ИТМ – Дискретна математика

Душан Ђукић

4. Теорија бројева

4.1. Дељивост

Централни појам у теорији бројева је *дељивост*. Ми у овом курсу подразумевамо да је референтни скуп $\mathbb{Z}$ (скуп целих бројева):

Дефиниција 4.1. Цео број b је *дељив* целим бројем $a \neq 0$ (тј. *a дели b*) ако је и количник $\frac{b}{a} = q$ цео број, тј. $b = q \cdot a$ за неко $q \in \mathbb{Z}$. Тада кажемо да је *a делилац* броја b и записујемо као $a \mid b$.

У ствари, појам дељивости има смисла у сваком скупу који је опскрбљен операцијом множења. Напредна теорија бројева се уобичајено бави дељивошћу на неким маштовитим скуповима, као што је нпр. *скуп Гаусових целих бројева* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, где је i имагинарна јединица. С друге стране, дељивост на скупу реалних бројева $\mathbb{R}$ је потпуно незанимљива, јер тамо се било шта може делити без остатка било чиме осим нулом.

Неколико тривијалних својстава дељивости:

(i) ако $a \mid b$ и $b \neq 0$, онда је $|b| \geqslant |a|$;

(ii) ако $a \mid b$ и $b \mid c$, онда $a \mid c$;

(iii) ако $a \mid b$ и $a \mid c$, онда $a \mid mb + nc$ за све $m, n \in \mathbb{Z}$;

(iv) ако $a \mid b$ и $b \mid a$, онда је $a = \pm b$;

(v) ако $a \mid b$ и $c \mid d$, онда $ac \mid bd$.

Онда када a није дељиво са b, прибегавамо дељењу са остатком.

Тврђење 4.1. Нека је a цео и b природан број. Тада постоје јединствени цели бројеви q и r такви да је

$$a = b \cdot q + r, \quad \text{где је} \quad 0 \leqslant r < b.$$

Број q се назива *количником*, а r *остатком* при дељењу a са b.

Доказ. Услов $0 \leqslant r = a - bq < b$ је еквивалентан са $bq \leqslant a < bq + b$, тј. са $q \leqslant \frac{a}{b} < q + 1$, што значи да је $q = \lfloor \frac{a}{b} \rfloor$. Одавде следи и постојање и јединственост одговарајућих бројева q и r. □

Пример 4.1. Дељење броја 100 бројем 25 даће количник 4 и остатак 0 ($100 = 4 \cdot 25$).

Дељење броја 100 бројем 29 даће количник 3 и остатак 13 ($100 = 3 \cdot 29 + 13$).

Пример 4.2. Да ли је број $2^{58} + 1$ дељив бројем $2^{29} + 2^{15} + 1$?

Решење. Дати број можемо записати овако:

$$2^{58} + 1 = 2^{58} + 2 \cdot 2^{29} + 1 - 2^{30} = (2^{29} + 1)^2 - (2^{15})^2 = (2^{29} + 2^{15} + 1)(2^{29} - 2^{15} + 1).$$

Посматрајмо два цела броја a и b који нису оба нуле. Број 1 је свакако један њихов заједнички делилац (али не нужно највећи). Такође, ако је $ab \neq 0$, број $|ab|$ је њихов заједнички садржалац (не нужно најмањи)

Дефиниција 4.2. Највећи заједнички делилац (НЗД) бројева a и b је највећи природан број d који дели и a и b.

Означавамо га са $d = \text{нзд}(a, b)$ или, ако не постоји могућност забуне, само $d = (a, b)$.

Ако је $\text{нзд}(a, b) = 1$, кажемо да су a и b *узајамно прости*.

Најмањи заједнички садржалац (НЗС) бројева a и b је најмањи природан број s број који је дељив и са a и са b.

Означавамо га са $s = \text{нзс}(a, b)$ или, ако не постоји могућност забуне, само $s = [a, b]$.

Обе дефиниције се очигледно могу проширити и на више целих бројева $a_1, a_2, \ldots, a_n$. Такође, можемо да сматрамо да су сви дати бројеви позитивни - промена знака не утиче на вредности НЗД и НЗС.

Дакле, како одредити највећи заједнички делилац датих бројева a и b? За почетак, приметимо да за свако $n \in \mathbb{N}$ важи

$$(a, b) = (a - nb,\ b).$$

Заиста, ако $d \mid b$, онда $d \mid a$ ако и само ако $d \mid a - nb$. Дакле, ако a поделимо са b са остатком: $a = bq + r$, $0 \leqslant r < b$, онда је $(a, b) = (b,\ a - qb) = (b, r)$. Овако проблем са бројевима a и b $(a \geqslant b)$ сводимо на проблем с мањим бројевима. То је основа *Еуклидовог*[1] *алгоритма*:

- Означимо $r_0 = a$ и $r_1 = b$.
- Ако су дати r_{i-1} и r_i, при чему је $r_i \neq 0$, означимо са r_{i+1} остатак при дељењу r_{i-1} са r_i. Наставимо овај поступак све док по први пут не добијемо $r_{n+1} = 0$.
- Тако добијамо опадајући низ $r_0 > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$. Тада је $d = r_n$.

Заиста, по претходном важи $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_n, r_{n+1}) = r_n$.

Пример 4.3. Одредити НЗД бројева 518 и 851 помоћу Еуклидовог алгоритма.

Решење. Овде је $r_0 = 851$ и $r_1 = 518$. Спроводимо низ дељења са остатком:

$$\begin{array}{lcll} 851 = 1 \cdot 518 + 333 & \Rightarrow & r_2 = 333; & \\ 518 = 1 \cdot 333 + 185 & \Rightarrow & r_3 = 185; & \\ 333 = 1 \cdot 185 + 148 & \Rightarrow & r_4 = 148; & \\ 185 = 1 \cdot 148 + 37 & \Rightarrow & r_5 = 37; & \\ 148 = 4 \cdot 37 \ + 0 & \Rightarrow & r_6 = 0 \quad \Rightarrow & (851, 518) = r_5 = 37. \end{array}$$

При томе је

$$\begin{array}{ll} 37 = 185 - 148 & \\ \quad = 185 - (333 - 185) & = 2 \cdot 185 - 333 \\ \quad = 2(518 - 333) - 333 & = 2 \cdot 518 - 3 \cdot 333 \\ \quad = 2 \cdot 518 - 3(851 - 518) & = 5 \cdot 518 - 3 \cdot 851. \end{array}$$

Мада се у пракси може и оптимизовати, Еуклидов алгоритам је теоријски веома значајан.

4.2. Прости бројеви

Многи природни бројеви могу се представити као производ два или више мањих: нпр. $60 = 6 \cdot 10 = (2 \cdot 3) \cdot (2 \cdot 5) = 2^2 \cdot 3 \cdot 5$. Онда када то није могуће учинити, реч је о „простом" броју.

