ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿՐԹՈՒԹՅԱՆ ԵՎ ԳԻՏՈՒԹՅԱՆ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ՀԱՅԱՍՏԱՆԻ ՊԵՏԱԿԱՆ ՃԱՐՏԱՐԱԳԻՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆԻ
(ՊՈԼԻՏԵԽՆԻԿ)
ԳՈՐԻՍԻ ՄԱՍՆԱՃՅՈՒՂ

Մաթեմատիկայի ամբիոն

ԹՎԵՐԻ ՏԵՍՈՒԹՅՈՒՆ ԽՆԴԻՐՆԵՐԻ ԵՎ ՎԱՐԺՈՒԹՅՈՒՆՆԵՐԻ ԺՈՂՈՎԱԾՈՒ

Ուսումնական ձեռնարկ

ԵՐԵՎԱՆ 2005

ՀՏԴ 517, 53

Կազմողներ՝ Յու. Սաֆարյան
Հ. Մալինցյան:

Թվերի տեսություն: Խնդիրների և վարժությունների ժողովածու: / Հայաստանի Պետական ճարտարագիտական Համալսարան: Երևան: 2005թ.:

Տրված են խնդիրներ և վարժություններ թվերի տեսությունից, դրանց տեսական հիմնավորումները, ցուցումներ կատարման համար:
Նախատեսված է ՀՊՃՀ ուսանողների համար:

Գրախոս՝ Վ.Ռ. Նարինյան

Մասնագետ խմբագիր՝ Վ. Կ. Վարդազարյան
Խմբագիր՝ Հ. Ց. Պետրոսյան

ՆԵՐԱԾՈՒԹՅՈՒՆ

Ուսումնական ձեռնարկում ընդգրկված խնդիրները և վարժությունները կազմված են "Թվերի տեսություն" առարկայական ծրագրին համապատասխան: Ձեռնարկը նպատակ ունի լրացնելու այդ դասընթացից հայերեն լեզվով խնդրագրքի պակասը: Բերված է խնդիրների լուծման համար անհրաժեշտ տեսական նյութը: Պատասխանների բաժինը լրացված է որոշ խնդիրների լուծումներով և ցուցումներով:

1. ԱՄԲՈՂՋ ԹՎԵՐԻ ԲԱԺԱՆԵԼԻՈՒԹՅՈՒՆԸ: ՄՆԱՑՈՐԴՈՎ ԲԱԺԱՆՈՒՄ:

Հետագայում տառերով նշանակված են միայն ամբողջ թվերի Z բազմության տարրերը: Մենք հստակ կնշենք այն դեպքերը, երբ տառերով նշանակված են նաև ոչ ամբողջ թվեր: a և b ամբողջ թվերի $a+b$ գումարը, $a-b$ տարբերությունը և ab արտադրյալը նույնպես ամբողջ թվեր են, իսկ a թիվը b թվի վրա բաժանումից ստացված քանորդը (եթե $b \neq 0$) կարող է լինել ինչպես ամբողջ, այնպես էլ ոչ ամբողջ թիվ: Երբ $\frac{a}{b}$ քանորդն ամբողջ թիվ է, նշանակելով այն q, կունենանք $a = bq$, և կարող ենք ասել, որ a-ն բաժանվում է b-ի $(a \vdots b)$, կամ b-ն բաժանում է a-ին $(b|a)$: Այդ դեպքում a-ն կոչվում է b-ի բազմապատիկ, իսկ b-ն՝ a-ի բաժանարար: Եթե b-ն a-ի բաժանարար չէ, ապա կգրենք $(b \nmid a)$: Ընդհանուր դեպքում տեղի ունի հետևյալ թեորեմը մնացորդով բաժանման մասին՝ ցանկացած a և b ամբողջ թվերի համար $(b \neq 0)$ գոյություն ունեն միակ ձևով որոշվող այնպիսի q և r թվեր, երբ $a = bq + r$, ընդ որում՝ $q \in Z$, $0 \leq r < |b|$:

q-ն կոչվում է թերի քանորդ, իսկ r-ը՝ մնացորդ, որոնք ստացվում են a-ն b-ի վրա բաժանելիս: $r = 0$ դեպքում "քանորդ" և "թերի քանորդ" հասկացությունները համընկնում են:

Եթե b-ն ևս ամբողջ թիվ է և $b \neq 0$, ապա $a = bq + r$, որտեղ $q \in Z$, $0 \leq r < |b|$:

1.1 Կատարել a թվի մնացորդով բաժանում b-ի վրա, եթե.

1) a=134, b=26; 2) a=134, b=-26; 3) a=-134, b=26
4) a=-134, b=-26; 5) a=168, b=35; 6) a=134, b=-35
7) a=-168, b=35; 8) a=-168, b=-35:

1.2 a թիվը որևէ b դրական թվի վրա բաժանելիս քանորդում ստացվել է q: Գտնել b բաժանարարը և r մնացորդը, եթե.

