МАТЕМАТИЧКИ ФАКУЛТЕТ
УНИВЕРЗИТЕТ У БЕОГРАДУ

Марина Маркагић

ЕКСПОНЕНЦИЈАЛНЕ КОНГРУЕНЦИЈЕ И ПРОБЛЕМСКИ ЗАДАЦИ

Мастер рад

Београд, 2020.

Ментор:

проф. др Горан Ђанковић, ванредни професор
Универзитет у Београду, Математички факултет

Чланови комисије:

проф. др Зоран Петровић, редовни професор
Универзитет у Београду, Математички факултет

др Марко Радовановић, доцент
Универзитет у Београду, Математички факултет

Датум одбране:

Мами, тати и сестри

Садржај

Предговор

Међу старим Грцима било је људи као што је Демокрит који су увиђали, као и ми данас, да је знање нешто што имамо право и дужност да поделимо са другима. Први, који су желели да распростиру своје знање, били су математичари. Међу њима се истакао Питагора, који је путовао и држао предавања о геометријским облицима и о бројевима пред многобројним слушаоцима још у шестом веку пре нове ере. Од тог доба па све до данас, велике математичаре, али и обичне људе, интригира појам броја, који је увек био инспиративна тема за проучавање.

Проучавање броја и његових особина кроз историју, резултирало је развојем читаве науке, јер, математика се не може замислити без теорије бројева.

На развој теорије бројева, осим практичних проблема са којима су се људи сусретали, доста су утицала и математичка надметања и трагање за решењима проблема који су у том тренутку били актуелни. Чак се и имена врсних математичара, попут Гауса и Лежандра, спомињу у том контексту.

Некада, математички двобоји и надметања, а сада, разни математички квизови и такмичења. Данас се готово не може замислити иједно математичко такмичење или квиз без задатака из теорије бројева. Засигурно један од разлога за то, поред велике примене и утицаја који теорија бројева има на готово све гране математике, али и рачунарства, дефинитивно је и велики број још увек нерешених проблема који захтевају добро познавање особина бројева и њихових међусобних односа.

Надарени ученици, али и сви они којима је математика на било који начин привлачна, кроз припреме за такмичења уче неке основне концепте математике, развијају своју интелигенцију, интересовање, али и моћ запажања и закључивања, што их може одвести ка новим идејима и пробудити жељу за бављењем овом науком.

Овај рад се бави једним делом теорије бројева, а свакако су математичка такмичења послужила као инспирација. Посвећен је свим ученицима заинтересо-

ваним за ову област, али и њиховим наставницима који треба да буду саставни део читавог процеса. Идеја је била изложити теорију неопходну за разумевање особина конгруенција, посебно експоненцијалних, праћену одговарајућим примерима, а све са циљем доброг разумевања идеја и поступака за решавање задатака из ове области.

Рад је подељен на три главе:

Прва глава је уводног типа. У њој су изложени неки основни појмови и тврђења везана за конгруенције, а која су неопходна за разумевање теорема и доказа у другој и трећој глави.

У другој глави уведени су појмови као што је поредак броја по модулу и примитивни корен, као и две теореме о експоненцијалним конгруенцијама.

У трећој глави је највише акценат на тврђењима везаним за експоненцијалне конгруенције. Изложене су две Лежандрове теореме и тзв. "Лема о подизању експонента".

На крају сваке главе изложени су задаци, углавном са разних такмичења, и неки од могућих поступака за њихово решавање. Ученицима се саветује да, пре него што погледају решења, а након ишчитавања теорије са разумевањем, сами покушају да дођу до сопствених решења.

Захвалила бих се свом ментору, проф. др Горану Ђанковићу, на помоћи око одабира теме, као и свим идејама, корисним примедбама и помоћи у току израде рада. Такође, захваљујем се на саветима и осталим члановима комисије, проф. др Зорану Петровићу и др Марку Радовановићу.

Неке ознаке које ћемо користити

Нека су a и b природни бројеви. Са (a, b) означаваћемо *највећи заједнички делилац* бројева a и b, а са $[a, b]$ *најмањи заједнички садржалац* тих бројева.

Нека је p прост, α природан и m цео број. Користићемо ознаку $p^\alpha \| m$ и говорићемо "p^α тачно дели m", ако је α највећи степен броја p који дели m, тј. $p^\alpha \mid m$ и $p^{\alpha+1} \nmid m$.

Нека је x реалан број. Са $\lfloor x \rfloor$ ћемо означавати највећи цео број x који је мањи или једнак x.

ГЛАВА 1

Конгруенције

Дефиниција 1.1 Нека је дат природан број $n, n > 1$. Цели бројеви a и b су конгруентни по модулу n ако дају исти остатак при дељењу са n. Пише се $a \equiv b \pmod{n}$.

Пример 1.1 а) $18 \equiv 3 \pmod{5}$, б) $45 \equiv 24 \pmod{7}$, в) $121 \equiv 57 \pmod{8}$.

Теорема 1.1 *Нека су a и b цели бројеви и n природан број већи од* 1. *Тада важи:*

(1) $a \equiv b \pmod{n}$ *ако и само ако је* $a = nt + b$ *за неки цео број* t;

(2) $a \equiv b \pmod{n}$ *ако и само ако је разлика бројева a и b дељива са n*;

(3) Бити конгруентан по датом модулу је релација еквиваленције у скупу целих бројева.

Теорема 1.2 *Нека су a, b, c и d цели бројеви и n природан број већи од* 1. *Тада важи:*

(1) Ако је $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$, *онда за свака два цела броја* x, y *важи* $ax + cy \equiv bx + dy \pmod{n}$;

(2) Ако је $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$, *онда је* $ac \equiv bd \pmod{n}$;

(3) Ако је $a \equiv b \pmod{n}$ *и* $n = \alpha m,\ \alpha, m \in \mathbb{N},\ m > 1$, *онда је* $a \equiv b \pmod{m}$;

(4) Ако је $P(x)$ полином по x са целобројним коефицијентима, онда из $a \equiv b \pmod{n}$ *следи да је* $P(a) \equiv P(b) \pmod{n}$.

Доказ: (1) Ако је $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, онда $n \mid a - b$ и $n \mid c - d$, па важи и $n \mid (a - b)x$ и $n \mid (c - d)y$. Дакле,

$$n \mid (a - b)x + (c - d)y \implies n \mid (ax + cy) - (bx + dy),$$

тј. $ax + cy \equiv bx + dy \pmod{n}$.

(2) Из $a \equiv b \pmod{n}$ следи да $n \mid a - b$, па и $n \mid (a-b)c$. Такође, из $c \equiv d \pmod{n}$ следи да $n \mid c - d$, па и $n \mid (c-d)b$. Дакле,

$$n \mid (ac - bc) + (cb - db) \implies n \mid ac - bd,$$

тј. $ac \equiv bd \pmod{n}$.

(3) Ако $n \mid a - b$ и $m \mid n, m > 1$, онда због транзитивности релације дељивости, имамо да и $m \mid a - b$, тј. да је $a \equiv b \pmod{m}$.

(4) Према (2) имамо да за сваки природан број m важи следећа импликација

$$a \equiv b \pmod{n} \implies a^m \equiv b^m \pmod{n},$$

а одавде и из (1) имамо да

$$a \equiv b \pmod{n} \implies P(a) \equiv P(b) \pmod{n},$$

за сваки полином $P(x)$ са целобројним коефицијентима.

□

Теорема 1.3 *Нека су a, b, n природни бројеви већи од 1 и x, y цели бројеви. Тада важи:*

(1) Ако су a и n узајамно прости и $ax \equiv ay \pmod{n}$, онда је $x \equiv y \pmod{n}$;

(2) $ax \equiv ay \pmod{n}$ ако и само ако $x \equiv y \pmod{\frac{n}{(a,n)}}$;

(3) $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$ ако и само ако $x \equiv y \pmod{[a,b]}$.

Доказ: (1) Из $ax \equiv ay \pmod{n}$, тј. из $n \mid a(x-y)$, због услова $(a,n) = 1$, следи да $n \mid x - y$, тј. $x \equiv y \pmod{n}$.

(2) Ако је $ax \equiv ay \pmod{n}$, онда је $a(x-y) = kn$, за неки цео број k, па је и $\frac{a}{(a,n)}(x-y) = k\frac{n}{(a,n)}$. Дакле, $\frac{n}{(a,n)} \mid \frac{a}{(a,n)}(x-y)$. Како је $\left(\frac{n}{(a,n)}, \frac{a}{(a,n)}\right) = 1$, следи да $\frac{n}{(a,n)} \mid x - y$, тј. да је $x \equiv y \pmod{\frac{n}{(a,n)}}$.

Обрнуто, ако је $x \equiv y \pmod{\frac{n}{(a,n)}}$, онда је $x - y = k\frac{n}{(a,n)}$, за неки цео број k, па је и $ax - ay = \frac{ak}{(a,n)}n$ ($\frac{a}{(a,n)}$ је природан, па је $\frac{ak}{(a,n)}$ цео број), тј. $ax \equiv ay \pmod{n}$.

(3) Из $x \equiv y \pmod{a}$ следи $a \mid x - y$. Такође, из $x \equiv y \pmod{b}$ следи $b \mid x - y$. Ово значи да $[a,b] \mid x - y$, тј. $x \equiv y \pmod{[a,b]}$.

□

1.1 Ојлерова функција

Дефиниција 1.2 Скуп од n целих бројева у коме не постоји ни један пар бројева конгруентних по модулу n, где је n природан број већи од 1, зове се **потпуни систем остатака по модулу** n.

Пример 1.2 Скупови $\{0,1,2,3,4,5,6,7\}$ и $\{16,-7,34,11,-36,21,-10,31\}$ су потпуни системи остатака по модулу 8.

Дефиниција 1.3 Скуп свих елемената потпуног система остатака по модулу n који су узајамно прости са n назива се **сведени (редуковани) систем остатака по модулу** n.

Пример 1.3 Скупови $\{1,3,5,7\}$ и $\{-7,11,21,31\}$ су сведени системи остатака по модулу 8.

Дефиниција 1.4 Број природних бројева који нису већи од датог природног броја n, $n>1$, и узајамно су прости са њим, тј. број елемената произвољног сведеног система остатака по модулу n, означава се са $\varphi(n)$. Функција φ дефинисана на овај начин, при чему је $\varphi(1)=1$, зове се **Ојлерова функција.**

Ако је p прост број, онда је $\varphi(p)=p-1$.
$\varphi(1)=\varphi(2)=1,\ \varphi(3)=\varphi(4)=\varphi(6)=2$ итд.

Теорема 1.4 *Нека је n природан број већи од 1 и a цео број, тако да је $(a,n)=1$. Ако је $\{x_1,x_2,...,x_{\varphi(n)}\}$ сведени систем остатака по модулу n, онда је и $\{ax_1,ax_2,...,ax_{\varphi(n)}\}$ сведени систем остатака по модулу n.*

Доказ: Тврђење следи из чињенице да скуп $\{ax_1,ax_2,...,ax_{\varphi(n)}\}$ садржи $\varphi(n)$ целих бројева, међу којима нема конгруентних по модулу n и сваки од њих је узајамно прост са n.

□

Пример 1.4 Нека је $n=12$ и $a=7$. Тада су n и a узајамно прости, па је скуп $\{7\cdot 0,7\cdot 1,7\cdot 2,...,7\cdot 11\}=\{0,7,14,...,77\}$ потпуни систем остатака по модулу 12, а скуп $\{7\cdot 1,7\cdot 5,7\cdot 7,7\cdot 11\}=\{7,35,49,77\}$ је сведени систем остатака по модулу 12.

Теорема 1.5 *Ојлерова функција је мултипликативна у аритметичком смислу, тј. ако су m и n узајамно прости природни бројеви, онда је $\varphi(mn)=\varphi(m)\varphi(n)$.*

Теорема 1.6 *Нека су p_i прости и α_i природни бројеви, $1\leqslant i\leqslant k$. Ако је $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација природног броја n, онда је*

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

Доказ: Нека је $n = p^\alpha$, за неки прост број p и неки природан број α. Међу природним бројевима од 1 до p^α има $p^{\alpha-1}$ бројева који нису узајамно прости са p^α, тј. бројева који су дељиви са p. То су

$$p, 2p, ..., p^2, ..., p^\alpha.$$

Дакле, међу природним бројевима од 1 до p^α има $p^\alpha - p^{\alpha-1}$ бројева узајамно простих са p^α, тј.

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Ако је, сада, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n, применом претходне теореме (више пута) имамо:

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

□

Пример 1.5 $\varphi(2020) = \varphi(2^2 \cdot 5^1 \cdot 101^1) = 2^1 \cdot 5^0 \cdot 101^0(2-1)(5-1)(101-1) = 800.$

Теорема 1.7 (Ојлерова теорема) *Нека је n природан број већи од 1, а цео број a и $(a, n) = 1$. Тада важи:*

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

Доказ: Нека је $\{x_1, x_2, ..., x_{\varphi(n)}\}$ сведени систем остатака по модулу n. Тада је и $\{ax_1, ax_2, ..., ax_{\varphi(n)}\}$ сведени систем остатака по модулу n, јер је $(a, n) = 1$. Према томе, за свако x_i постоји тачно један ax_j такав да је $x_i \equiv ax_j \pmod{n}$, па је

$$(ax_1)(ax_2) \cdots (ax_{\varphi(n)}) \equiv x_1 x_2 \cdots x_{\varphi(n)} \pmod{n},$$

односно

$$a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \equiv x_1 x_2 \cdots x_{\varphi(n)} \pmod{n}.$$

Како је $(x_1 x_2 \cdots x_{\varphi(n)}, n) = 1$, имамо да је

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

□

Напомена 1.1 Број $\varphi(n)$ није најмањи природан број k такав да је $a^k \equiv 1 \pmod{n}$.

Теорема 1.8 (Мала Фермаова теорема) *Нека је p прост број, а цео број и $p \nmid a$. Тада је $a^{p-1} \equiv 1 \pmod{p}$.*

Доказ: Ако p не дели a, онда је $(a,p)=1$. Како за сваки прост број p важи $\varphi(p)=p-1$, закључујемо да је ово специјалан случај Ојлерове теореме.

□

Последица 1.1 *Ако је p прост број и a произвољан цео број, онда важи $a^p \equiv a \pmod{p}$.*

Дефиниција 1.5 Нека су a и b цели бројеви различити од 0 и n природан број већи од 1, при чему је $(a,n)=1$. Број b за који важи $ab \equiv 1 \pmod{n}$ назива се **инверз** броја a по модулу n. Пишемо $a^{-1} = b \pmod{n}$.

Пример 1.6 Инверз броја 3 по модулу 4 је 3, јер је $3 \cdot 3 = 9 \equiv 1 \pmod{4}$. Инверз броја 3 по модулу 5 је 2, јер је $3 \cdot 2 = 6 \equiv 1 \pmod{5}$.

Лема 1.1 *Нека су a, b, x цели бројеви, $a \neq 0$ и n природан број већи од 1. Конгруенција $ax \equiv b \pmod{n}$ увек има решење (по x) када су a и n узајамно прости бројеви.*

Доказ: Узмимо да је $x \equiv a^{-1}b \pmod{n}$.

□

Теорема 1.9 (Кинеска теорема о остацима) *Нека су $a_1, a_2, \ldots, a_r$ произвољни цели бројеви и нека су $n_1, n_2, \ldots, n_r$ по паровима узајамно прости природни бројеви већи од 1, тј. $(n_i, n_j) = 1$ за $i \neq j$. Тада постоји решење система конгруенција:*

$$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_r \pmod{n_r}. \tag{1.1}$$

Ако је x_0 једно решење система (1.1), онда је x решење система (1.1) ако и само ако је облика $x_0 + kn$, где је k произвољан цео број, а $n = n_1 n_2 \cdots n_r$.

Доказ: Доказ ћемо извести за систем две конгруенције:

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2},$$

при чему је $(n_1, n_2) = 1$.

