\alpha) = f_9(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1) = f_9(a_n + a_{n-1} + \ldots + a_2 + a_1) = 0.$$

Važi i obrat**.**

Zadatak 7. Bilo koji prirodni broj je djeljiv s 3, onda i samo onda, ako mu je suma znamenaka djeljiva s 3.

Uputa za rješenje: Postupamo kao u Zadatku 6, samo ćemo uvažiti da je $f_3(10) = 1.$

Zadatak 8. Bilo koji prirodni broj je djeljiv s 11, onda i samo onda, ako mu je razlika suma znamenaka na neparnim i parnim mjestima djeljiva s 11. Znamenka

jedinica je na prvom, tj. na neparnom mjestu; znamenke stotica na drugom, tj. na parnom mjestu; ...

Rješenje: Ako je

$$\alpha = (a_n a_{n-1}..a_2 a_1)_{(10)} = 10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10^1 a_2 + a_1,$$

tada slijedi

$$f_{11}(\alpha) = f_{11}(a_1 + 10^1 a_2 + 10^2 a_3 + 10^3 a_4 + ... + 10^{n-1}a_n) =$$

$$= f_{11}(a_1 + (11-1)a_2 + (99+1)a_3 + (1001-1)a_4 + (9999+1)a_5 + ...) = 0$$

To je nužan i dovoljan uvjet, ali treba još dokazati da je

$$f_{11}(\underbrace{99...9}_{2n}) = 0 \text{ i } f_{11}(\underbrace{100...01}_{2n}) = 0.$$

Važi da je

$$f_{11}(\underbrace{99...9}_{2n}) = f_{11}(10^{2n}-1) = f_{11}((11-1)^{2n}-1) = 0;$$

$$f_{11}(\underbrace{100..01}_{2n}) = f_{11}(10^{2n-1}+1) = = f_{11}((11-1)^{2n-1}+1) = f_{11}(-1+1) = 0,$$

pa je time dokaz u potpunosti napravljen, dakle

$$f_{11}(\alpha) = f_{11}((a_1 + a_3 + a_5 + ...) - (a_2 + a_4 + a_6 + ...)) = 0.$$

Zadatak 9. Ako je $g(x) = a_n x^n + a_{n-1}x^{n-1} + ...a_1 x + a_0$, gdje je $a_0, a_1, ..., a_n \in \mathbb{Z}$, $m, n \in \mathbb{N}$; $m > 1$; i ako je $f_m(a) = b$, tada je $f_m(g(a)) = f_m(g(b))$.

Rješenje:

$$f_m(g(a)) = f_m(a_n a^n + a_{n-1}a^{n-1} + ... + a_1 a + a_0) =$$

$$= f_m(a_n(f_m(a))^n + ... + a_1(f_m(a)) + a_0) = f_m(a_n b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0) = f_m(g(b)).$$

Zadatak 10. Dokazati da je $f_5(3333^{9999} + 9999^{3333}) = 1.$

Rješenje: $f_5(3333^{9999} + 9999^{3333}) = f_5(3^{9999} + 4^{3333}) = f_5(3^{4\cdot 2499+3} + 4^{2\cdot 1666+1}) =$

$$= f_5(81^{2499}\cdot 27 + 16^{1666}\cdot 4) = f_5(1\cdot 27 + 1\cdot 4) = 1.$$

Zadatak 11. Neka su $m_1, ..., m_n, n \in \mathbb{N} \setminus \{1\}$ relativno prosti brojevi i neka je a cio broj. Tada $f_{m_1}(a) = ... = f_{m_n}(a) = 0$ ako i samo je $f_{m_1 \cdot ... \cdot m_n}(a) = 0.$

$$((f_{m_1}(a)=0)\,\&\,\ldots\,\&\,(f_{m_n}(a)=0))\Leftrightarrow(f_{m_1\cdot\ldots\cdot m_n}(a)=0)\ za\ \ n\in\mathbb{N}\setminus\{1\},\ (14)$$

gdje su $m_1,\ldots,m_n,$ međusobno relativno prosti.

Uputa za rješenje: Na osnovi Definicije 1, za $n=2$ prije dokažemo ekvivalenciju

$$((f_{m_1}(a)=0)\,\&\,(f_{m_2}(a)=0))\Leftrightarrow(f_{m_1m_2}(a)=0),$$

a onda pomoću matematičke indukcije dobivamo (14).

Zadatak 12. Dokazati da je

$$f_{99}(3\cdot 6^{2n}+3^{n+3}+3^{n+1})=0\ \ za\ \ n\in\mathbb{N}. \qquad (15)$$

Rješenje: $f_9(3\cdot 36^n+27\cdot 3^n+3^{n+1})=f_9(3\cdot 0^n+0\cdot 3^n+3^{n+1})=f_9(3^{n+1})=0.$

Nadalje

$$f_{11}(3\cdot 36^n+27\cdot 3^n+3\cdot 3^n)=f_{11}(3\cdot 3^n+5\cdot 3^n+3\cdot 3^n)=f_{11}(11\cdot 3^n)=0,$$

a to znači da je (15) točno, jer smo primijenili (14).

Zadatak 13. Dokazati da je broj $a=6^{2n}+11^n+13^{4n}+17^{4n}+2^{4n}$, $n\in\mathbb{N}_0$ djeljiv s 5.

Rješenje:

$$f_5(a)=f_5(1+1+3^{4n}+2^{4n}+2^{4n})=f_5(2+81^n+2\cdot 16^n)=f_5(5)=0.$$

Zadatak 14. Dokazati da je $f_{11}(6\cdot 7^{2n}+5^{n+1})=0,\ n\in\mathbb{N}_0.$

Rješenje: $f_{11}(6\cdot 49^n+5\cdot 5^n)=f_{11}(6\cdot 5^n+5\cdot 5^n)=f_{11}(11\cdot 5^n)=0.$

Zadatak 15. Odrediti znamenku stotica od broja 2^{1000}.

Rješenje:

$$f_{10^3}(2^{1000})=f_{10^3}(2^{10\cdot 100})=f_{10^3}(1024^{100})=f_{10^3}(24^{3\cdot 33}\cdot 24)=f_{10^3}(824^{33}\cdot 24)=$$

$$=f_{10^3}(824^{2\cdot 16}\cdot 824\cdot 24)=f_{10^3}(976^{2\cdot 8}\cdot 776)=f_{10^3}(576^{2\cdot 4}\cdot 776)=\ldots=376.$$

Dakle, znamenka stotica je 3.

Napomena 4. Zašto smo račun u Zadatak 15 tako „razvukli“?! Pa, to smo napravili zbog toga, da pokažemo, kako možemo do rezultata doći i pomoću „slabog“ kalkulatora, a u krajnjoj liniji i „pješke“. Budući da imamo u **W10** instaliran i znanstveni kalkulator (scientific calculator), ali i pomoću njega ne možemo dobiti izravno točnu razvijenu vrijednost broja 2^{1000}, jer on ima 302 znamenke, a to što

kaklulator „kaže“ da je $2^{1000} = 1.071\,508\,...\cdot 10^{301}$, tada iz toga ne možemo zaključiti kolike su znamenke stotica. Međutim, pomoću toga kalkulatora možemo točno dabiti da je

$$2^{100} = 1\,267\,650\,600\,228\,229\,401\,496\,703\,205\,376,$$

dakle $f_{10^3}(2^{100}) = 376$. Prema tome imali bi

$$f_{10^3}(2^{1000}) = f_{10^3}((f_{10^3}(2^{100}))^{10}) = f_{10^3}(376^{10}) = 376.$$

No, postoje programi, da računala mogu točno izračunati razvijene vrijednosti potencija točno na milijarde znamenaka. Mogli bi istim postupkom naći npr. $f_{213}(2^{1000}) = 190$. U Definiciji 1. smo rekli, da za bazu eksplicitne kongruencije možemo uzeti bilo koji broj iz $\mathbb{N}\setminus\{1\}$.

