

1. Вјежбе

* Дјеливост *

1. Наћи све $n \in \mathbb{N}$ за које је $3^{2n+1} - 2^{2n+1} - 6^n$ прост број.

$$\begin{aligned}
 3^{2n+1} - 2^{2n+1} - 6^n &= 3 \cdot 3^{2n} - 2 \cdot 2^{2n} - 2^n \cdot 3^n \\
 &= \underline{2 \cdot 3^{2n}} + \underline{3^{2n}} - \underline{2 \cdot 2^{2n}} - \underline{2^n 3^n} \\
 &= 2(3^{2n} - 2^{2n}) + 3^n(3^n - 2^n) \\
 &= 2(3^n - 2^n)(3^n + 2^n) + 3^n(3^n - 2^n) \\
 &= (3^n - 2^n)(2 \cdot 3^n + 2^{n+1} + 3^n) \\
 &= (3^n - 2^n) \underbrace{(3^{n+1} + 2^{n+1})}_1
 \end{aligned}$$

Овај број ће бити прост ако је $3^n - 2^n = 1$. То је случај само за $n=1$. Проверимо:

$$n=1 : 3^3 - 2^3 - 6 = 27 - 8 - 6 = 13 \rightarrow \text{прост} \checkmark$$

2. Наћи $\text{NZD}(8 \ 303 \ 668 \ 297, 8 \ 287 \ 306 \ 393)$

Користимо Еуклидов алгоритам:

$$8 \ 303 \ 668 \ 297 = 1 \cdot 8 \ 287 \ 306 \ 393 + 16 \ 361 \ 904$$

$$8 \ 287 \ 306 \ 393 = 506 \cdot 16 \ 361 \ 904 + 8 \ 182 \ 969$$

$$16 \ 361 \ 904 = 1 \cdot 8 \ 182 \ 969 + 4034$$

$$8 \ 182 \ 969 = 2027 \cdot 4034 + \textcircled{2017} \rightarrow \text{ово је NZD}$$

$$4034 = 2 \cdot 2017$$

$$a = 2017 \cdot 2029^2$$

$$b = 2017 \cdot 2027^2$$

3. Наћи све бројне системе у којима се број 20 записује само помоћу цифара из скупа $\{0, 1, 2, \dots, 9\}$.

Прво примјетимо да су сви бројеви системи са основом не већом од 10 у реду, јер се у њима користе све цифре које су дозвољене.

На примјер:

$$20 = 2 \cdot 7^1 + 6 \cdot 7^0 = \langle 2, 6 \rangle_7$$

Бројни системи са основом 21 и више нису у реду, јер је у њима 20 једноцифрени број, а та цифра није међу дозвољеним.

$$20 = 20 \cdot 21^0 = \langle 20 \rangle_{21}$$

Бројне системе са основом 11, 12, ..., 20 ћемо и даље проверити.

$$20 = 1 \cdot 11^1 + 9 \cdot 11^0 \quad 20 = \langle 1, 9 \rangle_{11}$$

$$20 = 1 \cdot 12^1 + 8 \cdot 12^0 \quad 20 = \langle 1, 8 \rangle_{12}$$

$$20 = 1 \cdot 13^1 + 7 \cdot 13^0 \quad 20 = \langle 1, 7 \rangle_{13}$$

$$20 = 1 \cdot 14^1 + 6 \cdot 14^0 \quad 20 = \langle 1, 6 \rangle_{14}$$

$$20 = 1 \cdot 15^1 + 5 \cdot 15^0 \quad 20 = \langle 1, 5 \rangle_{15}$$

$$20 = 1 \cdot 16^1 + 4 \cdot 16^0 \quad 20 = \langle 1, 4 \rangle_{16}$$

$$20 = 1 \cdot 17^1 + 3 \cdot 17^0 \quad 20 = \langle 1, 3 \rangle_{17}$$

$$20 = 1 \cdot 18^1 + 2 \cdot 18^0 \quad 20 = \langle 1, 2 \rangle_{18}$$

$$20 = 1 \cdot 19^1 + 1 \cdot 19^0 \quad 20 = \langle 1, 1 \rangle_{19}$$

$$20 = 1 \cdot 20^1 + 0 \cdot 20^0 \quad 20 = \langle 1, 0 \rangle_{20}$$

Дакле, сви бројни системи са основом од 2 до 20 су добри.

4. Доказати да производ 5 узастопних природних бројева никада није потпуни квадрат.

Пис. $n(n+1)(n+2)(n+3)(n+4) = m^2$.

Прво примјетимо да сви бројеви фактори са исте стране јављају са парним експонентом. Сви бројеви ≥ 5 се јављају у тачно једном од ових чинилаца, па се они увјек јављају у тачно једном са парним експонентом.

Одатиме закључујемо да су сви чиниоци неки од следећих облика:

$$k^2, 2k^2, 3k^2, 6k^2$$

Како је чиниоца 5, а облика 4 $\Rightarrow$ постоје 2 чиниоца са истом шифром:

$$n+i = sk_i^2, \quad n+j = sk_j^2 \quad 0 \leq i < j \leq 4, \quad s \in \{1, 2, 3, 6\}.$$

Тада је:

$$4 \geq j-i = s(k_j^2 - k_i^2) \geq k_j^2 - k_i^2 \Rightarrow k_j^2 - k_i^2 \leq 4$$

Ово је могуће само за $k_j = 2$ и $k_i = 1$, јер разлике узастопних квадрата расту. $(3^2 - 2^2 = 9 - 4 = 5 > 4)$

$$\text{За } k_i = 1 \text{ и } k_j = 2 \text{ је } k_j^2 - k_i^2 = 3 \Rightarrow 3s \leq 4 \Rightarrow s = 1.$$

Закле, како је $n+i = 1$, први чинилац је 1, а остали 2, 3, 4, 5.

Али $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5! = 120$, а ово није потпуни квадрат.

Тиме је доказ завршен.

Теорема: (Ердош-Селфриџ) Производ на колико узастопних природних бројева (бар 2) никада није потпуни степени природног броја.

5. Обзначено са $f(x)$ суму цифара природног броја x . Доказати да за сваки природан број n постоји природан број p такав да j -на $f(npx) = f(x)$ ита рјешенје x које не садржи цифру 9 у свом декадном запису.

Треба да : • сума цифара $npx =$ сума цифара xs и
• x нема 9 у декадном запису

Нека је $n \in \mathbb{N}$ задат.

Посматрајмо бројеве $9, 99, 999, \dots, \underbrace{99 \dots 9}_{n+1}$.

Како их има $n+1$, нека 2 међу њима дају исти остатак при дијелењу са n .

Нека су то $\underbrace{99 \dots 9}_i$ и $\underbrace{99 \dots 9}_j$ и $i > j$. Дакле,

$$\underbrace{99 \dots 9}_i \equiv \underbrace{99 \dots 9}_j \pmod{n} \Leftrightarrow n \mid \underbrace{99 \dots 9}_i - \underbrace{99 \dots 9}_j = \underbrace{99 \dots 90 \dots 0}_{i-j} \underbrace{0 \dots 0}_j$$

Одаберимо : $p = \frac{\underbrace{9 \dots 90 \dots 0}_n}{n}$. Тврдимо да је ово изражење p .

Сада још треба показати да $f(\underbrace{9 \dots 9}_k x) = f(x)$ ита рјешенје $x \in \mathbb{N}$ које нема 9 у свом ^{декадном} запису.

Обично $k = 8t + r$, $0 \leq r \leq 7$ (овај облик ће нас довести до рј.).

Доказаћемо да за изражење рјешенје можемо узети

$$x = \underbrace{88 \dots 88}_t r \underbrace{88 \dots 88}_k$$

$$f(x) = 8t + r + 8k = k + 8k = 9k$$

$$\begin{array}{r} \underbrace{99 \dots 9}_k x = (10^k - 1)x = 10^k x - x = \begin{array}{r} \underbrace{88 \dots 88}_t r \underbrace{88 \dots 880 \dots 0}_k \\ - \underbrace{8 \dots 88}_t r \underbrace{8 \dots 8}_k \\ \hline \underbrace{8 \dots 8}_t r \underbrace{8 \dots 80 \dots 00}_{(k-1-t)} \underbrace{7-r}_{t} \underbrace{1 \dots 11}_k 2 \end{array} \end{array}$$

$$f(\underbrace{9 \dots 9}_k x) = 8t + r + (k-1-t)8 + 7-r + 2 + k-1 = 9k.$$

6. Наћи све десетичноуформене бројеве $\overline{a_0 a_1 \dots a_9}$ такве да је:

- a_0 - број појављивања цифре 0 у том броју
- $\vdots$
- a_9 - број појављивања цифре 9 у том броју.

Нека је k број позитивних цифара међу $a_1, a_2, \dots, a_9$. Приметићемо да је

$$\underbrace{a_1 + a_2 + \dots + a_9}_{\text{неких } k \text{ је поз.}} = k + 1$$

(ијеро је укупан број јединица, двојки, ..., деветки укупан број позитивних цифара у десетичном броју, а то је једнак броју поз. цифара међу $a_1, \dots, a_9 + 1$ јер је a_0 ст. позитивна).

Једина могућност је да у $k-1$ од њих биди 1, а 1 је 2 (осим у 0).

Закле, једина цифра која може бити већа од 2 је a_0 .

Такође, уколико за неко $i > 2$ важи $a_i > 0$ (нпр. $a_5 > 0$), онда $a_i = i$

($a_0 = 5$), јер се само то може јавити број већи од 2.

Закле, колико има позитивних цифара међу $a_1, \dots, a_9$?

$a_1 \geq 0, a_2 \geq 0$ и неко $a_i \geq 0$, па највише $k \leq 3$.

$k=1$ 8 могућ $\rightarrow a_0 = 8$
 $a_9 = 1$, па $a_1 > 1$ ∇ са $k=1$

$k=2$ 7 могућ $\rightarrow a_0 = 7$
 $a_7 = 1$
 $a_1 > 0$ $\overline{7 a_1 0 0 0 0 0 1 0 0}$

Немогуће, јер ако $a_1 = 1, a_1 = 2$ ∇ , ако $a_1 = 2, a_2 > 0$ ∇ $k=2$.

$k=3$ 6 могућ $\rightarrow a_0 = 6$ $\overline{6 a_1 a_2 0 0 0 1 0 0 0}$
 $a_6 = 1$
 $a_1 > 0$ $\downarrow \quad \downarrow$
 $2 \quad 1$

Закле, једино решење је број 6210001000 .

2. вјесноб

* Конструкције по модулу *

Знајте: Ејлерова функција броја каже да је бројева од 1 до n узастопних са n . Означавано је са $\varphi(n)$.

Примјер: • $\varphi(10) = 4$

① 2, ③ 4, 5, 6, ⑦ 8, ⑨ 10

• $\varphi(7) = 6$

①, ②, ③, ④, ⑤, ⑥

• $\varphi(p) = p-1$ за сваки p -проста

Теорема: Нека је $n \geq 2$ природан број дат у каноничком облику $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots$

Тада је

$$\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \cdot \prod_{\substack{p|n \\ (p \text{ проста})}} \left(1 - \frac{1}{p}\right).$$

Теорема: (Ејлерова теорема) Нека је $a \in \mathbb{Z}$, $m > 0$ и $(a, m) = 1$. Тада је

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Последица (Мала Ферматова Т.) Нека је p проста, $a \in \mathbb{Z}$, $p \nmid a$. Тада је

$$a^{p-1} \equiv 1 \pmod{p}.$$

1. Наћи све $n \in \mathbb{N}$ тако да се број 2012^n завршава цифром 2012.

• $n=1 \checkmark$

• $n=2$

Погледајте: • Број је један са 4 ако му је десеторици завршетак један са 4.
• $\sim 11 \sim 8$ десеторици $\sim 11 \sim 8$ десеторици

2012 је један са 4 $\Rightarrow 2012^n$ је један са 8.

Али сваки број чије у десеторици завршетак 2012 није један са 8 (даје остатак 4). Стога је једино рјешење $n=1$.

2. Наћи све природне бројеве p и q тако да је $p^2 + 2012pq + q^2$ потпуни квадрат.

Разгледајмо на случајеве:

• $p=q=2$

$$p^2 + 2012pq + q^2 = 8 + 4 \cdot 2012 = 8056 \text{ што није потпуни квадрат!}$$

• $p=2, q \geq 3$

Бити због тога да објектима дају износ до модула 8. Могући остаци потпуних квадрата при дијеленју са 8 су:

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 1 \pmod{8}, \quad 4^2 \equiv 0 \pmod{8}, \quad 5^2 \equiv 1 \pmod{8}, \quad 6^2 \equiv 4 \pmod{8}, \quad 7^2 \equiv 1 \pmod{8}$$

Квадрати свих непарних бројева дају остатак 1 при дијеленју са 8. (*)

$$p^2 + 2012pq + q^2 = 4 + 4024q + q^2 \stackrel{(*)}{\equiv} 4 + 0 + 1 \equiv 5 \pmod{8}$$

Дакле, $p^2 + 2012pq + q^2$ не може у овом случају бити потпуни квадрат јер 5 не јавља међу остацима.

Остало је још да анализирамо случај:

$$p, q \geq 3$$

Сада ћемо анализирали по модулу 4. Хајде да видимо какве ће остацик
имати квадрати по модулу 4.

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 \equiv 0 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

Парни квадрати дају остатак 0, а непарни 1.

$$p^2 + 2012pq + q^2 \equiv 1 + 0 + 1 = 2 \pmod{4} \rightarrow \text{није никада остатак}$$

одувног квадрата по мод 4.