Дефиниција 4.3. Природан број $p > 1$ је *прост* ако није дељив ниједним природним бројем, осим бројем 1 и самим собом.

Природан број већи од 1 је *сложен* ако није прост.

Број 1 се не сматра ни простим ни сложеним: он је, једноставно, неутралан елемент и множење или дељење њиме нема значај.

Поновљено растављање природног броја и његових чинилаца на мање чиниоце завршиће се тако што ће сви чиниоци бити прости, тј. неће се моћи даље растављати. Растављање природног броја на просте чиниоце зове се *канонска факторизација*. Испоставља се да сваки број има тачно једну канонску факторизацију (растављања која се разликују само у распореду чинилаца сматрају се истим). Пошто доказ овог тврђења почива на Еуклидовом алгоритму, прво ћемо навести неке његове последице.

Тврђење 4.2. (а) За све $a, b \in \mathbb{N}$ постоје цели бројеви x и y такви да је $\text{нзд}(a, b) = ax + by$.

(б) Ако $d \mid a$ и $d \mid b$ (где су d, a, b цели бројеви), онда такође $d \mid \text{нзд}(a, b)$.

(в) За све $a, b, c \in \mathbb{N}$ важи $\text{нзд}(ca, cb) = c \cdot \text{нзд}(a, b)$.

(г) Ако $c \mid ab$ и $\text{нзд}(c, a) = 1$, онда $c \mid b$.

(д) Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$.

[1] *Ευκλειδης* (IV-III век п.н.е), тајанствени старогрчки математичар

Доказ. (а) Ово је демонстрирано у примеру 4.3.

(б) Ако $d \mid a$ и $d \mid b$, онда $d \mid ax + by = \text{нзд}(a, b)$ за погодно одабране x, y.

(в) Ако се $r_0 = a$ и $r_1 = b$ у Еуклидовом алгоритму помноже са c, сваки од чланова r_i се множи са c. То важи и за последњи ненула члан, који је једнак $c \cdot \text{нзд}(a, b)$, односно $\text{нзд}(ca, cb)$.

(г) $c \mid ba \;\Rightarrow\; c \mid \text{нзд}(bc, ba) = b \cdot \text{нзд}(c, a) = b$.

(д) Ако $p \mid ab$ и $p \nmid a$, онда је $\text{нзд}(p, a) = 1$, па из дела (г) следи $p \mid b$.

Сада је на реду доказ да је канонска факторизација јединствена.

Тврђење 4.3 (Основна теорема аритметике). Сваки природан број се на јединствен начин може представити у облику производа простих бројева.

Доказ. Већ знамо да се n може раставити на просте факторе. Треба да покажемо да се свака два оваква растављања броја n могу разликовати само у поретку. Дакле, нека је

$$n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Пошто $p_1 \mid q_1 q_2 \cdots q_m$, бар један од простих фактора q_i мора бити дељив са p_1 (тврђење 4.2(д)), тј. једнак p_1. Можемо да га скратимо и наставимо поступак. □

Ако су нам познате канонске факторизације двају бројева, одређивање њиховог НЗД или НЗС постаје тривијално.

Тврђење 4.4. Нека су $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ природни бројеви, при чему су $p_1, \ldots, p_k$ различити прости бројеви, а неки од експонената α_i, β_i могу бити и нула. Тада је

$$\text{нзд}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}} \quad \text{и} \quad \text{нзс}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}.$$

Доказ. Број $d = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}}$ очигледно дели и a и b. С друге стране, бројеви $\frac{a}{d}$ и $\frac{b}{d}$ су узајамно прости, па је $\text{нзд}(a, b) = d \cdot \text{нзд}(\frac{a}{d}, \frac{b}{d}) = d$.

Слично се проверава и једнакост са НЗС. □

Пример 4.4. Канонске факторизације бројева $a = 3000$ и $b = 5040$ су

$$3000 = \boxed{2^3} \cdot \boxed{3^1} \cdot 5^3 \cdot \cancel{\boxed{7^0}},$$
$$5040 = 2^4 \cdot 3^2 \cdot \boxed{5^1} \cdot 7^1.$$

Одавде налазимо

$$\text{нзд}(3000, 5040) = \boxed{2^3} \cdot \boxed{3^1} \cdot \boxed{5^1} \cdot \boxed{7^0} = 120,$$
$$\text{нзс}(3000, 5040) = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7^1 = 126000.$$

Прости бројеви су истински фасцинантни објекти. Још је Еуклиду било познато да их има бесконачно много:

Тврђење 4.5. Скуп простих бројева је бесконачан.

Доказ. Претпоставимо да је коначан. Дакле, можемо да излистамо *све* просте бројве: $p_1, p_2, \ldots, p_n$. А сад посматрајмо број $P = p_1 p_2 \cdots p_n + 1$. Он је већи од свих наведених простих бројева, па мора бити сложен. Међутим, он при дељењу сваким простим бројем даје остатак 1, па није дељив ниједним од њих, што је контрадикција. □

Међутим, низ простих бројева не показује никакву правилност, тако да нема лаког начина да проверимо да ли је дати велики број прост или му нађемо канонску факторизацију. Многи математичари су уложили читаву своју каријеру не би ли бар мало одгонетнули просте бројеве, али сви њихови резултати су само асимптотски, а често и одударају од хеуристичких података за више редова величине. Наводимо без доказа два класична резултата о простим бројевима:

Теорема о простим бројевима. Означимо са $\pi(x)$ број простих бројева не већих од x. Тада је $\pi(x) \sim \frac{x}{\ln x}$, тј. $\lim_{x \to +\infty} \pi(x) \cdot \frac{\ln x}{x} = 1$.

Дирихлеова теорема. Ако су a и $d > 0$ узајамно прости цели бројеви, онда у аритметичкој прогресији $a, a + d, a + 2d, \ldots$ има бесконачно много простих бројева.

Ако је задати природан број n сложен, тј. $n = ab$ за неке бројеве $1 < a \leqslant b$, онда је свакако $a^2 \leqslant n$, тј. n има делиоца $a \leqslant \sqrt{n}$. Значи, ако нас занима само да ли је број n прост, довољно је да проверимо има ли делилаца међу (простим) бројевима не већим од $\sqrt{n}$. Међутим, у пракси је то веома тешко извести већ ако број n има више од двадесетак цифара.

Један од првих алгоритама за проналажење свих простих бројева до неке границе N било је *Ератостеново*[2] *сито*. Значајно бољих алгоритама ове врсте заправо и нема:

- Напишимо све бројеве од 2 до N.
- Број 2 је прост; уоквиримо га, а све остале бројеве дељиве са 2 (тј. сваки други) прецртајмо.
- Најмањи непрецртан број (3) је прост; уоквиримо га, а све остале бројеве дељиве са 3 прецртајмо (тј. сваки трећи, чак и ако су већ прецртани).
- Наставимо овај поступак све док сви бројеви до $\lfloor\sqrt{N}\rfloor$ не буду прецртани или уоквирени.