Zadatak 16. Ako je $n \in \mathbb{N}$ i $a = 6^n + 7^n + 8^n + 9^n$, tada vrijedi

$$(f_4(n) \neq 0) \Rightarrow (f_{10}(a) = 0).$$

Rješenje: Vidljivo je, da je $f_2(a) = 0$; pa ako dokažemo da je $f_5(a) = 0$ tada slijedi da

$f_{10}(a) = 0$. Ako je $n = 4k$ $(k \in \mathbb{N}) \Rightarrow$

$f_4(a) = f_4(6^{4k} + 7^{4k} + 8^{4k} + 9^{4k}) =$

$= f_4(36^{2k} + 49^{2k} + 64^{2k} + 81^{2k}) = f_4(0 + 1^{2k} + 0^{2k} + 1^{2k}) = 2$,

Dakle $f_4(n) \neq 0$.

Promotrimo još slučajeve: $n = 4k+1, n = 4k+2, n = 4k+3,\ k \in \mathbb{N}$.

1.slučaj: $(n = 4k+1) \Rightarrow f_5(a) = f_5(1 + 2^n + 3^n + 4^n) =$

$$f_5(1 + 2^{4k+1} + 3^{4k+1} + 4^{4k+1}) =$$

$= f_5(1 + 16^k \cdot 2 + 81^{k\cdot} \cdot 3 + 256^{k\cdot} \cdot 4) = f_5(1 + 1^k \cdot 2 + 1^{k\cdot} \cdot 3 + 1^{k\cdot} \cdot 4) = f_5(10) = 0.$

2.slučaj: $(n = 4k+2) \Rightarrow f_5(a) = f_5(1 + 2^n + 3^n + 4^n) =$

$$f_5(1 + 2^{4k+2} + 3^{4k+2} + 4^{4k+2}) =$$

$= f_5(1 + 16^k \cdot 4 + 81^{k\cdot} \cdot 9 + 256^{k\cdot} \cdot 16) = f_5(1 + 1^k \cdot 4 + 1^{k\cdot} \cdot 4 + 1^{k\cdot} \cdot 1) = f_5(10) = 0.$

3.slučaj: $(n = 4k+3) \Rightarrow f_5(a) = f_5(1 + 2^n + 3^n + 4^n) =$

$$f_5(1 + 2^{4k+3} + 3^{4k+3} + 4^{4k+3}) =$$

$= f_5(1 + 16^k \cdot 8 + 81^{k\cdot} \cdot 27 + 256^{k\cdot} \cdot 64) = f_5(1 + 1^k \cdot 3 + 1^{k\cdot} \cdot 2 + 1^{k\cdot} \cdot 4) = f_5(10) = 0.$

Dakle dokazana je dana implikacija, jer smo uvažili i $f_2(a) = 0$.

Zadatak 17. Dokazati da je $f_3\left(\sum_{k=1}^{2016} k^{2016}\right)=0.$

Rješenje:

$$f_3(\,672\,(\,1^{2016}+2^{2016}+0^{2016}\,))=\,f_3(\,672\,\cdot 2)=\,f_3(\,0\cdot 2)=0.$$

Uvažili smo, da je:

$$f_3(1)=\,f_3(4)=\,f_3(7)=\ldots=\,f_3(2014\,)=1,\;\,f_3(2)=\,f_3(5)=\ldots=\,f_3(2015\,)=2,$$

$$f_3(3)=\,f_3(6)=\,f_3(9)=\ldots=\,f_3(2016\,)=0,\;\,f_3(2^{2016})=\,f_3(4^{1008})=1 \text{ i}$$

$$2016:3=672.$$

Zadatak 18. Riješiti jednadžbu po *x*

$$f_a(x)=0. \tag{16}$$

Kada ta jednadžba ima najmanji broj rješenja?

Rješenje: Znamo da je $a\in\mathbb{N}\setminus\{1\}$. Nadalje znamo, da svaki prirodni broj možemo prikazati u kanonskom obliku

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}, \tag{17}$$

gdje su: $p_1, p_2, \ldots, p_n$ različiti prosti brojevi. Možemo pokazati, da je ukupni broj djelilaca od (17) dan s vezom $\tau(a)=(\alpha_1+1)(\alpha_2+1)\cdot\ldots\cdot(\alpha_n+1),$ gdje je uključen broj 1 i sam *a*. No, broj 1 ne dolazi u obzir za eksplicitno kongruiranje, pa možemo reći da je minimalni broj rješenja te jednadžbe dan s vezom

$$\delta(a)=\tau(a)-1=(\alpha_1+1)(\alpha_2+1)\cdot\ldots\cdot(\alpha_n+1)-1. \tag{18}$$

Dokaz ove tvrdnje slijedi iz ekvivalencije (14).

Zadatak 19. Odrediti makar osam rješenja jednadžbe

$$f_x\left(\sum_{k=1}^{2001} k^{2001}\right)=0.$$

Uputa za rješenje: Ako uvažimo identitet

$$a^{2n+1}+b^{2n+1}\equiv(a+b)(a^{2n}-a^{2n-1}b^1+a^{2n-2}b^2-\ldots+b^{2n}),\; n\in\mathbb{N},$$

tada je

$$\sum_{k=1}^{2001} k^{2001}=(1^{\,2001}+2000^{\;2001})+(2^{\,2001}+1999^{\;2001})+\ldots+(500^{\;2001}+501^{\;2001})+2001^{\;2001}=$$

$$=2001\,(\ldots)+2001\,(\ldots)+\ldots+2001\,(\ldots)+2001^{\,2001},$$

pa vidimo da je $f_{2001}\left(\sum_{k=1}^{2001} k^{2001}\right)=0.$ Budući je $2001=3\cdot 23\cdot 29,$ tada su makar ovi brojevi: $x=3, 23, 29, 69, 87, 667, 2001$ rješenja dane jednadžbe. Do sedam

mogućnosti dolazimo iz (18), jer je $x = 2001 = 3^1 \cdot 23^1 \cdot 29^1$. Dakle ukupni broj rješenja iznosi $\delta(2001) = \tau(2001) - 1 = (1+1)(1+1)\cdot(1+1) - 1 = 7,$ koje smo već konkretno nabrojali, a to je istina, jer su faktori prosti brojevi. Nakon izlučivanja broja 2001 u zagradi bi dobili još i osmo rješenje

$$x_8 = 2001^{2000} + \sum_{p=1}^{500}\sum_{q=0}^{2000} p^q \cdot (2001 - p)^{2000-q}.$$

Zadatak 20. Dokazati, da diofantska jednadžba

$$f_x(1998^{2017} + 1999^{2017} + 2001^{2017} + 2002^{2017}) = 0 \tag{19}$$

ima barem 24 rješenja u skupu prirodnih brojeva.