3. Нека је $A = 2022^{2023}$. Нека је B збир цифара броја A , нека је
 C збир цифара броја B и D збир цифара броја C . Наћи D .

Подајемо: Број је глатан са 9 ако му је збир цифара глатан са 9.

$$A \equiv 0 \pmod{9}$$

$$A \equiv B \equiv C \equiv D \pmod{9} \Rightarrow 9 \mid D \text{ и } D \geq 1 \Rightarrow D \geq 9.$$

$$A < 10\,000^{2023} = (10^4)^{2023} = 10^{8092}$$

$$A \leq \underbrace{9 \dots 9}_{8092}$$

$$B \leq 9 \cdot 8092 = 72\,828 < 99\,999$$

$$C \leq 5 \cdot 9 = 45$$

$$D \leq 3 + 9 = 12 \quad \text{и} \quad D \equiv 0 \pmod{9}$$

$$\Rightarrow \boxed{D = 9}$$

4. У скупу $\mathbb{N}$ ријешити једначину $2^x = 3^y + 5$.

Лакко нађемо два рјешења: $(x_1, y_1) = (3, 1)$ и $(x_2, y_2) = (5, 3)$.

Претпоставимо да је $x \geq 6$. Показати ћемо да имага нема рјешења.

$$2^x \equiv 0 \pmod{64}$$

$$3^y + 5 \equiv 0 \pmod{64}$$

$$3^y \equiv -5 \pmod{64}$$

$$3^y \equiv 59 \pmod{64}$$

$$3^i \pmod{64} : \underbrace{3, 9, 27, 17, 51, 25, 11, 33, 35, 41, 59, 49, 19, 57, 43, 1, 3, 9, \dots}_{\text{ових 16 се врати у кругу}}$$

$$\Rightarrow y = 16k + 11 \quad (16k \text{ због периодичности})$$

$$3^y = 3^{16k+11} = (3^{16})^k \cdot 3^{11} \equiv 1^k \cdot 7 = 7 \pmod{17}$$

$$\downarrow \\ 3^{\varphi(17)} \equiv 1 \pmod{17}$$

$$3^i \pmod{17} : 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7$$
$$\downarrow \\ 3^{11} \equiv 7 \pmod{17}$$

$$\text{Дакле је } 3^y + 5 \equiv 12 \pmod{17}$$

$$\Rightarrow 2^x \equiv 12 \pmod{17}$$

$$2^i \pmod{17} : \underbrace{2, 4, 8, 16, 15, 13, 9, 1, 2, 4, \dots}_{\text{нема 12!}}$$

$$\Rightarrow 2^x \not\equiv 12 \pmod{17} \rightarrow \text{нема рјешења за } x \geq 6.$$

Да је 12 било у овом низу кренути исцрпљено са $x \geq 7$ или $y \geq 4$...

Шта ако $16+1$ није био прави број?

Зовемо је да $\varphi(\text{модула}) = 16$ иу. број који нам треба.

5. Наћи све $n \in \mathbb{N}$ за које је:

а) $\varphi(n) = 4$; б) $\varphi(n) = 18$; в) $\varphi(n) = 12$.

а) Разложимо 4 на множоре

$$4 = 1 \cdot 4 = 2 \cdot 2 = 1 \cdot 2 \cdot 2 \quad n = p_1^{\alpha_1} \cdot p_k^{\alpha_k}$$

$$\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1)$$

• 4 $k=1$

$$p_1^{\alpha_1-1} (p_1 - 1) = 4$$

• $\alpha_1 = 1$ $p_1 = 5$ $(p_1, \alpha_1) = (5, 1)$

• $\alpha_1 > 1$ $p_1 | 4 \Rightarrow p_1 = 2$

$$\alpha_1 = 3$$

$$(p_1, \alpha_1) = (2, 3)$$

$$n = 5^1 = 5 \quad n = 2^3 = 8$$

• 2 · 2 $k=2$

$$p_1^{\alpha_1-1} (p_1 - 1) = 2$$

$$p_2^{\alpha_2-1} (p_2 - 1) = 2$$

• $\alpha_1 = 1$ $p_1 = 3$ $(p_1, \alpha_1) = (3, 1)$

• $\alpha_1 > 1$ $p_1 | 2 \Rightarrow p_1 = 2$ $\alpha_1 = 2$ $(p_1, \alpha_1) = (2, 2)$

Како $(p_2, \alpha_2) = (3, 1)$

$$(p_2, \alpha_2) = (2, 2)$$

(обрати пажњу да су р-ови могуће различити у n)

$$n = 3^1 \cdot 2^2 = 3 \cdot 4 = 12$$

$$1 \cdot 4 \quad p_1^{\alpha_1-1}(p_1-1)=1 \Rightarrow (p_1, \alpha_1) = (2, 1)$$

$$p_2^{\alpha_2-1}(p_2-1)=4 \Rightarrow (p_2, \alpha_2) = (5, 1) \quad (p_2, \alpha_2) = (2, 3)$$

$$n = 2^1 \cdot 5^1 = 10$$

$$\cdot 1 \cdot 2 \cdot 2 \quad (p_1, \alpha_1) = (2, 1)$$

$$(p_1, \alpha_2) = (3, 1) \quad (p_1, \alpha_2) = (2, 2)$$

$$(p_3, \alpha_3) = (3, 1) \quad (p_3, \alpha_3) = (2, 2) \quad \text{Нема таквот } n!$$

$$n \in \{5, 8, 10, 12\}$$

Можемо ипорисати све случајеве 1. Непуно, само кадс нм се јави
Непарни n годано и $n \cdot 2$.

$$u) \quad \varphi(n) = 12$$

$$12 = 2 \cdot 6 = 2 \cdot 2 \cdot 3 = 3 \cdot 4$$

$$\cdot 12 \quad p_1^{\alpha_1-1}(p_1-1) = 12$$

$$\cdot \alpha_1 = 1 \quad p_1 = 13 \quad (p_1, \alpha_1) = (13, 1)$$

$$\cdot \alpha_1 > 1 \quad p_1 \mid 12 \Rightarrow p_1 = 2 \vee p_1 = 3$$

$$p_1 = 2$$

$$p_1 = 3$$

$$2^{\alpha_1-1} = 12 \quad \text{Нема } p_j!$$

$$3^{\alpha_1-1} \cdot 2 = 12 \quad \text{Нема } p_j!$$

$$\Rightarrow n = 13 \quad \text{и} \quad \text{годано} \quad n = 26$$

$$\cdot 2 \cdot 6 \quad p_1^{\alpha_1-1}(p_1-1) = 2$$

$$\cdot \alpha_1 = 1 \quad p_1 = 3 \quad (\alpha_1, p_1, \alpha_1) = (3, 1)$$

$$\cdot \alpha_1 > 1 \quad p_1 \mid 2 \quad p_1 = 2 \quad \alpha_1 = 2$$

$$(p_1, \alpha_1) = (2, 2)$$

$$p_2^{\alpha_2-1} (p_2-1) = 6$$

$$\cdot \alpha_2 = 1 \quad p_2 = 7 \quad (p_2, \alpha_2) = (7, 1)$$

$$\cdot \alpha_2 > 1 \quad p_2 \mid 6 \Rightarrow p_2 = 3 \vee p_2 = 2$$

$$p_2 = 2$$

$$2^{\alpha_2-1} = 6 \text{ Нема } p_j.$$

$$p_2 = 3$$

$$3^{\alpha_2-1} \cdot 2 = 6$$

$$\alpha_2 = 2$$

$$(p_2, \alpha_2) = (3, 2)$$

$$n = 3^1 \cdot 7^1 = 21 \quad \text{и} \quad n = 42$$

$$n = 2^2 \cdot 7^1 = 28$$

$$n = 2^2 \cdot 3^2 = 36$$

$$\cdot 3 \cdot 4 \quad p_1^{\alpha_1-1} (p_1-1) = 3$$

$$\cdot \alpha_1 = 1 \quad p_1 = 4 \quad \times$$

$$\cdot \alpha_1 > 1 \quad p_1 \mid 3$$

$$p_1 = 3$$

$$3^{\alpha_1-1} \cdot 2 = 3 \quad \times \quad \text{Нема рјешетка!}$$

Лакше, не морамо никада разматрати отко радозналост где се јави $3 \cdot 42$
 $n \in \{12, 21, 26, 28, 36\}$

$$\delta) \quad \varphi(n) = 18 \quad (\text{гопати})$$

$$18 = 2 \cdot 9 = 3 \cdot 6 = 2 \cdot 3 \cdot 3$$

годње се : $n \in \{19, 22, 38, 54\}$.

* Конструкције по модулу - наставак *

1. Доказати да је сваки непаран прост чинилац броја n^2+1 облика $4k+1$.

Сваки непаран прост број је облика $p=4k+1$ или $p=4k+3$.

Пос. $\exists p \mid n^2+1$ и $p=4k+3$.

$$p \mid n^2+1 \Leftrightarrow n^2+1 \equiv 0 \pmod{p}$$

$$\Leftrightarrow n^2 \equiv -1 \pmod{p} \quad /^{2k+1}$$

$$n^{2 \cdot (2k+1)} \equiv (-1)^{2k+1} \pmod{p}$$

$$n^{4k+2} \equiv -1 \pmod{p}$$

$$n^{p-1} = n^{4k+2} \equiv -1 \pmod{p} \quad \downarrow \text{ са законом Фермаовог Т.}$$

2. У корпи се налази одређен број јаја. Ако их бројито са 2, остаци 1, ако их бројито са 3, остаци 2, ако их бројито са 5 остаци 3, ако их бројито са 7 остаци 4. Колико најмање јаја може бити у корпи?

Записујемо изражено најмање x које задовољава све дате конструкције:

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

Показатељно поступак који се рјешавају овакве конструкције.

Рјешенје x добићемо као збир 4 појединачна рјешенја:

$$x = x_1 + x_2 + x_3 + x_4$$

тј. x_1, x_2, x_3, x_4 изађу из ове:

$$x_1 \equiv 1 \pmod{2} \quad , \quad x_1 \equiv 0 \pmod{105}$$

$$x_2 \equiv 2 \pmod{3} \quad , \quad x_2 \equiv 0 \pmod{70}$$

$$x_3 \equiv 3 \pmod{5} \quad , \quad x_3 \equiv 0 \pmod{42}$$

$$x_4 \equiv 4 \pmod{7} \quad , \quad x_4 \equiv 0 \pmod{30}$$

Замисли, онако x ће бити оно које изађу из ове.

Уземо појединачно:

$$x_1 = 105k_1 \quad \text{и} \quad 105k_1 \equiv 1 \pmod{2} \quad \text{узмено } k_1 = 1 \Rightarrow \boxed{x_1 = 105}$$

$$x_2 = 70k_2 \quad \text{и} \quad 70k_2 \equiv 2 \pmod{3} \quad \text{узмено } k_2 = 2 \Rightarrow \boxed{x_2 = 140}$$

$$x_3 = 42k_3 \quad \text{и} \quad 42k_3 \equiv 3 \pmod{5} \quad \text{узмено } k_3 = 4 \Rightarrow \boxed{x_3 = 168}$$

$$x_4 = 30k_4 \quad \text{и} \quad 30k_4 \equiv 4 \pmod{7} \quad \text{узмено } k_4 = 2 \Rightarrow \boxed{x_4 = 60}$$

Сада је:

$$x = 105 + 140 + 168 + 60 = 473.$$

Закле, једно рјешенје система је 473.

На основу кинеске Т. о остацима знамо да ова рјешенја могу бити конгруентна по модулу $2 \cdot 3 \cdot 5 \cdot 7 = 210$.

Како је

$$473 \equiv 53 \pmod{210}$$

53 је најмање рјешенје.

3. Да ли постоји низ од 2011 узajаmних природних бројева так да ниједан од њих није апсолутно прост број?

Такав низ бројева постоји.

Нека у $p_1, p_2, \dots, p_{4022}$ први 4022 апсолутно простих бројева. Посматрајмо систем конгруенција:

$$x \equiv 0 \pmod{p_1 p_2}$$

$$x \equiv -1 \pmod{p_3 p_4}$$

$$x \equiv -2 \pmod{p_5 p_6}$$

$$\vdots$$

$$x \equiv -2010 \pmod{p_{4021} p_{4022}}$$

Како у модули узajаmно апсолутно простих парова по кинеској теорем о овом систему има рјешење x . Посматрајмо бројеве

$$x, x+1, \dots, x+2010.$$

Они чине низ од 2011 узajаmних природних бројева, а како сваки од њих има бар 2 различита апсолутно проста дјелитеља, овај низ испуњава услове из поставке.

4. Покажите да за све $a_1, a_2, \dots, a_n$ постоји природан број b такав да у $\{ba_1, ba_2, \dots, ba_n\}$ сви појединачни аспекти.