Свако решење прве од ових конгруенција је облика $x = a_1 + yn_1, y \in \mathbb{Z}$. Оно је решење и друге од ових конгруенција ако и само ако је $n_1 y \equiv a_2 - a_1 \pmod{n_2}$. Пошто су n_1 и n_2 узајамно прости, на основу претходне леме следи да последња конгруенција има бар једно решење y_0, па је $x_0 = a_1 + n_1 y_0$ једно заједничко решење датог система конгруенција.

Даље, ако су x_0 и x_0' било која заједничка решења датих конгруенција, из $x_0 \equiv a_1 \pmod{n_1}$ и $x_0' \equiv a_1 \pmod{n_1}$ следи да $n_1 \mid x_0 - x_0'$. Слично се доказује да $n_2 \mid x_0 - x_0'$, па $[n_1, n_2] \mid x_0 - x_0'$. Како су n_1 и n_2 узајамно прости, онда је $[n_1, n_2] = n_1 n_2$, тј. $x_0 \equiv x_0' \pmod{n_1 n_2}$.

□

Пример 1.7 Решимо следећи систем линеарних конгруенција:

$$x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod{11}.$$

Приметимо да x можемо записати у облику $5k + 3$ и $11m + 4$, за неке целе бројеве k и m. Дакле,

$$x = 5k + 3 = 11m + 4.$$

Посматрањем конгруенције по модулу 5 добијамо:

$$11m + 4 \equiv 3 \pmod 5 \implies m \equiv -1 \pmod 5.$$

Из једнакости $m = 5m_1 - 1,\ m_1 \in \mathbb{Z}$, добијамо $x = 11(5m_1 - 1) + 4 = 55m_1 - 7$.

Дакле, $x \equiv -7 \equiv 48 \pmod{55}$, што нас доводи до решења почетног система линеарних конгруенција $x = 55k_1 + 48$, за неки цео број k_1.

1.2 Задаци

1.1. Израчунати $2^{98} \pmod{33}$.

Задатак ћемо решити на два начина.

Начин 1: Приметимо да 33 није прост број и да из тог разлога не можемо директно да искористимо Малу Фермаову теорему. Међутим, ова теорема ће нам бити веома корисна у овом начину решавања. Наиме, како је $33 = 3 \cdot 11$ и $2 \nmid 3, 11$, можемо израчунати колико је $2^{98} \pmod 3$ и $2^{98} \pmod{11}$ коришћењем Мале Фермаове теореме, а затим искористити ове резултате и применити Кинеску теорему о остацима како бисмо дошли до жељеног решења.

Важи следеће: $2^{3-1} = 2^2 \equiv 1 \pmod 3$ и $2^{11-1} = 2^{10} \equiv 1 \pmod{11}$. Коришћењем ових конгруенција добијамо:

$$2^{98} = \left(2^2\right)^{49} \equiv 1^{49} \equiv 1 \pmod 3$$

и

$$2^{98} = \left(2^{10}\right)^9 \cdot 2^8 \equiv 1 \cdot 256 \equiv 3 \pmod{11}.$$

Нека је сада $2^{98} = x$. Решимо систем конгруенција:

$$x \equiv 1 \pmod 3, \quad x \equiv 3 \pmod{11}.$$

Из наведеног система добијамо следећу једнакост: $x = 3k + 1 = 11l + 3$, за неке целе бројеве k и l. Коришћењем ове једнакости имамо $11l + 3 \equiv 1 \pmod 3 \implies 2l \equiv 1 \pmod 3$. Како нам је потребно $l \pmod 3$, морамо наћи инверз броја 2 по модулу 3. Провером налазимо да је инверз броја $2 \pmod 3$ једнак 2, па множењем последње

конгруенције са 2, добијамо $l \equiv 2 \pmod 3$, тј. $l = 3m + 2$, за неки цео број m. Коришћењем ове једнакости добијамо:

$$x = 11(3m + 2) + 3 = 33m + 25,$$

што нас доводи до решења задатка

$$2^{98} = x \equiv 25 \pmod{33}.$$

Начин 2: Како Ојлерова теорема важи код сложених модула, у овом случају ћемо њу искористити.

Најпре, пронађимо вредност Ојлерове функције за 33. $\varphi(33) = \varphi(3 \cdot 11) = 33\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = (3 - 1)(11 - 1) = 20$. Сада, применом Ојлерове теореме, добијамо $2^{\varphi(33)} = 2^{20} \equiv 1 \pmod{33}$. Применом на задати проблем, добијамо

$$x = 2^{98} = \left(2^{20}\right)^5 2^{-2} \equiv 4^{-1} \pmod{33}.$$

Множењем последње конгруенције са 4, добијамо $4x \equiv 1 \pmod{33}$. У овом тренутку је потребно да нађемо инверз броја 4 (mod 33). Провером налазимо да је 25 инверз броја 4 (mod 33), па множењем са 25 добијамо $x \equiv 25 \pmod{33}$. Ово нам даје тражено решење задатка $x = 2^{98} \equiv 25 \pmod{33}$. $\triangle$

1.2. Показати да је $2^{n-1} \equiv 1 \pmod n$ за $n = 73 \cdot 37$.

Решење: Приметимо да су 73 и 37 прости бројеви. Покушајмо са Малом Фермаовом теоремом. Применом ове теореме добијамо:

$$2^{72} \equiv 1 \pmod{73} \text{ и } 2^{36} \equiv 1 \pmod{37}.$$

Коришћењем друге конгруенције можемо закључити да

$$2^{72} = (2^{36})^2 \equiv 1^2 \equiv 1 \pmod{37}.$$

Сада, применом Теореме 1.3 на претходне конгруенције, закључујемо да је $2^{72} \equiv 1 \pmod{[73, 37]}$, а како је $(73, 37) = 1$, онда је $2^{72} \equiv 1 \pmod{73 \cdot 37}$. Из овога можемо закључити да је $2^{72 \cdot 37} \equiv 1^{37} \equiv 1 \pmod{73 \cdot 37}$. Посматрајмо сада 2^{n-1}, тј. $2^{73 \cdot 37 - 1}$.

$$2^{73 \cdot 37 - 1} = 2^{72 \cdot 37 + 37 - 1} = 2^{72 \cdot 37} \cdot 2^{36} \equiv 2^{36} \pmod{73 \cdot 37}.$$

Како је $2^{36} = (2^9)^4 \equiv 1^4 \equiv 1 \pmod{73}$, закључујемо да је $2^{36} \equiv 1 \pmod{73 \cdot 37}$. Дакле, $2^{73 \cdot 37 - 1} \equiv 1 \pmod{73 \cdot 37}$. $\triangle$

1.3. Доказати да је за сваки паран број n број $20^n + 16^n - 3^n - 1$ дељив са 323.

Решење: Како је број 323 сложен, ако докажемо да је дати број дељив сваким од простих чиниоца броја 323, завршили смо са доказом.

$323 = 17 \cdot 19$. Нека је n произвољан паран број.

Испитајмо прво случај дељивости са 17. Кренимо од основа које су дате. Приметимо да важи $20 \equiv 3 \pmod{17}$. Применом Теореме 1.2 на ову конгруенцију, добијамо $20^n \equiv 3^n \pmod{17}$. Такође, важи и следећа импликација: $16 \equiv -1 \pmod{17} \Longrightarrow 16^n \equiv (-1)^n \pmod{17}$. Како је n паран број, $(-1)^n = 1$, што значи да је $16^n \equiv 1 \pmod{17}$. Ако се вратимо на проблем дат у задатку и применимо добијене конгруенције по модулу 17, добијамо

$$20^n + 16^n - 3^n - 1 \equiv 3^n + 1 - 3^n - 1 \equiv 0 \pmod{17}.$$

Дакле, показали смо да $17 \mid 20^n + 16^n - 3^n - 1$.

Посматрајмо сада шта се дешава по модулу 19. Поново, применом Теореме 1.2, добијамо следеће импликације:

$$20 \equiv 1 \pmod{19} \Longrightarrow 20^n \equiv 1 \pmod{19}$$

и

$$16 \equiv -3 \pmod{19} \Longrightarrow 16^n \equiv (-3)^n \equiv 3^n \pmod{19}.$$

Из овога следи

$$20^n + 16^n - 3^n - 1 \equiv 1 + 3^n - 3^n - 1 \equiv 0 \pmod{19}.$$

Дакле, показали смо и да $19 \mid 20^n + 16^n - 3^n - 1$.

Из овога следи да $323 \mid 20^n + 16^n - 3^n - 1$. $\triangle$

1.4. Доказати да је број $2222^{5555} + 5555^{2222}$ дељив са 7.

Решење: Оно што одмах можемо приметити јесте да је $2222 + 5555 = 7777 \equiv 0 \pmod{7}$, што значи да је $5555 \equiv -2222 \pmod{7}$. Може се проверити да је остатак који добијамо приликом дељења броја 2222 са 7 једнак 3, па је $2222 \equiv 3 \pmod{7}$.

Овим разматрањем задатак сводимо на испитивање дељивости са 7 броја $3^{5555} + 3^{2222}$. Овај збир можемо записати на следећи начин:

$$3^{5555} + 3^{2222} = 3^{2222}\left(3^{3333} + 1\right).$$

Како 3^{2222} није дељиво са 7, остаје нам да покажемо да је $3^{3333} + 1$ дељиво са 7. Применом Мале Фермаове теореме закључујемо да је $3^6 \equiv 1 \pmod{7}$. Како је $3333 \equiv 3 \pmod{6}$, добијамо да је

$$3^{3333} + 1 = 3^{6k+3} + 1 = \left(3^6\right)^k 3^3 + 1 \equiv 1 \cdot 27 + 1 \equiv 0 \pmod{7},$$

а ово смо желели да докажемо. $\triangle$

1.5. Израчунати последње 2 цифре броја $14^{3^{2020}}$.

Решење: Научили смо до сад да остатак који добијемо приликом дељења неког броја неком декадном јединицом представља последње цифре тог броја, и то онолико последњих цифара колико нула има декадна јединица којом делимо. Ову чињеницу ћемо користити приликом решавања задатака овог типа, када се траже последње цифре неког броја. У овом конкретном случају тражићемо остатак приликом дељења задатог броја са 100, односно $14^{3^{2020}} \pmod{100}$.

Како је $100 = 4 \cdot 25$ и $(4, 25) = 1$, биће нам лакше да израчунамо колико је $14^{3^{2020}} \pmod 4$ и $14^{3^{2020}} \pmod{25}$, а затим да применимо Кинеску теорему о остацима и дођемо до коначног решења.

Израчунајмо прво $14^{3^{2020}} \pmod 4$. Јасно је да је сваки паран број, дигнут на експонент који је већи или једнак од два, дељив са 4. Како је 14 паран број, одмах можемо закључити да је $14^{3^{2020}} \equiv 0 \pmod 4$.

Пронађимо сада $14^{3^{2020}} \pmod{25}$. Како је $(14, 25) = 1$ и $\varphi(25) = 5(5-1) = 20$, из Ојлерове теореме следи $14^{20} \equiv 1 \pmod{25}$. Остаје нам да видимо шта се дешава са $3^{2020} \pmod{20}$. Приметимо да је $3^4 = 81 \equiv 1 \pmod{20}$. Из овога следи:

$$3^{2020} = \left(3^4\right)^{505} \equiv 1^{505} \equiv 1 \pmod{20} \Longrightarrow 3^{2020} = 20k + 1,\ k \in \mathbb{Z}$$

$$\Longrightarrow 14^{3^{2020}} = 14^{20k+1} = \left(14^{20}\right)^k 14^1 \equiv 1^k \cdot 14 \equiv 14 \pmod{25}.$$

Нека је $14^{3^{2020}} = x$. Из претходног разматрања добијамо следећи систем конгруенција чије решење ће бити тражено решење задатка:

$$x \equiv 0 \pmod 4, \quad x \equiv 14 \pmod{25}.$$

Из друге конгруенције имамо $x = 25l + 14$ за неки цео број l. Убацивањем ове једнакости у прву конгруенцију, добијамо $25l + 14 \equiv 0 \pmod 4$. Како је $25 \equiv 1 \pmod 4$ и $14 \equiv 2 \pmod 4$, из претходне конгруенције следи $l + 2 \equiv 0 \pmod 4 \Longrightarrow l \equiv -2 \pmod 4 \Longrightarrow l = 4m - 2$ за неки цео број m. Дакле,

$$x = 25(4m - 2) + 14 = 100m - 36 \Longrightarrow 14^{3^{2020}} = x \equiv -36 \equiv 64 \pmod{100}.$$

Овим смо показали да се број $14^{3^{2020}}$ завршава на 64. $\triangle$

1.6. (а) Ако је a цео, а n природан број, доказати да је број $a\left(a^{2n}-1\right)$ дељив са 6.
(б) Ако је a непаран цео број, а n природан број, доказати да је број $a\left(a^{2n}-1\right)$ дељив са 24.

Решење: Примећујемо да и у делу (а) и у делу (б) испитујемо дељивост броја $a\left(a^{2n}-1\right)$. Како је $a^{2n}-1=\left(a^2\right)^n-1^n$, ово можемо расписати као разлику n-тих степена:

$$\left(a^2\right)^n-1^n=\left(a^2-1\right)\left(a^{2(n-1)}+a^{2(n-2)}+\ldots+a^2+1\right).$$

Из овога следи $a^2-1 \mid a^{2n}-1$.

(а) Посматрајмо шта се дешава са $a(a^2-1)$. Можемо приметити следеће:

$$a(a^2-1)=a(a-1)(a+1)=(a-1)a(a+1).$$

Примећујемо да је на десној страни претходне једнакости производ 3 узастопна цела броја. Ово значи да је тачно један од тих бројева дељив са 3 и бар један број дељив са 2. Дакле, $2 \mid a(a^2-1),\ 3 \mid a(a^2-1)$. Ово значи да:

$$6 \mid a(a^2-1) \implies 6 \mid a(a^{2n}-1).$$

(б) Како је a непаран цео број, можемо га записати у облику $a=2m+1$, за неки цео број m. Тада је

$$a(a^2-1)=(a-1)a(a+1)=2m(2m+1)(2m+2)=4m(m+1)(2m+1).$$

Очигледно је да $4 \mid a(a^2-1)$. Како $2 \mid m(m+1)$, закључујемо да $8 \mid a(a^2-1)$. С обзиром на то да смо у делу под (а) доказали да $3 \mid a(a^2-1)$, закључујемо да $24 \mid a(a^2-1)$, а овим доказујемо да је број $a\left(a^{2n}-1\right)$ дељив са 24. $\triangle$

1.7. Без употребе калкулатора одредити цифре које стоје уместо слова a и b у изразу

$$45^{10}=34050628ab6015625.$$

Решење: Приметимо следеће: $45 \equiv 0 \pmod 9$, што значи да је $45^{10} \equiv 0 \pmod 9$. Знамо да је број дељив са 9 ако и само ако је збир његових цифара дељив са 9. Применом на задати број добијамо следеће:

$$53+a+b \equiv 0 \pmod 9 \implies a+b \equiv -53 \equiv 1 \pmod 9.$$

Како $a,b \in \{0,1,2,...,9\}$, могућа су два случаја:

$$a+b=1 \quad \vee \quad a+b=10. \tag{1.2}$$

Међутим, ово нам није довољно да бисмо дошли до решења. Да ли можемо на сличан начин да дођемо до везе између a и b која би нас довела до решења задатка? Одговор је потврдан, али морамо мало да се довијамо. Било би добро ако бисмо на неки начин искористили правило дељивости са 11. Оно каже да је дати број дељив са 11 ако и само ако је збир цифара на парним позицијама датог броја конгруентан са збиром цифара на непарним позицијама тог броја по модулу 11.