Rješenje: Uvažavajući rastav iz Zadatka 19. slijede rastavi:

$$1998^{2017} + 2002^{2017} = (1998 + 2002)(1998^{2016} - 1998^{2015}\cdot 2002^{1} + ... + 2002^{2016}),$$

$$1999^{2017} + 2001^{2017} = (1999 + 2001)(1999^{2016} - 1999^{2015}\cdot 2001^{1} + ... + 2001^{2016});$$

koje kada uvrstimo u (19) dobivamo jedno rješenje te jednadžbe je $x = 4000$. Budući je $x = 4000 = 2^5 \cdot 5^3,$ tada dobivamo

$$\delta(4000) = \tau(4000) - 1 = (5+1)(3+1) - 1 = 23$$

rješenja. Nadalje, vrijednost izraza u drugoj zagradi u zadnjem rastavu je dvadesetčetvrto rješenje

$$x_{24} = \sum_{p=0}^{2016} (-1)^p \cdot 1999^{2016-p} \cdot 2001^{p}.$$

Zadatak 21. Dokazati da je, za svaki prirodni broj *n*, zadovoljeno

$$f_3(n^2) \in \{0,1\}. \tag{20}$$

Rješenje: Svaki prirodni broj $n \in \mathbb{N}$ prima jedan od oblika: $3k-2, 3k-1, 3k;$ gdje je $k \in \mathbb{N}$. Dalje je

$$f_3((3k-2)^2) = f_3(9k^2 - 12k + 4) = 1, \quad f_3((3k-1)^2) = f_3(9k^2 - 6k + 1) = 1$$

i $f_3((3k)^2) = f_3(9k^2) = 0,$ pa smo time dokazali danu implikaciju.

Sada ćemo navesti primjere, kako se nekiput može dokazati, da neka diofantska jednadžba nema rješenja, a primijenit ćemo *funkciju eksplicitne kongruencije*.

Posjetimo se nekih najelementarnijih činjenica iz matematičke logike:

istina je, da iz istine slijedi istina, i to pišemo $\underbrace{\mathrm{T} \Rightarrow \mathrm{T}}_{\mathrm{T}}$;

neistina je, da iz istine slijedi neistina, i to pišemo $\underbrace{\mathrm{T} \Rightarrow \bot}_{\bot}$;

istina je, da iz neistine slijedi istina, i to pišemo $\underbrace{\bot \Rightarrow \mathrm{T}}_{\mathrm{T}}$;

istina je, da iz neistine slijedi neistina, i to pišemo $\underbrace{\bot \Rightarrow \bot}_{\mathrm{T}}$.

Napomena 5. *Neka je dana diofantska jednadžba* $A = B$ *i ako za svaku vrijednost iz njezinog područja definicije za neki m vrijedi* $f_m(A) \neq f_m(B)$, *tada ta jednadžba nema rješenja. No, ako je* $f_m(A) = f_m(B)$, *tada još ne možemo znati da li ona ima rješenja.*

Zadatak 22. Dokazati da diofantska jednadžba

$$2^{2^x} + 4^{4^x} + 6^{6^x} + \ldots + 2018^{2018^x} + 2020^{2020^x} = y^2, \tag{21}$$

nema rješnja $(x, y) \in \mathbb{N} \times \mathbb{N}$.

Rješenje: Uočimo, da lijeva strana od (21) ima 1010 sumanda. Uzmimo, da je $x = 1$, tada iz (21) dobivamo da je

$$f_3(2^2 + 4^4 + 6^6 + \ldots + 2018^{2018} + 2020^{2020}) =$$
$$= f_3((-1)^2 + 1^4 + 0^6 + (-1)^8 + 1^{10} + 0^{12} + \ldots + (-1)^{2018} + 1^{2020}) = ((\textit{vrijedi } 1010 = 336 \cdot 3 + 2)) =$$
$$= f_3(\underbrace{((1+1+0)+(1+1+0)+\ldots+(1+1+0))}_{336} + (-1)^{2020} + 1^{2020}) = f_3(336 \cdot (1+1+0) + 2) = 2.$$

Jasno je, da se u zadanoj jednadžbi ništa ne mijenja, što je u vezi sa ostatkom kod eksplicitnog kongruiranja po bazi 3, ako se taj postupak primjeni za proizvoljno $x \in \mathbb{N}$, jer je nakon eksplicitnog kongruiranja baza potencije 1 ili 2, a eksponent je uvijek paran broj pa je

$$f_3(2^{2^x} + 4^{4^x} + 6^{6^x} + \ldots + 2020^{2020^x}) = 2.$$

Znamo da je za svako $y \in \mathbb{N}$ zadovoljeno $f_3(y^2) \in \{0, 1\}$, pa iz toga slijedi da je uvijek $2^{2^x} + 4^{4^x} + 6^{6^x} + \ldots + 2020^{2020^x} \neq y^2$. Dakle, ova jednadžba nema rješenja jer $2 \notin \{0, 1\}$.

Zadatak 23. Dokazati da diofantska jednadžba

$$5^{2x-1} + y = 4^x y + 1$$

nema rješenja u skupu $\mathbb{N} \times \mathbb{Z}$.

Rješenje: Zadanu jednadžbu možemo pisati u obliku $5^{2x-1} - 1 = y(4^x - 1)$. Očigledno je, da vrijedi $f_3(y(4^x - 1)) = 0;\ \forall (x, y) \in \mathbb{N} \times \mathbb{Z}$. Nadalje je

$$f_3(5^{2x-1} - 1) = f_3(2^{2x-1} - 1) = f_3((-1)^{2x-1} - 1) = f_3(-1 - 1) = 1, \forall x \in \mathbb{N}.$$

Iz ovog razmatranja slijedi da je $f_3(5^{2x-1}-1) \neq f_3(y(4^x-1))$ nad domenom $\mathbb{N} \times \mathbb{Z}$ dane jednadžbe, dakle ona nema rješenja.

Zadatak 24. Dokazati da je

$$f_5\left(7^{2016^{2015}} - 3^{2012^{2011}}\right) = 0. \tag{22}$$

Rješenje: Budući je

$$f_4(2016^{2015}) = f_4(2012^{2011}) = 0,$$

tada je $2016^{2015} = 4m$ i
$2012^{2011} = 4n$, gdje je $m,n \in \mathbb{N}$. Prema tome je

$$f_5(7^{2016^{2015}} - 3^{2012^{2011}}) = f_5(2^{4m} - (-2)^{4n}) =$$
$$= f_5(16^m - 16^n) = f_5(1^m - 1^n) = f_5(0) = 0,$$

a to je i trebalo dokazati.

Zadatak 25. Dokazati da je

$$f_{19}(5^{2n+1} \cdot 2^{n+1} + 3^{n+2} \cdot 2^{2n}) = 0 \text{ za svaki } n \text{ iz } \mathbb{N} \cup \{0\}.$$

Rješenje:

$$f_{19}(5^{2n+1} \cdot 2^{n+1} + 3^{n+2} \cdot 2^{2n}) = f_{19}(10 \cdot 50^n + 9 \cdot 12^n) = f_{19}(10 \cdot 12^n + 9 \cdot 12^n) = f_{19}(19 \cdot 12^n) = 0.$$

Zadatak 26. Dokazati da je $f_{13}(2^{12n+8} - 3^{6n+1} - 6) = 0$ za svaki n iz $\mathbb{N} \cup \{0\}$.