Замислимо

$$\begin{aligned} a_1 &= p_1^{\alpha_{11}} p_2^{\alpha_{12}} \dots p_k^{\alpha_{1k}} \\ &\vdots \\ a_n &= p_1^{\alpha_{n1}} p_2^{\alpha_{n2}} \dots p_k^{\alpha_{nk}} \end{aligned}$$

тј. у $p_1, \dots, p_k$ различити прости бројеви, при чему допуштамо да неки експоненти буду 0. Тражимо $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ тако да ba_i буде појединачни аспект за све $1 \leq i \leq n$. Примјетимо

$$ba_i = p_1^{\alpha_{i1} + \beta_1} \dots p_k^{\alpha_{ik} + \beta_k}$$

Овај број ће бити појединачни g -ти аспект ако $g \mid \alpha_{ij} + \beta_j$ за све $1 \leq j \leq k$. Стога, ми можемо „најједнотипније“ тако да ba_1 буде појединачни квадрат, ba_2 појединачни куб, ba_3 појединачни четврти аспект, ..., а ba_n појединачни g_n -ти аспект, тј. је g_n n -ти прост број. Да би било чакљиво, може се

за би

$$2 \mid \alpha_{11} + \beta_1, \quad 3 \mid \alpha_{21} + \beta_1, \quad \dots, \quad g_n \mid \alpha_{n1} + \beta_1. \quad \text{Односно:}$$

$$\beta_1 \equiv -\alpha_{11} \pmod{2}$$

$$\beta_1 \equiv -\alpha_{21} \pmod{3}$$

$$\beta_1 \equiv -\alpha_{31} \pmod{5}$$

$\vdots$

$$\beta_1 \equiv -\alpha_{n1} \pmod{g_n}$$

Како у модули узјачно прости, из Кинеске Т. следи да постоји рјешење β_1 . Тако редом нађемо $\beta_2, \dots, \beta_k$ и на крају смо и b .

4. вјежбе

* Конгруенције по модулу - наставак *

1. Докажити да за $\forall n \in \mathbb{N}$ постоји аритметички низ од n чланова који су сви поделљиви са n .

Искористити задатак са претходних вјежби:

За сваки скуп $\{a_1, \dots, a_n\}$ $\exists b \in \mathbb{N}$ такво да су $ba_1, \dots, ba_n$ поделљиви са n .

Узмемо скуп $\{1, \dots, n\}$ $\Rightarrow \exists b \in \mathbb{N}$ такво да су $b, 2b, \dots, nb$ поделљиви са n , а уједно чине и аритметички низ дужине n .

* Теорема (Вилсонова): За израваан прост број p важи:

$$(p-1)! \equiv -1 \pmod{p}$$

Корисна је и следећа варијација: $(p-2)! \equiv 1 \pmod{p}$

2. Докажити да за p -број и непаран важи: $(p-3)! \equiv \frac{p-1}{2} \pmod{p}$.

$$(p-2)! = (p-2)(p-3)! \equiv 1 \pmod{p}$$

$$\text{Да ли је } (p-2) \cdot \frac{(p-1)}{2} \equiv 1 \pmod{p} ?$$

$$\frac{1}{2} (p-2)(p-1) \equiv \frac{1}{2} (-2)(-1) \equiv 1 \pmod{p}$$

$$\Rightarrow (p-2) \frac{(p-1)}{2} \equiv (p-2)(p-3)! \pmod{p} \quad /: (p-2)$$

$$\frac{(p-1)}{2} \equiv (p-3)! \pmod{p}$$

3. Доказати да $p^3 \mid (p!)^2 - p^2$ за прост број p .

$$(p!)^2 - p^2 = (p! - p)(p! + p) = p^2((p-1)! - 1)((p-1)! + 1)$$

Треба показати да $p \mid ((p-1)! - 1)((p-1)! + 1)$

Из Високог Т. $(p-1)! \equiv -1 \pmod{p} \Leftrightarrow p \mid (p-1)! + 1$

$$\Rightarrow p^3 \mid (p!)^2 - p^2.$$

4. Изračunати $NZD(n!+1, (n+1)!)$.

Како је $(n+1)! = (n+1) \cdot n!$ и $(n!, n!+1) = 1$, јер су сусједни

$$\Rightarrow NZD(n!+1, (n+1)!) = NZD(n!+1, n+1).$$

Разликујемо 2 случаја:

• $n+1$ је прост

$p \mid n+1$, $p \leq n$, онда $p \mid n!$ али $p \nmid n!+1$

$$\Rightarrow NZD(n!+1, n+1) = 1.$$

$n+1$ је прост

$$n+1 = p \Rightarrow n = p-1$$

$$\text{Тада је } n!+1 = (p-1)!+1 \equiv -1+1 = 0 \pmod{p}$$

$$\Rightarrow p \mid n!+1 \quad \text{ај, } n+1 \mid n!+1$$

$$NZD(n!+1, n+1) = n+1.$$

Коначно, одговор је:

$$NZD(n!+1, n+1) = \begin{cases} 1 & , \text{ ако је } n+1 \text{ прост} \\ n+1 & , \text{ ако је } n+1 \text{ композитан} \end{cases}$$

5. Докажити да не постоје природни бројеви k и n за које важи;

$$k! + 48 = 48(k+1)^n.$$

$$48 \mid k! + 48 \Rightarrow 48 \mid k! \Rightarrow k \geq 6$$

$$\begin{array}{r|l} 48 & 2 \\ 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \end{array} \quad 48 = 2^4 \cdot 3$$

$$k! + 48 = 48(k+1)^n \quad / : 48 \Rightarrow \underbrace{\frac{k!}{48}} + 1 = (k+1)^n$$

испробујемо за $k=6$ и $k=7$

$$\bullet k=6 \quad \frac{6!}{48} + 1 = 15 + 1 = 16 \neq 7^n$$

$$\bullet k=7 \quad \frac{7!}{48} + 1 = 105 + 1 = 106 \neq 8^n$$

$$\bullet k \geq 8 \quad \text{Тада је } \frac{k!}{48} \text{ исрван, ај. } \frac{k!}{48} + 1 \text{ је непаран број.}$$

$$2, 3 \mid \frac{k!}{48} \Rightarrow 2, 3 \nmid \frac{k!}{48} + 1 = (k+1)^n$$

$\Rightarrow k+1$ није један од неједних простила $\leq k \Rightarrow k+1=p$ мора бити прост!

Сада је довољно ј-на:

$$\equiv (p-1)! + 48 = 48p^n \equiv 0 \pmod{p}$$

$$-1 + 48 = 47 \Rightarrow p \mid 47 \Rightarrow p = 47 \Rightarrow \boxed{k=46}$$

Покажићемо сада да не постоји n које ће испуњити услове задатка.

Ако постоји, онда мора бити;

$$\frac{46!}{48} + 1 = 47^n$$

Треба доказати да $\frac{46!}{48} + 1$ има бар један прост фактор различит од 47.

Нефјутур

$$\frac{46!}{48} + 1 = 47 \cdot \underbrace{17}_{\text{уифарс}} \cdot \underbrace{18}_{\text{уифарс}} \cdot \underbrace{21}_{\text{уифарс}}$$

Па до њих не можемо доћи иједном, него само атомбу рачунара.

Зато ћемо показати да иједна и једна атомбу не могу бити ошатак до неке због одабраном модулу.

Није због иједан модулу мањи од 47. Зато постављамо до модулу 53 (први број већи од 47).

$$\text{Тада је } \frac{46!}{48} \equiv 13 \pmod{53}$$

$$\Rightarrow \frac{46!}{48} \equiv 14 \pmod{53}$$

Постављамо:

$$47^i \pmod{53} \quad 47, 36, 49, 24, 15, 16, 10, 46, 42, 13, 28, 44, 1, 42, \dots$$

Нема 14.

Тражени број n не постоји.

6. y степен $\mathbb{N}$ решених: $10x! + 3 = 3(x+1)^y$

$$3 \mid 10x! + 3 \Rightarrow 3 \mid x! \Rightarrow x \geq 3$$

• $x=3$ $60+3 = 3 \cdot 4^y$

$$63 = 3 \cdot 4^y \Rightarrow 4^y = 21 \times$$

• $x=4$ $243 = 3 \cdot 5^y$

$$5^y = 81 \times$$

• $x=5$ $1203 = 3 \cdot 6^y$

$$6^y = 401 \times$$

• $x=6$ $7203 = 3 \cdot 7^y$

$$7^y = 2401 \Rightarrow y=4 \Rightarrow (x,y) = (6,4) \text{ једино решење!}$$

• $x \geq 6$ Тада $3 \mid 10x! + 3$, али $9 \nmid 10x! + 3$ (јер $9 \nmid 10x!$).

$$\text{Закле} \Rightarrow 3 \nmid x+1.$$

• $x+1$ прост

$$\exists p \leq x \quad p \mid x+1 \quad p \neq 3$$

$$\Rightarrow p \mid x! \text{ али } p \nmid 3 \text{ па не делимо изразу } \nabla$$

• $x+1$ прост

$$x+1 = p$$

$$\Rightarrow x+1 \mid 10x! + 3 \text{ тј. } p \mid 10(p-1)! + 3$$

$$0 \equiv 10(p-1)! + 3 \equiv -7 \pmod{p} \Rightarrow \boxed{p=7}$$

$$\boxed{x=6}$$

Па је једино решење пар $(x,y) = (6,4)$.

5. вјешбе

* Конгруенције вишег реда *

Деф: Нека је $(a, m) = 1$. Тада је ред ел. a до модула m најмањи број t тако да је $a^t \equiv 1 \pmod{m}$. Означа $\sigma_m(a)$ и важи $\sigma_m(a) \leq \varphi(m)$.

Особине: $(a, m) = 1$

а) $a^t \equiv 1 \pmod{m} \Leftrightarrow \sigma_m(a) \mid t$;

б) $a^u \equiv a^v \pmod{m} \Leftrightarrow u \equiv v \pmod{\sigma_m(a)}$

у) $\sigma_m(a) \mid \varphi(m)$

Деф: g је примитивни корен до модула m ако је $\sigma_m(g) = \varphi(m)$.

Примјер: $\sigma_{10}(3) = 4$ јер је $3 \cdot 3 \cdot 3 \cdot 3 = 81 \equiv 1 \pmod{10}$

$\varphi(10) = 4 \Rightarrow 3$ је прим. корен до модула 10.

Твђење: Ел. услови су еквивалентни:

а) $g \in \mathbb{Z}$ је прим. корен до модула m ;

б) $1, g, g^2, \dots, g^{\varphi(m)-1}$ је редукциони систем модла m ;

у) $\mathbb{U}_m$ је циклическа група генерисана елем. $g \pmod{m}$.

1. Одредити најмање $n \in \mathbb{N}$ так да $2^{2013} \mid 17^n - 1$.

$$2^{2013} \mid 17^n - 1 \Leftrightarrow 17^n \equiv 1 \pmod{2^{2013}}$$

Третињу n је заправо $\sigma_{2^{2013}}(17)$ Значи да $\sigma_{2^{2013}}(17) \mid \varphi(2^{2013}) = 2^{2012}$

$$\varphi(2^{2013}) = 2^{2013} - 2^{2012} = 2^{2012}(2 - 1) = 2^{2012}$$

$$\text{Користимо } \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

$$\Rightarrow n = \sigma_{2^{2013}}(17) = 2^k$$

Стога, израњито најмање k тако да је $2^{2013} \mid 17^{2^k} - 1$.

$$17^{2^k} - 1 = (17^{2^{k-1}})^2 - 1 = (17^{2^{k-1}} - 1)(17^{2^{k-1}} + 1) =$$

$$= (17^{2^{k-2}} - 1)(17^{2^{k-2}} + 1)(17^{2^{k-1}} + 1) =$$

$$= \dots =$$

$$= \underbrace{(17 - 1)}_{2^1} \underbrace{(17 + 1)(17^2 + 1)(17^4 + 1) \dots (17^{2^{k-1}} + 1)}_{\substack{k \text{ фактора} \\ \text{све су непарне са 2, али не са 4}}}$$

Треба нам још 2009 фактора $\Rightarrow \boxed{k = 2009}$

Коначан одговор: Најмање израњито $n = 2^k = 2^{2009}$.

2. Рјешити конгруенцу $723k \equiv 373 \pmod{257}$.

Да ли рјешење постоји и кога $\gcd(723, 257) \mid 373$, ✓
 Како и де поступак рјешавања?

1) Треба наћи z так да је $723z \equiv 1 \pmod{257}$.

2) Онда је $723 \cdot (373z) \equiv 373 \pmod{257}$

$\Rightarrow k = 373z$.

Тако да само треба научити како урадити 1), иј. како наћи z

II начин: Еуклидов алгоритам $723z \equiv 1 \pmod{257}$.

$$723 = 2 \cdot 257 + 209$$

$$257 = 1 \cdot 209 + 48$$

$$209 = 4 \cdot 48 + 17$$

$$48 = 2 \cdot 17 + 14$$

$$17 = 1 \cdot 14 + 3$$

$$14 = 4 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + \textcircled{1} \rightarrow \text{NZD}(723, 257) = 1$$

$$2 = 2 \cdot 1$$

$$1 = 3 - 1 \cdot 2 = 3 - 1(14 - 4 \cdot 3) = 5 \cdot 3 - 1 \cdot 14 = 5(17 - 1 \cdot 14) - 1 \cdot 14 = 5 \cdot 17 - 6 \cdot 14 =$$

$$= 5 \cdot 17 - 6 \cdot (48 - 2 \cdot 17) = 17 \cdot 17 - 6 \cdot 48 = 17 \cdot (209 - 4 \cdot 48) - 6 \cdot 48 =$$

$$= 17 \cdot 209 - 74 \cdot 48 = 17 \cdot 209 - 74(257 - 209) = 91 \cdot 209 - 74 \cdot 257 =$$

$$= 91(723 - 2 \cdot 257) - 74 \cdot 257 = 91 \cdot 723 - 256 \cdot 257$$

$$\Rightarrow 723 \cdot 91 \equiv 1 \pmod{257} \Rightarrow \boxed{z = 91}$$

Третице

$$\boxed{k = 91 \cdot 373}$$

II начин : $723^{P(257)^{256}} \equiv 1 \pmod{257}$

(можно $z = 723^{255}$, или известно малое z из того диапазона

723^{255} до модулю 257)

$$723 \equiv 209 \equiv -48 \pmod{257}$$

$$723^2 \equiv (48)^2 = 2304 \equiv -9 \pmod{257}$$

$$723^4 \equiv (-9)^2 = 81 \pmod{257}$$

$$723^8 \equiv 136 \pmod{257}$$

$$\left. \begin{array}{l} 723^{16} \equiv \\ 723^{32} \equiv \\ 723^{64} \equiv \\ 723^{128} \equiv \end{array} \right\} \text{еще их надо рассчитать}$$

Когда известно все число искомое достаточно дано 723^{255} .

$$\sum_{i=0}^7 2^i = \frac{2^8 - 1}{2^1 - 1} = 256 - 1 = 255.$$

3. Наћи све просте p и q так да $p^2+1 \mid 2003^q+1$ и $q^2+1 \mid 2003^p+1$.