Како је $45 \equiv 1 \pmod{11}$, имамо да је $45^{10} \equiv 1 \pmod{11}$. Из овога закључујемо да је $45^{10} - 1$ дељиво са 11, па ћемо посматрати цифре на парним и непарним местима овог броја. Тако долазимо до следеће конгруенције:

$$22 + a \equiv 30 + b \pmod{11} \implies a - b \equiv 8 \pmod{11}.$$

Како су a и b цифре, имамо да важи $-9 \leqslant a - b \leqslant 9$. Ова чињеница и претходно разматрање дају нам следеће две могућности:

$$a - b = -3 \quad \vee \quad a - b = 8. \tag{1.3}$$

Из (1.2) и (1.3) добијамо 4 система једначина. Једноставним рачуном видећемо да само један систем има решење. То је систем једначина $a + b = 10;\ a - b = 8$. Решавањем долазимо до решења $a = 9$ и $b = 1$. $\triangle$

1.8. Нека су $n_1 < n_2 < \cdots < n_{31}$ прости бројеви. Доказати да ако 30 дели $n_1^4 + n_2^4 + \cdots + n_{31}^4$, онда су међу датим бројевима 3 узастопна проста броја.

Решење: Означимо најпре $S = n_1^4 + n_2^4 + \cdots + n_{31}^4$ и $\mathbb{A} = \{n_1, n_2, \ldots, n_{31}\}$. Ако $30 \mid S$, онда и $2 \mid S,\ 3 \mid S$ и $5 \mid S$.

Чињеница да $2 \mid S$ говори нам да је S паран број, а ово ће значити да $2 \in \mathbb{A}$. Како? Претпоставимо супротно, $2 \notin \mathbb{A}$. Ово значи да су сви $n_i,\ i \in \{1, 2, \ldots, 31\}$, непарни, па и сви n_i^4 су непарни, што значи да је S збир непарног броја непарних бројева, па је S непаран. Контрадикција. Дакле, $2 \in \mathbb{A}$.

На сличан начин ћемо показати да $3 \in \mathbb{A}$. Претпоставимо супротно, $3 \notin \mathbb{A}$. Ово значи да је $n_i \equiv \pm 1 \pmod{3}$, тј. $n_i^4 \equiv 1 \pmod{3}$, за $i \in \{1, 2, \ldots, 31\}$. Из овога следи да је $S \equiv 31 \equiv 1 \pmod{3}$. Контрадикција, јер смо видели на почетку да $3 \mid S$. Дакле, и $3 \in \mathbb{A}$.

Можемо ли показати да и $5 \in \mathbb{A}$? Претпоставимо да $5 \notin \mathbb{A}$. Тада, применом Мале Фермаове теореме, закључујемо да је $n_i^4 \equiv 1 \pmod{5}$, за $i \in \{1, 2, \ldots, 31\}$. Ово нам говори да је $S \equiv 31 \equiv 1 \pmod{5}$, а ово је у контрадикцији са чињеницом да $5 \mid S$. Дакле, и $5 \in \mathbb{A}$.

Како су 2, 3 и 5 три узастопна проста броја, претходним разматрањем смо доказали задато тврђење. $\triangle$

1.9. Одредити, ако постоји, прост број p такав да $p^2 \mid 5^{p^2}+1$.

Решење: Претпоставимо да постоји прост број p који задовољава тражени услов. Тада, према Последици 1.1 Мале Фермаове теореме, имамо $5^p \equiv 5 \pmod{p}$. Степеновањем ове конгруенције са p добијамо $5^{p^2} \equiv 5^p \pmod{p}$, па је

$$5^{p^2} \equiv 5^p \equiv 5 \pmod{p},$$

а одавде закључујемо да је

$$5^{p^2}+1 \equiv 6 \pmod{p}. \tag{1.4}$$

С друге стране, из услова $p^2 \mid 5^{p^2}+1$, следи да $p \mid 5^{p^2}+1$, тј.

$$5^{p^2}+1 \equiv 0 \pmod{p}. \tag{1.5}$$

Из (1.4) и (1.5) следи $6 \equiv 0 \pmod{p}$, што значи да $p \in \{2,3\}$. Испитајмо сваки од ових бројева.

За $p=2$ имамо

$$5^{2^2}+1 = 5^4+1 = 626 \equiv 2 \pmod{2^2},$$

што значи да $p=2$ не задовољава услов задатка.

За $p=3$ имамо

$$5^{3^2}+1 = 5^9+1 = 1\ 953\ 126 = 9 \cdot 217\ 014 \equiv 0 \pmod{3^2}.$$

Дакле, $p=3$ је једини прост број који задовољава услов задатка. $\triangle$

1.10. У таблици 10×10

$$\begin{array}{ccccc} 0 & 1 & 2 & \dots & 9 \\ 9 & 0 & 1 & \dots & 8 \\ 8 & 9 & 0 & \dots & 7 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2 & 3 & \dots & 0 \end{array}$$

заокружено је 10 елемената, у свакој врсти и колони по један. Доказати да су међу њима барем два једнака.

Решење: Идеја је да посматрамо сваки од бројева у таблици и да закључимо на који начин су дати бројеви повезани са врстама и колонама којима припадају.

Ако мало боље погледамо, можемо уочити да је сваки број у таблици конгруентан по модулу 10 са збиром првог броја у врсти и првог броја у колони којој припада. Како је заокружен по један број из сваке врсте и сваке колоне,

претходни закључак ће нам бити веома користан. Наиме, збир заокружених бројева је по модулу 10 конгруентан са

$$(0+1+2+\cdots+9)+(0+9+8+\cdots+1)=90\equiv 0 \pmod{10}.$$

Да бисмо доказали тврђење претпоставићемо супротно, тј. да су сви заокружени бројеви међусобно различити. Тада за збир тих бројева важи

$$0+1+2+\cdots+9=45\equiv 5 \pmod{10},$$

а ово је у контрадикцији са претходном конгруенцијом. Дакле, међу заокруженим бројевима су бар два једнака. $\triangle$

ГЛАВА 2

Поредак броја по датом модулу

Задатак 2.1. Испитујући случај $n = 561$, доказати да *није тачно* следеће: ако за свако $a \in \mathbb{Z}$ узајамно просто са n важи $a^{n-1} \equiv 1 \pmod{n}$, онда је n прост број.

Решење: Имамо $n = 561 = 3 \cdot 11 \cdot 17$. За свако a које није дељиво са $3, 11$ или 17 важи $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ и $a^{16} \equiv 1 \pmod{17}$. Степеновањем ове три конгруенције са експонентима $280, 56, 35$ редом добијамо $a^{560} \equiv 1$ по модулима $3, 11$ и 17. Дакле, $a^{560} \equiv 1 \pmod{561}$. $\triangle$

Напомена 2.1 Бројеви n са овим својством се зову *Кармајклови бројеви.* Једини Кармајклов број мањи од 1000 је $n = 561$.

Приметимо да из решења претходног задатка следи да је $a^{80} \equiv 1 \pmod{561}$, што је јаче од тврђења Ојлерове теореме по коме је $a^{320} \equiv 1 \pmod{561}$ (јер је $\varphi(561) = 2 \cdot 10 \cdot 16 = 320$). Ово нам сугерише да експонент $\varphi(n)$ у Ојлеровој теореми може у општем случају да се побољша.

2.1 Кармајклова функција

Дефиниција 2.1 Кармајклова функција $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ дефинише се на следећи начин:

(1) $\lambda(1) = 1,\ \lambda(2) = 1,\ \lambda(4) = 2,\ \lambda(2^\alpha) = 2^{\alpha-2}$, за $\alpha \geqslant 3$

(2) $\lambda(p^\alpha) = p^{\alpha-1}(p-1)$, за непаран прост број p и природан број α

(3) $\lambda(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = [\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), ..., \lambda(p_k^{\alpha_k})]$

Очигледно, $\lambda(n)$ дели $\varphi(n)$. На пример, $\lambda(56) = \left[\lambda(7^1), \lambda(2^3)\right] = \left[7-1, 2^{3-2}\right] = [6, 2] = 6$ дели $\varphi(56) = 56\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{2}\right) = 24$.

Теорема 2.1 (Кармајклова теорема) *Нека је n природан број већи од 1, a цео број и $(a, n) = 1$. Тада важи:*

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Доказ: Довољно је показати да важи $a^{\lambda(p^\alpha)} \equiv 1 \pmod{p^\alpha}$ за сваки прост број p и $\alpha \geqslant 0$. Пошто $\lambda(p^\alpha) \mid \lambda(n)$ кад год $p^\alpha \mid n$, степеновањем са $\lambda(n)/\lambda(p^\alpha)$ ће следити да $p^\alpha \mid a^{\lambda(n)} - 1$ и одатле $n \mid a^{\lambda(n)} - 1$.
Ако је p непарно, $a^{\lambda(p^\alpha)} = a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$ важи по Ојлеровој теореми. У случају $p = 2$ и $\alpha \geqslant 3$ је $a^{\lambda(2^\alpha)} - 1 = a^{2^{\alpha-2}} - 1 = (a^2 - 1)\prod_{k=1}^{\alpha-3}(a^{2^k} - 1)$, при чему $2^3 \mid a^2 - 1$ и сви остали чиниоци су парни, одакле следи тврђење.

□

Ако је n прост број, Кармајклова теорема не даје побољшање Фермаове јер је тада $\lambda(n) = n - 1$. Међутим, у општем случају побољшање је често значајно.

Пример 2.1 По Кармајкловој теореми је $a^{60} \equiv 1 \pmod{N}$ за $(a, N) = 1$, где је $N = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$, јер је $\lambda(N) = [4, 6, 20, 6, 10, 12, 30, 60] = 60$. Поређења ради, $\varphi(N) = 2^{13} \cdot 3^5 \cdot 5^4 = 1\ 244\ 160\ 000$.

2.2 Поредак по модулу

Ојлерова, Мала Фермаова и Кармајкова теорема важе за сваки цео број a који је узајамно прост са датим модулом n. У циљу испитивања понашања степена датог броја a по датом модулу n, уводимо појам поретка по модулу.

Дефиниција 2.2 За природан број $n > 1$ и цео број a узајамно прост са n, **поредан броја a по модулу** n је најмањи природан број δ за који важи
$a^\delta \equiv 1 \pmod{n}$, односно,

$$\delta_n(a) = min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{n}\}.$$

На пример, $\delta_{11}(3) = 5$, јер је $3^5 \equiv 1 \pmod{11}$ и $3^i \not\equiv 1 \pmod{11}$ за $1 \leqslant i \leqslant 4$.

Пример 2.2 У табели испод дат је поредак броја a по модулу 11, односно 13.

a	(mod 11)	(mod 13)	a	(mod 11)	(mod 13)
1	1	1	7	10	12
2	10	12	8	10	4
3	5	3	9	5	3
4	5	6	10	2	6
5	5	4	11		12
6	10	12	12		2

Теорема 2.2 *Нека је n природан број већи од 1 и a цео број узајамно прост са n. Тада, за $m \in \mathbb{N}_0$, важи следећа еквиваленција:*

$$a^m \equiv 1 \pmod{n} \iff \delta_n(a) \mid m.$$

Доказ: Ако $\delta_n(a) \mid m$, онда је $m = q \cdot \delta_n(a)$ за неки цео број q. Дакле,

$$a^m = \left(a^{\delta_n(a)}\right)^q \equiv 1 \pmod{n}.$$

Обрнуто, нека је $m = (\delta_n(a))q + r,\ 0 \leqslant r < \delta_n(a),\ q \in \mathbb{Z}$. Приметимо следеће:

$$a^{(\delta_n(a))q+r} = a^m \equiv 1 \pmod{n}$$

$$\implies a^{(\delta_n(a))q} a^r \equiv 1 \pmod{n}$$

$$\implies a^r \equiv 1 \pmod{n}.$$

Како је $r < \delta_n(a)$, а према Дефиницији 2.2 $\delta_n(a)$ је најмањи природан степен броја a који је конгруентан са 1 по модулу n, следи да r није природан број. Дакле, $r = 0$, тј. $\delta_n(a) \mid m$. Овим смо доказали дату еквиваленцију.

□

Теорема 2.3 *Нека је n природан број већи од 1 и a цео број узајамно прост са n. Поредак $\delta_n(a)$ броја a по модулу n дели број $\varphi(n)$. Низ $1, a, a^2, ...$ је периодичан по модулу n са минималним периодом $\delta = \delta_n(a)$.*

Доказ: Из Ојлерове теореме имамо $a^{\varphi(n)} \equiv 1 \pmod{n}$. Коришћењем претходне теореме за $m = \varphi(n)$, доказујемо први део тврђења, тј. $\delta_n(a) \mid \varphi(n)$.

Периодичност можемо једноставно показати. Наиме, важи:

$$a^{k+\delta} = a^k a^\delta \equiv a^k \cdot 1 = a^k \pmod{n}.$$

□

Напомена 2.2 $1, a, a^2, ..., a^{\delta-1}$ су међусобно различити по модулу n.

Пример 2.3 Посматрајмо остатке бројева $1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, ...$ при дељењу са 7. Остаци су редом $1, 2, 4, 1, 2, 4, 1, 2, 4, ...$ - примећујемо да се низ $1, 2, 4$ периодично понавља, са периодом 3, и да се не појављују остаци $0, 3, 5, 6$. Међутим, ако уместо степена броја 2 посматрамо степене броја 3 при дељењу са 7, добијамо редом остатке $3, 2, 6, 4, 5, 1$. Овога пута, остаци се понављају са периодом 6 и сви остаци по модулу 7 осим нуле су ту. Примећујемо да је $\delta_7(2) = 3$ и $\delta_7(3) = 6$.

Следеће једноставно помоћно тврђење је веома важно.

Теорема 2.4 *Нека је a цео број и m, n природни бројеви. Тада важи:*

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Доказ: Означимо $d = (a^m - 1, a^n - 1)$. Како $a^{(m,n)} - 1$ дели бројеве $a^m - 1$ и $a^n - 1$ (нпр. ако је $m = k(m,n)$, онда је $a^m - 1 = (a^{(m,n)} - 1)(a^{(k-1)(m,n)} + \cdots + a^{(m,n)} + 1)$), број d је дељив са $a^{(m,n)} - 1$.

С друге стране, познато је да постоје природни бројеви x, y такви да је $(m,n) = mx - ny$, одакле следи $1 \equiv a^{mx} \equiv a^{ny} \cdot a^{(m,n)} \equiv a^{(m,n)} \pmod{d}$. Дакле, d дели $a^{(m,n)} - 1$, што повлачи $d = a^{(m,n)} - 1$.

□

Последица 2.1 *Нека су a и b узајамно прости цели бројеви и m, n природни бројеви. Тада важи:*

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

Доказ: Означимо $d = (a^m - b^m, a^n - b^n)$. Очигледно $a^{(m,n)} - b^{(m,n)} \mid d$.

С друге стране, ако је $c \in \mathbb{Z}$ такво да је $bc \equiv 1 \pmod{d}$, онда d дели $(ac)^m - 1$ и $(ac)^n - 1$. Дакле, $d \mid (ac)^{(m,n)} - 1$, што множењем са $b^{(m,n)}$ даје $d \mid a^{(m,n)} - b^{(m,n)}$.

□

У Примеру 2.3 смо видели да је $2^n - 1$ дељиво са 7 за $3 \mid n$, тј. $\delta_7(2) = 3$. Занимаће нас и за које n је $2^n - 1$ дељиво неким већим степеном седмице.

Задатак 2.2. Наћи све $n \in \mathbb{N}$ за које је $2^n - 1$ дељиво са 49.

Решење: Јасно је да је такво n дељиво са 3. Означимо $n = 3m,\ m \in \mathbb{N}$. Тада је $2^n = 2^{3m} = 8^m = (1+7)^m$, што се по биномној формули развија као

$$(1+7)^m = 1 + \binom{m}{1}7 + \binom{m}{2}7^2 + \cdots + \binom{m}{m-1}7^{m-1} + \binom{m}{m}7^m.$$

Сви сабирци осим прва два су дељиви са 7^2. Према томе, $2^n \equiv 1 + 7m \pmod{7^2}$. Закључујемо да је $2^n \equiv 1 \pmod{7^2}$ ако и само ако је m дељиво са 7, тј. ако и само ако $21 \mid n$. Другим речима, $\delta_{49}(2) = 21$. △

Напомена 2.3 Аналоган начин размишљања можемо применити и у општем случају.