Rješenje: $f_{13}(256 \cdot 4096^n - 3 \cdot 729^n - 6) = f_{13}(9 \cdot 1^n - 3 \cdot 1^n - 6) = f_{13}(9-9) = 0.$

Zadatak 27. Dokazati da suma kvadrata pet uzastopnih prirodnih brojeva nije kvadrat prirodnog broja.

Rješenje: Pretpostavimo da postoje prirodni brojevi x,y takvi da je

$$x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 + (x+4)^2 = y^2. \tag{23}$$

Primijenimo li funkciju f_4 na (23), tada dobivamo da je

$$f_4(5x^2 + 20x + 30) = f_4(x^2 + 2) = f_4(y^2). \tag{24}$$

Sada ćemo promotriti sve mogućnosti za $x \in \{4k, 4k+1, 4k+2, 4k+3\}$, jer je time skup prirodnih brojeva rastavljen u četiri disjunktne klase, pa odatla dobivamo da je:

$$f_4(x^2+2) = f_4((4k)^2+2) = 2,\ f_4(x^2+2) = f_4((4k+1)^2+2) = 3,$$

$$f_4(x^2+2) = f_4((4k+2)^2+2) = 2,\ \ f_4(x^2+2) = f_4((4k+3)^2+2) = 3. \tag{25}$$

Ako je *n* prirodni broj, tada se lako pokaže da je

$$f_4(n^2) \in \{0,1\}. \tag{26}$$

Uvažimo li (25) i (26), tada slijedi da je (24), odnosno (23), u kotradikciji, a to znači da je tvrdnja dokazana.

Zadatak 28. Dokazati da hiperbola

$$5x^2 - y^2 + 20x + 30 = 0 \tag{27}$$

nema točaka s cjelobrojnim koordinatama.

Rješenje: Dakle jednadžbu (27) ćemo eksplicitno kongruirati. A to ćemo napraviti, tako, da istu napišemo u obliku

$$5x^2 + 20x + 30 = y^2,$$

kojega ćemo eksplicitno kongruirati po bazi $m = 4$. No, znamo $f_4(y^2) \in \{0,1\}$, ali moramo promotriti slučajeve:

$$f_4(x) = 0,\ f_4(x) = 1,\ f_4(x) = 2,\ f_4(x) = 3.$$

Dakle, dobivamo da je

$$f_4(5x^2 + 20x + 30) = f_4(f_4(x^2) + 2) = f_4(y^2).$$

Na osnovi iznesenog dobivamo implikacije:

$$(f_4(x) = 0) \Rightarrow (f_4(f_4(0^2) + 2) = 2),\ (f_4(x) = 1) \Rightarrow (f_4(f_4(1^2) + 2) = 3),$$
$$(f_4(x) = 2) \Rightarrow (f_4(f_4(2^2) + 2) = 2),\ (f_4(x) = 3) \Rightarrow (f_4(f_4(3^2) + 2) = 3).$$

Vidimo, da vrijednosti konzekvente ovih implikacija nisu iz skupa $\{0,1\}$, a $f_4(y^2) \in \{0,1\}$, pa iz toga slijedi da je

$$f_4(5x^2 + 20x + 30) \neq f_4(y^2),\ \forall (x,y) \in \mathbb{Z}^2,$$

dakle jednadžba (27) nema rješenja.

Napomena 6. Moglo bi se reći, da bez argumentiranja tvrdimo da je rješenje jednadžbe nad domenom $\mathbb{Z}^2$, a razmatranje smo vršili nad $\mathbb{N}^2$. Naime, od lijeve strane eksplicitno kongruirane vrijednosti sume $f_4(5x^2 + 30)$ su iste u $\mathbb{N}$ i u $\mathbb{Z}$, jer ionako je $f_4(20x) = 0$ za oba slučaja, pa je onda logično, da smo domenu mogli proširiti. No, suvišno je razmatranje, da je $f_4(x) = f_4(4 - f_4(|x|))$, i opet bi dobili isti rezultat, da ne postoji rješenje od (27) nad $\mathbb{Z}^2$.

Zadatak 29. Odrediti makar 11 rješenja jednadžbe

$$f_x\left(\sum_{l=0}^{2n^3+10n-1} 2^l\right) = 0.$$

Rješenje: Budući je $f_6(n^3 + 5n) = f_6((n-1)n(n+1) + 6n) = 0$, a to znači da je

$$2n^3+10n=12k,\ k\in\mathbb{N}.$$

Dakle $1+2+2^2+2^3+\ldots+2^{2n^3+10n-1}=1+2+2^2+2^3+\ldots+2^{12k-1}=12^{12k}-1=(4095+1)^k-1$, pa je $f_x((4095+1)^k-1)=0$, dakle $f_x(4095)=0.$ Budući je $4095=3^2\cdot 5\cdot 91,$ pa iz toga kanonskog prikaza dobivamo broj njegovih djelilaca $\tau(4095)=(2+1)(1+1)(1+1)=12$. Jednadžba ima ovih 11 rješenja: $x=3,5,9,15,45,91,273,455,819,1365,4095$; jer broj 1 ne dolazi u obzir. No, postoji makar još jedno rješenje, koje je u nesređenom obliku ne iznosimo, a to smo već prije napominjali.

Zadatak 30. Dokazati da je, za svako $n\in\mathbb{N}$, zadovoljeno

$$f_9(7^n+3n)=1. \tag{28}$$

Rješenje: Ako je $r\in\{0,1,2\}$, tada direktno provjerimo da je

$$f_9(7^r+3r)=1. \tag{29}$$

Budući se svaki $n\in\mathbb{N}$ može prikazati u obliku $n=3k+r,\ k\in\mathbb{N}_0$, to onda povlači, da je $f_9(7^{3k+r}+3(3k+r))=f_9(343^k\cdot 7^r+9k+3r)=f_9((38\cdot 9+1)^k\cdot 7^r+3r)=f_9(7^r+3r)=1,$ jer smo uvažili (29), pa je time zadatak u potpunosti napravljen.

Zadatak 31. Riješiti diofantsku jednadžbu

$$5x^4-x^2-y^2-227=0,$$

(30) tako da je x prost a y prirodan.

Rješenje: Jednadžbu (30) možemo pisati u obliku

$$5x^4-x^2-227=y^2. \tag{31}$$

Za $x=2$, jer je to prvi prosti broj, relacija (31) nije zadovoljena jer je $5\cdot 2^4-2^2-227<0$ a $y^2\geq 0$. jer dobivamo da je $y^2<0.$ Znamo, da su oni oblika $x=6k\pm 1,\ k\in\mathbb{N}$, pa vrijedi implikacija

$$(x=6k\pm 1)\Rightarrow(f_3(x^2)=f_3(x^4)=1). \tag{32}$$

Prije smo pokazali, da je

$$f_3(y^2)\in\{0,1\};\ \forall y\in\mathbb{N}. \tag{33}$$

Ako uvažimo te relacije, tada dobivamo

$$f_3(5x^4-x^2-227)=f_3(5\cdot 1-1-227)=2. \tag{34}$$

Iz (34) i (33) slijedi kontradikcija, pa je tada jasno da je jedino rješenje jednadžbe (30) upravo $(x,y)\equiv(3,13)$, jer prost broj 3 nije oblika (32). No, formalno gledajući jednadžba je parna pa nju zadovoljava i trojka $(x,y)\equiv(-3,-13)$, a to znači da postoje zapravo 4 rješenja koja je zadovoljavaju, to su:

$(x, y) \in \{(3,13), (-3,13), (3,-13), (-3,-13)\}$, a to vrijedi za početne dane uvjete. Napomenimo još, da (30) predstavlja jednadžbu krivulje, a ne funkcije.