Када се алгоритам заврши, прости бројеви ће бити управо они који остану непрецртани.

Пример 4.5. (а) Ератостеново сито показује да има тачно 25 простих бројева од 2 до 100. Сложени бројеви дељиви са 2, 3, 5 и 7 прецртани су редом у правцима $\rightarrow, \nearrow, \uparrow, \nwarrow$. Прости су уоквирени.

(2)	(3)	4	(5)	6	(7)	8	9	10	(11)	12	(13)	14	15	16	(17)	18	(19)	20
21	22	(23)	24	25	26	27	28	(29)	30	(31)	32	33	34	35	36	(37)	38	39	40
(41)	42	(43)	44	45	46	(47)	48	49	50	51	52	(53)	54	55	56	57	58	(59)	60
(61)	62	63	64	65	66	(67)	68	69	70	(71)	72	(73)	74	75	76	77	78	(79)	80
81	82	(83)	84	85	86	87	88	(89)	90	91	92	93	94	95	96	(97)	98	99	100

(б) Број 10007 је прост. Наиме, да је сложен, морао би да има бар један прост фактор мањи од 100, али није тешко тестирати наведених 25 простих бројева и видети да није дељив ниједним.

(в) Овај огромни број са 100 цифара је прост:

$$1.234.567.890.123.456.789.000.000.000.000.000.000.000.000.000.000.000.000.000.133.556.804.790.000.000.000.000.000.000.000.000.000.000.012.247.$$

Али то је проверено једним напреднијим алгоритмом. Тестирање дељивости простим бројевима до 50 цифара за данашње рачунаре било би чак и у теорији неизводљиво.

4.3. Конгруенције

Знамо да целе бројеве можемо поделити на парне и непарне у складу са њиховим остатком при дељењу са 2. На сличан начин, бројеве можемо класификовати и у складу са остатком при дељењу ма којим бројем $n \in \mathbb{N}$. Тако долазимо до појма *конгруенције* који је увео Гаус[3].

Дефиниција 4.4. Цели бројеви a и b су *конгруентни по модулу* n ($n \in \mathbb{N}$) ако дају исти остатак при дељењу са n, тј. ако је разлика $a - b$ дељива са n. То означавамо са $a \equiv b \pmod{n}$.

Очигледно је да је конгруентност по модулу датог броја n релација еквиваленције. У односу на њу, скуп целих бројева се распада на n класа еквиваленције - *класа остатака*. Када кажемо „по модулу n", мислимо на остатак при дељењу на n, тј. на класу остатака. Сваком од n могућих остатака при дељењу са n одговара по једна класа.

Конгруенције се слажу са сабирањем и множењем:

Тврђење 4.6. Нека су a, b, c, d цели и m, n природни бројеви.

(а) Ако је $a \equiv b \pmod{n}$, онда је и $a \equiv b \pmod{m}$ кад год $m \mid n$.

(б) Ако је $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, онда је $a \pm c \equiv b \pm d \pmod{n}$ и $ac \equiv bd \pmod{n}$.

(в) Важи $P(a) \equiv P(b) \pmod{n}$ за сваки полином $P(x)$ са целобројним коефицијентима.

(г) Ако је $ma \equiv mb \pmod{n}$ и нзд$(m, n) = 1$, онда је и $a \equiv b \pmod{n}$.

Доказ. (а) $a \equiv b \pmod{n} \Rightarrow m \mid n$ и $n \mid a - b \Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod{m}$.

(б) Из $n \mid a - b$ и $n \mid c - d$ следи $n \mid (a+c) - (b+d)$ и $n \mid (a-b)c + b(c-d) = ac - bd$.

(в) Следи из (а) и (б).

(г) Ако $n \mid ma - mb = m(a - b)$ и нзд$(m, n) = 1$, по тврђењу 4.2(г) следи $n \mid a - b$. □

[2] *Ερατοσθενης* (276-194 п.н.е), старогрчки научник

[3] Carl Friedrich Gauß (1777-1855), немачки математичар

Тврђење 4.5(г) није тачно ако се изостави услов нзд$(m,a)=1$. На пример, иако је $2\cdot 3\equiv 2\cdot 8 \pmod{10}$, не важи $3\equiv 8 \pmod{10}$.

Пример 4.6. Израчунајмо остатак који даје 3^{60} при дељењу са 97. Имамо редом

$$3^5=243\equiv 49 \pmod{97},\quad 3^{10}\equiv 49^2=2401\equiv -24 \pmod{97},\quad 3^{20}\equiv(-24)^2=576\equiv -6 \pmod{97}$$

и, најзад, $3^{60}\equiv(-6)^3=-216\equiv 75 \pmod{97}$.

Пошто у једној класи остатака сви бројеви дају исти остатак при дељењу са n, има смисла из сваке класе одабрати по једног представника. Тако ћемо добити потпун систем остатака.

Дефиниција 4.5. Цели бројеви $a_1,a_2,\ldots,a_m$ чине *потпун систем остатака* по модулу n ако дају сваки остатак тачно по једном.

Ако бројеви $a_1,a_2,\ldots,a_m$ дају само остатке узајамно просте са n, и то сваки такав остатак по једном, они чине *сведен систем остатака* по модулу n.

Пошто свака класа остатака има бесконачно много елемената, система остатака, како потпуних тако и сведених, има бесконачно много.

Пример 4.7. (а) При дељењу са 10 могући остаци су $0,1,2,3,4,5,6,7,8,9$. Скуп $\{-4,-3,-2,-1,0,1,2,3,4,5\}$ даје сваки од ових остатака по једном, те је он потпун систем остатака по модулу 10. Има и маштовитијих примера, нпр. $\{0,3,6,9,12,15,18,21,24,27\}$.

С друге стране, једини остаци који су узајамно прости са 10 су 1, 3, 7 и 9. Зато је нпр. $\{-3,-1,1,3\}$ сведен систем остатака по модулу 10, јер сваки од ових остатака даје по једном.

Јасно је да потпун систем остатака по модулу n има тачно n елемената. Сведен систем остатака има мање од n елемената, али колико тачно? Убрзо ће нам затребати одговор на ово питање.

Дефиниција 4.6. За дати природан број n, *Ојлерова*[4] *функција* $\varphi(n)$ представља број елемената у сведеном систему остатака по модулу n.

Другим речима, $\varphi(n)$ је број природних бројева не већих од n и узајамно простих са n.