Теорема 2.5 *Нека је $p > 2$ прост број, $a \neq 1$ цео и n природан број. Ако $p^k \| a - 1$ и $p^l \| n$, за $k \in \mathbb{N},\ l \in \mathbb{N}_0$, онда $p^{k+l} \| a^n - 1$.*

Доказ: Имамо $a = p^k B + 1$ за неки цео број B који није дељив са p. Тада је по биномној формули

$$a^n - 1 = \left(1 + p^k B\right)^n - 1 = np^k B + \binom{n}{2} p^{2k} B^2 + \cdots + p^{nk} B^n. \tag{2.1}$$

Тврђење доказујемо индукцијом по l. За $l = 0$ и $l = 1$, очигледно су сви сабирци на десној страни једнакости (2.1) осим првог дељиви са p^{k+l+1}, док је први тачно дељив са p^{k+l}, одакле следи $p^{k+l} \| a^n - 1$.

Нека је $l = t > 1$. На основу случаја $l = 1$ важи $p^{k+1} \| a^p - 1$. Пошто $p^{t-1} \| N$, где је $N = n/p$, по индуктивној претпоставци за $l = t - 1$ примењеној на $A = a^p$ и N имамо $p^{(k+1)+(t-1)} \| A^N - 1$, тј. $p^{k+t} \| a^n - 1$, чиме смо доказали индукцијски корак.

□

Последица 2.2 *Нека је $p > 2$ прост број, а цео број и $\delta = \delta_p(a)$ поредак броја a по модулу p. Тада, за $k \in \mathbb{N}$, $l \in \mathbb{N}_0$, из $p^k \| a^\delta - 1$ следи $\delta_{p^{k+l}}(a) = p^l \delta$.*

Доказ: Следи из Теореме 2.5 примењене на a^δ.

□

За $p = 2$ Теорема 2.5 није тачна: на пример, $2 \| 3 - 1$, али $2^3 | 3^2 - 1$. Наиме, у овом случају немамо безусловну гаранцију да p^{k+l+1} дели други сабирак у (2.1) - ако је $k = 1$, онда $p^{l-1} \| \binom{n}{2}$ и одатле $p^{k+l} \| \binom{n}{2} p^{2k} B^2$. Зато Теорема 2.5 за $p = 2$ важи у мало измењеном облику, уз практично исти доказ.

Теорема 2.6 *Нека је a ($|a| > 1$) непаран цео број, $k, l \in \mathbb{N}_0$ и нека $2^k \| a^2 - 1$. Тада, $2^{k+l} | a^n - 1$ ако и само ако $2^{l+1} | n$.* □

Претходне две теореме су специјалан случај "Леме о подизању експонента", о којој ће више речи бити у наредном поглављу. На овом месту их наводимо из разлога што ћемо их користити у доказима појединих теорема у наставку овог поглавља.

2.3 Примитивни корен

Видели смо да поредак $\delta_n(a)$ дели број $\varphi(n)$. Можемо ли за дато n одабрати a тако да је поредак $\delta_n(a)$ тачно једнако $\varphi(n)$? У Примеру 2.3 можемо уочити следеће: $\varphi(7) = 6 = \delta_7(3)$. Међутим, да ли можемо пронаћи такво a за било које n?

Дефиниција 2.3 Нека је a цео број, n природан број већи од 1 и $(a, n) = 1$. Тада је број a *примитивни корен* по модулу n ако је $\delta_n(a) = \varphi(n)$.

Пример 2.4 Знамо да је $\varphi(11) = 10$ и $\varphi(13) = 12$. Испоставља се да је $a = 2$ примитивни корен и по модулу 11 и по модулу 13. Погледајмо следећу таблицу.

2^n	(mod 11)	(mod 13)
2^1	2	2
2^2	4	4
2^3	8	8
2^4	5	3
2^5	10	6
2^6	9	12
2^7	7	11
2^8	3	9
2^9	6	5
2^{10}	1	10
2^{11}		7
2^{12}		1

Приметимо да је $2^5 \equiv 10 \equiv -1 \pmod{11}$ и $2^6 \equiv 12 \equiv -1 \pmod{13}$. Квадрирањем добијамо $2^{10} \equiv 1 \pmod{11}$ и $2^{12} \equiv 1 \pmod{13}$. Такође можемо приметити да је управо $\delta_{11}(2) = 10$ и $\delta_{13}(2) = 12$, што нас заиста уверава да је $a = 2$ примитивни корен по модулима 11 и 13.

Теорема 2.7 *Нека је a примитивни корен по модулу n. Тада бројеви*

$$1 = a^0, a^1, a^2, \ldots, a^{\varphi(n)-1}$$

образују сведени систем остатака по модулу n.

Доказ: Довољно је доказати да међу бројевима

$$a^0, a^1, a^2, \ldots, a^{\varphi(n)-1}$$

не постоје два која су конгруентна по модулу n. Претпоставимо супротно, да постоје i и j такви да је

$$a^i \equiv a^j \pmod{n}, \quad 0 \leqslant i < j \leqslant \varphi(n) - 1.$$

Тада је

$$a^{j-i} \equiv 1 \pmod{n}, \quad 0 < j - i \leqslant \varphi(n) - 1$$

што је супротно претпоставци да је a примитивни корен по модулу n.

□

Последица 2.3 *Нека је p прост број и a примитивни корен по модулу p. Тада бројеви*

$$1, a, a^2, \ldots, a^{p-2}$$

образују сведени систем остатака по модулу p.

Ово се веома лепо може видети у Примеру 2.4.
Провером налазимо да се примитивни корен може наћи за $n = 2, 3, 5, 7, 11, 13, 17, ...$ - на пример, $a = 1, 2, 2, 3, 2, 2, 3, ...$ редом. Испоставља се да примитивни корен постоји по сваком простом модулу. Да бисмо ово показали, подсетићемо се једног основног тврђења о полиномима.

Тврђење 2.1 *Полином степена d са коефицијентима у пољу $\mathbb{F}$ има највише d нула у пољу $\mathbb{F}$.*

На пример, $\mathbb{F}$ може да буде поље реалних или комплексних бројева. Међутим, нас овде занима $\mathbb{Z}_p$ - поље остатака по модулу простог броја p. У том пољу, Тврђење 2.1 нам заправо каже следеће:

Тврђење 2.2 *Нека је p прост број и $P(x)$ полином степена d са целим коефицијентима, при чему водећи коефицијент није дељив са p. Тада једначина $P(x) \equiv 0 \pmod{p}$ има највише d решења по модулу p.*

Лема 2.1 *Нека је d природан број и p прост број за који $d \mid p-1$. Тада је број решења конгруенције $x^d \equiv 1 \pmod{p}$ једнак је d.*

Доказ: Полином $x^d - 1$ има највише d нула по модулу p. С друге стране, полином $\frac{x^{p-1}-1}{x^d-1}$ је степена $p-1-d$, па има највише $p-d$ нула по модулу p. Како полином $x^{p-1} - 1$ има тачно $p-1$ нула $\pmod{p}$, следи тврђење.

□

Лема 2.2 (Гаусова лема) *За сваки природан број n важи*

$$\sum_{d|n} \varphi(d) = n.$$

Доказ: Тврдимо да је, за свако d $(d \mid n)$, број елемената $x \in \{1, 2, ..., n\}$, за које је $(x, n) = \frac{n}{d}$ једнак $\varphi(d)$. Заиста, $(x, n) = \frac{n}{d}$ је еквивалентно са $x = \frac{n}{d} \cdot k$, где је k $(1 \leqslant k \leqslant d)$ цео и $(k, d) = 1$, а оваквих бројева k има тачно $\varphi(d)$.
Следи да је сума $\varphi(d)$ по свим $d \mid n$ једнака броју свих елемената $x \in \{1, 2, ..., n\}$, а то је n.

□

Пример 2.5

$$\sum_{d|12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6)$$
$$= 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Теорема 2.8 *За сваки прост број p постоји примитиван корен по модулу p.*

Доказ: Показујемо индукцијом по природним делиоцима d броја $p-1$ да постоји тачно $\varphi(d)$ елемената из $\mathbb{Z}_p$ поретка d.

Ово је тривијално за $d = 1$.

Претпоставимо да је тачно за све делиоце броја $p-1$ мање од d. На основу Леме 2.1 постоји тачно d елемената $\mathbb{Z}_p$ чији поредак дели d. По индукцијској претпоставци, међу тих d елемената тачно $\varphi(e)$ има поредак e, где је e ма који делилац d мањи од d. Преосталих $d - \sum_{d>e|d} \varphi(e)$ елемената имају поредак d, а по Леми 2.2 је $d - \sum_{d>e|d} \varphi(e) = \varphi(d)$, што завршава индукцију.

Специјално, има $\varphi(p-1)$ елемената поретка $p-1$, тј. примитивних корена.

□

Последица 2.3 *Ако је $a^n - 1$ дељиво простим бројем p за свако a, $(a,p) = 1$, $n \in \mathbb{N}_0$, $a \in \mathbb{Z}$, онда је n дељиво са $p-1$.*

Доказ: Довољно је убацити $a = g$, где је g примитивни корен по модулу p.

□

Постојање примитивног корена g по простом модулу p значи да је мултипликативна група $\mathbb{Z}_p^*$ циклична, генерисана елементом g. То је и разлог што примитивни корен често означавамо словом g.

Примећујемо да, осим по простим модулима, примитивни корен постоји и за модуле $n = 4, 6, 9, 10$ који нису прости - нпр. $g = 3, 5, 2, 3$ редом.

Теорема 2.9 *Ако је p непаран прост број и α природан, постоји примитивни корен по модулима p^α и $2p^\alpha$.*

Доказ: Нека је g примитивни корен по модулу p. Покажимо прво да постоји примитивни корен по модулу p^2.

Тврдимо да је бар један од бројева $g, g+p$ примитивни корен по модулу p^2 - тј. да има поредак $\varphi(p^2) = p(p-1)$ по модулу p^2. Поретци ових бројева по модулу p су једнаки $p-1$, па су њихови поретци по модулу p^2 дељиви са $p-1$ - дакле, једнаки су $p-1$ или $p(p-1)$. Ако ни g ни $g+p$ нису примитивни корени по модулу p^2, имамо $g^{p-1} \equiv (g+p)^{p-1} \equiv 1 \pmod{p^2}$. Међутим, биномни развој нам даје $(g+p)^{p-1} - g^{p-1} \equiv (p-1)pg^{p-2} \not\equiv 0 \pmod{p^2}$, контрадикција.

Нека је сада g примитивни корен по модулу p^2. Покажимо да је то такође

примитивни корен по модулу p^α.
Како p тачно дели $g^{p-1}-1$, по Теореми 2.5 имамо да је g^m-1 дељиво са p^α ако и само ако је m дељиво са $p^{\alpha-1}(p-1)$, тј. поредак g по модулу p^α је једнак $\varphi(p^\alpha)$, што смо и тврдили.

Најзад, како је $\varphi(2p^\alpha)=\varphi(p^\alpha)$, сваки непаран примитивни корен по модулу p^α је уједно и примитивни корен по модулу $2p^\alpha$. Дакле, g или $g+p^\alpha$ задовољава услове.

□

С друге стране, за неке модуле попут $n=8,12,15$ не постоји примитивни корен, јер по Кармајкловој теореми ниједан број нема ред већи од $2,2,4$ редом по датим модулима.

Ако постоји број a чији је поредак по модулу n једнак $\varphi(n)$, из Кармајклове теореме следи да мора бити $\lambda(n)=\varphi(n)$. То одмах искључује степене двојке веће од 2^2. Шта више, искључује и све бројеве n који су једнаки производу два узајамно проста броја n_1,n_2 већа од 2, јер су $\lambda(n_1)$ и $\lambda(n_2)$ парни по дефиницији, па је $\lambda(n)=[\lambda(n_1),\lambda(n_2)]\leqslant\frac{1}{2}\lambda(n_1)\lambda(n_2)\leqslant\frac{1}{2}\varphi(n_1)\varphi(n_2)=\frac{1}{2}\varphi(n)<\varphi(n)$. Тако добијамо:

Теорема 2.10 *Примитивни корен по модулу n ($n\in\mathbb{N}$) постоји ако и само ако $n\in\{2,4\}$, $n=p^\alpha$ или $n=2p^\alpha$ за неки непаран прост број p и природан број α.*

Доказ: Свако $n\in\mathbb{N}$ које није у неком од наведених облика је или степен двојке већи од 4 или производ два узајамно проста броја већа од 2, па тврђење следи из претходног разматрања.

□

Теорема 2.11 *Ако је a^m-1, $m\in\mathbb{N}_0$, дељиво природним бројем n за сваки цео број $a,(a,n)=1$, онда је експонент m дељив са $\lambda(n)$ (где је λ Кармајклова функција).*

Доказ: Нека је $n=2^\alpha p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$, где су p_i различити непарни прости бројеви и α_i природни, $1\leqslant i\leqslant r$. По Теореми 2.9, за свако i постоји g_i чији је поредак по модулу $p_i^{\alpha_i}$ једнак $\varphi(p_i^{\alpha_i})$. Примитивни корен по модулу 2^α не постоји за $\alpha\geqslant 3$. Уместо тога, важи да је поредак нпр. броја 5 по модулу 2^α једнак $2^{\alpha-2}$ - ово следи директно из Теореме 2.10.

По Кинеској теореми о остацима постоји a такво да је $a\equiv 5\pmod{2^\alpha}$ и, за све i, $a\equiv g_i\pmod{p_i^{\alpha_i}}$. Тада је a^m-1 дељиво са n ако и само ако је дељиво са 2^α и са $p_i^{\alpha_i}$ за све i, а то важи ако и само ако је m дељиво са $\lambda(2^\alpha)$ и $\lambda(p_i^{\alpha_i})$, што је еквивалентно са $\lambda(n)\mid m$.

□

Тврђење 2.3 *Нека је p прост број. Сваки примитивни корен по модулу p^α, $\alpha\in\mathbb{N}$, је примитивни корен и по модулу p.*

Доказ: Нека је a примитивни корен по модулу p^α. Претпоставимо супротно, a није примитивни корен по модулу p. Тада постоји природан број t, $1 \leqslant t < p-1$ и важи $a^t \equiv 1 \pmod{p}$, тј. $a^t = 1 + pq$, за неки цео број q. Према биномној формули имамо да је

$$\begin{aligned} a^{tp^{\alpha-1}} &= (1+pq)^{p^{\alpha-1}} \\ &= 1 + p^{\alpha-1}pq + \binom{p^{\alpha-1}}{2}(pq)^2 + \cdots \\ &\equiv 1 \pmod{p^\alpha}, \end{aligned}$$

при чему је $tp^{\alpha-1} < p^{\alpha-1}(p-1) = \varphi(p^\alpha)$, па број a није примитивни корен по модулу p^α. Контрадикција.

□

2.4 Задаци

2.1. Колико позитивних целих бројева дељивих са 1001 можемо изразити у облику $10^i - 10^j$, где су i и j цели бројеви за које важи $0 \leqslant j < i \leqslant 99$?

Решење: Кренимо са разматрањем чињенице која је задата:

$$1001 \mid 10^i - 10^j \Longrightarrow 1001 \mid 10^j \left(10^{i-j} - 1\right).$$

Како $1001 \nmid 10^j$, онда следи да $1001 \mid 10^{i-j} - 1$. Ово заправо значи да је $10^{i-j} \equiv 1 \pmod{1001}$.

Потражимо сада поредак броја 10 по модулу 1001. Приметимо да је $10^3 \equiv -1 \pmod{1001}$ и $10^1, 10^2, 10^4, 10^5 \not\equiv 1 \pmod{1001}$. Дакле, $\delta_{1001}(10) = 6$. Применом Теореме 2.2 долазимо до закључка да $6 \mid i-j$. Ако израчунамо колико има уређених парова (i,j) који задовољавају овај, као и услов у задатку, доћи ћемо до траженог решења. Овим смо задатак свели на комбинаторни проблем.