Zadatak 32. Dokazati da je zadovoljeno

$$f_y((x^2+1)^{n+2}+(x^2+2)^{2n+1})=0, n\in\mathbb{N}_0,\ x\in\mathbb{N}; \tag{35}$$

gdje je $y=x^4+3x^2+3.$

Rješenje: Važi da je

$$(x^2+1)^{n+2}+(x^2+2)^{2n+1}=(x^2+1)^n\left((x^4+3x^2+3)-(x^2+2)\right)+$$

$$\left((x^4+3x^2+3)+(x^2+1)\right)^n(x^2+2)=$$

$$(x^2+1)^n(x^4+3x^2+3)-(x^2+1)^n(x^2+2)+$$

$$+(x^4+3x^2+3)^n(x^2+2)+\binom{n}{1}(x^4+3x^2+3)^{n-1}(x^2+1)^1(x^2+2)+\ldots+$$

$$\binom{n}{n-1}(x^4+3x^2+3)^1(x^2+1)^{n-1}(x^2+2)+(x^2+1)^n(x^2+2)=$$

$$(x^4+3x^2+3)\left((x^2+1)^n+\right.$$

$$(x^4+3x^2+3)^{n-1}(x^2+2)+\binom{n}{1}(x^4+3x^2+3)^{n-2}(x^2+1)^1(x^2+2)+\ldots+$$

$$\left.\binom{n}{n-1}(x^2+1)^{n-1}(x^2+2)\right).$$

Ako uzmemo, da je $n=2015$, tada (35) prima oblik

$$f_y((x^2+1)^{2017}+(x^2+2)^{4031})=0.$$

Zadatak 33. Dokazati da je zadovoljeno

$$f_y((2^{2x}+1)^{2n+1}+(2^{2x}+2)^{4n-1})=0, \text{ ako je } n,x\in\mathbb{N},$$

gdje je $y=2^{4x}+3\cdot 2^{2x}+3.$

Uputa za rješenje: Ako u (35) n zamjenimo s $2n-1$ a x sa 2^x dobivamo danu jednakost.

Zadatak 34. Dokazati jednakost

$$f_3\left(\sqrt{\underbrace{44\ldots4}_{2018}\underbrace{88\ldots8}_{2017}9}\right)=1.$$

Generalizirajte !

Uputa za rješenje. Trebamo najprije pokazati da je

$\left(\frac{2\cdot 10^n+1}{3}\right)^2 = \underbrace{44\ldots4}_{n}\underbrace{88\ldots8}_{n-1}9$, $\forall n \in \mathbb{N}$, a odatle je sve vidljivo. Generalizirani oblik glasi

$$f_3\left(\sqrt{\underbrace{44\ldots4}_{n}\underbrace{88\ldots8}_{n-1}9}\right)=1.$$

Zadatak 35. Dokazati da je

$$f_{24}(p^2-1)=0, \tag{36}$$

ako je p prost broj veći od 3.

Rješenje: Znamo da je produkt tri uzastopna prirodna broja djeljiv s $3!=1\cdot 2\cdot 3=6$. Ako je prvi faktor paran, tada je taj produkt uzastopnih brojeva djeljiv još s 4 produkt, dakle on je djeljiv s 24. Na osnovi izrečenog slijedi da je $f_{24}((p-1)p(p+1)) = f_{24}((p-1)(p+1))$, jer brojevi 24 i *p* relativno prosti, dakle tvrdnja (36) je točna.

Zadatak 36. Dokazati da je

$$f_{30}(p^5q-pq^5)=0;\ p,q\in\mathbb{N}.$$

Rješenje: Jasan je rastav

$$p^5q-pq^5 = pq(p-q)(p+q)(p^2+q^2), \tag{37}$$

a odatle zaključujemo, da je $f_2(p^5q-pq^5)=0$, jer je barem jedan od brojeva *p*,*q* $p-q$, paran (ukoliko su brojevi *p i q* neparni, njihova razlika je paran broj).

Dokažimo da je $f_3(p^5q-pq^5)=0$. Nadalje, možemo pisati da je

$p=3k_1+r_1,\ q=3k_2+r_2;\ r_1,r_2\in\{0,1,2\}, k_1,k_2\in\mathbb{N}_0$

Ako uvažimo (37), te izvršimo eksplicitno kongruiranje, tada dobijemo

$f_3(p^5q-pq^5) = f_3(r_1r_2(r_1-r_2)(r_1+r_2)(r_1^2+r_2^2))=0.$

Analogno postupamo za dokaz $f_5(p^5q-pq^5)=0$. Samo je sada

$p=5k_1+r_1,\ q=5k_2+r_2;\ r_1,r_2\in\{0,1,2,3,4\}, k_1,k_2\in\mathbb{N}_0.$

Iz tih uvjeta i dobivenog rastava dobivamo

$$f_5(p^5q-pq^5) = f_5(r_1r_2(r_1-r_2)(r_1+r_2)(r_1^2+r_2^2))=0, \tag{38}$$

jer smo uvažili dane sve mogućnosti za vrijednosti ostataka iz $\{0,1,2,3,4\}$.

Dakle, dokazali smo da je:

$$f_2(p^5q-pq^5)=0,\ f_3(p^5q-pq^5)=0,\ f_5(p^5q-pq^5)=0;$$

pa je pa na ovaj način zadatak riješen.

Napomenimo, da je ovaj zadatak uzet iz [3]**,** *(strana 95), a tamo je za njega dano i rješenje u ovom obliku pomoću kongruencija.*

1° Ako su *p* i *q* prirodni brojevi, dokazati kongruenciju

(1) $$p^5q - pq^5 \equiv (\text{mod } 30).$$

2° da li relacija (1) važi ako su *p* i *q* proizvoljni celi brojevi?

Rješenje pomoću kongruencija: ([3], strana 95, D. Đoković**)** 1° Promatrajmo broj

(2) $$S(p,q) = p^5q - pq^5.$$

Broj $S(p,1)$ može se napisati u obliku

(3) $$S(p,1) = (p-1)p(p+1)(p^2+1).$$

Produkt $(p-1)p(p+1)$ od tri uzastopna broja uvijek je djeljiv sa 6.

Svaki prirodni broj *p* može se izraziti u obliku

$p = 5N + r \quad (N \text{ prirodni broj}; r = 0, 1, 2, 3, 4).$

Ako je $r = 0, 1, 4$ produkt $(p-1)p(p+1)$ je djeljiv je s 5.

U slučajevima kada je $p = 5N + 2$ i $p = 5N + 3$, izraz $p^2 + 1$ postaje respektivno

$$5(5N^2 + 4N + 1), \quad 5(5N^2 + 6N + 2).$$

Prema tome, dokazali smo kongruenciju

(4) $$S(p,1) = p^5 - p \ (\text{mod } 30).$$

Formirajmo sada razliku

(5) $$S(p,q+1) - S(p,q) = (p^5(q+1) - p(q+1)^5) - (p^5q - pq^5) =$$
$$= S(p,1) - 5pq(q^3 + 2q^2 + 2q + 1).$$

Pokazat ćemo da je izraz

$$R(q) = q(q^3 + 2q^2 + 2q + 1) = q(q+1)(q^2 + q + 1)$$

djeljiv sa 6 kada je *q* proizvoljan prirodni broj.