б.у.о. $q \geq p$.

• $p=2$

$$5 \mid 2003^q+1 \Leftrightarrow 2003^q \equiv -1 \pmod{5}$$

$$2003^q \equiv 4 \pmod{5}$$

$$2003^i \pmod{5} : 3, \textcircled{4}, 2, 1, \dots$$

$$\hookrightarrow q = 4k+2$$

Како је q прост, једина могућа је $q=2$

Проверимо $5 \mid 2003^2+1 \vee \Rightarrow (p,q)=(2,2) \rightarrow$ једно једино решење.

• $p > 2$

Тражимо особине простих чинилаца броја p^2+1 . Нека $r \mid p^2+1$ и r прост.

$$r \mid p^2+1 \Rightarrow r \mid 2003^q+1 \Rightarrow 2003^q \equiv -1 \pmod{r}$$

$$2003^{2q} \equiv 1 \pmod{r}$$

$$\Rightarrow \sigma_r(2003) \mid 2q$$

$$\Rightarrow \sigma_r(2003) \in \{1, 2, q, 2q\}$$

Раздвајамо на 2 случаја:

$$1^\circ \sigma_r(2003) \in \{1, 2\}$$

$$\text{Тада } \sigma_r(2003) \mid 2 \Rightarrow 2003^2 \equiv 1 \pmod{r}$$

$$\Rightarrow r \mid 2003^2-1 = 2002 \cdot 2004 = \overbrace{2 \cdot 7 \cdot 11 \cdot 13}^{2002} \cdot \underbrace{4 \cdot 3 \cdot 167}_{2004}$$

Користимо задатак са прошлим рјешенијем:

Сваки непаран прост гјенилац броја n^2+1 је облика $4k+1$.

$$\Rightarrow r \in \{2, 13\}$$

За $r=13$, имамо

$$13 \mid 2003^2 + 1 \quad \text{и} \quad 2003^2 + 1 \equiv 1^2 + 1 = 2 \pmod{13} \quad \nabla$$

Према томе, једина могућност је $r=2$.

$$2^\circ \quad \sigma_r(2003) \in \{g, 2g\}$$

$$\text{Када } 2 \mid \sigma_r(2003) \mid \varphi(r) = r-1 \Rightarrow 2 \mid r-1 \Rightarrow r \equiv 1 \pmod{2}$$

Дакле, сви нетривијални једначини броја $p^{t+1} \equiv 1 \pmod{2}$. Када је

$$p^{t+1} = 2 \cdot r_1 \cdot \dots \cdot r_k, \quad \text{где } r_i \equiv 1 \pmod{2} \quad 1 \leq i \leq k.$$

$$\Rightarrow p^{t+1} \equiv 2 \pmod{2}$$

$$\Rightarrow 2 \mid p^{t+1} - 2 = p^t - 1 = (p-1)(p+1)$$

$$\Rightarrow 2 \mid p-1 \quad \vee \quad 2 \mid p+1$$

× јер је $2 \geq p$

Како је $2 \geq p$, једина могућност
је го је $2 = p+1$, тј. $2=3$ и $p=2$,
али овај избор не ради!
(јер смо им. $p > 2$)

4. Доказати да је 27 примитивни корјен по модулу 50.

Треба да покажемо да је $\sigma_{50}(27) = \varphi(50)$

$$\varphi(50) = 50 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 50^5 \cdot \frac{1}{2} \cdot \frac{4}{5} = 20$$

Значи да $\sigma_{50}(27) \mid \varphi(50) = 20$. Зато $\sigma_{50}(27) \in \{1, 2, 4, 5, 10, 20\}$.

Дакле, треба одбацити све мање могућности нј. 1, 2, 4, 5, 10.

- $27 \equiv 27 \pmod{50} \rightarrow$ није 1
- $27^2 \equiv 729 \equiv 29 \equiv -21 \not\equiv -1 \pmod{50} \rightarrow$ није 2
- $27^4 \equiv 29^2 \equiv -9 \equiv 41 \pmod{50} \rightarrow$ није 4
- $27^5 \equiv (-9) \cdot 27 \equiv 7 \pmod{50} \rightarrow$ није 5
- $27^{10} = 27^5 \cdot 27^5 \equiv 49 \equiv -1 \pmod{50} \rightarrow$ није 10

$\Rightarrow \sigma_{50}(27) = \varphi(50) = 20$ што је и требало доказати.

5. Наћи остатак при дијелењу броја $1^k + 2^k + \dots + p^k$ са p , где је p неки прост број, а $k \in \mathbb{N}$.

Нека је g примитивни корјен до модулу p (знамо да постоји за p прост).

Тада $1, g, g^2, \dots, g^{p(p)-1}$ чине комплетан систем остатака до модулу p .

Ју, по y баш бројеви $y = 1, \dots, p-1$ у неком поретку (инверзних до $\text{mod } p$).

$$\{1, 2, \dots, p-1\} \equiv \{1, g, g^2, \dots, g^{p-2}\} \pmod{p}$$

$$\begin{aligned} 1^k + 2^k + \dots + p^k &\equiv (g^0)^k + (g^1)^k + (g^2)^k + \dots + (g^{p-1})^k = \\ &= (g^k)^0 + (g^k)^1 + (g^k)^2 + \dots + (g^k)^{p-1} = \\ &= \frac{(g^k)^{p-1} - 1}{g^k - 1} = \frac{(g^{p-1})^k - 1}{g^k - 1} \equiv \frac{1 - 1}{g^k - 1} = 0 \pmod{p} \end{aligned}$$

• $g^k \not\equiv 1 \pmod{p}$, онда је изражени остатак 0, ју. $p \mid 1^k + 2^k + \dots + p^k$

• $g^k \equiv 1 \pmod{p}$ како је $\sigma_p(g) = \phi(p) = p-1 \Rightarrow p-1 \mid k$

$$\text{Тада је } 1^k + 2^k + \dots + p^k \equiv \underbrace{1 + 1 + \dots + 1}_{p-1} + 0 = p-1$$

$$\text{Одговор : } 1^k + 2^k + \dots + p^k \equiv \begin{cases} 0 \pmod{p} & \text{ако } p-1 \nmid k \\ p-1 \pmod{p} & \text{ако } p-1 \mid k \end{cases}$$

6. Доказати Винонову Т. користећи аритметички корисен.

Треба доказати: $(p-1)! \equiv -1 \pmod{p}$

• $p=2$

$$(p-1)! = 1 \equiv -1 \pmod{2} \quad \checkmark$$

• p непаран број

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) = 1 \cdot g \cdot g^2 \cdots g^{p-2} = g^{1+2+\cdots+p-2} = g^{\frac{(p-1)(p-2)}{2}}$$

↑
Нека је g прим. остатак по модулу p

На основу мале Фермаове Т. је

$$g^{(p-1)(p-2)} = (g^{p-1})^{(p-2)} \equiv 1^{(p-2)} = 1 \pmod{p}$$

$$\Rightarrow p \mid g^{(p-1)(p-2)} - 1 = \left(g^{\frac{(p-1)(p-2)}{2}} - 1 \right) \left(g^{\frac{(p-1)(p-2)}{2}} + 1 \right)$$

Видљиво још да се доказује да $p \nmid g^{\frac{(p-1)(p-2)}{2}} - 1$.

$$\text{Пис. } g^{\frac{(p-1)(p-2)}{2}} \equiv 1 \pmod{p} \Rightarrow \sigma_p(g) = A(p) = p-1 \mid \frac{(p-1)(p-2)}{2}$$

$\Rightarrow \frac{p-2}{2}$ је цијели број, а то је немогуће, јер је p непаран број.

6. Вјезбе

* Конгруенције вишег реда - наставак *

Теорема: Нека је p прост и $(a, p) = 1$. Тада биномна конгруенција $x^k \equiv a \pmod{p}$ има рјешење ако је

$$a^{\frac{p-1}{k(p-1)}} \equiv 1 \pmod{p}.$$

Квадратни остаци: $a \in \mathbb{Z}$ је кв. остатак $\pmod{p}$ ако је $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
и- није и- $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Лемма: Лежандров симбол изражава својство "бити квадратни остатак".

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ако је кв. ост. mod } p \\ -1 & \text{ако није кв. ост. mod } p \end{cases}$$

(ако није другачије наведено одређује се $p \nmid a$ и $p > 2$)

Ејлеров критеријум: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$

Твђење: а) ако је $a \equiv b \pmod{p}$, тада је $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

$$\delta) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right);$$

$$\eta) \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{ако је } p \equiv 1 \pmod{4} \\ -1 & \text{ако је } p \equiv -1 \pmod{4}. \end{cases}$$

Ако је $a = g^{\alpha_1} \dots g^{\alpha_k} \rightarrow \left(\frac{a}{p}\right) = \left(\frac{g}{p}\right)^{\alpha_1} \dots \left(\frac{g}{p}\right)^{\alpha_k}$

Твђење:

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{ако је } p \equiv \pm 1 \pmod{8} \\ -1 & \text{ако је } p \equiv \pm 3 \pmod{8} \end{cases}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{ако је } p \equiv 1 \pmod{4} \\ -1 & \text{ако је } p \equiv 3 \pmod{4} \end{cases}$$

Теорема: (Закон квадратне реципроцити)

Нека су $p, q > 2$ различити прости бројеви. Тада је:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \quad , \text{одатуда}$$

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{ако је } p \equiv q \equiv -1 \pmod{4} \\ \left(\frac{p}{q}\right) & \text{иначе.} \end{cases}$$

Лемма: Јакобијев симбол за $m > 1$ непаран. Ако је $m = p_1 \dots p_t$, онда је $\chi(a, m) = 1$

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_t}\right)$$

Тврђење: а) Ако је $a \equiv b \pmod{m}$ онда је $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$;

$$\delta) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \quad , \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right);$$

$$\zeta) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$$

$$\eta) \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

$$\epsilon) \left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{ако је } n \equiv m \equiv -1 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{иначе.} \end{cases}$$

Последица Т1: Број по паровима неконгруентних остатака који
подељени са модулом p је

$$\frac{p-1}{(k, p-1)}$$

1. Изračунати vrijednost Legendrovog simbola $\left(-\frac{63}{11}\right)$.

$$\begin{array}{l|l} 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & 7 \end{array} \quad -63 = (-1) \cdot 3^2 \cdot 7$$
$$\left(-\frac{63}{11}\right) = \left(\frac{-1}{11}\right) \underbrace{\left(\frac{3}{11}\right)^2}_1 = \left(\frac{7}{11}\right) = \left(\frac{-1}{11}\right) \left(\frac{7}{11}\right).$$

$$\left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = (-1)^{\frac{10}{2}} = (-1)^5 = -1$$

Према закону квадратне реципрокности, што је

$$\left(\frac{7}{11}\right) \cdot \left(\frac{11}{7}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{11-1}{2}} = (-1)^{3 \cdot 5} = (-1)^{15} = -1$$

$$\Rightarrow \left(\frac{7}{11}\right) = -1 \left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) - \left(\frac{2}{7}\right)^2 = -1$$

$$\text{Коначно, } \left(\frac{-63}{11}\right) = \left(-\frac{1}{11}\right) \left(\frac{7}{11}\right) = (-1)(-1) = 1.$$

II Начин:

$$-63 \equiv -8 \equiv 3 \pmod{11} \Rightarrow \left(-\frac{63}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{-8}{11}\right)$$

$$\left(\frac{-63}{11}\right) = \left(\frac{-8}{11}\right) = \left(-\frac{1}{11}\right) \cdot \left(\frac{2}{11}\right)^3 = (-1)^{\frac{11-1}{2}} \cdot \left(\frac{2}{11}\right) = (-1) \cdot (-1)^{\frac{11^2-1}{8}} = (-1)(-1)^{\frac{120}{8}}$$

$$= (-1) \cdot (-1)^{15} = (-1)(-1) = 1.$$

2. Изračunajti vrijednost Legendrovog simbola $\left(\frac{98!}{101}\right)$.