Из чињенице да $6 \mid i-j$ можемо закључити да i и j дају исти остатак приликом дељења са 6, тј. $i \equiv j \equiv k \pmod{6}$, $k \in \{0,1,2,3,4,5\}$.

Размотримо случај $i \equiv j \equiv 0 \pmod{6}$. Из ове конгруенције и услова у задатку, закључујемо да $i, j \in \{0, 6, 12, 18, \ldots, 90, 96\}$, што је укупно 17 могућности за i, j. Међутим, i и j морају бити различити, па одабиром две различите вредности од датих 17, долазимо до укупног броја могућности у овом случају, што је $\binom{17}{2}$. Наравно, посматрамо уређене парове (i,j) такве да је $i > j$.

У случају $i \equiv j \equiv 1 \pmod{6}$, $i \equiv j \equiv 2 \pmod{6}$ и $i \equiv j \equiv 3 \pmod{6}$, такође имамо 17 могућности за i, j од којих бирамо две различите. Дакле, и у овим случајима имамо $\binom{17}{2}$ могућности.

У случају $i \equiv j \equiv 4 \pmod{6}$ и $i \equiv j \equiv 5 \pmod{6}$, имамо укупно 16 могућности за i, j које долазе у обзир. Поново, бирањем две различите вредности, долазимо

до укупног броја парова (i, j), што је $\binom{16}{2}$.

Претходно разматрање нас доводи до решења задатка. Укупан број тражених бројева је

$$4 \cdot \binom{17}{2} + 2 \cdot \binom{16}{2} = 4 \cdot \frac{17 \cdot 16}{2 \cdot 1} + 2 \cdot \frac{16 \cdot 15}{2 \cdot 1} = 4 \cdot 136 + 2 \cdot 120 = 544 + 240 = 784. \quad \triangle$$

2.2. Доказати да је, за свако $n \in \mathbb{N}$, број $2^{3^n} + 1$ дељив са 3^{n+1}, а није са 3^{n+2}.

Решење: Овај задатак бисмо могли решити коришћењем принципа математичке индукције по n. Међутим, морали бисмо да докажемо оба тврђења на овај начин, што би од нас захтевало доста писања. Ученици могу урадити задатак на овај начин, за вежбу. Ми ћемо, ипак, урадити на другачији начин, коришћењем Теореме 2.5.

Задатак нам је, дакле, да покажемо да $3^{n+1} \| 2^{3^n} + 1$. Како је $2^{3^n} + 1 = -(-2^{3^n} - 1)$, покушајмо да покажемо да $3^{n+1} \| -2^{3^n} - 1$. Знамо да је 3^n непаран број, па важи $-2^{3^n} - 1 = (-2)^{3^n} - 1$.

Приметимо да важи следеће: $3^1 \| (-2) - 1$ и $3^n \| 3^n$. Ако узмемо да је $p = 3$ и $a = -2$, применом Теореме 2.5, добијамо $3^{n+1} \| (-2)^{3^n} - 1$, што смо и желели да покажемо. $\triangle$

2.3. Доказати да се бројеви $1, 2, 3, ..., 100$ могу распоредити у поља таблице 10×10 тако да су у сваком квадрату 2×2 производи по два броја по дијагонали једнаки по модулу 101.

Решење: Оно што одмах можемо приметити јесте да је 101 прост број и да дати бројеви $1, 2, \ldots, 99, 100$ образују сведени систем остатака по модулу 101. Како је 101 прост број, Теорема 2.8 нам гарантује постојање примитивног корена по модулу 101. Обележимо тај примитивни корен са g. Сада, коришћењем Последице 2.3 долазимо до закључка да бројеви

$$g^0, g^1, g^2, \ldots, g^{98}, g^{99}$$

такође образују сведени систем остатака по модулу 101, тј. међу остацима ових бројева по модулу 101 су сви бројеви из скупа $\{1, 2, \ldots, 99, 100\}$. С обзиром на то да ћемо разматрати производе бројева по модулу 101, испоставиће се као веома корисно да у наставку посматрамо овај нови сведени систем остатака.

Приметимо да сваки од тих бројева можемо записати у облику g^{10i+j}, $i, j \in \{0, 1, 2 \ldots, 9\}$. Нумеришимо сада поља дате таблице 10×10 индексима врста и колона на следећи начин:

$$\begin{array}{ccccc} 00 & 01 & 02 & \dots & 09 \\ 10 & 11 & 12 & \dots & 19 \\ 20 & 21 & 22 & \dots & 29 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 90 & 91 & 92 & \dots & 99 \end{array}$$

На који начин сада можемо повезати нумерацију поља ij и бројева g^{10i+j} тако да буде испуњен услов задатка? Посматрањем обележја сваког поља таблице као двоцифрен број, можемо уочити да је збир бројева на главној дијагонали увек једнак збиру бројева на споредној дијагонали у сваком квадрату 2×2. Ако на поља ij распоредимо бројеве g^{10i+j}, посматрањем квадрата одређеног врстама i и $i+1$ и колонама j и $j+1$, долазимо до следећег закључка. Производ бројева на главној дијагонали је

$$g^{10i+j} \cdot g^{10(i+1)+j+1} = g^{20i+2j+11}.$$

Производ бројева на споредној дијагонали је

$$g^{10i+j+1} \cdot g^{10(i+1)+j} = g^{20i+2j+11}.$$

Ако бисмо посматрали бројеве g^{10i+j}, оваквим распоређивањем бисмо решили задатак. Међутим, како су нама дати бројеви $1, 2, 3, \dots, 100$, до коначног решења долазимо распоређивањем у поље ij остатка који добијамо при дељењу броја g^{10i+j} са 101. $\triangle$

2.4. Нека је p непаран прост број и нека су q и r прости бројеви такви да $p \mid q^r + 1$. Доказати да или $2r \mid p - 1$ или $p \mid q^2 - 1$.

Решење: Задатак ћемо решити прилично праволинијски, уз коришћење почетне идеје која ће бити веома корисна у задацима у којима се као делилац збира бројева појављује неки непаран прост број.

Дато је да $p \mid q^r + 1$, где је p прост број већи или једнак од 3. Ово значи да $p \nmid q^r + 1 - 2$ тј. $p \nmid q^r - 1$. Такође, можемо закључити да $p \mid (q^r + 1)(q^r - 1)$, тј. $p \mid q^{2r} - 1$. Сада, применом Теореме 2.2, закључујемо да

$$\delta_p(q) \mid 2r,$$

где је $\delta_p(q)$ поредак броја q по модулу p. Како $p \nmid q^r - 1$, закључујемо да $\delta_p(q) \neq r$. Дакле, $\delta_p(q) \in \{1, 2, 2r\}$.

У случају $\delta_p(q) = 1$ следи $q \equiv 1 \pmod{p}$, тј. $p \mid q - 1$, а самим тим и $p \mid q^2 - 1$.

Слично, у случају $\delta_p(q) = 2$ видимо да $q^2 \equiv 1 \pmod{p}$, тј. $p \mid q^2 - 1$.

У случају $\delta_p(q) = 2r$, применом Теореме 2.3, добијамо $2r \mid \varphi(p)$, тј. $2r \mid p - 1$.

Овим смо тврђење доказали. $\triangle$

2.5. Нека су a и b узајамно прости цели бројеви. Доказати да је било који непаран делилац броја $a^{2^n}+b^{2^n}$ облика $2^{n+1}m+1$.

Решење: Задатак заправо каже да ако је k непаран делилац броја $a^{2^n}+b^{2^n}$, онда је $k \equiv 1 \pmod{2^{n+1}}$. Дакле, ако покажемо да је сваки прост делилац броја $a^{2^n}+b^{2^n}$ конгруентан са 1 $(\mathrm{mod}\ 2^{n+1})$, множењем простих делиоца добићемо да су сви делиоци броја $a^{2^n}+b^{2^n}$ конгруентни са 1 $(\mathrm{mod}\ 2^{n+1})$.

Нека је q неки непаран прост делилац броја $a^{2^n}+b^{2^n}$. Како су a и b узајамно прости, мора да важи и $(q,a)=1$ и $(q,b)=1$. У супротном q не би делио $a^{2^n}+b^{2^n}$.

Како $q \mid a^{2^n}+b^{2^n}$, онда $q \mid a^{2^n}\left(1+(b\cdot a^{-1})^{2^n}\right)$. Из $(q,a)=1$ следи да $q \nmid a^{2^n}$, а ово повлачи $q \mid (b\cdot a^{-1})^{2^n}+1$. Како је q непаран прост број, $q \nmid (b\cdot a^{-1})^{2^n}-1$, али зато

$$q \mid (b\cdot a^{-1})^{2^{n+1}}-1.$$

Применом Теореме 2.2 закључујемо да $\delta_q(b\cdot a^{-1}) \mid 2^{n+1}$, где је $\delta_q(b\cdot a^{-1})$ поредак броја $b\cdot a^{-1}$ по модулу q, а из претходног разматрања закључујемо да $\delta_q(b\cdot a^{-1}) \nmid 2^n$. Дакле, $\delta_q(b\cdot a^{-1})=2^{n+1}$.

Применом Теореме 2.3 закључујемо да $\delta_q(b\cdot a^{-1}) \mid \varphi(q)$, тј. $2^{n+1} \mid q-1$. Дакле, $q \equiv 1 \pmod{2^{n+1}}$, што смо и желели да покажемо. $\triangle$

2.6. Наћи све парове простих бројева p,q такве да $pq \mid (5^p-2^p)(5^q-2^q)$.

Решење: Како су 5^p-2^p и 5^q-2^q непарни бројеви, онда је и њихов производ непаран број, што значи да су p и q непарни бројеви. Такође, приметимо да важи или $p \mid 5^p-2^p$ или $p \mid 5^q-2^q$.

Претпоставимо да $p \mid 5^p-2^p$. Применом Мале Фермаове теореме долазимо до следећег закључка:

$$5^p-2^p \equiv 3 \equiv 0 \pmod{p} \implies p=3.$$

Такође, мора да важи или $q \mid (5^3-2^3)=117$ или $q \mid 5^q-2^q$. Поново, применом Мале Фермаове теореме, из $q \mid 5^q-2^q$ добијамо $q=3$, док из $q \mid 117$ добијамо $q=13$. Како уочавамо симетрију између p и q, долазимо до следећих решења:

$$(p,q) \in \{(3,3),(3,13),(13,3)\}.$$

Посматрајмо сада случај $p,q \neq 3$. Тада морамо имати $p \mid 5^q-2^q$ и $q \mid 5^p-2^p$. Претпоставимо да је $p \neq 5$. Применом Мале Фермаове теореме имамо да је $5^{p-1}-2^{p-1} \equiv 0 \pmod{p}$, тј. $p \mid 5^{p-1}-2^{p-1}$. Ово значи да $p \mid \left(5^q-2^q, 5^{p-1}-2^{p-1}\right)$, па применом Последице 2.1, закључујемо да $p \mid 5^{(q,p-1)}-2^{(q,p-1)}$. Како су q и $p-1$ узајамно прости, добијамо да $p \mid 5^1-2^1$, тј. $p \mid 3$, што је контрадикција.
У случају $p=5$ одмах се може проверити да немамо ниједно решење.

Као и у првом делу задатка, дискусија по q није потребна, јер нас на аналоган начин води у контрадикцију.

Дакле, једина решења су

$$(p,q) \in \{(3,3),(3,13),(13,3)\}. \quad \triangle$$

2.7. Наћи све природне бројеве $m,n \geqslant 2$ такве да је

$$\frac{1+m^{3^n}+m^{2\cdot 3^n}}{n}$$

цео број.

Решење: Нека m и n задовољавају услове задатка. Шта можемо одмах да закључимо о овим бројевима? Приметимо да је $1+m^{3^n}+m^{2\cdot 3^n}$ непаран број. Из тог разлога n мора бити непаран. Такође, m и n морају бити узајамно прости бројеви. У супротном, $1+m^{3^n}+m^{2\cdot 3^n}$ не би било дељиво са n.

Нека је $n=3$. Тада је $m \equiv 1 \pmod 3$, јер бисмо у случају $m \equiv -1 \pmod 3$ имали

$$1+m^{3^n}+m^{2\cdot 3^n} \equiv 1-1+1 \equiv 1 \pmod 3.$$

Нека је сада $n>3$. Тада важи $m^{3^n} \not\equiv 1 \pmod n$, јер би у супротном следило $1+m^{3^n}+m^{2\cdot 3^n} \equiv 3 \pmod n$, тј. $n \mid 3$. Пошто је

$$1+m^{3^n}+m^{2\cdot 3^n} = \frac{m^{3^{n+1}}-1}{m^{3^n}-1},$$

онда је $m^{3^{n+1}} \equiv 1 \pmod n$. Применом Теореме 2.2 закључујемо да $\delta_n(m) \mid 3^{n+1}$, где је $\delta_n(m)$ поредак броја m по модулу n. Како из претходног разматрања видимо да $\delta_n(m) \nmid 3^n$, онда долазимо до закључка да је $\delta_n(m) = 3^{n+1}$. Из Теореме 2.3 закључујемо да $\delta_n(m) \mid \varphi(n)$, а како је $\varphi(n) \leqslant n-1$, то значи да је $3^{n+1} \leqslant n-1$, што је немогуће.

Дакле, тражени бројеви су $n=3$ и сви бројеви $m \geqslant 4$ такви да је $m \equiv 1 \pmod 3$. $\triangle$

2.8. Нека је m природан број. Доказати да ако $2^{m+1}+1$ дели $3^{2^m}+1$, онда је $2^{m+1}+1$ прост број.

Решење: Нека је $q = 2^{m+1}+1$. Тада из датог услова следи

$$3^{2^m} \equiv -1 \pmod q. \tag{2.2}$$

одакле следи да су 3 и q узајамно прости. Квадрирањем конгруенције (2.2) добијамо $3^{2^{m+1}} \equiv 1 \pmod q$, одакле следи да поредак броја 3 по модулу q дели број

$2^{m+1} = q-1$. Према томе, поредак броја 3 по модулу q је облика 2^r, за неки природан број $r \leqslant m+1$. Ако би било $r \leqslant m$, онда би из Теореме 2.2 важило $3^{2^m} \equiv 1 \pmod{q}$, што је контрадикција са (2.2). Дакле, $r = m+1$.

С друге стране, поредак броја 3 по модулу q је делилац броја $\varphi(q)$. Тако $2^{m+1} = q-1$ дели $\varphi(q)$. Како је $\varphi(q) \leqslant q-1$, долазимо до закључка да је $\varphi(q) = q-1$, што заиста значи да је $q = 2^{m+1}+1$ прост. $\triangle$

2.9. Нека је p прост број и $\alpha \geqslant 2$. Ако је a примитивни корен по модулу p и важи

$$a^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha},$$

доказати да је a примитивни корен по модулу p^α.

Решење: Нека је $\delta = \delta_{p^\alpha}(a)$ поредак броја a по модулу p^α. Тада је $a^\delta \equiv 1 \pmod{p^\alpha}$ и $\delta \mid \varphi(p^\alpha)$, тј. $\delta \mid p^{\alpha-1}(p-1)$.

Како је $a^\delta \equiv 1 \pmod{p}$ и a је примитивни корен по модулу p ($p-1$ је његов поредак по модулу p) имамо да $p-1 \mid \delta$, тј. $\delta = (p-1)q$, за неки цео број q. Ово значи да $(p-1)q \mid p^{\alpha-1}(p-1)$. Дакле, $q \mid p^{\alpha-1}$, тј. $q = p^\beta,\ 0 \leqslant \beta \leqslant \alpha-1$, па је

$$a^{p^\beta(p-1)} \equiv 1 \pmod{p},\ 0 \leqslant \beta \leqslant \alpha-1. \tag{2.3}$$

Ако би било $0 \leqslant \beta \leqslant \alpha-2$, степеновањем конгруенције (2.3) са $p^{\alpha-2-\beta}$, добили бисмо

$$a^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p},$$

супротно претпоставци задатка. Дакле, $\beta = \alpha-1$, па је

$$\delta = p^{\alpha-1}(p-1) = \varphi(p^\alpha). \quad \triangle$$

2.10. Наћи све парове (x, y) који задовољавају једначину $7^x + 2 = 3^y$, при чему су x и y ненегативни цели бројеви.