Svaki prirodan broj *q* može se napisati u obliku

$q = 6n + s \quad (n \text{ prirodni broj}; r = 0, 1, 2, 3, 4, 5).$

Prema tome, $R(q)$ ima ove oblike

$$6n(6n+1)(36n^2 + 6n + 1),$$
$$(6n+1)(6n+2)(36n^2 + 18n + 3),$$
$$(6n+2)(6n+3)(36n^2 + 30n + 7),$$
$$(6n+3)(6n+4)(36n^2 + 42n + 13),$$
$$(6n+4)(6n+5)(36n^2 + 54n + 21),$$
$$(6n+5)(6n+6)(36n^2 + 66n + 31).$$

Odavde slijedi $6 \mid R(q)$.

Polazeći od jednakosti (5), dolazimo do ovog zaključka:
Budući da je

$$6 \mid S(p,1) \;\; i \;\; 30 \mid 5q(q+1)(q^2+q+1)$$

i ako se pretpostavi da je $30 \mid S(p,q)$, dobiva se $30 \mid S(p,q+1)$. Ovim je dokazana kongruencija (1).

No, treba reći, da je i kod ovog zadatka postupak rješenja kraći i pregledni, jer smo upotrebili eksplicitnu kongruenciju, premda ovo je rješenje pomoću kongruencije lucidno.

Zadatak 37. Koliko rješenja ima diofantska jednadžba

$$f_x(n) = 0; \; n \in \mathbb{N}. \tag{39}$$

Rješenje: Svaki prirodni broj n se može prikazati u kanonskom obliku $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, gdje su $p_1 \neq p_2 \neq \ldots \neq p_k$ prosti brojevia, a broj njegovih djlilaca je $\tau(n) = (e_1+1)(e_2+1)\cdot \ldots \cdot (e_k+1)$, pa je broj rješenja jednadžbe (39) jednak $\delta(x) = \tau(n) - 1 = (e_1+1)(e_2+1)\cdot \ldots \cdot (e_k+1) - 1$, jer $x = 1$ ne dolazi u obzir.

Napomena 7. Npr. jednadžba $f_x(2^3 \cdot 5^2 \cdot 7 \cdot 11) = 0$ ima

$$\delta(n) = \tau(n) - 1 = 4 \cdot 3 \cdot 2 \cdot 2 - 1 = 47$$

rješenja.

Zadatak 38. Dokazati da je

$$f_9(7^n - 6n - 1) = 0, \; n \in \mathbb{N}_0. \tag{40}$$

Rješenje: Budući je $n = 9k + r \; (r = 0,1,2,3,\ldots,8)$, tada je

$$f_9(7^{9k+r} - 6(9k+r) - 1) =$$

$$= f_9(343^{3k} \cdot 7^r - 6r - 1) = f_9(1^{3k} \cdot 7^r - 6r - 1) = f_9(7^r - 6r - 1) = 0,$$

jer je

$$f_9(7^0 - 6 \cdot 0 - 1) = 0, \; f_9(7^1 - 6 \cdot 1 - 1) = 0, \ldots, \; f_9(7^8 - 6 \cdot 8 - 1) = 0.$$

Možemo (40) dokazati i matematičkom indukcijom, tada iz $g(n) = 7^n - 6n - 1$ slijedi $9 \mid g(0)$. Ako pretpostavimo, da je $g(n) = 7^n - 6n - 1 = 9k$ ($n \in \mathbb{N}$), tada dobivamo

$$g(n+1) = 7^{n+1} - 6(n+1) - 1 = 7(7^n - 6n - 1) + 36n = 9k + 36n,$$

dakle $9 \mid g(n+1)$, pa je time (40) dokazano.

Zadatak 39. (*Mali Fermatov teorem* ili samo *Fermatov teorem*) Ako je $\mathbb{P}$ skup prostih brojeva a $\mathbb{N}$ skup prirodnih brojeva, tada vrijede implikacije:

a) Za svaki $(p,n)\in \mathbb{P}\times \mathbb{N}$ slijedi $f_p(n^p-n)=0;$ (41)

b) Za svaki $(p,n)\in \mathbb{P}\times \mathbb{N}$ i $M(p,n)=1$ slijedi $f_p(n^{p-1})=1.$ (42)

Rješenje: Konzekventa u (42) se može pisati i u obliku $f_p(n^{p-1}-1)=0,$ jer su p i n relativno prosti, dakle $M(p,n)=1$ (najveća zajednička mjera od *p* i *n*).
a) Dokažimo (41) matematičkom indukciom. Vidimo, da je ta implikacija točna za $n=1.$ Pretpostavimo, da vrijedi $f_p(n^p-n)=0\,(n>1).$ Znamo, da je

$$(n+1)^p=n^p+\binom{p}{1}n^{p-1}+\binom{p}{2}n^{p-2}+\ldots+\binom{p}{p-1}p+1,$$

a odatle slijedi

$$f_p((n+1)^p)=f_p(n^p+1), \tag{43}$$

jer je svaki binomni koeficijent u binomnom razvoju djeljiv s p. A odatle dobivamo, da je

$$f_p((n+1)^p-(n+1))=f_p((n^p+1)-(n+1))=f_p(n^p-n)=0,$$

pa je time dokaz u potpunosti napravljen.
b): $f_p(n^p-n)=f_p(n(n^{p-1}-1))=0,$ a odatle je $f_p(n^{p-1}-1)=0,$ jer je $f_p(n)\neq 0$ zbog $M(p,n)=1.$

Zadatak 40. Odrediti prost broj *x* i ceo broj *y* tako da važi

$$1^{x-1}+2^{x-1}+3^{x-1}+\ldots+(x-1)^{x-1}=y^{x-1}.$$

Rješenje: Ako jednadžbu eksplicitno kongruiramo i primijenimo *Fermatov teorem,* tada dobivamo

$$f_x(1^{x-1})+f_x(2^{x-1})+f_x(3^{x-1})+\ldots+f_x((x-1)^{x-1})=f_x(y^{x-1}).$$

Jasno je, da je $f_x(1^{x-1})=f_x(2^{x-1})=f_x(3^{x-1})=\ldots=f_x((x-1)^{x-1})=1,$ jer je *x* prost broj, koji je relativno prost s brojevima: $1,2,3,\ldots,x-1;$ dakle $\underbrace{1+1+1+\ldots+1}_{x-1}=x-1,$ a to znači da je $x-1=f_x(y^{x-1}).$ No, $f_x(y^{x-1})$ je 0 ili 1, što slijedi iz Fermatovog teorema. Ako je $f_x(y^{x-1})=0,$ tada bi dobili da je $x-1=0,$ a to znači da je $x=1,$ što je kontradikcija, jer 1 nije prost broj. Ostala je mogućnost, da je $f_x(y^{x-1})=1,$ a to znači $x-1=1,$ dakle $x=2.$ Ako tu vrijednost uvrstimo u jednadžbu, tada dobivamo da je $y=3.$ Prema tome uređeni par $(x,y)\equiv(2,3)\in \mathbb{P}\times\mathbb{Z}$ je jedino rješenje jednadžbe za dane uvjete.