Тврђење 4.7. Ако је $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ канонска факторизација броја $n\in\mathbb{N}$ (где су $p_1,\ldots,p_k$ различити прости бројеви, а експоненти α_i строго позитивни), онда је $\varphi(n)$ дато формулом

$$\varphi(n)=n\cdot\frac{p_1-1}{p_1}\cdot\frac{p_2-1}{p_2}\cdot\ldots\cdot\frac{p_k-1}{p_k}.$$

Доказ. Користићемо формулу укључења и искључења. Означимо са A_i $(1\leqslant i\leqslant k)$ скуп бројева од 1 до n који су дељиви простим бројем p_i. Јасно је да је $|A_i|=\frac{n}{p_i}$. Штавише, пресек m скупова $A_{i_1},\ldots,A_{i_m}$ $(m\leqslant k)$ састоји се од бројева дељивих са $p_{i_1}\cdots p_{i_m}$, па је

$$|A_{i_1}\cap\cdots\cap A_{i_m}|=\frac{n}{p_{i_1}\cdots p_{i_m}}.$$

Према томе, кардиналност скупа $\{1,2,\ldots,n\}\setminus(A_1\cup\cdots\cup A_k)$ је

$$n-\sum\frac{n}{p_i}+\sum\frac{n}{p_{i_1}p_{i_2}}-\sum\frac{n}{p_{i_1}p_{i_2}p_{i_3}}+\cdots+(-1)^k\frac{n}{p_1p_2\cdots p_k}=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big).\quad\square$$

Пример 4.8. (а) Ако је p прост број, онда је $\varphi(p)=p-1$.

(б) Ако је p прост и n природан број, важи $\varphi(p^n)=p^{n-1}(p-1)$.

(в) Пошто је $7!=5040=2^4\cdot 3^2\cdot 5\cdot 7$, имамо $\varphi(5040)=5040(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7})=1152$.

Тврђење 4.8. Нека је a узајамно просто са n. Ако је скуп $\{a_1,a_2,\ldots,a_m\}$ (а) потпун или (б) сведен систем остатака по модулу n, онда је то и скуп $\{aa_1,aa_2,\ldots,aa_n\}$.

Доказ. (а) Ако бројеви $a_1,\ldots,a_m$ дају међусобно различите остатке по модулу n, онда и бројеви $aa_1,\ldots,aa_m$ дају међусобно различите остатке. Заиста, ако је $aa_i\equiv aa_j \pmod{n}$ за неке $i\neq j$, онда је и $a_i\equiv a_j \pmod{n}$ по тврђењу 4.5(г).

(б) Сличан доказ, уз примедбу да ако је нзд$(a_i,n)=1$, онда је и нзд$(aa_i,n)=1$. $\square$

[4]Leonhard Euler (1707-1783), швајцарски математичар

Из тврђења 4.7 можемо да закључимо да, ако је нзд$(a,n)=1$, бројеви $0,a,2a,\ldots,(n-1)a$ чине потпун систем остатака по модулу n, тј. међу њима се налазе сви могући остаци, и то по једном. Између осталог, и јединица је међу њима, тј. постоји тачно један број $b\in\{0,1,\ldots,n-1\}$ такав да је $ab\equiv 1 \pmod n$.

Дефиниција 4.7. Нека су a и $n>0$ узајамно прости цели бројеви. Цео број b такав да је $ab\equiv 1 \pmod n$ (заправо, његова класа остатака) зове се *мултипликативни инверз* броја a по модулу n. У појединим контекстима за њега се користи ознака a^{-1}.

Пример 4.9. Испишимо мултипликативне инверзе бројева $1,2,3,4,5,6,7,8,9,10$ по модулу 11:

$$1^{-1}\equiv 1,\quad 2^{-1}\equiv 6,\quad 3^{-1}\equiv 4,\quad 4^{-1}\equiv 3,\quad 5^{-1}\equiv 9,\quad 6^{-1}\equiv 2,\quad 7^{-1}\equiv 8,\quad 8^{-1}\equiv 7,\quad 9^{-1}\equiv 5,\quad 10^{-1}\equiv 10.$$

Овако се бројеви $2,3,\ldots,9$ деле у парове $\{2,6\},\{3,4\},\{5,9\},\{7,8\}$, при чему је у сваком пару неки број и његов инверз, тј. производ је конгруентан 1 (mod 11).

Ако је нзд$(a,n)=1$, на основу тврђења 4.2(а) постоје цели бројеви x и y такви да је $ax+ny=1$. Тада је $ax\equiv 1 \pmod n$, тј. x је мултипликативни инверз броја a по модулу n.

Пример 4.10. Нађимо мултипликативни инверз броја 358 по модулу 997 Еуклидовим алгоритмом:

$$\begin{aligned}
281 &= && && 997-2\cdot 358\\
77 &= 358-1\cdot 281 &&= 358-(997-2\cdot 358) &&= -997+3\cdot 358\\
50 &= 281-3\cdot 77 &&= (997-2\cdot 358)-3(-997+3\cdot 358) &&= 4\cdot 997-11\cdot 358\\
27 &= 77-1\cdot 50 &&= (-997+3\cdot 358)-(4\cdot 997-11\cdot 358) &&= -5\cdot 997+14\cdot 358\\
23 &= 50-1\cdot 27 &&= (4\cdot 997-11\cdot 358)-(-5\cdot 997+14\cdot 358) &&= 9\cdot 997-25\cdot 358\\
4 &= 27-1\cdot 23 &&= (-5\cdot 997+14\cdot 358)-(9\cdot 997-25\cdot 358) &&= -14\cdot 997+39\cdot 358\\
3 &= 23-5\cdot 4 &&= (9\cdot 997-25\cdot 358)-5(-14\cdot 997+39\cdot 358) &&= 79\cdot 997-220\cdot 358\\
1 &= 4-1\cdot 3 &&= (-14\cdot 997+39\cdot 358)-(79\cdot 997-220\cdot 358) &&= -93\cdot 997+259\cdot 358
\end{aligned}$$

Према томе, $358^{-1}\equiv 259 \pmod{997}$. (Уједно је и $997^{-1}\equiv -93 \pmod{358}$.)

4.4. Експоненцијалне конгруенције

У овом одељку посматраћемо низ степена неког броја a по модулу n, где су a и n узајамно прости:

$$1,a,a^2,a^3,a^4,\ldots \pmod n$$

Тај низ је бесконачан, те се нека вредност мора поновити. Онда се морају поновити и следећа и све наредне, а такође и све претходне. Долазимо до следећег закључка.

Тврђење 4.9. Нека су a и n $(n>0)$ узајамно прости цели бројеви. Тада постоји природан број d такав да је

$$a^d\equiv 1 \pmod n.$$

Низ $1,a,a^2,\ldots$ је периодичан по модулу n са периодом d. Другим речима, $a^{i+d}\equiv a^i \pmod n$.