На основу задатка са вјерношћу знамо да је (из Вилсонове Т.)

$$(p-3)! \equiv \frac{p-1}{2} \pmod{p}$$

$$98! = (101-3)! \equiv \frac{101-1}{2} = 50 \pmod{101}$$

$$\left(\frac{98!}{101}\right) = \left(\frac{50}{101}\right) = \left(\frac{2 \cdot 5^2}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{5}{101}\right)^2 = (-1)^{\frac{(101)^2-1}{8}} \cdot (-1) \quad (\text{jer } 101 \equiv 5 \pmod{8})$$

3. Нека је p непаран прост број. Израчунајте $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right)$

$$\left(\frac{i}{p}\right) = \begin{cases} 1 & i \text{ је кв. ост. mod } p \\ -1 & i \text{ није кв. ост. mod } p \end{cases}$$

Ума имамо $\frac{p-1}{2}$ кв. остатака до mod. p . (из доказује Т1)

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = \frac{p-1}{2} \cdot 1 + \frac{p-1}{2} \cdot (-1) = 0.$$

4. Докажи да број 2^n+1 нема простих дјелилаца облика $8k+5$

Птс. нека је $p = 8k+7 \mid 2^n+1$

1° n је паран ($n=2t$)

$$2^{2t} \equiv -1 \pmod{p}$$

$$(2^t)^2 \equiv -1 \pmod{p} \rightarrow -1 \text{ је кв. остатак до mod } p$$

Са друге стране,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{8k+7-1}{2}} = (-1)^{\frac{8k+6}{2}} = (-1)^{4k+3} = (-1)$$

$\hookrightarrow -1$ није квадратни остатак до mod p ∇

2° n је непарно ($n = 2t+1$)

$$2^{2t+1} \equiv -1 \pmod{p} \quad / \cdot 2 \Rightarrow 2^{2(t+1)} \equiv -2 \pmod{p}$$

$$(2^{t+1})^2 \equiv -2 \pmod{p}$$

$\hookrightarrow -2$ је из. оид. до модула p

Са груте стране,

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) \underbrace{\left(\frac{-1}{p}\right)}_{-1} = (-1) \left(\frac{2}{p}\right) = (-1) \cdot 1 = (-1)$$

$\hookrightarrow -2$ није из. оид. до мод $p \frac{4}{p}$.

У оба случаја сто доводи до контрадикције, па не постоје прости једноставни изражавања облика.

5. Наћи све природне n такве $2^n - 1 \mid 3^n - 1$.

Прво, уочило да израза страна не може бити једнака са 3, јер би то онда била и једна страна $\frac{4}{p}$

$$2^i \pmod{3}: 2, 1, 2, 1, \dots$$

Закључе, $2^n - 1 \equiv 1 - 1 = 0 \pmod{3}$ када је n паран број.

Закључујемо да n мора бити непаран.

$$\bullet n=1 \quad \checkmark \quad 1 \mid 2$$

$\bullet n > 1$ и n непарно

Посматрајмо $2^i \pmod{12}$.

$$2^i \pmod{12}: 2, 4, \textcircled{8}, 4, \textcircled{8}, 4, \textcircled{8}, \dots \quad \text{Закључе за непарно } n, \quad \begin{matrix} n > 1 \\ \checkmark \end{matrix} \quad 2^n \equiv 8 \pmod{12}$$

$$\Rightarrow 2^n - 1 \equiv 7 \pmod{12}$$

$\Rightarrow 2^n - 1$ мора имати прости једноставни облици 12 ± 5 , јер ако би са била облици 12 ± 1 , онда $2^n - 1 \equiv \pm 1 \pmod{12}$.

Закле, $\exists p = 12k \pm 5$ гд $p \mid 2^n - 1 \Rightarrow p \mid 3^n - 1$.

$$\Rightarrow 3^n - 1 \equiv 0 \pmod{p}$$

$$3^n \equiv 1 \pmod{p} \quad / : 3$$

$\hookrightarrow 3^{n+1} \equiv 3 \pmod{p} \rightarrow 3$ је кв. остатак по модулу $p \rightarrow \left(\frac{3}{p}\right) = 1$
(јер је $n+1$ парно)

$$\left\{ \begin{aligned} \underbrace{\left(\frac{3}{p}\right)}_1 \left(\frac{p}{3}\right) &= (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = (-1)^{\frac{12k \pm 5 - 1}{2}} = \pm 1 \Rightarrow \left(\frac{p}{3}\right) = \pm 1 \\ \left(\frac{p}{3}\right) &= \left(\frac{12k \pm 5}{3}\right) = \left(\frac{\pm 5}{3}\right) = \left(\frac{\mp 1}{3}\right) = \mp 1 \end{aligned} \right\} \quad \downarrow$$

$\rightarrow$ Једино решење је $n=1$.

II начин:

$$3^n \equiv 1 \pmod{2^n - 1}$$

$3^{n+1} \equiv 3 \pmod{2^n - 1} \rightarrow 3$ је кв. остатак по модулу $2^n - 1$

$$\hookrightarrow \left(\frac{3}{2^n - 1}\right) = 1 \quad (\text{Јакобијев симбол})$$

$$\underbrace{\left(\frac{3}{2^n - 1}\right)}_1 \cdot \left(\frac{2^n - 1}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{2^n - 1 - 1}{2}} = (-1)^{2^{n-1} - 1} = (-1) \rightarrow 2^n - 1 \text{ није кв. остатак по модулу } 3$$

Са друге стране, како је n непарно $\rightarrow 2^n \equiv 2 \pmod{3}$

$$2^n - 1 \equiv 1 = 1^2 \pmod{3}$$

$\hookrightarrow 2^n - 1$ је кв. остатак по модулу 3 $\downarrow$

6. Нека је p прост број и нека за $a, b \in \mathbb{Z}$ важи $p = a^2 + 4b^2$. Докажи да a мора бити квадратни остатак по модулу p .

Треба показати: $\left(\frac{a}{p}\right) = 1$

Прво како $a, b \in \mathbb{Z}$, p не може бити 2, па је p непаран прост број.

Слика a мора бити непаран.

$$\text{Зато је } a^2 \equiv 1 \pmod{4} \Rightarrow p = a^2 + 4b^2 \equiv 1 \pmod{4}$$

$$\text{Како је } p \equiv 1 \pmod{4} \rightarrow \left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$$

↳ Не знамо где ми је a прост па

$\left(\frac{p}{a}\right)$ морамо тумачити као Јакобијев симбол!

$$\text{Сада је } \left(\frac{p}{a}\right) = \left(\frac{a^2 + 4b^2}{a}\right) = \left(\frac{2^2 \cdot b^2}{a}\right) = \left(\frac{2}{a}\right)^2 \cdot \left(\frac{b}{a}\right)^2 = 1 \cdot 1 = 1$$

$\Rightarrow \left(\frac{a}{p}\right) = 1 \Rightarrow a$ је квадратни остатак по модулу p што је и требало доказати.

1. Нека је број N квадратни остатак по сваком простом модулу осим највише коначно много. Доказати да је N тада потпуни квадрат.

Доказ дајемо контрапозицијом. Пр. да N није потпуни квадрат. Доказати да постоји бесконачно много простих бројева таквих да N није квадратни остатак ни по једном од тих модула.

Раздвајамо на 2 случаја:

1° $N = 2^k$, $2 \nmid k$ (N је нестан двојке)

$$\left(\frac{N}{p}\right) = \left(\frac{2^k}{p}\right) = \left(\frac{2}{p}\right)^k = \underbrace{\left(\frac{2}{p}\right)}_1 \left(\frac{2}{p}\right)^{\overbrace{k-1}^{\text{парно}}} = -1 \quad (\text{јер знамо да } N \text{ није кв. ост.})$$

1. за све $p \equiv \pm 3 \pmod{8}$, а таквих p има бесконачно много

2° Пр. да N садржи и неки непарни фактор

$$N = j^2 p_1 \dots p_r = j^2 n, \quad \text{гдје } n \text{ није једнако ниједном изразају } n$$

Нека је p_r непарни (то нам осигурава 1 непарни)

Нека је a квадратни кв. неостатак $\pmod{p_r}$ $\left(\frac{a}{p_r}\right) = -1$

Нека је b_i кв. остатак $\pmod{p_i}$ $1 \leq i \leq r-1$ $\left(\frac{b_i}{p_i}\right) = 1$

Посматрајмо систем конгруенција:

$$x \equiv \begin{cases} b_i \pmod{p_i} & , \text{ за } p_i \neq 2 \\ 1 \pmod{8} & , \text{ за } p_i = 2 \end{cases} \quad 1 \leq i \leq r$$

$$x \equiv a \pmod{p_r}$$

Сви посматрани модули су узјачно прости осим у случају $p_i = 2$, али
тада можемо занемарити прву ј-ту јер је она садржана у $x \equiv 1 \pmod{8}$,

Сада према кинеској Т. о одлауча овај шаблон има бесконачно много рј.
и има у облику $x = 4nk + s$ (где s је најмање остатак модула 4, а s је најмање
рј. система).

Оштрије, из шаблона видно је $(4n, s) = 1$.

Лемма Т.: У сваком ар. низу имају се подједнаки број чланова и корак узјачно
прости, имајући бесконачно много простих бројева.

Пошто, имајући бесконачно много простих облика $x = 4nk + s$.

Желимо да добијемо да је $\left(\frac{N}{x}\right) = -1$, где N није кв. ост. за
све x .

$$\left(\frac{N}{x}\right) = \left(\frac{j}{x}\right)^2 \left(\frac{p_1}{x}\right) \dots \left(\frac{p_r}{x}\right) = -1$$

$$\text{Како је } x \equiv 1 \pmod{4} \Rightarrow \left(\frac{p_i}{x}\right) = \left(\frac{x}{p_i}\right)$$

$$\left(\frac{x}{p_i}\right) = \left(\frac{b_i}{p_i}\right) = 1$$

$$\left(\frac{p_r}{x}\right) = \left(\frac{x}{p_r}\right) = \left(\frac{a}{p_r}\right) = -1$$

Тиме је доказ завршен.

* Ако је $p_i = 2$, онда је $x \equiv 1 \pmod{8}$, па $\left(\frac{2}{x}\right) = 1$.

2. Нека је f полином другог степена са цјелим коефицијентима и нека за сваки прост број p постоји природан број n такав да $p \mid f(n)$. Доказати да f има рационалну нулу.

$$f(x) = ax^2 + bx + c \quad \text{где } a, b, c \in \mathbb{Z}$$

Довољно је показати да је $b^2 - 4ac$ потпуно квадрат.

Ми ћемо доказати да је $b^2 - 4ac$ кв. одакле до свих простих модула, одакле следи да је $b^2 - 4ac$ кв. из задатка 1.

Нека је p прост. Онда $\exists n \in \mathbb{N}$ такв $p \mid f(n)$.

$$p \mid f(n) = an^2 + bn + c \quad | \quad 4af(n) = 4a^2n^2 + 4abn + 4ac$$

$$\text{Дакле, } p \mid 4a^2n^2 + 4abn + 4ac \Leftrightarrow -4ac \equiv 4a^2n^2 + 4abn \pmod{p}$$

$$\text{Сада је } b^2 - 4ac \equiv b^2 + 4abn + 4a^2n^2 = (b + 2an)^2 \pmod{p}.$$

3. Доказати да, за сваки прост број $p > 5$, постоје 2 узajимно природна броја која су оба квадратни остаци по модулу p .

Посматрајмо пар $(9, 10)$. Нека је $p > 5$ произвољан прост.

$$\left(\frac{9}{p}\right) = \left(\frac{3}{p}\right)^2 = 1$$

$$\left(\frac{10}{p}\right) = \begin{cases} a) = 1 \\ b) = -1 \end{cases} \Rightarrow (9, 10) \text{ је квадратички пар}$$

$$\delta) \left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) = -1$$

$$\hookrightarrow \left(\frac{2}{p}\right) = 1 \quad \vee \quad \left(\frac{5}{p}\right) = 1$$

↓

↓

$(4, 5)$ је квадратички пар

$(1, 2)$ је квадратички пар

1) Нека је број $F_n = 2^{2^n} + 1$ Фроат (сфернао Фроат број)

а) Доказати: $\varphi(F_n - 1) = \frac{F_n - 1}{2}$;

б) Доказати да је сваки квадратни неостатак до модулу F_n такође
и примитивни коруен до модулу F_n .

а) $\varphi(F_n - 1) = \varphi(2^{2^n}) = 2^{2^n} - 2^{2^n - 1} = 2^{2^n - 1} (2 - 1) = 2^{2^n - 1} = \frac{2^{2^n}}{2} = \frac{F_n - 1}{2}$.

б) За најаран Фроат број p такође $\frac{p-1}{2}$ кв. неостатака до
 $\text{mod } p$ и $\varphi(p-1)$ примитивних коруена $\text{mod } p$. Ако је F_n Фроат,
онда шта $\frac{F_n - 1}{2} = \varphi(F_n - 1)$ кв. неостатака $\text{mod } F_n$ и тако
тако примитивних коруена $\text{mod } F_n$.

Дакле, за почетак их шта једнако.

Ми ћемо доказати да је сваки примитивни коруен $\text{mod } p$ квадратни
неостатак $\text{mod } p$, а како их шта довањо то ће бити крај доказа.

Нека је g прим. коруен $(\text{mod } p)$ и шт. $g \equiv x^2 (\text{mod } p)$ за неко x .

Тада је $g^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (\text{mod } p) \Rightarrow \varphi(g) \leq \frac{p-1}{2}$
 $\uparrow$
Малс Формалс

што је у контроридикују са Фроат Фроат $\varphi_p(g) = p-1$.

Штоа што доказати Фроат.

5. Доказати: За n који Фермаов прост број F_n за $n \geq 1$, број 3 је аритметички коријен до модулу F_n .

На основу претходног задатка, довољно је доказати да је 3 квадратички невањатак до модулу F_n .

$$F_n = 2^{2^n} + 1 \equiv 1 \pmod{4}$$

$$\left(\frac{3}{F_n}\right) \underset{\substack{\uparrow \\ \text{закон квадратичног} \\ \text{реку.}}}{=} \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$$

закон квадратичног реку.