Zadatak 41. Ako je $a,b,k\in\mathbb{Z}$; $n\in\mathbb{N},$ tada treba dokazati da iz $a+b=km$ slijedi

$$f_m(a^{2n+1}+b^{2n+1})=0.$$

Uputa za rješenje: Uvažavamo identitet

$$a^{2n+1}+b^{2n+1}\equiv(a+b)(a^{2n}-a^{2n-1}b+\ldots-ab^{2n-1}+b^{2n}).$$

Napomena 8. (*Eulerov teorem ili Poopćeni Fermatov teorem*) Ako su a i m relativno prosti brojevi, tj. $M(a,m)=1$, tada važi relacija

$$f_m(a^{\varphi(m)})=1, \tag{44}$$

gdje je $\varphi(m)$ broj prirodnih brojeva, koji su manji od m i s njime su relativno prosti (tu uključujemo i jedinicu). Inače se $\varphi(m)$ računa po formuli

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_r}\right), \tag{45}$$

gdje je kanonski prikaz broja m dan s $m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r}$. Dokaz formule (45) se može naći npr. u $[6]$. Nadalje, vrijedi odnos $\varphi(m)\le\tau(m)$, gdje je broj djelilaca od m dan s

$$\tau(m)=(\alpha_1+1)(\alpha_2+1)\cdot\ldots\cdot(\alpha_r+1). \tag{46}$$

Npr. $m=3\cdot5=15\Rightarrow\varphi(m)=8$, jer

$M(1,m)=M(2,m)=M(4,m)=M(7,m)=M(8,m)=$

$M(11,m)=M(13,m)=M(14,m)=1$, dakle $\Phi(m)=\{1,2,4,7,8,11,13,14\}$ je skup brojeva, koji su relativno prosti s brojem $m=15$ i od njega su manji, pa je kardinalni broj toga skupa jednak 8, dakle $\varphi(m)=\kappa\Phi(m)=8.$

Zadatak 42. Dokazati da je

$$f_6(1^1+2^7+3^{13}+4^{19}+5^{25}+6^{31}+\ldots+2016^{\,12\,091})=0. \tag{47}$$

Rješenje: Da bi zadatak riješili u razumnom vremenu primijenit ćemo teorem *J. Dyer Bennet-a,* koji glasi: Za svaki $a,b,c,d\in\mathbb{N}$ i $x\in\{1,2,6,42,1806\}$ vrijedi da iz antecedente $(f_x(a)=b)\,\&\,(f_x(c)=d)$ slijedi konzekventa $f_x(a^c)=f_x(b^d)$.

Ako primijenimo navedeni teorem dobivamo slijedeće implikacije;

$$((f_6(1)=1)\wedge(f_6(1)=1))\Rightarrow(f_6(1^1)=f_6(1^1)=1),$$
$$((f_6(2)=2)\wedge(f_6(7)=1))\Rightarrow(f_6(2^7)=f_6(2^1)=2),$$
$$((f_6(3)=3)\wedge(f_6(13)=1))\Rightarrow(f_6(3^{13})=f_6(3^1)=3),$$
$$((f_6(4)=4)\wedge(f_6(19)=1))\Rightarrow(f_6(4^{19})=f_6(4^1)=4),$$
$$((f_6(5)=5)\wedge(f_6(25)=1))\Rightarrow(f_6(5^{25})=f_6(5^1)=5),$$
$$((f_6(6)=0)\wedge(f_6(31)=1))\Rightarrow(f_6(6^{31})=f_6(0^1)=0).$$

Uvažimo li ove implikacije i rastav $2016=336\cdot6$, tada je (47) zapravo

$$f_6\left(\sum_{k=1}^{2016} k^{6k-5}\right) =$$

$$= f_6(336\,(1+2+3+4+5+0)) = f_6(56\cdot 15) = f_6(2\cdot 15) = 0,$$

što je i trebalo pokazati.

Napomenimo, da bi dobili:

$$f_6\left(\sum_{k=1}^{2017} k^{6k-5}\right) = 1,\ f_6\left(\sum_{k=1}^{2018} k^{6k-5}\right) = 3,\ f_6\left(\sum_{k=1}^{2019} k^{6k-5}\right) = 0, \ldots$$

Zadatak 43. Ako su: $p_1,\ p_2,\ p_3, \ldots, p_{2016}$ prosti brojevi, ne moraju biti i međusobno različiti, ali niti jedan od njih nije 7, tada vrijedi relacija

$$f_7(p_1^{2016} + p_2^{2016} + p_3^{2016} + \ldots + p_{2016}^{2016}) = 0. \tag{48}$$

Rješenje: Jasno je, da je

$$f_7(p_i^{2016}) = f_7(p_i^{6\cdot 336}) = f_7((f_7(p_i^{7-1}))^{336}) = f_7(1^{336}) = 1.$$

Primijenili smo *Mali Fermatov teorem*, pa smo dobili

$$f_7(\underbrace{1+1+\ldots+1}_{2016}) = f_7(2016) = f_7(7\cdot 288) = 0.$$

Zadatak 44. Ako je $a = 1!\cdot 2!\cdot 3!\cdot \ldots \cdot 100!$ onda je

$$f_a(5050\,!) = 0. \tag{49}$$

Rješenje: Dokažimo da je $\dfrac{5050\,!}{1!\cdot 2!\cdot 3!\cdot \ldots \cdot 100\,!} \in \mathbb{N}.$

Znamo, da je

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!};\ 1+2+3+\ldots+100 = 5050. \tag{50}$$

Iz

$$\binom{1}{1}\binom{1+2}{2}\binom{1+2+3}{3}\cdot\ldots\cdot\binom{1+2+3+\ldots+100}{100} \in \mathbb{N}$$

i (50) slijedi

$$\frac{1!}{1!\,0!}\cdot\frac{(1+2)!}{2!\,1!}\cdot\frac{(1+2+3)!}{3!\,(1+2)!}\cdot\ldots\cdot\frac{(1+2+\ldots+99)!}{99!\,(1+2+\ldots+98)!}\cdot\frac{(1+2+\ldots+100)!}{100!\,(1+2+\ldots+99)!} =$$

$$= \frac{(1+2+\ldots+100)!}{1!\,2!\cdot\ldots\cdot 100\,!} = \frac{5050\,!}{1!\,2!\cdot\ldots\cdot 100\,!} \in \mathbb{N},$$

a to znači da je (49) točno.

Sličnim postupkom lako možemo dokazati i općenitije slučajeve;

Slučaj 1.: $\dfrac{(1+2+\ldots+n)!}{1!\,2!\cdot\ldots\cdot n!}\in\mathbb{N}$

Slučaj 2.: $\dfrac{(k_1+k_2+\ldots+k_n)!}{k_1!\,k_2!\cdot\ldots\cdot k_n!}\in\mathbb{N}$, gdje je $n,k_i\in\mathbb{N}$ $(1\le i\le n)$.

Zadatak 45. Dokazati da za svaki prost broj $p>3$ postoji $k\in\mathbb{N}$ tako da je

$$f_{p^2}(24k+1)=0. \tag{51}$$

Rješenje: U Zadatku 35. dokazano je $f_{24}(p^2-1)=0$, a to znači da je $p^2-1=24k$ ili $p^2=24k+1$, dakle (51) je točno.