Доказ. Нека је $a^k\equiv a^m \pmod n$ за неке $k<m$. Пошто је a^k узајамно просто са n, ову конгруенцију можемо поделити са a^k: дакле, $a^{m-k}\equiv 1$.

Ако је $a^d\equiv 1 \pmod n$, множењем са a^i одмах следи да је $a^{i+d}\equiv a^i \pmod n$. Према томе, након првог понављања остатка 1 низ постаје периодичан. □

Дефиниција 4.8. За дате узајамно просте a и $n>0$, *мултипликативни поредак* (или само *поредак*) броја a по модулу n је најмање $d\in\mathbb{N}$ за које је $a^d\equiv 1 \pmod n$, тј. најмањи период низа $1,a,a^2,\ldots$ по модулу n.

Пример 4.11. Низ $1,2,2^2,2^3,\ldots$ по модулу 73 даје редом остатке $1,2,4,8,16,32,64,55,37,1,\ldots$ Почев од прве поновне појаве јединице он се периодично понавља, те је његов најмањи период 9 - тј. поредак броја 2 по модулу 73 је једнак 9.

Пример 4.12. Доказати да је (а) a^2-1 дељиво са 8, (б) a^4-1 дељиво са 16 за све непарне бројеве a.

Решење. (а) У растављању $a^2-1=(a-1)(a+1)$ чиниоци $a+1$ и $a-1$ су два узастопна парна броја, па је бар један од њих дељив и са 4. Следи да је a^2-1 дељиво са 8.

(б) Пошто је $a^4-1=(a^2-1)(a^2+1)$, при чему је a^2-1 дељиво са 8 а a^2+1 је парно, следи да $16\mid a^4-1$.

На основу тврђења 4.9, $a^k \equiv 1 \pmod{n}$ важи ако и само ако је k дељиво поретком броја a по модулу n.

Следећа два тврђења дају једну вредност d из тврђења 4.9, али не обавезно најмању.

Тврђење 4.10 (Фермаова[5] теорема). Ако је p произвољан прост број и a цео број који није дељив са p, онда је

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

Доказ. Скуп $\{1, 2, \ldots, p-1\}$ је сведен систем остатака по модулу p.

Скуп $\{a, 2a, \ldots, (p-1)a\}$ је такође сведен систем остатака по модулу p. Према томе,

$$a^{p-1}(p-1)! = a \cdot (2a) \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) = (p-1)! \pmod{p}.$$

Скраћивањем израза $(p-1)!$ (будући узајамно простог са p) следи $a^{p-1} \equiv 1 \pmod{p}$. □

Фермаова теорема се понекад зове „Малом" Фермаовом теоремом, како се не би побркала са чувеном „Великом Фермаовом теоремом":

- Ако је $n \geqslant 3$ природан број, једначина $x^n + y^n = z^n$ нема решења у природним бројевима.

„Велика" теорема заправо није баш Фермаова, пошто је његов наводни доказ (оставио нас је само с познатом напоменом: „Нашао сам прелеп доказ, али не може да стане на ову маргину") готово сигурно био погрешан. Доказана је тек 1995. после вишевековних напора који су водили заснивању и развоју читавих нових грана математике, али то је већ друга прича.

Општије тврђење за сложене модуле гласи овако.

Тврђење 4.11 (Ојлерова теорема). Ако је n природан број и a цео број узајамно прост са n, онда је

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

Доказ. Аналогно доказу Фермаове теореме. □

Следеће тврђење је директна последица Ојлерове теореме.

Тврђење 4.12. Поредак целог броја a по модулу $n \in \mathbb{N}$ је делилац броја $\varphi(n)$. □

Пример 4.13. По Ојлеровој теореми поредак сваког непарног броја по модулу 16 дели $\varphi(16) = 8$.

У примеру 4.12 је, међутим, доказано и више од тога: поредак по модулу 16 увек дели 4.

4.5. Уводна криптографија

Познати математичар Харди[6], специјализован за теорију бројева, једном је написао: „Теорија бројева се одувек сматра једном од најочигледније бескорисних грана математике." У наставку је, међутим, овако објаснио израз „бескорисна":

> „Науку зовемо *корисном* ако њен развој подстиче постојеће разлике у расподели богатства, или још директније потпомаже уништавање људског живота. Ја никад нисам урадио ништа корисно. Моја открића нису ни на који начин утицала, а вероватно и неће, на устројство цивилизације.

Харди се вероватно ни данас не би предомислио, јер изгледа да све што би нам могло чинити добро, може се искористити и да нам нашкоди. Ипак, у једном је погрешио: данас и теорија бројева има примене, најпре у криптографији.

Криптографија изучава начине скривања информација, тј. шифровања поруке како би се заштитила од нежељених погледа. Онај коме је порука намењена мора да има *кључ за дешифровање*. Јасно је колико је у рату то важно, али и интернет је без тога незамислив: на пример, ако шаљете број кредитне картице, циљ криптографије је да га шифрује тако да само трговац може да га прочита.

Може се смислити много начина да се порука шифрује. Један од најједноставнијих је *Цезарова шифра*, позната још Јулију Цезару - свако слово се замени неким другим словом: на пример, заменимо свако слово А са Ц, Б са М, итд. Тај метод није нарочито добар: ако је порука иоле

[5] Pierre de Fermat (1607?-1665), француски адвокат; аматерски се бавио математиком и прославио у њој
[6] Godfrey Harold Hardy (1877-1947), енглески математичар

дужа, статистичка анализа би разбила шифру (нпр. у српском језику је најчешће слово А, а у поруци има много слова Џ...).

Свакако, слова можете да претворите у бројеве. На пример, словима А,Б,В,...,Ш могу да одговарају бројеви $1, 2, 3, \ldots, 30$. На тај начин свакој словној поруци одговара неки број. Зато надаље све поруке сматрамо бројевима. Ако је порука предугачка, увек је можемо раставити на делове.

Следећи пример даје једноставан начин шифровања бројевних порука помоћу кључа.

Пример 4.14. Претпоставимо да желите да трговцу пошаљете поруку (број ваше картице) која гласи

$$m = 4444333322223333.$$

Договорићете се да користите прост број $p = \boxed{27873875078709719}$ и фактор $a = \boxed{123456}$. Трговцу уместо броја m шаљете вредност $x = a \cdot m \pmod{p}$. Тако шифрована порука гласи

$$x = 123456 \cdot 4444333322223333 \pmod{27873875078709719} = \boxed{10257579081690052}.$$

Да би је дешифровао, трговцу је довољно да нађе инверз a^{-1} броја a по модулу p. Тада је $m = a^{-1} \cdot x \pmod{p}$.

У претходном примеру бројеви p и a представљају *кључ*. Ако и неко трећи зна кључ, ваше поруке више нису безбедне.