Решење: Приликом решавања дате једначине, прво ћемо проверити шта се дешава са малим вредностима за x и y, а затим ћемо за све остале вредности користити метод заснован на примени Теореме 2.2.

Нека су $x, y \leqslant 2$. Провером добијамо следећа решења за овај случај:

$$(x, y) \in \{(0,1), (1,2)\}.$$

Размотримо сада случај $x, y > 2$. Следећа идеја може бити веома корисна у једначинама овог типа. Умањимо за 9 обе стране почетне једнакости. На тај

начин добијамо $7^x - 7 = 3^y - 9$, тј. почетну једначину трансформишемо у следећи облик:

$$7\left(7^{x-1}-1\right) = 9\left(3^{y-2}-1\right). \tag{2.4}$$

Приметимо да је лева страна једнакости (2.4) дељива са 7, према томе, и десна страна мора бити дељива са 7. Како $7 \nmid 9$, онда мора да важи $7 \mid (3^{y-2}-1)$, тј. $3^{y-2} \equiv 1 \pmod 7$. Како је $\delta_7(3) = 6$, где је $\delta_7(3)$ поредак броја 3 по модулу 7, применом поменуте Теореме 2.2, добијамо $6 \mid y-2$, тј. $y-2 = 6k$, за неки цео број k. Враћањем у десну страну једнакости (2.4) добијамо:

$$9\left(3^{6k}-1\right) = 9\left(3^6-1\right)\left(3^{6(k-1)} + 3^{6(k-2)} + \cdots + 1\right).$$

Битна ствар коју овде треба да приметимо јесте да је $3^6 - 1$ дељиво са 13. Дакле, десну страну једнакости (2.4) можемо записати у облику $13 \cdot l$, за неки цео број l. Ово значи да је и лева страна једнакости (2.4) дељива са 13. Како 7 није дељиво са 13, онда $7^{x-1} - 1$ мора бити дељиво, тј. $7^{x-1} \equiv 1 \pmod{13}$. Провером добијамо да је $\delta_{13}(7) = 12$, где је $\delta_{13}(7)$ поредак броја 7 по модулу 13, што ће рећи да $12 \mid x-1$, тј. $x - 1 = 12m$, за неки цео број m. Враћањем у једнакост (2.4) лева страна постаје:

$$7\left(7^{12m}-1\right) = 7\left(7^{12}-1\right)\left(7^{12(m-1)} + \cdots + 1\right).$$

Сада треба приметити да је $7^{12} - 1$ дељиво са 19. Иако делује да је овај процес бесконачан, ипак није. Исти поступак ћемо поновити још два пута и доћи до коначног решења. Дакле, лева страна једнакости (2.4) је дељива са 19, па мора бити и десна. Закључујемо да је $3^{y-2} \equiv 1 \pmod{19}$, а како је $\delta_{19}(3) = 18$, где је $\delta_{19}(3)$ поредак броја 3 по модулу 19, следи $y - 2 = 18n,\ n \in \mathbb{Z}$. Сада, десна страна једнакости (2.4) постаје:

$$9\left(3^{18n}-1\right) = 9\left(3^{18}-1\right)\left(3^{18(n-1)} + \cdots + 1\right).$$

Како је $3^{18} - 1$ дељиво са 37, десна страна посматране једнакости је такође дељива овим бројем. Ова чињеница поново повлачи и дељивост леве стране са 37. Дакле, $7^{x-1} \equiv 1 \pmod{37}$. Како је $\delta_{37}(7) = 9$, где је $\delta_{37}(7)$ поредак броја 7 по модулу 37, добијамо $9 \mid x-1$, тј. $x - 1 = 9p,\ p \in \mathbb{Z}$. Лева страна једнакости сада постаје:

$$7\left(7^{9p}-1\right) = 7\left(7^9-1\right)\left(7^{9(p-1)} + \cdots + 1\right).$$

Можемо проверити да је $7^9 - 1$ дељиво са 27, што значи да је $7\left(7^{x-1}-1\right) \equiv 0 \pmod{27}$. Сада, посматрањем десне стране једнакости (2.4) и чињенице да је $y - 2 = 6k$, добијамо $9\left(3^{6k}-1\right) = 9\left((3^3)^{2k}-1\right) = 9\left(27^{2k}-1\right) \equiv -9 \pmod{27}$. Како смо добили да је лева страна једнакости $\equiv 0 \pmod{27}$, а десна страна $\equiv -9 \pmod{27}$,

дошли смо до контрадикције. Дакле, у случају $x, y > 2$ немамо решења, па су једина решења дате једначине

$$(x, y) \in \{(0, 1), (1, 2)\}. \quad \triangle$$

ГЛАВА 3

Експоненцијалне конгруенције

С обзиром на то да ћемо у наставку посматрати понашање степена простог броја p у разним ситуацијама, биће нам веома корисна следећа дефиниција.

Дефиниција 3.1 Нека је p прост број, $\alpha \in \mathbb{N}_0$ и $x \in \mathbb{Z} \setminus \{0\}$ тако да $p^\alpha \| x$. Тада можемо дефинисати функцију $v_p : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0,\ v_p(x) = \alpha$.

Пример 3.1 Знамо да је 3 највећи степен простог броја 3 који дели 54, тј. $3^3 \| 54$. Због тога имамо $v_3(54) = 3$.

Пример 3.2 Нека су p и q различити прости бројеви. Тада важи $v_p(p^\alpha q^\beta) = \alpha$ и $v_q(p^\alpha q^\beta) = \beta$.

Напомена 3.1 Функција v_p није дефинисана у 0, али је можемо додефинисати, да буде у складу са Дефиницијом 3.1, на следећи начин: $v_p(0) = \infty$, за све просте бројеве p.

Теорема 3.1 *Нека су x и y цели бројеви и p прост број. Тада важи:*

$$v_p(x \cdot y) = v_p(x) + v_p(y).$$

Доказ: Нека је $v_p(x) = e_1$ и $v_p(y) = e_2$. Тада је $x = p^{e_1} x_1$ и $y = p^{e_2} y_1$, где су x_1 и y_1 цели бројеви узајамно прости са p. Тада добијамо:

$$xy = p^{e_1+e_2} x_1 y_1 \Longrightarrow v_p(xy) = e_1 + e_2 = v_p(x) + v_p(y).$$

□

Пример 3.3 Израчунајмо $v_2(56 \cdot 96)$.

$$2^3 \| 56 \Rightarrow v_2(56) = 3 \text{ и } 2^5 \| 96 \Rightarrow v_2(96) = 5.$$

$$\implies v_2(56 \cdot 96) = v_2(56) + v_2(96) = 3 + 5 = 8.$$

Теорема 3.2 *Нека су x и y цели бројеви и p прост број. Тада важи:*

$$v_p(x) > v_p(y) \implies v_p(x+y) = v_p(y).$$

Доказ: Нека је $v_p(x) = e_1$ и $v_p(y) = e_2,\ e_1 > e_2$. Тада је $x = p^{e_1}x_1$ и $y = p^{e_2}y_1$, где су x_1 и y_1 цели бројеви узајамно прости са p. Уочимо следеће:

$$x + y = p^{e_1}x_1 + p^{e_2}y_1 = p^{e_2}(p^{e_1-e_2}x_1 + y_1).$$

Из $e_1 > e_2$ следи $e_1 \geqslant e_2 + 1$, тј $e_1 - e_2 \geqslant 1$. Зато можемо закључити следеће: $p^{e_1-e_2}x_1 + y_1 \equiv y_1 \pmod{p}$. Како су y_1 и p узајамно прости, онда важи $y_1 \not\equiv 0 \pmod{p}$, што значи да $p^{e_1-e_2}x_1 + y_1$ није дељиво са p. Дакле,

$$v_p(x+y) = v_p\left(p^{e_2}(p^{e_1-e_2}x_1 + y_1)\right) = e_2 = v_p(y).$$

□

Лема 3.1 *Нека је n природан и p прост број. Тада важи:*

$$\log_p n \geqslant v_p(n).$$

Доказ: Нека је $n = p^\alpha k,\ \alpha \in \mathbb{N}_0,\ k \in \mathbb{N}$ и $p \nmid k$. Тада је $v_p(n) = \alpha$ и важи следеће:

$$\log_p n = \log_p p^\alpha k = \log_p p^\alpha + \log_p k = \alpha + \log_p k \geqslant \alpha = v_p(n).$$

□

Теорема 3.3 (Лежандрова) *За све природне бројеве n и просте p имамо:*

$$v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor.$$

Доказ: Посматраћемо степене броја p који се садрже у $n!$.

- Број појављивања фактора p^1 у скупу $\{1, 2, ..., n\}$ једнак је $\lfloor \frac{n}{p} \rfloor$.
- Број појављивања фактора p^2 у скупу $\{1, 2, ..., n\}$ једнак је $\lfloor \frac{n}{p^2} \rfloor$. Све те бројеве смо већ рачунали једанпут приликом рачунања $\lfloor \frac{n}{p} \rfloor$, али пошто ово морамо да рачунамо 2 пута (јер је у питању p^2), онда додајемо $\lfloor \frac{n}{p^2} \rfloor$ једанпут.

Овај процес ћемо понављати док не дођемо до $i = k$, где је $p^k > n$. Приметимо да је $\lfloor \frac{n}{p^i} \rfloor = 0$ за $i \geqslant k$.

Понављањем претходног процеса онолико пута колико је потребно, добијамо жељени резултат $v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$.

□

Теорема 3.4 (Лежандрова) *За све природне бројеве n и просте p, имамо*

$$v_p(n!) = \frac{n - s_p(n)}{p-1}$$

где $s_p(n)$ представља збир цифара броја n у основи p.

Доказ: У основи p пишемо

$$n = \sum_{j=0}^{k} (a_j \cdot p^j),$$

где је $1 \leqslant a_k \leqslant p-1$ и $0 \leqslant a_j \leqslant p-1$ за $0 \leqslant j \leqslant k-1$.
Из Теореме 3.3 имамо следеће:

$$v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor = \sum_{i=1}^{\infty} \lfloor \frac{\sum_{j=0}^{k} a_j \cdot p^j}{p^i} \rfloor = \sum_{i=1}^{\infty} \lfloor \sum_{j=0}^{k} a_j \cdot p^{j-i} \rfloor$$

$$= \sum_{i=1}^{k} \lfloor \sum_{j=1}^{k} a_j \cdot p^{j-i} \rfloor = \sum_{j=1}^{k} a_j \left(p^{j-1} + p^{j-2} + \cdots + p + 1 \right)$$

$$\sum_{j=1}^{k} a_j \frac{p^j - 1}{p-1} = \frac{1}{p-1} \sum_{j=0}^{k} a_j (p^j - 1).$$

Сада ћемо оценити $\frac{n - s_p(n)}{p-1}$. Приметимо да је $s_p(n) = \sum_{j=0}^{k} a_j$, што повлачи следеће:

$$\frac{n - s_p(n)}{p-1} = \frac{1}{p-1} \left[\sum_{j=0}^{k} (a_j \cdot p^j) - \sum_{j=0}^{k} a_j \right]$$

$$= \frac{1}{p-1} \sum_{j=0}^{k} a_j (p^j - 1).$$

Дакле, $v_p(n!) = \frac{n - s_p(n)}{p-1}$, као што смо тврдили.

□

3.1 Лема о подизању експонента

Лему о подизању експонента изложићемо у два случаја - када је прост број p различит од 2, а затим и када је једнак 2. Пре него што пређемо на поменуту главну лему, изложићемо две важне и корисне леме.

Лема 3.2 *Нека су x, y цели бројеви, n природан и p прост број, такви да $(n,p) = 1,\ p \mid (x-y)$ и $p \nmid x, y$. Тада важи*

$$v_p(x^n - y^n) = v_p(x-y).$$

Доказ: Користићемо чињеницу да је

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}\cdot y + x^{n-3}\cdot y^2 + \cdots + y^{n-1}\right).$$

Ако покажемо да $p \nmid x^{n-1} + x^{n-2}\cdot y + x^{n-3}\cdot y^2 + \cdots + y^{n-1}$, завршили смо са доказом. Да бисмо ово показали, користићемо услов $p \mid (x-y)$. Према томе имамо $x - y \equiv 0 \pmod{p}$, тј. $x \equiv y \pmod{p}$. Користећи ову конгруенцију добијамо

$$\begin{aligned} & x^{n-1} + x^{n-2}\cdot y + x^{n-3}\cdot y^2 + \cdots + y^{n-1} \\ \equiv\ & x^{n-1} + x^{n-2}\cdot x + x^{n-3}\cdot x^2 + \cdots + x^{n-1} \\ =\ & nx^{n-1} \\ \not\equiv\ & 0 \pmod{p}. \end{aligned}$$

□

Лема 3.3 *Нека су x, y цели бројеви, n непаран природан и p прост број, такви да $(n,p) = 1,\ p \mid (x+y)$ и $p \nmid x, y$. Тада важи*

$$v_p(x^n + y^n) = v_p(x+y).$$

Доказ: Кренимо од следеће једнакости.

$$v_p(x^n + y^n) = v_p(x^n - (-y^n)).$$

Како је n непаран број, важи следећа једнакост $(-y)^n = -y^n$.
$\Longrightarrow v_p(x^n - (-y^n)) = v_p(x^n - (-y)^n)$. Сада можемо искористити Лему 3.1.

$$v_p(x^n - (-y)^n) = v_p(x - (-y)) \Longrightarrow v_p(x^n + y^n) = v_p(x+y).$$

□

Пређимо сада на лему о подизању експонента.