1) a=42157, q=231; 2) a=534, q=26; 3) a=-945, q=-16:

1.3 Ցույց տալ, որ եթե $mn+pq$ թիվը բաժանվում է $(m-p)$-ի վրա, ապա նաև $mq+np$ թիվը բաժանվում է $(m-p)$-ի վրա ($m,n,p,q \in Z$):

1.4 Ցույց տալ, որ եթե հնգանիշ թիվը բաժանվում է 41-ի, ապա բոլոր այն թվերը, որոնք ստացվում են այդ թվից թվանշանների շրջանաձև տեղափոխության արդյունքում, նույնպես կբաժանվեն 41-ի:

1.5 Ցույց տալ, որ ցանկացած n բնական թվի դեպքում $n \cdot (n^2 + 5)$ թիվը բաժանվում է 6-ի վրա:

1.6 Ցույց տալ, որ եթե կոտորակի համարիչը երկու կենտ թվերի քառակուսիների տարբերություն է, իսկ հայտարարը՝ նույն թվերի քառակուսիների գումար, ապա այդպիսի կոտորակը միշտ կրճատվում է 2-ով, բայց չի կրճատվում 4-ով:

1.7 a^5 թիվը $(a \in N)$ 7-ի բաժանելիս մնացորդը հավասար է 5: Ինչի՞ է հավասար a թիվը 7-ի բաժանելուց ստացված մնացորդը:

2. ԱՄԵՆԱՄԵԾ ԸՆԴՀԱՆՈՒՐ ԲԱԺԱՆԱՐԱՐ ԵՎ ԱՄԵՆԱՓՈՔՐ ԸՆԴՀԱՆՈՒՐ ԲԱԶՄԱՊԱՏԻԿ

l թիվը կոչվում է $a,b,...,c$ թվերի ընդհանուր բաժանարար, եթե l/a, l/b,..., l/c:

Ընդհանուր բաժանարարներից ամենամեծը կոչվում է ամենամեծ ընդհանուր բաժանարար և նշանակվում է $d=(a,b, ..., c)$:

Եթե $(a, b, ..., c)=1$, ապա $a, b, ..., c$ թվերը կոչվում են փոխադարձ պարզ: Եթե $a, b, ..., c$ թվերից յուրաքանչյուրը փոխադարձ պարզ է մնացած թվերից յուրաքանչյուրի հետ, ապա $a, b, ..., c$ թվերը կոչվում են զույգ առ զույգ փոխադարձ պարզ:

Երկու թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու համար օգտագործվում է էվկլիդեսի ալգորիթմը, որը հետևյալն է.

Եթե a և b բնական թվեր են, և $a>b$, ապա՝

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1 q_2 + r_2,\ 0 < r_2 < r_1,$$
$$r_1 = r_2 q_3 + r_3,\ 0 < r_3 < r_2,$$
$$\dots\dots\dots\dots\dots\dots$$
$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 < r_n < r_{n-1},$$
$$r_{n-1} = r_n q_{n+1},\ r_{n+1} = 0:$$

Զրոյից տարբեր վերջին r_n մնացորդը a և b թվերի ամենամեծ ընդհանուր բաժանարարն է՝ $r_n = (a,b)$:

k թիվը կոչվում է $a, b, \dots, c$ թվերի ընդհանուր բազմապատիկ, եթե $a|k, b|k, \dots, c|k$:

Ամենափոքր դրական ընդհանուր բազմապատիկը կոչվում է ամենափոքր ընդհանուր բազմապատիկ և նշանակվում է $m=[a, b, \dots, c]$:

a և b թվերի բոլոր ընդհանուր բազմապատիկների ընդհանուր տեսքը տրվում է $M = \frac{ab}{d}t$ հավասարությամբ, որտեղ t-ն ամբողջ թիվ է, իսկ $d=(a, b)$:

$t=1$ դեպքում կստանանք a և b թվերի ամենափոքր ընդհանուր բազմապատիկը՝

$$m = \frac{ab}{d}, \text{ կամ } [a,b] = \frac{ab}{(a,b)}:$$

Զույգ առ զույգ փոխադարձ պարզ թվերի ամենափոքր ընդհանուր բազմապատիկը հավասար է նրանց արտադրյալին: Ամենամեծ ընդհանուր բաժանարար և ամենափոքր ընդհանուր բազմապատիկ գտնելը, թվերը պարզ արտադրիչների վերածելու միջոցով, հայտնի է դպրոցական դասընթացից:

2.1 Էվկլիդեսի ալգորիթմով գտնել հետևյալ թվերի ամենամեծ ընդհանուր բաժանարարը.

1) 546 և 231; 2) 1001 և 6600; 3) 1517 և 2257;
4) 2737, 9163 և 9639; 5) 1411, 4641 և 5253:

2.2 Պարզ արտադրիչների վերլուծությամբ գտնել հետևյալ թվերի ամենափոքր ընդհանուր բազմապատիկը.

1) 360 և 504; 2) 2520 և 6253; 3) 187 և 533;
4) 9163, 2737 և 9639; 5) 374, 1599 և 9061:

2.3 $[a,b] = \frac{ab}{(a,b)}$ բանաձևով գտնել հետևյալ թվերի ամենափոքր ընդհանուր բազմապատիկը.