Дакле, све ове методе прати један озбиљан проблем - ако умете да шифрујете, умете и да дешифрујете. Ако неко ухвати поруку у којој се с трговцем договарате о методу шифровања, има све што му је потребно да вам направи невољу. Зато нам треба метод шифровања који не одаје кључ. Тако би трговац могао и да га објави у новинама, а да ипак само он може да дешифрује. То би се звало *криптографија с јавним кључем*.

Најједноставнији методи шифровања с јавним кључем користе експоненцијалне конгруенције. Пример који следи је једна имплементација *Дифи-Хелманове размене кључа*.

Нека је p прост број. Познато је (мада доказ није тежак, овог пута ћу га прескочити) да постоји број g чији је поредак по модулу p тачно $p-1$ - ово g се зове *примитиван корен*. То значи да низ $1, g, g^2, \ldots, g^{p-2}$ чини сведен систем остатака по модулу p.

- Анка и Бранка се јавно договоре да користе велики прост број p и примитиван корен g.
- Анка бира тајни број a и шаље Бранки број $A = g^a$ по модулу p.
- Бранка бира тајни број b и шаље Анки број $B = g^b$ по модулу p.
- Сада и Анка и Бранка знају број $x = g^{ab} = A^b = B^a$ по модулу p. То је њихов *тајни кључ*.

Бројеви p, g, $g^a \pmod{p}$ и $g^b \pmod{p}$ чине *јавни кључ*. С друге стране, није познат ниједан алгоритам који на основу ових вредности ефикасно проналази тајни кључ x. Овај кључ Анка и Бранка убудуће могу да користе да шифрују и дешифрују своје поруке.

Пример 4.15. Јавне бројеве ћемо уоквирити. Разгласићемо наш избор бројева p и g:

$$\boxed{p = 294017833605229} \quad \text{и} \quad \boxed{g = 2}.$$

(Питање: како бисте најлакше проверили да g заиста јесте примитиван корен по модулу p?).

Анка и Бранка бирају тајне бројеве $a = 156367924220121$ и $b = 65463550869546$, али једна другој шаљу бројеве

$$\left\{ \begin{array}{l} 2^a \equiv \boxed{A = \ \ 74364004319478} \\ 2^b \equiv \boxed{B = 115408895971512} \end{array} \right\} \pmod{294017833605229}.$$

Број a зна само Анка, број b само Бранка, те тајни кључ x могу да нађу само њих две:

$$115408895971512^a \equiv 74364004319478^b \equiv x = 270641540063119 \pmod{294017833605229}.$$

Следећи метод шифровања с јавним кључем, познат као *RSA алгоритам*, описан је 1977. и данас је у широкој употреби.

- Трговац одабере два огромна проста броја p и q, које ће чувати у тајности, и помножи их: $n = pq$. Он сада зна и број $\varphi(n) = (p-1)(q-1)$.
- Трговац бира број e узајамно прост са $\varphi(n)$ и израчунава инверз $d = e^{-1}$ по модулу $\varphi(n)$.

- Трговац обзнањује *јавни кључ*: бројеве n и e. Његов *тајни кључ* је број d, који чува у тајности.
- Ако је број купчеве кредитне картице x $(x < n)$, он шаље трговцу број $m \equiv x^e \pmod{n}$.

Знајући m, трговац лако налази број x: пошто је $de \equiv 1 \pmod{\varphi(n)}$, важи $m^d \equiv x^{de} \equiv x \pmod{n}$.

С друге стране, да би хакер дешифровао поруку, неопходан му је тајни кључ d, а њега може наћи само ако зна $\varphi(n)$. Да би, пак, дошао до вредности $\varphi(n)$, он мора да растави број n на просте чиниоце p и q, што је веома тешко.

Пример 4.16. Рецимо да купац има поруку $x = 4444333322223333$ (нпр. његов број картице). Трговац бира (у пракси недовољно велике) просте бројеве $p = 113309689$ и $q = 4302205157$. Тада је

$$\boxed{n = 487481528353866173}$$
$$\varphi(n) = 487481523938351328 = 2^5 \cdot 3 \cdot 37 \cdot 113 \cdot 127601 \cdot 9518153.$$

Даље ће одабрати $\boxed{e = 65537 = 2^{16} + 1}$. Бројеви n и e су јавни.

Пошто трговац зна број $\varphi(n)$, инверз d броја e по модулу $\varphi(n)$ наћи ће Еуклидовим алгоритмом:

$$d = 65537^{-1} \pmod{487481523938351328} = 230772148254991073.$$

Купац му шаље шифровану поруку m:

$$4444333322223333^{65537} \equiv \boxed{m = 324982529177796209} \pmod{487481528353866173}.$$

Само трговац може лако да одреди x: $x \equiv m^d \pmod{n}$. Нико други нема тајни кључ d.

У неким случајевима RSA-алгоритам је подложан хакерским нападима. На пример, у пракси порука често почиње или се завршава на неки предвидљив начин (нпр. „Ваша екселенцијо", „Извештај" итд.), што шифру чини рањивом. Зато се порука по правилу допуњује неким безвезним текстом (то се на енглеском зове padding).

Главно је да прости бројеви p и q буду *заиста* велики - да имају по више стотина цифара. Ако их не одаберемо добро, неко би могао да растави број n на просте чиниоце у реалном времену. На пример, у следећим случајевима су познати ефикасни напади на шифру:

- Ако су p и q међусобно блиски ($|p - q| < 2n^{1/4}$) или бројеви $p - 1$ и $q - 1$ имају мале просте делиоце, постоје алгоритми који значајно олакшавају факторизацију броја n.
- Не смемо да допустимо да буде $x^e < n$ (ако је $m = x^e$, хакер има лак посао).
- Ако је број d мали ($d < \frac{1}{3}n^{1/4}$) и $p < q < 2p$, постоје ефикасни алгоритми који налазе d.
- Мада није познато да одабир малог e (нпр. $e = 3$) представља проблем, чест избор је $e = 65537$.

4.6. Задаци

1. Ако је $p > 5$ прост број, доказати да је један од бројева $p^2 + 4$ и $p^2 + 6$ дељив са 5.
2. Написати канонску факторизацију броја (а) 20!; (б) $\binom{20}{10}$.
3. Колико је $\varphi(\varphi(\varphi(5^{10})))$?
4. Колико делилаца (међу природним бројевима) има број 2520?
5. Који је највећи експонент n такав да је 100! дељиво са 12^n?
6. Наћи све парове природних бројева x, y за које важи $xy = 9x - 3y + 1$.
7. Израчунати нзд$(8n + 3, 13n + 5)$, где је $n = 2^{100}$.
8. Наћи бар један природан број N такав да су сви бројеви $N, N+1, N+2, \ldots, N+1000$ сложени.
9. Доказати да за све природне бројеве a и b важи нзд$(a, b) \cdot$ нзс$(a, b) = a \cdot b$.
10. Решити једначину $25x - 36y = 7$ у скупу целих бројева.
11. Наћи мултипликативне инверзе бројева 15, 16 и 17 по модулу 1001.
12. Ако су a и b природни бројеви и $5a + 7b$ је дељиво са 43, доказати да је и $4a - 3b$ дељиво са 43.