3.1.1 $p \neq 2$

Теорема 3.5 (Први облик леме) *Нека су x, y цели бројеви, n природан и p непаран прост број, такви да $p \mid (x-y)$ и $p \nmid x, y$. Тада важи*

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$

Доказ: Најпре ћемо проверити случај $n = p$. Покажимо да је $v_p(x^p - y^p) = v_p(x-y) + 1$. Како је

$$x^p - y^p = (x-y)\left(x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1}\right),$$

применом Теореме 3.1 добијамо

$$v_p\left(x^p - y^p\right) = v_p\left(x-y\right) + v_p\left(x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1}\right).$$

Испитајмо зато колико је $v_p\left(x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1}\right)$. Како $p \mid x-y$, онда је $x \equiv y \pmod p$, па можемо закључити следеће:

$$x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1} \equiv p \cdot x^{p-1} \equiv 0 \pmod p.$$

Дакле, $p \mid \left(x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1}\right)$. Проверимо сада шта се дешава по модулу p^2. Нека је $y = x + kp$, где је $k \in \mathbb{Z}$. Биће нам згодан следећи запис:

$$x^{p-1} + x^{p-2}\cdot y + \cdots + y^{p-1} = x^{p-1} + \sum_{t=1}^{p-1} x^{p-1-t}y^t.$$

Посматрајмо сада чланове $x^{p-1-t}y^t = x^{p-1-t}(x+kp)^t, 1 \leqslant t \leqslant p-1$. Употребом биномног развоја долазимо до следећег:

$$(x+kp)^t = x^t + tx^{t-1}kp + \binom{t}{2}x^{t-2}(kp)^2 + \cdots + (kp)^t \equiv x^t + tx^{t-1}kp \pmod{p^2}.$$

Ово значи да је

$$x^{p-1-t}(x+kp)^t \equiv x^{p-1} + tx^{p-2}kp \pmod{p^2},\ 1 \leqslant t \leqslant p-1.$$

Користећи ово добијамо следеће:

$$x^{p-1} + \sum_{t=1}^{p-1} x^{p-1-t}(x+kp)^t \equiv x^{p-1} + \sum_{t=1}^{p-1}\left(x^{p-1} + tx^{p-2}kp\right) \pmod{p^2}.$$

Раздвајањем сума долазимо до следећих конгруенција:

$$x^{p-1} + x^{p-2} \cdot y + \cdots + y^{p-1} \equiv px^{p-1} + \sum_{t=1}^{p-1} tx^{p-2}kp$$

$$\equiv px^{p-1} + x^{p-2}kp \sum_{t=1}^{p-1} t$$

$$\equiv px^{p-1} + \frac{p(p-1)}{2} x^{p-2}kp$$

$$\equiv px^{p-1} + \frac{p-1}{2} x^{p-2}kp^2$$

$$\equiv px^{p-1}$$

$$\not\equiv 0 \pmod{p^2}.$$

Дакле, $p^2 \nmid x^{p-1} + x^{p-2} \cdot y + \cdots + y^{p-1}$, чиме смо показали да је заиста

$$v_p\left(x^{p-1} + x^{p-2} \cdot y + \cdots + y^{p-1}\right) = 1.$$

Испитајмо сада општи случај. Нека је $n = p^\alpha b,\ \alpha \in \mathbb{N}_0,\ b \in \mathbb{N}$ и $(p, b) = 1$. Како је $x^n - y^n = (x^{p^\alpha})^b - (y^{p^\alpha})^b$ и $(p, b) = 1$, можемо применити Лему 3.2.

$$v_p(x^n - y^n) = v_p((x^{p^\alpha})^b - (y^{p^\alpha})^b) = v_p(x^{p^\alpha} - y^{p^\alpha}).$$

Како је $p^\alpha = p^{\alpha-1}p$, долазимо до следеће једнакости:

$$v_p\left(x^{p^\alpha} - y^{p^\alpha}\right) = v_p\left((x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p\right).$$

Сада, применом претходно показаног, долазимо до следећег закључка:

$$v_p\left((x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p\right) = v_p\left(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\right) + 1.$$

Како је $p^{\alpha-1} = p^{\alpha-2}p$, применом истог поступка, долазимо до закључка да је

$$v_p\left(x^n - y^n\right) = v_p\left(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\right) + 2.$$

Ако исти овај поступак применимо још $\alpha-2$ пута, долазимо до коначног закључка:

$$v_p\left(x^n - y^n\right) = v_p\left(x^{p^{\alpha-\alpha}} - y^{p^{\alpha-\alpha}}\right) + \alpha = v_p(x-y) + v_p(n).$$

□

Теорема 3.6 (Други облик леме) *Нека су x, y цели бројеви, n непаран природан и p непаран прост број, такви да $p \mid (x+y)$ и $p \nmid x, y$. Тада важи*

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n).$$

Доказ: Да бисмо доказали ову теорему, користићемо идеју коју смо користили у доказу Леме 3.2. Наиме, користићемо једнакост $v_p(x^n + y^n) = v_p(x^n - (-y^n))$ и чињеницу да је $(-y)^n = -y^n$. Применом Теореме 3.5 добијамо

$$v_p(x^n - (-y^n)) = v_p(x^n - (-y)^n) = v_p(x - (-y)) + v_p(n)$$

$$\implies v_p(x^n + y^n) = v_p(x+y) + v_p(n).$$

□

3.1.2 $p = 2$

Теорема 3.7 *Нека су x, y непарни цели бројеви такви да $4 \mid x - y$. Тада важи*

$$v_2(x^n - y^n) = v_2(x-y) + v_2(n).$$

Доказ: Посматрајмо $n = m \cdot 2^k$, за $m \in \mathbb{N}$ и $k \in \mathbb{N}_0$, тако да $2 \nmid m$. Тада је $v_2(n) = k$ и $x^n - y^n = \left(x^{2^k}\right)^m - \left(y^{2^k}\right)^m$. Како су x, y непарни бројеви, такође су и x^{2^k}, y^{2^k} непарни. Уз услов да $2 \nmid m$, испуњени су сви услови за примену Леме 3.2. Дакле,

$$v_2\left(x^n - y^n\right) = v_2\left(\left(x^{2^k}\right)^m - \left(y^{2^k}\right)^m\right) = v_2\left(x^{2^k} - y^{2^k}\right).$$

Остаје нам да покажемо да је

$$v_2\left(x^{2^k} - y^{2^k}\right) = v_2(x-y) + k.$$

Овде можемо уочити разлику квадрата, па записати на следећи начин:

$$x^{2^k} - y^{2^k} = (x^{2^{k-1}} + y^{2^{k-1}})(x^{2^{k-2}} + y^{2^{k-2}})...(x+y)(x-y).$$

Из датих услова видимо да важи $x \equiv y \equiv \pm 1 \pmod 4$, тако да можемо закључити да је $x^{2^r} \equiv y^{2^r} \equiv 1 \pmod 4$ за свако $r \in \mathbb{N}$. Према томе, $x^{2^r} + y^{2^r} \equiv 2 \pmod 4$. Из овога видимо да је степен броја 2 који дели сваки од фактора једнак 1, осим фактора $(x-y)$, а како имамо k таквих фактора, овим смо управо показали да је

$$v_2\left(x^n - y^n\right) = v_2(x-y) + k = v_2(x-y) + v_2(n).$$

□

Теорема 3.8 *Нека су x, y непарни цели бројеви и n паран природан број. Тада важи*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Доказ: Нека је $n = 2k,\ k \in \mathbb{N}$. Тада је

$$v_2\left(x^n - y^n\right) = v_2\left(\left(x^2\right)^k - \left(y^2\right)^k\right).$$

Како је $x^2 - y^2 = (x - y)(x + y)$ и $x - y,\ x + y$ су парни бројеви (x, y су непарни), онда важи $4 \mid x^2 - y^2$. Сада можемо применити Теорему 3.7 :

$$v_2(x^n - y^n) = v_2\left(x^2 - y^2\right) + v_2(k).$$

Како је $v_2(n) = v_2(2k) = 1 + v_2(k)$, коришћењем ове чињенице и Теореме 3.1, добијамо:

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

□

3.2 Задаци

3.1. Наћи највећи степен броја 2019 који дели $Z = 2018^{2019^{2020}} + 2020^{2019^{2018}}$.

Решење: За почетак, растављањем броја 2019 на просте чиниоце добијамо $2019 = 3 \cdot 673$. Ако пронађемо највећи степен броја 3, а затим броја 673, који дели Z, бићемо на корак од решења. Посматрањем проблема на овај начин добијамо могућност примене Леме о подизању експонента. Нека је $X = 2018^{2019^{2020}} + 1$, а $Y = 2020^{2019^{2018}} - 1$. Приметимо да је тада $Z = X + Y$.

Испитајмо прво колико је $v_3(Z)$. Посматрањем збира $2018^{2019^{2020}} + 1^{2019^{2020}}$, можемо приметити да су испуњени сви услови за примену Теореме 3.6. Дакле,

$$v_3(X) = v_3\left(2018^{2019^{2020}} + 1^{2019^{2020}}\right) = v_3(2018 + 1) + v_3\left(2019^{2020}\right).$$

Како је $v_3(2019) = 1$ следи $v_3(X) = 1 + 2020 = 2021$. Слично, посматрањем броја $Y = 2020^{2019^{2018}} - 1^{2019^{2018}}$, примећујемо да су испуњени сви услови за примену Теореме 3.5.

$$v_3(Y) = v_3\left(2020^{2019^{2018}} - 1^{2019^{2018}}\right) = v_3(2020 - 1) + v_3\left(2019^{2018}\right).$$

$v_3\left(2019^{2018}\right) = 2018 \Longrightarrow v_3(Y) = 1 + 2018 = 2019$. Како је $v_3(Y) < v_3(X)$, употребом Теореме 3.2, закључујемо да је $v_3(Z) = v_3(X + Y) = v_3(Y) = 2019$. Дакле, највећи степен броја 3 који дели Z је 2019.

Сада, применом истог поступка у тражењу највећег степена броја 673 који дели Z, добијамо

$$v_{673}(X) = v_{673}\left(2018^{2019^{2020}} + 1^{2019^{2020}}\right) = v_{673}(2018+1) + v_{673}\left(2019^{2020}\right),$$

$$v_{673}(Y) = v_{673}\left(2020^{2019^{2018}} - 1^{2019^{2018}}\right) = v_{673}(2020-1) + v_{673}\left(2019^{2018}\right).$$

Како је $v_{673}(X) = 1 + 2020 = 2021$ и $v_{673}(Y) = 1 + 2018 = 2019$, следи $v_{673}(Z) = v_{673}(X+Y) = v_{673}(Y) = 2019$. Дакле, највећи степен броја 673 који дели Z је такође 2019. Из свега овога закључујемо да је тражени највећи степен броја 2019 који дели Z једнак 2019. $\triangle$

3.2. Израчунати збир свих делиоца d броја $X = 109^{2020} - 1$ који су облика $2^a 3^b$, где су a и b природни бројеви.

Решење: Како нам се тражи збир свих делиоца d који су облика $2^a 3^b$, биће нам кључно да израчунамо највећи степен броја 2 који дели X, као и највећи степен броја 3 који дели X. Другим речима, треба да израчунамо $v_2(X)$ и $v_3(X)$.

Израчунајмо прво колико је $v_2(X)$. Приметимо да су 109 и 1 непарни бројеви такви да $4 \mid (109-1) = 108$. Овим су испуњени услови за примену Теореме 3.7.

$$v_2(X) = v_2\left(109^{2020} - 1\right) = v_2(109-1) + v_2(2020).$$

Како је $108 = 2^2 \cdot 3^3$ и $2020 = 2^2 \cdot 5 \cdot 101$, добијамо $v_2(X) = 2 + 2 = 4$.

На сличан начин ћемо израчунати колико је $v_3(X)$. Како је 3 непаран прост број за који важи $3 \mid (109-1),\ 3 \nmid 109, 1$, испуњени су услови за примену Теореме 3.5.

$$v_3(X) = v_3\left(109^{2020} - 1\right) = v_3(109-1) + v_3(2020).$$

Из претходног разматрања закључујемо да $v_3(X) = 3 + 0 = 3$.

Овим смо добили да $a \in A = \{1,2,3,4\},\ b \in B = \{1,2,3\}$. Дакле,

$$d \in D = \{2^1 3^1, 2^1 3^2, 2^1 3^3, 2^2 3^1, \ldots, 2^4 3^2, 2^4 3^3\}.$$

Тражени збир делиоца d можемо записати на следећи начин:

$$\sum_{d \in D} d = \sum_{a \in A} 2^a \sum_{b \in B} 3^b = (2+4+8+16) \cdot (3+9+27) = 30 \cdot 39 = 1170. \quad \triangle$$

3.3. Наћи највећи степен броја 11 који дели 2020!.

Решење: Како је 11 прост број, можемо директно применити Лежандрове теореме. Задатак ћемо решити на два начина, прво применом Теореме 3.3, а затим и применом Теореме 3.4.

Начин 1: Ако посматрамо степене броја 11 долазимо до следећег запажања. $11^1 = 11,\ 11^2 = 121,\ 11^3 = 1331,\ 11^4 = 14\ 641 > 2020$. Дакле, $11^i > 2020$ за свако $i \geqslant 4$. Применом Теореме 3.3 долазимо до следећег закључка:

$$v_{11}(2020!) = \sum_{i=1}^{\infty} \lfloor \frac{2020}{11^i} \rfloor = \lfloor \frac{2020}{11} \rfloor + \lfloor \frac{2020}{121} \rfloor + \lfloor \frac{2020}{1331} \rfloor = 183 + 16 + 1 = 200.$$

Начин 2: Сада ћемо проблем решити применом друге Лежандрове теореме, тј. Теореме 3.4. Да бисмо применили ову теорему, морамо да израчунамо збир цифара броја 2020 у основи 11, дакле, треба прво да дођемо до репрезентације броја 2020 у овој основи. Да бисмо то решили искористићемо резултате које смо добили у првом делу.

Дељењем броја 2020 са 11, добијамо количник 183 и остатак 7. Сада, дељењем броја 183 са 11, добијамо количник 16 и остатак 7. На исти начин долазимо до једнакости $16 = 11 \cdot 1 + 5$ и $1 = 11 \cdot 0 + 1$.
Користећи остатке које смо добили на овај начин, број 2020 можемо записати као $2020 = 1 \cdot 11^3 + 5 \cdot 11^2 + 7 \cdot 11^1 + 7 \cdot 11^0$. Дакле, $2020 = (1577)_{11}$, па је $s_{11}(2020) = 1 + 5 + 7 + 7 = 20$. Сада можемо применити Теорему 3.4.

$$v_{11}(2020!) = \frac{2020 - s_{11}(2020)}{11 - 1} = \frac{2020 - 20}{10} = 200.$$

Дакле, највећи степен броја 11 који дели 2020! је 200. $\triangle$

3.4. Показати да за сваки природан број n важи следећа једнакост

$$n! = \prod_{i=1}^{n} \left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right].$$

Решење: Ако бисмо имали $v_p(a) = v_p(b)$ за све просте бројеве p, где су a и b природни бројеви, онда би то значило да је $a = b$, јер би a и b имали исту факторизацију. Из тог разлога ћемо искористити ову идеју и покушати да покажемо да за све просте бројеве p важи $v_p(n!) = v_p\left(\prod_{i=1}^{n} \left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]\right)$. Посматраћемо $p \leqslant n$, јер би у супротном очигледно било

$$v_p(n!) = v_p\left(\prod_{i=1}^{n} \left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]\right) = 0.$$

Применом Лежандрове теореме 3.3 добијамо $v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$. Сада ћемо показати да је овој суми једнако и $v_p\left(\prod_{i=1}^{n} \left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]\right)$.

Када $i \in \{1, 2, \ldots, \lfloor \frac{n}{p} \rfloor\}$ имамо бар један фактор p у $\left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]$. Због тога ћемо имати $\lfloor \frac{n}{p} \rfloor$ фактора p у овом случају.

Када $i \in \{1, 2, \ldots, \lfloor \frac{n}{p^2} \rfloor\}$ имамо бар два фактора p у $\left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]$. Сада морамо да додамо још 2 фактора за свако p^2 , али како смо их већ једанпут рачунали, остаје да додамо још по један фактор за свако i, дакле, додајемо $\lfloor \frac{n}{p^2} \rfloor$.

Понављањем овог процеса долазимо до закључка да је

$$v_p\left(\prod_{i=1}^{n} \left[1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\right]\right) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor,$$

што смо и желели да покажемо. $\triangle$

3.5. Наћи све природне пројеве n такве да $\dfrac{2^n + 1}{n^2}$ буде цео број.

Решење: Да би дати број био цео, мора да важи $n^2 \mid 2^n + 1$. Приметимо најпре да је $2^n + 1$ непаран број. Ово значи да и n мора да буде непаран.

Приметимо да је $n = 1$ једно тривијално решење.

Нека је сада $n > 1$. Идеја је да посматрамо просте факторе броја n, јер $p \mid n \Rightarrow p \mid n^2$, а како мора да важи $n^2 \mid 2^n + 1$, онда ће важити и $p \mid 2^n + 1$.

Нека је $p > 2$ најмањи прост фактор броја n. Како $p \mid n$ следи $p \mid 2^n + 1$, а из овога закључујемо да важи и $p \mid 2^{2n} - 1$. Из Мале Фермаове теореме имамо да $p \mid 2^{p-1} - 1$. Ово значи да $p \mid \left(2^{2n} - 1, 2^{p-1} - 1\right)$, па применом Теореме 2.4 долазимо до закључка да $p \mid 2^{(2n, p-1)} - 1$. Како је $p - 1$ паран број и $(n, p - 1) = 1$, јер n нема простих фактора мањих од p, онда мора бити $(2n, p - 1) = 2$. Дакле,

$$p \mid 2^2 - 1 \implies p = 3.$$

Нека је $v_3(n) = k,\ k \in \mathbb{N}$. Тада је $v_3(n^2) = 2k$. Применом Леме о подизању експонента (3.6) добијамо следеће:

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = 1 + k.$$

Како је $v_3(2^n + 1) \geqslant v_3(n^2)$, добијамо $1 + k \geqslant 2k$, што значи да је $k = 1$.