6. Испитати да ли је 111 аритметички коријен до модулу 2015 . (19) $\{1265 = 5 \cdot 11 \cdot 23\}$

$$\begin{array}{r|l} 111 & 3 \\ 37 & 37 \\ 1 & \end{array}$$

$$111 = 3 \cdot 37$$

$$\begin{array}{r|l} 2015 & 5 \\ 403 & 13 \\ 31 & 31 \\ 1 & \end{array}$$

$$2015 = 5 \cdot 13 \cdot 31$$

$$\begin{array}{r|l} 1265 & 5 \\ 253 & 11 \\ 23 & 23 \end{array}$$

Како 2015 није облика p^α ни $2p^\alpha$ за p прост, на основу Т. са претходног знамо да не постоје аритметички коријени до модулу 2015 .

7. Испитати да ли је 1581 аритметички коријен до модулу $2 \cdot 31^{32 \cdot 33 \cdot 34}$.

$$\begin{array}{r|l} 1581 & 3 \\ 527 & 17 \\ 31 & 31 \\ 1 & \end{array}$$

$$1581 = 3 \cdot 17 \cdot 31$$

Како 1581 и $2 \cdot 31^{32 \cdot 33 \cdot 34}$ нису узјачно просте, 1581 не може бити арит. коријен до модулу $2 \cdot 31^{32 \cdot 33 \cdot 34}$.

8. Вјешће

* О простим бројевима *

Део: $\pi(x)$ је број свих простих бројева не већих од x (за $x > 0$).

↳ Број простих у интервалу $[0, x]$.

* Теорема (Т. о простим бројевима): Важи $\pi(x) \sim x / \ln x$ кад $x \rightarrow \infty$.

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

* Теорема (Чебишев - Бернхардтв асимптот): За сваки $n \geq 1$ $\exists p$ прост
тако да је:

$$n < p \leq 2n.$$

* Проблем близанаца: 2 проста броја p и q су близанци ако је $|p - q| = 2$.

$$(\{3, 5\}, \{5, 7\}, \{11, 13\}, \dots)$$

Да ли их има коначно или бесконачно много?

* Голдбахова хипотеза: Да ли се сваки паран број ≥ 4 може приказати
као збир 2 проста броја?

1. У скупу $\mathbb{N}$ ријешити једначину

$$1! \cdot 3! \cdot 5! \cdots (2n-1)! = \left(\frac{n(n+1)}{2} \right)!$$

Поштом смо прво директним испробавањем.

• $n=1$ $1! = 1! \checkmark$

• $n=2$ $1! \cdot 3! \stackrel{?}{=} \left(\frac{2 \cdot 3}{2} \right)! = 3! \checkmark$

• $n=3$ $1! \cdot 3! \cdot 5! \stackrel{?}{=} \left(\frac{3 \cdot 4}{2} \right)! = 6! \checkmark$

• $n=4$ $1! \cdot 3! \cdot 5! \cdot 7! \stackrel{?}{=} \left(\frac{4 \cdot 5}{2} \right)! = (2 \cdot 5)! = 10!$

$$720 \cdot 2! = 3 \ 628 \ 800 = 10! \checkmark$$

• $n=5$ $1! \cdot 3! \cdot 5! \cdot 7! \cdot 9! \stackrel{?}{\neq} 15!$

Нје јер 11 и 13 дијеле десну страну, а не дијеле леву

• $n=6$ $1! \cdot 3! \cdot 5! \cdot 7! \cdot 9! \cdot 11! \neq 21!$

~~13~~ | $21!$, али 13 $\nmid$ леву страну...

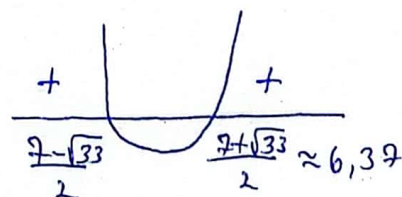
Покажимо да за $n \geq 7$ увијек постоји прости број између $2n-1$ и $\frac{n(n+1)}{2}$

Знато на основу Бернхардтовог твђења да $\exists p$ таку је $2n-1 < p \leq 2(2n-1)$

Ако покажемо да је $2(2n-1) \leq \frac{n(n+1)}{2}$ (*) за $n \geq 7$ онда је крај.

$$8n-4 \leq n^2+n$$

$$n^2 - 7n + 4 \geq 0 \quad n_{1,2} = \frac{7 \pm \sqrt{33}}{2}$$



За $n \geq 7$ је $n^2 - 7n + 4 \geq 0$, па важи (*) и онда је крај доказа.

Закључак, $n \in \{1, 2, 3, 4\}$.

2. Наћи све $n \in \mathbb{N}$ за које важи својство: Сваки број m такав да је $1 < m < n$ и априорно је узјачно прост са n мора бити прост.

Примијетићемо да ако за неко p важи $p \nmid n$, онда $n < p^2$. Јер ако је $p^2 \leq n$ и $(p^2, n) = 1$, на основу услова зад. бисмо добили да је p^2 прост.

Означимо са $p_1, p_2, \dots$ редом све просте бројеве, и нека је p_{k+1} најмањи прост који не дијели n . Тада како $p_1, \dots, p_k \mid n$ и $p_{k+1} \nmid n$, добијачемо

$$p_1 \cdots p_k \leq n < p_{k+1}^2. \quad (1)$$

• $k=0$

$p_1 \nmid n$, ај. $2 \nmid n$ и $n < 4 \Rightarrow n \in \{1, 3\}$, а они иауњавају услове зад.

• $k=1$

$2 \mid n$ и $3 \nmid n$ и $n < 9 \Rightarrow n \in \{2, 4, 8\}$

$n=2$ ✓

$n=4$ једина отуђа $m=3$, ај. и $n=4$ ✓

$n=8$ ипоућујачи ај. $m=3$ $m=5$, $m=7$, а сви они су прости ✓

• $k \geq 2$ Из Бернхардтовог шва, постоји прост између p_k и $2p_k$,

ај. је $p_{k+1} < 2p_k$. Из наше разлике је $p_k < 2p_{k-1}$, ај. је

$$p_{k+1} < 2p_k < 4p_{k-1} \Rightarrow p_{k+1} < 4p_{k-1} / p_{k+1} < 2p_k$$

$$\Rightarrow p_{k+1}^2 < 8p_{k-1}p_k \quad (2)$$

Сада је из (1) и (2) $\Rightarrow p_1 \cdot p_2 \cdots p_k < 8p_{k-1}p_k$

$$\Rightarrow p_1 \cdots p_{k-2} < 8.$$

Како је $2 \cdot 3 \cdot 5 > 8 \Rightarrow k-2 \leq 2 \Rightarrow k \leq 4$,

ај. $k \in \{2, 3, 4\}$ иаућујачи прости.

$$k=2: 2 \cdot 3 = 6 \mid n \text{ и } 5 \nmid n \text{ и } n < 25 \Rightarrow n \in \{6, 12, 18, 24\}.$$

$$n=6 \quad m=5 \quad \checkmark$$

$$n=12 \quad m \in \{5, 7, 11\} \quad \checkmark$$

$$n=18 \quad m \in \{5, 7, 11, 13, 17\} \quad \checkmark$$

$$n=24 \quad m \in \{5, 7, 11, 13, 17, 19, 23\} \quad \checkmark$$

$$k=3: 2 \cdot 3 \cdot 5 = 30 \mid n \quad 7 \nmid n \text{ и } n < 49 \Rightarrow n=30$$

$$m \in \{7, 11, 13, 17, 19, 23, 29\} \quad \checkmark$$

$$k=4: 2 \cdot 3 \cdot 5 \cdot 7 = 210 \mid n, 11 \nmid n \quad n < 121 \text{ Нема кандидата.}$$

$$\text{Закле, } n \in \{1, 2, 3, 4, 6, 8, 12, 18, 24, 30\}.$$

3. Докажете да постоји бесконачно много $n \in \mathbb{N}$ такво да $\pi(n) \mid n$.

Доказателно више: За свако $k \in \mathbb{N}, k > 1$, $\exists n \in \mathbb{N}$ такво да $n = k\pi(n)$.

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n} = \lim_{n \rightarrow \infty} \frac{\frac{\pi(n)}{n}}{\frac{n}{\ln n}} \cdot \frac{\ln n}{n} = \lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln n}} \cdot \lim_{n \rightarrow \infty} \frac{1}{\ln n} = 1 \cdot 0 = 0$$

↑
Т.о. први чинилац

За задато k неможемо узети најмање n такво да $\frac{\pi(n)}{n} \leq \frac{1}{k}$. За $k > 1$ је:

$$\frac{\pi(n)}{n} \leq \frac{1}{k} < \frac{\pi(n-1)}{n-1} \quad (n-1 < n \text{ и та за коју не важи})$$

$$\text{Одавде је: } k\pi(n) \leq n \quad \text{и} \quad n-1 < k\pi(n-1)$$

Закле, како је π нестрого убавна функција, имамо:

$$k\pi(n) \geq k\pi(n-1) \geq n-1 \geq k\pi(n)$$

$\Rightarrow k\pi(n) = n$, како смо и саједили доказати.

4. Испитати да ли postoji бесконачно много парова простih бројева облика $(p, p+2, p+4)$?

Ако посматрамо ове бројеве по модулу 3 они су конгруентни са $p, p+2, p+1$, што су 3 узастопна броја, па како ~~неки~~ ^{је} ~~неки~~ од њих ~~буде~~ конгруентан са 0 mod 3, онда 1 од њих мора бити 3.

Добијемо 3 пара $(3, 5, 7) \rightarrow$ ово је једина могућност
 $(1, 3, 5)$
 $(-1, 1, 3)$

5. Доказати да за сваки паран природан број $n < 4 \cdot 10^{18}$ важи
ако $a, b \in \mathbb{N}$ таку је $n = \varphi(a) + \varphi(b)$.

Тада је и $n+2$ паран природан и $2 < n+2 \leq 4 \cdot 10^{18}$, како је Голдбахово хипотеза потврђена за све парне бројеве $\leq 4 \cdot 10^{18}$, знамо да постоје прости p_1 и p_2 таку је $n+2 = p_1 + p_2$.

Сада је

$$\varphi(p_1) = p_1 - 1 \text{ и } \varphi(p_2) = p_2 - 1$$

$$\varphi(p_1) + \varphi(p_2) = p_1 - 1 + p_2 - 1 = p_1 + p_2 - 2 = n$$

Дакле, за датог n , узетомо $a = p_1$ и $b = p_2$.

6. Под претпоставком да постоји бесконачно много парова простих близанаца, докажи да постоји бесконачно много парова природних бројева (m, n) за које је $\sigma(m) = \varphi(n)$, где је $\sigma(m)$ збир дјелилаца природног броја n .

За сваки пар $(p, p+2)$ простих близанаца, узмемо

$$m = p \quad \text{и} \quad n = p+2.$$

$$\left. \begin{array}{l} \sigma(m) = m+1 = p+1 \\ \varphi(n) = n-1 = p+1 \end{array} \right\} \Rightarrow \sigma(m) = \varphi(n).$$

↑

n је прост

($p+2$ је прост)

* Напомена - о простим бројевима - ** Диофантске једначине *

* Отворен проблем: Да ли постоји бесконачно много простих бројева облика $2^k + 1$ (фермаови прости бројеви)? ($2^{2^n} + 1 \rightarrow$ овај облик је F_n)

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

$$F_5 = 641 \cdot 6700417 \quad (\text{показује да је } F_5 \text{ композитан})$$

* Пелјева једначина $\rightarrow$ теорема која је исписана у задатку

* Велика фермаова теорема

1. Докажити да постоји $k \in \mathbb{N}$ такав да је $2^n k + 1$ прост за $\forall n \in \mathbb{N}$

Примјетимо прво изјаву (ово ће нам бити потребно касније):

1) Уколико постоји $k \cdot 2^n + 1$ за неки модулу M так да је $k \equiv 1 \pmod{M}$ и n највише као $n = 2^l \cdot t$, где је t непарно (о l може бити и 0) онда:

$$k \cdot 2^n + 1 \equiv (2^{2^l})^t + 1^t = (2^{2^l} + 1)(\dots) = F_l(\dots) \pmod{M}$$

$= F_l \cdot A$
 $\hookrightarrow l$ -ти фермаов број

Докажи, за $l \geq 6$, $n = 2^6 \cdot s$ (s не мора бити непарно, може бити јачи број)

важи:

$$\begin{aligned} k \cdot 2^n + 1 &\equiv k \cdot 2^n - k + k + 1 = k(2^{2^6 \cdot s} - 1) + k + 1 = k(2^{2^6} - 1) + k + 1 = \\ &= k((2^{2^6})^s - 1^s) + k + 1 = k(2^{2^6} - 1)(\dots) + k + 1 = \\ &= k((2^{2^5})^2 - 1)(\dots) + k + 1 = k(2^{2^5} - 1)(2^{2^5} + 1)(\dots) + k + 1 = \\ &= k(F_5 - 2)F_5(\dots) + k + 1 = k(F_5 - 2) \cdot F_5 \cdot B + k + 1 \end{aligned}$$

1) ћемо користити за $0 \leq l \leq 5$, а 2) за $l \geq 6$.

Знамо да је петти фермаов број F_5 једнако са 641 ил. $F_5 = 641 \cdot G$.