13. (а) Ако је $n > 4$ сложен број, доказати да $n \mid (n-1)!$.

    (б) *(Вилсонова[7] теорема)* Ако је p прост број, доказати да важи $(p-1)! \equiv -1 \pmod{p}$.

14. (а) Ако $m \mid n$, доказати да $a^m - 1 \mid a^n - 1$ за сваки цео број a.

    (б) Ако је број $2^n - 1$ прост, доказати да и број n мора бити прост.

15. Нка је p прост број. Ако је $x \equiv y \pmod{p}$, доказати да је $x^p \equiv y^p \pmod{p^2}$.

16. Проверити да ли је број $2^{561} - 2$ дељив са 561. (Број $561 = 3 \cdot 11 \cdot 17$ је сложен.)

17. Која је последња цифра броја $3^{3^{3^3}}$?

18. Наћи поредак броја 5 по модулу 263.

19. Постоји ли природан број n такав да је $2^n + 1$ дељиво са 247?

4.7. Решења

1. Број p, будући прост, даје неки од остатака $1, 2, 3, 4$ при дељењу са p.
   - Ако је $p \equiv 1$ или $p \equiv 4 \pmod{5}$, онда је $p^2 \equiv 1 \pmod{5}$, па $5 \mid p^2 + 4$.
   - Ако је $p \equiv 2$ или $p \equiv 3 \pmod{5}$, онда је $p^2 \equiv 4 \pmod{5}$, па $5 \mid p^2 + 6$.

2. (а) $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

   (б) $\binom{20}{10} = \frac{20!}{10!^2}$, при чему канонску факторизацију $20!$ знамо, а $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.
   Дељењем $20!$ са $10!^2$ добијамо $\binom{20}{10} = 2^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

3. Користимо тврђење 4.7. Као прво,
$$\varphi(5^{10}) = 5^{10} \cdot \tfrac{4}{5} = 2^2 \cdot 5^9.$$
   Даље је
$$\varphi(2^2 \cdot 5^9) = 2^2 \cdot 5^9 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} = 2^3 \cdot 5^8 \quad \text{и} \quad \varphi(2^3 \cdot 5^8) = 2^3 \cdot 5^8 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} = 2^4 \cdot 5^7.$$
   Дакле, $\varphi(\varphi(\varphi(5^{10}))) = 2^4 \cdot 5^7$.

4. Канонска факторизација броја 2520 је $2^3 \cdot 3^2 \cdot 5 \cdot 7$. Делиоци овог броја не могу имати просте факторе различите од $2, 3, 5, 7$.

   На колико начина можемо изабрати експоненте $a, b, c, d \geqslant 0$ тако да
$$2^a \cdot 3^b \cdot 5^c \cdot 7^d \quad \text{буде делилац броја} \quad 2^3 \cdot 3^2 \cdot 5 \cdot 7?$$
   Мора бити $a \leqslant 3$, $b \leqslant 2$, $c \leqslant 1$ и $d \leqslant 1$; дакле, a се може одабрати на 4 начина. b на 3, c на 2, и d на 2. Укупно има $4 \cdot 3 \cdot 2 \cdot 2 = 48$ могућности, те је одговор 48.

5. Пошто је $12 = 2^2 \cdot 3$, потребно је одредити с којим степеном се двојке и тројке појављују у канонској факторизацији броја $100! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 100$.

   – Међу чиниоцима $1, 2, \ldots, 100$ има $\lfloor \frac{100}{2} \rfloor = 50$ парних, који дају 50 двојки;
   – њих $\lfloor \frac{100}{2^2} \rfloor = 25$ је дељиво и са 2^2, и они додају још 25 двојки;
   – њих $\lfloor \frac{100}{2^3} \rfloor = 12$ је дељиво и са 2^3, и они додају 12 нових двојки, итд.
   Укупно налазимо $50 + 25 + 12 + 6 + 3 + 1 = 97$ двојки у канонској факторизацији броја $100!$.

   Слично, имаћемо $\lfloor \frac{100}{3} \rfloor + \lfloor \frac{100}{3^2} \rfloor + \lfloor \frac{100}{3^3} \rfloor + \lfloor \frac{100}{3^4} \rfloor = 33 + 11 + 3 + 1 = 48$ тројки.

   Све у свему, $100! = 2^{97} \cdot 3^{48} \cdots = 12^{48} \times$ (нешто што није дељиво са 3), па је одговор $n = 48$.

6. Изразимо y преко x:
$$y = \frac{9x+1}{x+3} = 9 - \frac{26}{x+3}.$$
   Дакле, $x + 3$ мора да дели број 26 (и веће је од 3), а то је могуће само ако је $x + 3 = 13$ или 26. То нам даје $x = 10$ или $x = 23$. Одговарајуће вредности y су 7 и 8.

   Дакле, једина решења (x, y) су $(10, 7)$ и $(23, 8)$.

[7] John Wilson (1741-1793), енглески математичар; формулисао је ову теорему, али је није доказао

7. Применићемо Еуклидов алгоритам:

$$\begin{aligned} 13n+5 &= 1\cdot(8n+3)+(5n+2),\\ 8n+3 &= 1\cdot(5n+2)+(3n+1),\\ 5n+2 &= 1\cdot(3n+1)+(2n+1),\\ 3n+1 &= 1\cdot(2n+1)+n,\\ 2n+1 &= 2\cdot n+\boxed{1}. \end{aligned}$$

Дакле, тражени НЗД је 1. Дата вредност $n=2^{100}$ је била потпуно ирелевантна.

8. Може ли $N=1002!+2$?

За свако $i=0,1,2,\ldots,1000$, број $N+i=1002!+(i+2)$ је дељив са $i+2$. Заиста, $1002!$ је дељиво свим бројевима од 2 до 1002, укључујући и $i+2$.

9. Подсетимо се тврђења 4.4. На основу њега је

$$\text{нзд}(a,b)\cdot\text{нзс}(a,b)=\prod_{i=1}^{k}p_i^{\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}}=\prod_{i=1}^{k}p_i^{\alpha_i+\beta_i}=a\cdot b,$$

јер је експонент $\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}$ једнак $\alpha_i+\beta_i$ - заиста, један од ова два сабирка је α_i, а други је β_i (у зависности од тога који је већи).