Нека је $n = 3n_1$, где је n_1 неки непаран природан број. Извршимо сада дискусију по n_1.

За $n_1 = 1$ добијамо још једно решење $\left(\dfrac{2^3 + 1}{3^2} = 1\right)$.

Нека је сада $n_1 > 1$ и нека је $q > 2$ најмањи прост фактор броја n_1. Тада имамо

$$q \mid n_1 \implies q \mid n \implies q \mid 2^n + 1 \implies q \mid 8^{n_1} + 1.$$

Слично као мало пре, важиће $q \mid 8^{2n_1} - 1$, као и $q \mid 8^{q-1} - 1$, а ово значи да q дели и највећи заједнички делилац ових бројева. Поново, применом Теореме 2.4 долазимо до закључка да $q \mid 8^{(2n_1, q-1)} - 1$. Истим разматрањем као у претходном делу добијамо $(2n_1, q-1) = 2$. Дакле,

$$q \mid 8^2 - 1 \implies q = 7.$$

Међутим, $2^n + 1 = 8^{n_1} + 1 \equiv 1^{n_1} + 1 \equiv 2 \pmod 7$, што је контрадикција са $7 \mid 2^n + 1$. Овим смо завршили даљу дискусију случаја $n_1 > 1$, а тиме и случаја $n > 1$. Дакле, једина решења су $n = 1$ или $n = 3$. $\triangle$

3.6. Нека је $a > b > 1$, при чему је b непаран број и нека је n природан број. Ако $b^n \mid a^n - 1$ доказати да је $a^b > \dfrac{3^n}{n}$.

Решење: Најпре ћемо претпоставити да тврђење важи ако је b прост број (и оставити за касније доказ).

Нека је сада b сложен број и $q \mid b$, за неки непаран прост број q. Тада $q^n \mid b^n$, а како $b^n \mid a^n - 1$, онда важи и $q^n \mid a^n - 1$. Користећи сада претпоставку, из $q^n \mid a^n - 1$ следи $a^q > \frac{3^n}{n}$, а ово нас доводи до неједнакости $a^b > a^q > \frac{3^n}{n}$. Дакле, задатак се своди на доказ тврђења за непарне просте бројеве b.

Зато, нека је $b = p$ прост. Како $p^n \mid a^n - 1$, онда и $p \mid a^n - 1$, тј. $a^n \equiv 1 \pmod p$. Нека је $\delta_p(a)$ поредак броја a по модулу p. Тада имамо да важи $\delta_p(a) \mid n$. Такође, из Мале Фермаове теореме знамо да је $a^{p-1} \equiv 1 \pmod p$, па због тога и $\delta_p(a) \mid p-1$.

Нека је $\delta_p(a) = \delta \leqslant p-1$. Сада имамо $a^\delta \equiv 1 \pmod p$. Како $\delta \mid n$, нека је $n = \delta n_1$, за неки природан број n_1. Дакле, $p^n \mid (a^\delta)^{n_1} - 1$. Применом Леме о подизању експонента (3.5) добијамо:

$$v_p\left((a^\delta)^{n_1} - 1\right) = v_p\left(a^\delta - 1\right) + v_p(n_1) \geqslant n.$$

Сада, применом Леме 3.1 добијамо:

$$v_p\left(a^\delta - 1\right) \geqslant n - v_p(n_1) \geqslant n - \log_p n_1$$

$$\implies v_p\left(a^\delta - 1\right) \geqslant \log_p p^n - \log_p n_1 = \log_p \left(\frac{p^n}{n_1}\right).$$

Ово разматрање нас води до следећег закључка:

$$a^b > a^\delta - 1 \geqslant p^{v_p\left(a^\delta - 1\right)} \geqslant p^{\log_p \left(\frac{p^n}{n_1}\right)} = \frac{p^n}{n_1} = \frac{\delta \cdot p^n}{n}.$$

Како је b непаран број већи од 1, важи $p^n \geqslant 3^n$, а тиме доказујемо тврђење $a^b > \dfrac{3^n}{n}$. $\triangle$

3.7. Наћи све парове (x, y) који задовољавају једначину $3^x = 2^x y + 1$, при чему су x и y природни бројеви.

Решење: Задатак ћемо решавати дискусијом по x. Нека је $x = 1$. Из једнакости $3^1 = 2^1 y + 1$ следи $y = 1$, па ће једно решење бити $(x, y) = (1, 1)$.

Нека је сада $x \geqslant 2$. У том случају, приметимо да је $2^x y \equiv 0 \pmod 4$. Како је $2^x y = 3^x - 1$, онда важи и

$$3^x - 1 \equiv 0 \pmod 4 \implies 3^x \equiv 1 \pmod 4.$$

Како је $3 \equiv -1 \pmod 4$, онда је $3^x \equiv (-1)^x \pmod 4$, па из претходног разматрања имамо да је $(-1)^x \equiv 1 \pmod 4$. Из овога закључујемо да x мора бити паран број. Сада можемо применити Лему о подизању експонента (3.8).

$$v_2\left(3^x - 1\right) = v_2(3-1) + v_2(3+1) + v_2(x) - 1 = 2 + v_2(x).$$

Како је $v_2\left(2^x y\right) \geqslant x$ следи $2 + v_2(x) \geqslant x$, тј. $v_2(x) \geqslant x - 2$. Ова неједнакост је испуњена за $x \geqslant 2^{x-2}$. Одавде закључујемо да је $x \leqslant 4$.

У случају $x = 2$ имамо $3^2 = 2^2 y + 1 \implies y = 2$.

У случају $x = 4$ имамо $3^4 = 2^4 y + 1 \implies y = 5$.

Дакле, тражена решења су

$$(x, y) \in \{(1,1), (2,2), (4,5)\}. \quad \triangle$$

3.8. Наћи све природне бројеве x, y и просте p за које важи $p^x - y^p = 1$.

Решење: Најпре ћемо посматрати случај $p = 2$.

Тада имамо $2^x - y^2 = 1$. У случају $x = 1$ имамо $2^1 - y^2 = 1 \implies y = 1$. Дакле, једно решење ће бити $(x, y, p) = (1, 1, 2)$.

Нека је сада $x \geqslant 2$. Тада је

$$2^x \equiv 0 \pmod 4 \Longrightarrow -y^2 \equiv 1 \pmod 4.$$

Међутим, $y^2 \equiv -1 \pmod 4$ нема решења, па је решење које смо добили мало пре једино у случају $p = 2$.

Нека је сада $p \neq 2$.

У случају $p \mid y$ имали бисмо $p \mid p^x - y^p = 1 \Longrightarrow p \mid 1$, што је немогуће. Дакле, $p \nmid y$. Применом Мале Фермаове теореме добијамо:

$$y^p \equiv y \pmod p \implies p^x = y^p + 1 \equiv y + 1 \pmod p.$$

Сада можемо применити Лему о подизању експонента (3.6).

$$v_p\left(y^p+1\right) = v_p(y+1) + v_p(p) = v_p(p^x) = x.$$

Из овога закључујемо да је $v_p(y+1) = x-1$. Како је $p^{v_p(y+1)} \leqslant y+1$, из претходне једнакости добијамо $p^{x-1} \leqslant y+1 \implies p^x \leqslant (y+1)p$. Ово нас води до следеће неједнакости:

$$(y+1)p - y^p \geqslant 1,$$

а ово је еквивалентно са

$$(y+1)p \geqslant 1 + y^p = (1+y)(1+y+y^2+\cdots+y^{p-1}). \tag{3.1}$$

У случају $x = 1$ почетна једначина неће имати решења, па ћемо посматрати случај $x \geqslant 2$. У том случају добијамо да $p \mid y+1$, а како је $p > 2$, онда је $y \geqslant 2$. Међутим, лако се провери да у том случају неједнакост (3.1) неће бити задовољена за $p > 3$. Дакле, имаћемо још само једно решење и то $(x,y,p) = (2,2,3)$. Дакле, сва решења су

$$(x,y,p) \in \{(1,1,2),(2,2,3)\}. \quad \triangle$$

3.9. Нека су a, b и c природни бројеви такви да $c \mid a^c - b^c$. Доказати да тада $c \mid \dfrac{a^c-b^c}{a-b}$.

Решење: Задатак ћемо решавати испитивањем простих фактора p броја c. Нека је p произвољан прост фактор броја c и важи $v_p(c) = x$.

Посматрајмо прво случај $p \nmid a-b$. Имамо да важи

$$a^c - b^c = (a-b)\left(a^{c-1} + a^{c-2}b + \cdots + b^{c-1}\right).$$

Како $p^x \mid c$ и $c \mid a^c - b^c$, онда важи и $p^x \mid a^c - b^c$. Међутим, како је p^x узајамно просто са $a-b$, онда закључујемо да p^x мора да дели други фактор, тј. $p^x \mid a^{c-1} + a^{c-2}b + \cdots + b^{c-1}$. Дакле, $p^x \mid \dfrac{a^c-b^c}{a-b}$ за свако $p \nmid a-b$.

Сада ћемо посматрати случај $p \mid a-b$. Нека је најпре $p \neq 2$. Применом Теореме 3.5 добијамо:

$$v_p\left(\frac{a^c-b^c}{a-b}\right) = v_p(a^c-b^c) - v_p(a-b) = v_p(a-b) + v_p(c) - v_p(a-b) = v_p(c) = x.$$

Дакле, и у овом случају $p^x \mid \dfrac{a^c-b^c}{a-b}$. Остаје нам још случај када је $p = 2$. У овом

случају добијамо:

$$v_2\left(\frac{a^c-b^c}{a-b}\right) = v_2(a^c-b^c) - v_2(a-b) = v_2(a-b) + v_2(a+b) + v_2(c) - 1 - v_2(a-b).$$

Како $2 \mid a-b$, закључујемо да су a и b исте парности, па важи и $2 \mid a+b$. Дакле, $v_2(a+b) \geqslant 1$. Ово значи да је $v_2\left(\frac{a^c-b^c}{a-b}\right) \geqslant v_2(c) \implies 2^x \mid \frac{a^c-b^c}{a-b}$. Овим смо показали да за сваки прост фактор p, $v_p(c) = x$ важи следећа импликација

$$p^x \mid a^c - b^c \Longrightarrow p^x \mid \frac{a^c-b^c}{a-b},$$

чиме смо доказали задато тврђење. $\triangle$

3.10. Наћи све парове (x,p), где је x природан и p прост број, такве да је $x \leqslant 2p$ и $x^{p-1} \mid (p-1)^x + 1$.

Решење: Приметимо најпре да су парови $(1,p)$ тривијална решења за било који прост p.

Размотримо сада случај $p \neq 2$. Нека је q најмањи прост делилац броја x. Тада важи

$$q \mid (p-1)^x + 1 \Longrightarrow q \mid \left((p-1)^2\right)^x - 1.$$

Ово значи да $\delta_q\left((p-1)^2\right) \mid x$, где је $\delta_q\left((p-1)^2\right)$ поредак броја $(p-1)^2$ по модулу q, а како је $\varphi(q) = q-1$, такође важи $\delta_q\left((p-1)^2\right) \mid q-1$. Из овога можемо закључити да $\delta_q\left((p-1)^2\right) \mid (x, q-1)$, а како је $(x, q-1) = 1$, то онда значи да је $\delta_q\left((p-1)^2\right) = 1$, тј.

$$(p-1)^2 - 1 \equiv 0 \pmod{q}.$$

Из овога закључујемо да је $p(p-2) \equiv 0 \pmod{q}$. Дакле, $p \equiv 0 \pmod{q}$ или $p \equiv 2 \pmod{q}$. Такође, знамо да је $(p-1)^x + 1 \equiv 0 \pmod{q}$. Ако би било $p \equiv 2 \pmod{q}$, онда бисмо имали $(p-1)^x + 1 \equiv 2 \pmod{q}$. Ово би значило да је $q = 2$, али онда бисмо дошли до контрадикције јер је $p-1$ паран број. Дакле, $p \equiv 0 \pmod{q}$, а како су p, q прости, следи $p = q$. Сада можемо применити Теорему 3.6.

$$v_p\left((p-1)^x + 1\right) = v_p(p-1+1) + v_p(x) = 1 + v_p(x).$$

Како $p^{p-1} \mid (p-1)^x + 1$, онда је $1 + v_p(x) \geqslant p-1$. Ово значи да је $x \geqslant p^{p-2} > 2p$ за $p > 3$. Међутим, дат нам је услов $x \leqslant 2p$, што ће рећи $p \in \{2, 3\}$.

У случају $p = 2$ имамо $x \mid 2$, тј. $x = 1 \vee x = 2$.

У случају $p = 3$ имамо $x^2 \mid 2^x + 1$ и $x \leqslant 6$. Провером добијамо $x = 1 \vee x = 3$. Коначно, тражени парови су

$$(x,p) \in \{(1,p), (2,2), (3,3)\}. \quad \triangle$$

Биографија

Марина Маркагић рођена је 03.08.1995. године у Урошевцу. Од јуна 1999. године живи у Смедереву.

Основну школу ,,Бранислав Нушић" у Смедереву завршила је 2010. године као носилац Вукове дипломе.

Гимназију у Смедереву завршила је 2014. године као носилац Вукове дипломе. Током основне и средње школе учесница је многих математичких такмичења и квизова, међу којима се издвајају републичка такмичења 2012, 2013. и 2014. године, као и ,,Архимедесови" математички турнири. Добитница похвала и награда на такмичењима.

Основне студије на Математичком факултету Универзитета у Београду уписала 2014. године на смеру ,,Статистика, актуарска и финансијска математика". Године 2016. одлучује да студије настави на смеру ,,Професор математике и рачунарства", из љубави према педагошком раду и преношењу знања.

Дипломирала на Математичком факултету Универзитета у Београду 11. септембра 2019. године са просечном оценом 8,42.
Током основних студија предавала је математику и рачунарство у Четрнаестој београдској гимназији од октобра до децембра 2018. године.

Мастер студије на Математичком факултету Универзитета у Београду уписује 2019. године.
Током мастер студија предавала је математику у основној школи ,,Младост" у Београду од септембра 2019. године до јануара 2020. године.

Током студија, али и у животу иначе, највећу подршку пружа јој мама Зорица, тата Славиша и сестра Александра, којима посвећује мастер рад.

Литература

[1] A. Adler, J. E. Coury, *The Theory of Numbers - A Text and Source Book of Problems,* Jones and Bartlett Publishers International, 1995.

[2] T. Andreescu, B. Enescu, *Mathematical Olympiad Treasures,* Birkhäuser, New York, 2010.

[3] T. Andreescu, R. Gelca, *Mathematical Olympiad Challenges,* Birkhäuser, New York, 2005.

[4] E. Chen, *Orders Modulo A Prime,* 2015.

[5] G. Đanković, *Teorija brojeva,* Matematički fakultet Univerziteta u Beogradu, 2013.

[6] Д. Ђукић, *Конгруенције вишег степена,* Додатна настава из математике у Математичкој гимназији, 2012.

[7] L. Hogben, *Brojevi i stvarnost - matematika za svakoga,* Novo pokolenje, Beograd, 1953.

[8] М. Лукић, *Експоненцијалне конгруенције,* Додатна настава за трећи разред, Математичка гимназија у Београду, 2006.

[9] A. H. Parvardi, *Lifting The Exponent Lemma (LTE)*, 2011.

[10] A. Pejčev, *Eksponencijalne kongruencije,* Dodatna nastava iz matematike u Matematičkoj gimnaziji, 2006.

[11] D. Shanks, *Solved and Unsolved Problems in Number Theory,* Chelsea Publishing Company, New York, 1978.

[12] R. Sparkes, *Lifting The Exponent Lemma LTE,* 2016.

[13] М. Станић, Н. Икодиновић, *Теорија бројева - збирка задатака,* Завод за уџбенике, Београд, 2004.

[14] J. Stevens, *Olympiad Number Theory Through Challenging Problems*