На основу кинеске теореме о остацима можемо обратити к њему:

$$k \equiv 1 \pmod{F_0}$$

$$k \equiv 1 \pmod{F_1}$$

$$k \equiv 1 \pmod{F_2}$$

$$k \equiv 1 \pmod{F_3}$$

$$k \equiv 1 \pmod{F_4}$$

$$k \equiv 1 \pmod{641}$$

$$k \equiv -1 \pmod{G}$$

Трговало да је за овакво k , број 2^{n_k+1} савршен за $\forall n \in \mathbb{N}$.

Сада чека је n неки произвољан природан број и наћи ћемо га као $n=2^l \cdot s$,
гдје s је непаран. Тада:

1) ако је $l \leq 4$, онда $k \cdot 2^n + 1 \equiv F_l \cdot A \pmod{M}$

Како је $k \equiv 1 \pmod{F_l}$ $l \leq 4$, онда имамо:

$$k \cdot 2^n + 1 \equiv F_l \cdot A \equiv 0 \pmod{F_l}$$

$$\Rightarrow F_l \mid k \cdot 2^n + 1, \text{ а како је } k \cdot 2^n + 1 > F_l$$

$\Rightarrow k \cdot 2^n + 1$ је савршен

2) $l = 5$, узмемо $M = 641$ и $k \equiv 1 \pmod{641}$

$$k \cdot 2^n + 1 \equiv F_5 \cdot A \equiv 0 \pmod{641} \Rightarrow 641 \mid k \cdot 2^n + 1 \Rightarrow k \cdot 2^n + 1 \text{ је савршен.}$$

3) За $l \geq 6$ је: $(k \equiv -1 \pmod{6})$

$$k \cdot 2^n + 1 \equiv k \cdot (F_5 - 2) (F_5) (\dots) + k + 1 \equiv 0 - 1 + 1 = 0 \pmod{6}$$

$$\Rightarrow 6 \mid 2^n \cdot k + 1 \Rightarrow 2^n \cdot k + 1 \text{ је савршен}$$

* Напомена: $\forall k \in \mathbb{N}$ за које је $2^n \cdot k + 1$ савршен за $\forall n \in \mathbb{N}$ се зове број

СЕРПИЊСКОГ.

Отворен проблем: Најмањи број Серпињског?

Чврсто се вјерује да је то 78 557.

2 Под претпоставком да су сви фермаови бројеви F_k за $k \geq 5$ сложени, наћи све $n \in \mathbb{N}$ таку да је $n^n + 1$ прост број.

Да би $n^n + 1$ био прост, n не смеје имати непаран фактор, тј. мора бити степ двојке или 1 јер $1^1 + 1 = 2 \checkmark$. ($n=1$)

Посматрајмо $(2^k)^{2^k} + 1$. Примјећујемо да иако важи за k , мора бити 1 или степ двојке. За $k=1$ $2^2 + 1 = 5 \checkmark$. ($n=2$)

Закључе, надаље посматрамо бројеве облика $(2^{2^l})^{2^{2^l}} + 1$ за $l \geq 1$.

$$(2^{2^l})^{2^{2^l}} + 1 = 2^{2^l \cdot 2^{2^l}} + 1 = 2^{2^{l+2^l}} + 1 = F_{l+2^l}$$

Како знамо да је F_k прост за $k \geq 5$, морас $l+2^l \leq 4$.

Једина могућност је $l=1 \Rightarrow n=2^2=4$. Тада је $n^n + 1 = 4^4 + 1 = 256 + 1 = 257$, што је заиста прост број.

Закључе, $n \in \{1, 2, 4\}$.

3 Дати су бројеви m и n , оба постојни 17-шестени и имају по 15 062 017 цифара. Да ли природан број који се добија истисивањем ова 2 броја једног иза другог може бити асоц. 17-шестен?

$$m = x^{17}, n = y^{17}, k = 15\,062\,017 (= 17 \cdot 886\,001)$$

$$m = \overline{a_{k-1} \dots a_0}, n = \overline{b_{k-1} \dots b_0}, mn = \overline{a_{k-1} \dots a_0 b_{k-1} \dots b_0} \stackrel{?!}{=} z^{17}$$

$$mn = x^{17} \cdot 10^{\frac{k}{17}} + y^{17} = (10^{\frac{886001}{17}} x)^{17} + y^{17} \stackrel{?!}{=} z^{17} \quad \text{нису множење}$$

Не може, јер ј-на $x^{17} + y^{17} = z^{17}$ нема рјешења у $\mathbb{N}$.

(из Велике Фермаове Теореме)

4. Наћи најмање рјешење једначине $x^2 - 7y^2 = 1$ у $\mathbb{N}$.

$x^2 - 7y^2 = 1$ је Писеова ј-на ($x^2 - my^2 = 1$, $m > 0$ и није потпуни квадрат)

Тривијална рјешења сваке Писеове ј-не су $x = \pm 1$ и $y = 0$, сва остала су нетривијална. Ако Писеова ј-на има 1 нетривијално рјешење, има их и бесконачно много (предозања), а нетривијално рјешење увијек постоји (не доказујемо).

Рјешење овдје можемо доћи брзо и једноставно: $(x, y) = (8, 3)$,

(најмање у смислу да је $x + \sqrt{7}y$ минимално)

Зато што општи резултат за рјешавање Писеових ј-на:

$$x^2 - dy^2 = 1$$

Прво треба $\sqrt{d}$ написати у облику:

$$(*) \sqrt{d} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots a_k + \frac{1}{a_0 + \sqrt{d}}}}}$$

гдје су $a_0, \dots, a_k$ природни бројеви.

Показатићемо на примјеру како се то ради.

Када то устичемо, онда је минимално рјешење ј-не пар уздјачних фразаци (x_1, y_1) и k парно:

$$\frac{x_1}{y_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots a_{k-1} + \frac{1}{a_k}}}}$$

$$\frac{x_1}{y_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots a_k + \frac{1}{2a_0 + \frac{1}{a_1 + \frac{1}{\ddots a_{k-1} + \frac{1}{a_k}}}}}}}$$

Вратимо се сада на нашу првијер: $x^2 - 7y^2 = 1$

$$\sqrt{7} = a_0 + \frac{1}{B} \quad , B = a_1 + \frac{1}{C} \quad , C = a_2 + \frac{1}{D} \quad , D = a_3 + \frac{1}{E}$$

$$a_0 = \lfloor \sqrt{7} \rfloor = 2$$

$$B = \frac{1}{\sqrt{7} - 2} \cdot \frac{\sqrt{7} + 2}{\sqrt{7} + 2} = \frac{\sqrt{7} + 2}{3} \quad a_1 = \left\lfloor \frac{\sqrt{7} + 2}{3} \right\rfloor = 1$$

$$C = \frac{1}{B - a_1} = \frac{1}{\frac{\sqrt{7} + 2}{3} - \frac{3}{3}} = \frac{1}{\frac{\sqrt{7} - 1}{3}} = \frac{3}{\sqrt{7} - 1} \cdot \frac{\sqrt{7} + 1}{\sqrt{7} + 1} = \frac{3(\sqrt{7} + 1)}{6} = \frac{\sqrt{7} + 1}{2}$$

$$a_2 = \left\lfloor \frac{\sqrt{7} + 1}{2} \right\rfloor = 1$$

$$D = \frac{1}{C - a_2} = \frac{1}{\frac{\sqrt{7} + 1}{2} - \frac{2}{2}} = \frac{1}{\frac{\sqrt{7} - 1}{2}} = \frac{2}{\sqrt{7} - 1} \cdot \frac{\sqrt{7} + 1}{\sqrt{7} + 1} = \frac{\sqrt{7} + 1}{3}$$

$$a_3 = \left\lfloor \frac{\sqrt{7} + 1}{3} \right\rfloor = 1$$

$$E = \frac{1}{D - a_3} = \frac{1}{\frac{\sqrt{7} + 1}{3} - \frac{3}{3}} = \frac{1}{\frac{\sqrt{7} - 2}{3}} = \frac{3}{\sqrt{7} - 2} \cdot \frac{\sqrt{7} + 2}{\sqrt{7} + 2} = \frac{3(\sqrt{7} + 2)}{3} = 2 + \sqrt{7}$$

$\underbrace{2}_{a_0} \quad \underbrace{\sqrt{7}}_{\sqrt{D}}$

$\Rightarrow k=3 \quad \Rightarrow k$ је Нитарно

$$\frac{x}{y} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = 2 + \frac{1}{1 + \frac{1}{2}} = 2 + \frac{1}{\frac{3}{2}} = 2 + \frac{2}{3} = \frac{8}{3}$$

Дакле, најмање рјешење је пар $(x, y) = (8, 3)$.

Напомена 1: $(a_1, \dots, a_k)$ је увјек пашиндром.

Напомена 2: $x^2 - dy^2 = -1$ се рјешава слично, ако представимо $\sqrt{d}$ у облику $(*)$ $\frac{p}{q}$. Најчешће $a_0, a_1, \dots, a_k$. Тада, ако је k непарно, постоји ј-на нека рјешења, а ако је k парно, ^{минимално} рјешење је дато као за $x^2 - dy^2 = 1$ у случају када је k непарно.
(извр. 199.)

5. Наћи најмањи природан број $n > 1$ за који је квадратна средина првих n природних бројева такође природан број.

$$\sqrt{\frac{1^2 + 2^2 + \dots + n^2}{n}} = m, \quad m \in \mathbb{N}$$

$$\sqrt{1^2 + 2^2 + \dots + n^2} = \sqrt{n} \cdot m$$

$$1^2 + 2^2 + \dots + n^2 = n \cdot m^2$$

$$\frac{n(n+1)(2n+1)}{6} = n \cdot m^2$$

$$(n+1)(2n+1) = 6m^2$$

$$2n^2 + 3n + 1 = 6m^2$$

$$2n^2 + 3n + (1 - 6m^2) = 0$$

$$n_{1,2} = \frac{-3 \pm \sqrt{9 - 8(1 - 6m^2)}}{4} = \frac{-3 \pm \sqrt{48m^2 + 1}}{4}$$

За да ово био природан број мора $48m^2 + 1 = s^2$, $s \in \mathbb{N}$.

$$s^2 - 48m^2 = 1 \rightarrow \text{Пеловс } j\text{-на}$$

Минимално рјешење можемо изразити на описани начин, али је очигледно да је то пар $(s, m) = (7, 1)$.

Међутим за овај пар се добије $n_1 = \frac{-3 + 7}{4} = 1$, а ми изражавамо $n > 1$.

Стога пронађено сведено рјешење, користити сведену формулу:

Теорема: Ако је (x_1, y_1) једно рјешење ј-не $x^2 - dy^2 = 1$, тада су рјешења и сви парови (x_n, y_n) одређени рекурентним рекурентним

$$x_{n+1} = x_1 x_n + d y_1 y_n$$

$$y_{n+1} = x_1 y_n + y_1 x_n$$

При томе, ако је (x_1, y_1) минимално рјешење, тада горње рекурентне рекурентне дају сва рјешења постављене једначине.

(слично са $x^2 - dy^2 = 1$ (за нешто к), погледајте збирку страна 195).

Закључак, свега је рјешење је:

$$(s_1, m_1) = (7 \cdot 7 + 48 \cdot 1 \cdot 1, 7 \cdot 1 + 1 \cdot 7) = (97, 14)$$

$$\text{Тада је: } n = \frac{-3 + 97}{4} = \frac{94}{4} = \frac{47}{2} \notin \mathbb{N}$$

Свега је рјешење је:

$$(s_2, m_2) = (97 \cdot 7 + 48 \cdot 14 \cdot 1, 7 \cdot 14 + 1 \cdot 97) = (1351, 195)$$

$$\text{Тада је: } n = \frac{-3 + 1351}{4} = \frac{1348}{4} = 337 \quad \text{и ово је наше изражено } n$$

6. Уређен пар $(x, y) = (1155, 34)$ представља рјешење одређене Пелове ј-не. Да ли је тој пар минимално рјешење?

$$1155^2 - m \cdot 34^2 = 1 \Rightarrow m = 1154, \text{ па. шта? } \left\{ \begin{array}{l} \text{Пелова} \\ \text{једначина} \end{array} \right. \text{ облика:}$$

$$x^2 - 1154 y^2 = 1 \rightarrow \text{Тражили смо минимално рјешење описаног облика... (домаћи)}$$

$$\text{Добије се: } \frac{x}{y} = \frac{1155}{34} \Rightarrow \text{дато рјешење јесте минимално}$$

1. Доказати да се ниједан број који даје остатак 3 при дијеленју са 4 не може представити као збир квадрата 2 уједна броја.

$$n \equiv 3 \pmod{4}$$

Пис. $\exists a, b \in \mathbb{Z}$ такв је $a^2 + b^2 = n$. (*)

Које остатке дају квадрати до модула 4?

1 4 9 16 25 36 49...

1 0 1 0 1 0 1 ... Дакле, само 0 и 1.

Ако је $a^2 + b^2 \equiv m \pmod{4}$, онда је $m \in \{0, 1, 2\}$. ∇ са (*).

2. Доказати да ј-на $a^2 + b^2 + c^2 + d^2 = -1$ нема рјешења у $\mathbb{Z}$, али да за $\forall p$, p прост $\exists a, b, c, d \in \mathbb{Z}$ такв је $a^2 + b^2 + c^2 + d^2 \equiv -1 \pmod{p}$.

Како је $a^2 + b^2 + c^2 + d^2 \geq 0$, дакле ј-на нема рјешења у $\mathbb{Z}$.