10. Циљ нам је да нађемо све целе бројеве y за које је $11y\equiv 36y\equiv -7 \pmod{25}$, што радимо овако: ако са 11^{-1} означимо инверз броја 11 по модулу 25, онда множењем са 11^{-1} имамо

$$y\equiv 11y\cdot 11^{-1}\equiv -7\cdot 11^{-1} \pmod{25}.$$

Тражимо $11^{-1} \pmod{25}$. Користићемо Еуклидов алгоритам:

$$\begin{aligned} 25=2\cdot 11+3 \quad &\Rightarrow \quad 3=25-2\cdot 11,\\ 11=3\cdot 3+2 \quad &\Rightarrow \quad 2=11-3(25-2\cdot 11)=7\cdot 11-3\cdot 25,\\ 3=2+1 \quad &\Rightarrow \quad 1=3-2=(25-2\cdot 11)-(7\cdot 11-3\cdot 25)=4\cdot 25-9\cdot 11. \end{aligned}$$

Дакле, $11\cdot(-9)\equiv 1 \pmod{25}$, тј. $11^{-1}\equiv -9 \pmod{25}$. Најзад, $y\equiv -7\cdot(-9)=63\equiv 13 \pmod{25}$.

Следи да је $y=25t+13$ за неко $t\in\mathbb{Z}$, одакле из $25x=36y+7=36(25t+13)+7=900t+475$ налазимо $x=36t+19$. Опште решење (x,y) је $(36t+19,25t+13)$.

11. Услови $43\mid 5a+7b$ и $43\mid 4a-3b$ су редом еквивалентни са $7b\equiv -5a \pmod{43}$ и $3b\equiv 4a \pmod{43}$, Испитајмо да ли из првог услова обавезно следи други.

Дато нам је $7b\equiv -5a \pmod{43}$, а множењем са $7^{-1}\equiv -6 \pmod{43}$ добијамо $b\equiv(-6)(-5)a=30a \pmod{43}$. Следи да је $3b\equiv 90a\equiv 4a \pmod{43}$. Доказ је завршен.

12. Веома инспиративно. Одговори су $15^{-1}\equiv 267$, $16^{-1}\equiv 438$ и $17^{-1}\equiv 530 \pmod{1001}$.

13. (а) Ако је n сложен број, онда је $n=ab$ за неке бројеве $2\leqslant a<b<n-1$.
Број $(n-1)!=1\cdot 2\cdot\ldots\cdot a\cdot\ldots\cdot b\cdot\ldots\cdot(n-2)(n-1)$ је очигледно дељив са $a\cdot b=n$.

(б) Као што је показано у примеру 4.9, бројеви $2,3,\ldots,p-2$ се деле у парове, при чему је у сваком пару неки број и његов инверз. Производ бројева у сваком пару је $1 \pmod p$. Закључујемо да је $2\cdot 3\cdots(p-2)=(p-2)!\equiv 1 \pmod p$. Множењем са $p-1\equiv -1 \pmod p$ најзад добијамо $(p-1)!\equiv -1 \pmod p$.

14. (а) Нека је $n=k\cdot m$. Тада је $a^n=(a^m)^k\equiv 1^k=1 \pmod{a^m-1}$, тј. $a^m-1\mid a^n-1$.

(б) Ако је број n сложен, он има делиоца m $(1<m<n)$, па је по делу (а) број 2^m-1 делилац броја 2^n-1 (различит од јединице и њега самог).

15. Из $x\equiv y \pmod p$ следи да је $x-y$ дељиво са p, а и количник $\frac{x^p-y^p}{x-y}$ је дељив са p, јер је

$$\frac{x^p-y^p}{x-y}=x^{p-1}+x^{p-2}y+x^{p-3}y^2+\cdots+y^{p-1}\equiv x^{p-1}+x^{p-2}x+x^{p-3}x^2+\cdots+x^{p-1}=px^{p-1}\equiv 0 \pmod p.$$

Према томе, $x^p-y^p=(x-y)\cdot\frac{x^p-y^p}{x-y}$ је дељиво са p^2, тј. $x^p\equiv y^p \pmod{p^2}$.

16. По Малој Фермаовој теореми имамо:
- $2^2\equiv 1 \pmod 3 \Rightarrow 2^{560}\equiv 1^{280}=1 \pmod 3$;

- $2^{10} \equiv 1 \pmod{11} \Rightarrow 2^{560} \equiv 1^{56} = 1 \pmod{11}$;
- $2^{16} \equiv 1 \pmod{17} \Rightarrow 2^{560} \equiv 1^{35} = 1 \pmod{17}$.

Према томе, $2^{560} - 1$ је дељиво са $3 \cdot 11 \cdot 17 = 561$, а самим тим $561 \mid 2^{561} - 2 = 2(2^{560} - 1)$.

17. По модулу 10 низ $1, 3, 3^2, 3^3, \ldots$ има период 4: $1, 3, 9, 7, 1, 3, 9, 7, \ldots$. Према томе, задња цифра броја 3^n (где је $n = 3^{3^3}$) зависи само од остатка броја n при дељењу са 4. У нашем случају је $n \equiv (-1)^{3^3} = -1 \equiv 3 \pmod{4}$, па је $3^n \equiv 3^3 \equiv 7 \pmod{10}$, тј. последња цифра је 7.

18. Број 263 је прост. По тврђењу 4.12, поредак броја 5 по модулу 263 дели $\varphi(263) = 262 = 2 \cdot 131$, чији су једини делиоци 1, 2, 131 и 262. Поредак очито није 1 или 2. Проверимо 131:

$$5^4 \equiv 99, \quad 5^8 \equiv 70, \quad 5^{16} \equiv 166, \quad 5^{32} \equiv 204, \quad 5^{64} \equiv 62, \quad 5^{128} \equiv 162, \quad 5^{131} \equiv -1 \pmod{263}.$$

Добили смо да ни 131 није тражени поредак, тако да је одговор 262.

19. Број $247 = 13 \cdot 19$ је сложен. Проверимо када је $2^n + 1$ дељиво са 13, а када са 19.

- По модулу 13 низ степена двојке је $1, 2, 4, 8, 3, 6, \boxed{12}, 11, 9, 5, 10, 7, 1, \ldots$, с периодом 12. Видимо да $13 \mid 2^n + 1$ ако и само ако је $n \equiv 6 \pmod{12}$.
- По модулу 19 низ степена двојке је $1, 2, 4, 8, 16, 13, 7, 14, 9, \boxed{18}, 17, 15, 11, 3, 6, 12, 5, 10, 1, \ldots$, с периодом 18, те $19 \mid 2^n + 1$ ако и само ако је $n \equiv 9 \pmod{18}$.

Међутим, ниједан број n не задовољава истовремено $n \equiv 6 \pmod{12}$ и $n \equiv 9 \pmod{18}$ (из прве конгруенције следи да је n парно, а из друге да је непарно), па тражено n не постоји.