Zadatak 46. (*Poopćeni Wilsonov teorem*). Dokazati da je, za svaki prost broj p i svaki prirodni broj *n*, zadovoljena jednakost

$$f_p(((p-1)!)^{2n-1})=p-1.$$

Rješenje: Napomenimo, da *Wilsonov teorem* u standardnoj oznaci glasi $(p-1)!\equiv -1(\mathrm{mod}\,p)$ ili $(p-1)!\equiv p-1(\mathrm{mod}\,p)$.

Općenito iz razvoja $(p-1)^{2n-1}=p^{2n-1}-\binom{2n-1}{1}p^{2n-2}+\ldots+\binom{2n-1}{2n-2}p-1$ vidimo da slijedi $f_p(((p-1)!)^{2n-1})=f_p((p-1)^{2n-1})=f_p(-1)=p-1,$ pa je time teorem dokazan.

Napomena 9. Odredimo jednu klasu rješenja diofantske jednadžbe

$$f_p(x^{p-1}+((p-1)!)^y)=0;\ p\in\mathbb{P}.$$

Naime, ako uvažimo *Fermatov teorem* i *Poopćeni Wilsonov teorem*, tada dobivamo jednu klasu rješenja (x,y) uz uvjete: $x\in\mathbb{N}$, $M(x,p)=1$, $y\in 2\mathbb{N}-1$. Svakako, da ne znači da je ovo i opće rješenje dane jednadžbe.

Zadatak 47. Ako je $f_7(a)\ne 0$ i $f_7(b)\ne 0$ onda je

$$f_{49}(a^{42}-b^{42})=0. \tag{52}$$

Rješenje: Neka je

$$a=7k_1+m_1,\ b=7k_2+m_2;\ m_1,m_2\in\{1,\ldots,6\}. \tag{53}$$

Tada važi

$$f_{42}(a^{42})=f_{42}((7k_1+m_1)^{42})=f_{42}((7k_1)^{42}+\binom{42}{1}(7k_1)^{41}m_1^1+\ldots+\binom{42}{41}(7k_1)^1m_1^{41}+m_1^{42}),$$

odatle je $f_{49}(a^{42})=f_{49}(m_1^{42})$. Analogno dobivamo i $f_{49}(b^{42})=f_{49}(m_2^{42})$. Iz te dvije relacije slijedi, da je

$$f_{49}(a^{42}-b^{42})=f_{49}(m_1^{42}-m_2^{42}). \tag{54}$$

Ako uvažimo *Mali Fermatov teorem*, tada je

$$f_7(f_7(m_1^6)^7 - (f_7(m_2^6)^7) = f_7((1)^7 - (1)^7) = 0,$$

a pogotovo je $f_{49}(m_1^{42} - m_2^{42}) = 0$. Odatle i iz (54) slijedi da je tvrdnja zadatka zadovoljena.

Zadatak 48. Ako je $f_p(a) \neq 0$, $f_p(b) \neq 0$ i p prost broj, onda je

$$f_{p^2}(a^{p(p-1)} - b^{p(p-1)}) = 0.$$

Uputa za rješenje: To je generalizacija Zadatka 47.

Zadatak 49. Riješiti diofantsku jednadžbu

$$x_1^2 + x_2^2 + x_3^2 = 2016\ x_4^2 + 7. \tag{55}$$

Rješenje: Svaki se prirodni broj može prikazati u obliku $a = 8k + r$, gdje je $r \in \{0,1,2,...,7\}$. Tada iz:

$$f_8(0^2) = 0,\ f_8(1^2) = 1,\ f_8(2^2) = 4,\ f_8(3^2) = 1,\ f_8(4^2) = 0,...$$

slijedi da je $f_8(a^2) \in \{0,1,4\}$. Ako (55) eksplicitno kongruiramo, tada je

$$f_8(x_1^2) + f_8(x_2^2) + f_8(x_3^2) = 7. \tag{56}$$

Na osnovi iznesenog slijedi da je $f_8(x_1^2), f_8(x_2^2), f_8(x_3^2) \in \{0,1,4\}$, pa odatle i iz (56) slijedi:

$0+0+0 \neq 7, 0+0+1 \neq 7, 0+1+1 \neq 7, 1+1+1 \neq 7, 0+0+4 \neq 7, 0+1+4 \neq 7, 1+1+4 \neq 7;$

a to znači da jednadžba (55) nema rješenja za $x_1, x_2, x_3, x_4 \in \mathbb{N}$, ili čak za $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.

Zadatak 50. Riješiti diofantsku jednadžbu

$$x_1^{2016} + x_2^{2016} + ... + x_{14}^{2016} = 2015. \tag{57}$$

Rješenje: Svaki se prirodni broj može prikazati u obliku $a = 16k + r$, gdje je $r \in \{0,1,2,..., 15\}$.

Lako dobivamo da je $f_{16}(a^4) \in \{0,1\}$. Ako (57) eksplicitno kongruiramo po bazi 16, tada je

$$(f_{16}(x_1^4))^{504} + (f_{16}(x_2^4))^{504} + ... + (f_{16}(x_{14}^4))^{504} = 15,$$

jer je $f_{16}(2015) = 15$. No, to je kontradikcija, jer je

$$(f_{16}(x_1^4))^{504} + (f_{16}(x_2^4))^{504} + ... + (f_{16}(x_{14}^4))^{504} \leq 14.$$

Prema tome, dana jednadžba nema rješenja.

Zadatak 51. Dokazati da je

$$f_{13}(3^{10^n}) = 3 \text{ za proizvoljno } n \in \mathbb{N}.$$

Rješenje: $f_{13}(3^{10^n}) = f_{13}((3^3)^{\underbrace{33\ldots3}_{n}} \cdot 3) = f_{13}((1)^{\underbrace{33\ldots3}_{n}} \cdot 3) = 3.$

Napomena 10. Vratimo se na Napomenu 1. i recimo da možemo generalizirati taj zadatak u obliku, koji glasi $f_7(2222^{\underbrace{55\ldots5}_{n}} + 5555^{\underbrace{22\ldots2}_{n}}) = 0, n \in \mathbb{N}$, a možemo ga dokazati po analogiji s prvom verzijom. Ako izvršimo specijalizaciju da je $n = 10$, tada bi dobili broj $2222^{\underbrace{55\ldots5}_{10}} + 5555^{\underbrace{22\ldots2}_{10}}$, koji ima 18 596 022 524 znamenaka.

Literatura:

[1] Š. Arslanagić, *Dokaz Leme 1.; Direktna korespodencija,* Sarajevo, 2016.

[2] H. Jamak, *Kongruencije* , Triangle, Vol. 3 (1999), No 2, No 3, Sarajevo, 1999.

[3] D.S. Mitrinović, *Zbornik matematickih problema*, Zavod za izdavanje udžbenika, Beograd, 1962.

[4] I. Niven & H. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons (2000).

[5] B. Pavković, *O djeljivosti brojeva*, HMD, Zbornik radova (Prvi kongres nastavnika matematike); Zagreb, 2000.

[6] B. Pavković, B. Dakić, P. Mladinić, *Elementarna teorija brojeva*, HMD, Zagreb, 1994.

[7] S.Y. Yan, *Number Theory for Computing,* Springer – Verlang, Berlin, 2002.

Primljeno u redakciju 22.07.2017; Revidirana verzija 02.09.2017. i 08.09.2017.
Dostupno na internetu 11.09.2017.