Нека је сада p неки прост број. Тада је $p-1 \in \mathbb{N}$, па $\exists a, b, c, d \in \mathbb{Z}$

тако да је $a^2 + b^2 + c^2 + d^2 = p-1$ (Легендрово Т.)

$$\Rightarrow a^2 + b^2 + c^2 + d^2 \equiv -1 \pmod{p}.$$

3. (Зонаћи) (22. јун 2020.)

Нека су $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ неки уједн бројеви различити од нуле. Нека притом важе следеће 2 услова:

- сваки a_i је узјатно прост са сваком b_j
- сваки прост број мањи од или једнак са k дијели неки од бројева a_i .

Поставићемо полиноме $P_1(x), P_2(x), \dots, P_k(x)$ такв да $P_i(x) = a_i x + b_i$, за $1 \leq i \leq k$.

Доказати да ова колекција полинома имајуна узајамне Ликсандр шифре

3. Одредити све парове (x, y) елемената из $\mathbb{Z}[\sqrt{2}]$ за које је $\frac{1}{x} + \frac{1}{y} = 2$.

$$\frac{1}{x} + \frac{1}{y} = 2 \Leftrightarrow y + x = 2xy \Leftrightarrow 2xy - x - y = 0 \Leftrightarrow 4xy - 2x - 2y + 1 = 1$$

$$2x(2y-1) - 1(2y-1) = 1 \Leftrightarrow (2x-1)(2y-1) = 1$$

$$\Rightarrow N(2x-1) \cdot N(2y-1) = N(1) = 1$$

$$\Rightarrow \left. \begin{array}{l} N(2x-1) = \pm 1 \\ N(2y-1) = \pm 1 \end{array} \right\} \Rightarrow 2x-1 \text{ и } 2y-1 \text{ у јединични у } \mathbb{Z}[\sqrt{2}]$$

Како изгледају јединични елементи у $\mathbb{Z}[\sqrt{2}]$?

$x \in \mathbb{Z}[\sqrt{2}]$ је облика $x = a + b\sqrt{2}$ (ово x неће дозв са оним горе x) (**)

Он је јединичан ако је $N(x) = \pm 1$.

$$N(x) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Рјешавамо ју $a^2 - 2b^2 = \pm 1 \rightarrow$ Пелова ј-на чије је минимално

рјешење $(1, 1) \rightarrow$ сва рјешења у $\pm (1 + \sqrt{2})^n$ (из T са арадовања).
 $n \in \mathbb{Z}$.

$$\Rightarrow x = \pm (1 + \sqrt{2})^n, n \in \mathbb{Z} \quad (**)$$

$$\text{Дакле, } \begin{array}{l} 2x-1 = \pm (1 + \sqrt{2})^n \\ 2y-1 = \pm (1 + \sqrt{2})^n \end{array}, n \in \mathbb{Z}$$

За да x и y буду уједно елементи, мора

$$a + b\sqrt{2} = (1 + \sqrt{2})^n \equiv 1 \pmod{2} \Rightarrow a \equiv 1 \pmod{2} \text{ и } b \equiv 0 \pmod{2}$$

$$\Rightarrow \text{ако је } n = 2k, k \in \mathbb{Z}$$

(само за парне n -ове)

*Напомена: Наћи све јединичне елементе у $\mathbb{Z}[\sqrt{2}]$.

$$a^2 - 2b^2 = \pm 1 \rightarrow \text{Пелова ј-на}$$

$$a^2 - 2b^2 = 1$$

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}}$$

↓

$a_0 \rightarrow k$ је парно

Минимално рјешење је

$$\frac{x}{y} = 1 + \frac{1}{2} = \frac{3}{2} \quad (x, y) = (3, 2) \rightarrow \text{сва рјешења су } \pm (3 + 2\sqrt{2})^n, n \in \mathbb{Z}$$

$$a^2 - 2b^2 = -1$$

Минимално рјешење је $(x, y) = (1, 1)$ (из формуле коју је k непарно)
(а и још је очигледно да је то мин.)

$\rightarrow$ сва рјешења су још $\pm (1 + \sqrt{2})^n, n \in \mathbb{Z}$.

Закључак, рјешење је : сви ел. облика $\pm (3 + 2\sqrt{2})^n$ или $\pm (1 + \sqrt{2})^n, n \in \mathbb{Z}$.

Али примјетимо $(3 + 2\sqrt{2})^n = ((1 + \sqrt{2})^2)^n = (1 + \sqrt{2})^{2n}, n \in \mathbb{Z}$.

Тако да су сва рјешења још $\pm (1 + \sqrt{2})^n$.

4. Рјешити једначину $x^2 + 2 = y^3$, $y \in \mathbb{Z}$.

Прво примјетимо да x не може бити парно, јер у том случају

$$y^3 \equiv 2 \pmod{4} \Rightarrow x \text{ је непарно} \Rightarrow y \text{ је непарно.}$$

Напишимо лјеву страну као $(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$.

Идеја: Проверити јесу ли $(x + \sqrt{-2})$ и $(x - \sqrt{-2})$ узajачно просте? ($y \in \mathbb{Z}[\sqrt{-2}]$).

Пис. $\exists z$, нејединични елементи, тако да

$$z \mid x + \sqrt{-2} \text{ и } z \mid x - \sqrt{-2} \Rightarrow z \mid x + \sqrt{-2} - (x - \sqrt{-2}) = 2\sqrt{-2}$$

$$\Rightarrow N(z) \mid N(2\sqrt{-2}) = 8 \Rightarrow N(z) \in \{2, 4, 8\} \Rightarrow \text{паран број}$$

$$N(x + \sqrt{-2}) = x^2 + 2 \rightarrow \text{непарно!}$$

Када се аддујемо, добијемо да $z \mid x + \sqrt{-2} \Rightarrow \underbrace{N(z)}_{\text{парно}} \mid \underbrace{N(x + \sqrt{-2})}_{\text{непарно}} \nmid$

$\Rightarrow x + \sqrt{-2}$ и $x - \sqrt{-2}$ су узajачно просте и њихов производ је апсолутно 3-адамен $\Rightarrow$ сваки од њих је апсолутно 3-адамен

$\Rightarrow \exists a, b \in \mathbb{Z}$ таку је

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2}$$

$$\Rightarrow x = a(a^2 - 6b^2)$$

$$1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2) \Rightarrow b = -1$$

$$b = 1$$

$$3a^2 - 2 = -1$$

$$3a^2 - 2 = 1$$

$$3a^2 = 1 \nmid$$

$$3a^2 = 3$$

$$\text{неч } p \nmid y \nmid$$

$$a = \pm 1$$

$$\Rightarrow x = \pm 5 \text{ и } y = \pm 3$$

$(5, 3)$ и $(-5, 3)$ су једина узajачно проста рјешења издвојене ј-не.

5. Нека је дати прост број $p \equiv 1 \pmod{6}$. Докажити да постоје $a, b \in \mathbb{Z}$ такв да је $p = a^2 - ab + b^2$.

Довољно је показати да је p сирмен. Зашто?

Нп. да је p сирмен $\Rightarrow \exists z \in \mathbb{Z}[\omega]$ прост ($\omega = \frac{-1+i\sqrt{3}}{2}$) такав да

$z \mid p$. Тада и $\bar{z} \mid \bar{p} = p$, а како $(z, \bar{z}) = 1 \Rightarrow z \cdot \bar{z} = N(z) \mid p$

$\Rightarrow N(z) = p$, а ако z написати као $z = a + b\omega \Rightarrow N(z) = a^2 - ab + b^2 = p$

и то је крај доказа.

Дакле, довољно је показати да је p сирмен. Значи $p \equiv 1 \pmod{6}$.

Покажимо да је -3 кв. остаток по модулу $p = 6k+1$.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2} \frac{p-1}{2}} = \left(\frac{6k+1}{3}\right) = \left(\frac{1}{3}\right) = 1 \quad \checkmark$$

То значи да $\exists u$ такв да је $u^2 \equiv -3 \pmod{p} \Rightarrow p \mid u^2 + 3$.

$$p \mid (u^2 + 3) = 4m^2 - 4mn + 4n^2 = 4(m^2 - mn + n^2)$$

$\parallel$ $2m-n \rightarrow$ овако ми увек можемо одабрати такв m, n

$\Rightarrow p \mid m^2 - mn + n^2 = (m + n\omega)(\overline{m + n\omega})$, ако је p прост, онда

$\Rightarrow p \mid m + n\omega \vee p \mid \overline{m + n\omega}$

Али ми увек можемо одабрати m и n такв да не буде јавича

са p , па p не може бити прост.

Нпр. узмемо $n=2$ и $m=u+1$.

$$(u^2 + 3 = 4m^2 - 4mn + 4n^2 \text{ па } u^2 + 3 = 4(u+1)^2 - 8(u+1) + 16 = 4u^2 + 4u + 4 \checkmark)$$

6. Одредити све јединичне елементе у $\mathbb{Z}[\sqrt{2021}]$.

Нека $x = a + b\sqrt{2021} \in \mathbb{Z}[\sqrt{2021}]$.

Тада је $N(x) = (a + b\sqrt{2021})(a - b\sqrt{2021}) = a^2 - b^2 \cdot 2021$.

x је јединични ако је $N(x) = \pm 1 \Leftrightarrow a^2 - 2021b^2 = \pm 1$

$\Rightarrow$ то је Пелова ј-на ... ирационално рјешенје Пелове ј-не..

7. Под условом да важи Ликатова хипотеза, докажи да постоји бесконачно много простих бројева p , таквих да су p , $p+6$, и $p+12$ прости.

Покажи да полиноми $f_1(x) = x$, $f_2(x) = x+6$ и $f_3(x) = x+12$

задовољавају услове Д.Х. Ово су линеарни полиноми са одз. водетим коефицијентима и њихове вриједности су уједнобројне за ма коју уједнобројан аргумент.

Покажи још да не постоји p прост так да $p \mid x(x+6)(x+12)$ за $\forall x \in \mathbb{Z}$.

Пис. ипак p постоји.

$$Q(x) = x(x+6)(x+12)$$

$$Q(-1) = -5 \cdot 11 \Rightarrow p \in \{5, 11\}$$

$$Q(1) = 7 \cdot 11 \quad \text{и} \quad 5 \nmid Q(1) \quad \text{и} \quad 11 \nmid Q(1) \quad \downarrow$$

$\Rightarrow$ Ови полиноми задовољавају услове Ликатове хипотезе

$\Rightarrow$ Постоји бесконачно много $m \in \mathbb{Z}$ так да m , $m+6$, $m+12$ прости.

8. Задана функција S на $\mathbb{N}$ са: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, онда је
 $S(n) = \alpha_1 p_1 + \alpha_2 p_2 + \dots + \alpha_k p_k$. Пог утв. да важи Минуенова асимптота и
 покажимо да постоји бесконачно много природних бројева n за које
 је $S(n) = S(n+1)$.

Улога: Ако је $k \in \mathbb{N}$ такав да су s, p, q, r сви прости за

$$s = 2k+1; \quad q = 48k^2 + 24k - 1;$$

$$p = 8k+5; \quad r = 48k^2 + 30k - 1; \quad \text{показати: } S(pq) = S(pq+1).$$

$$S(p \cdot q) = p + q = 8k+5 + 48k^2 + 24k - 1 = 48k^2 + 32k + 4$$

$$p \cdot r = (8k+5)(48k^2 + 30k - 1) = 384k^3 + 240k^2 - 8k + 240k^2 + 150k - 5 =$$

$$= 384k^3 + 480k^2 + 142k - 5 \stackrel{*}{=} p \cdot q + \underbrace{48k^2 + 30k}_{r} - 1 + 1 = p \cdot q + r + 1 \Rightarrow$$

$$\begin{aligned} * p \cdot q &= (8k+5)(48k^2 + 24k - 1) = 384k^3 + 192k^2 - 8k + 240k^2 + 120k - 5 = \\ &= 384k^3 + 432k^2 + 112k - 5 \end{aligned}$$

$$\Rightarrow \boxed{p \cdot q + 1} = pr - r = r(p-1) = r \cdot (8k+4) = 4 \cdot r \cdot s \quad \boxed{= 2^2 \cdot r \cdot s}$$

$S(p \cdot q + 1) = 2 \cdot 2 + r + s = 4 + 48k^2 + 30k - 1 + 2k + 1 = 48k^2 + 32k + 4 = S(pq)$ и тако
 је и пређашње доказано.

Треба још доказати да постоји бесконачно много простих облика s, p, q, r
 (име гласи да за бесконачно много $n \in \mathbb{N}$ са израженим особинама).

Постављамо полиноме: $f_1(x) = 2x+1, f_2(x) = 8x+5, f_3(x) = 48x^2 + 24x - 1, f_4(x) = 48x^2 + 30x$.

Ово су непродуживи поли. са одз. одређеним коеф., према само провери да и

$\exists p$ прост такв $p \mid Q(x) \forall x \in \mathbb{Z}$. Пог да тако p постоји.

$$\cdot x=0 \quad Q(0) = 1 \cdot 5 \cdot (-1) \cdot (-1) = 5 \Rightarrow p=5 \text{ једина могућа}$$

$$\cdot x=-1 \quad Q(-1) = (-1) \cdot (-3) \cdot 23 \cdot 17 = 3 \cdot 17 \cdot 23 \Rightarrow p \in \{3, 17, 23\} \quad \frac{4}{7}$$

Сада из М.Х. $\exists$ бесконачно много m такв да су $f_1(m), f_2(m), f_3(m), f_4(m)$ прости.