1) 252 և 468; 2) 279 և 372; 3) 178 և 381;
4) 318 և 477; 5) 758 և 1137:

2.4 Դիցուք x-ը և y-ը բնական թվեր են, և $(x,y)=d$: Լուծեք հետևյալ համակարգերը.

1) $\begin{cases} x + y = 180 \\ d = 30 \end{cases}$; 2) $\begin{cases} x + y = 168 \\ d = 24 \end{cases}$;

3) $\begin{cases} \frac{x}{y} = \frac{11}{7} \\ d = 45 \end{cases}$; 4) $\begin{cases} xy = 720 \\ d = 4 \end{cases}$:

2.5 Դիցուք a և b բնական թվեր են, $(a,b)=d$, $[a, b]=m$: Գտնել a և b, եթե.

1) $\begin{cases} d = 15 \\ m = 420 \end{cases}$; 2) $\begin{cases} d = 12 \\ m = 840 \end{cases}$; 3) $\begin{cases} d = 5 \\ m = 260 \end{cases}$;

4) $\begin{cases} a + b = 667 \\ \frac{m}{d} = 120 \end{cases}$; 5) $\begin{cases} m \cdot d = 504 \\ \frac{m}{d} = 14 \end{cases}$:

2.6 Տրված են a և b թվերը: Գտնել $d=(a, b)$ և որոշել x և y թվերը, որոնցով կարելի է իրականացնել d-ի գծային ներկայացումը հետևյալ տեսքով՝ $d=ax+by$, եթե.

1) $a=899$, $b=493$; 2) $a=1445$, $b=629$; 3) $a=903$, $b=731$;
4) $a=1786$, $b=705$; 5) $a=2576$, $b=154$:

2.7 Ապացուցել, որ եթե (a, b)=1, ապա $\frac{1}{a} + \frac{1}{a+b}$ կոտորակն անկրճատելի է:

3. ՊԱՐԶ ԵՎ ԲԱՂԱԴՐՅԱԼ ԹՎԵՐ

$p>1$ բնական թիվը կոչվում է պարզ, եթե այն ունի միայն երկու բնական բաժանարար (1 և p): Բնական թիվը կոչվում է բաղադրյալ, եթե այն ունի երկուսից ավելի տարբեր բաժանարարներ: a բաղադրյալ թվի՝ 1-ից տարբեր փոքրագույն դրական բաժանարարը պարզ թիվ է և չի գերազանցում $\sqrt{a}$ թվին:

1-ից մեծ յուրաքանչյուր a ամբողջ թիվ կարելի է միակ ձևով (առանց հաշվի առնելու արտադրիչների հերթականությունը) ներկայացնել $p_1, p_2, \ldots, p_k$ պարզ արտադրիչների արտադրյալի տեսքով. $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.

Որոշ արտադրիչներ կարող են կրկնվել, և, նշանակելով $\alpha_1, \alpha_2, \ldots, \alpha_n$-ով a-ի վերլուծության մեջ նրանց պատիկությունը, կստանանք a թվի <u>կանոնական վերլուծությունը.</u> $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$: a թվի ցանկացած D բաժանարար կունենա հետևյալ տեսքը. $D = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$, որտեղ $0 \le \beta_1 \le \alpha$, $0 \le \beta_2 \le \alpha_2, \ldots, 0 \le \beta_n \le \alpha_n$:

3.1 Գտնել հետևյալ թվերի միջև եղած պարզ թվերը.
1) 2320 և 2350; 2) 2640 և 2680:

3.2 Ցույց տալ, որ $n>1$ բնական թվի դեպքում՝
1) n^4+4 թիվը բաղադրյալ է,
2) n^4+n^2+1 թիվը բաղադրյալ է:

3.3 Գտեք երկվորյակ պարզ թվերի եռյակ (այսինքն պարզ թվերի այնպիսի եռյակ, որոնք կազմում են 2 տարբերությամբ թվաբանական պրոգրեսիա), և ցույց տալ, որ այն միակն է:

3.4 Դիցուք p-ն պարզ թիվ է: Ապացուցել, որ՝
1) եթե $5p^2-2$ պարզ թիվ է, ապա $5p^2-4$ և $5p^2+2$ թվերը ևս պարզ են;
2) եթե $2p^2+13$ պարզ թիվ է, ապա $2p^2+1$ և $2p^2+11$ թվերը ևս պարզ են;

3) եթե $11p-7$ պարզ թիվ է, ապա $11p+7$ բաղադրյալ թիվ է:

3.5 Գտնել p-ն, եթե հետևյալ թվերը պարզ են.
1) $p, p+10, p+14$; 2) $p, p+4, p+14$:

3.6 Գտնել p-ն, եթե հետևյալ թվերը պարզ են.
1) p, p^2-6, p^2+6; 2) $p, 2p^2-9, 2p^{2+}9$:

3.7 Գտնել ամենափոքր բնական թիվը, որը 2-ի բաժանելիս տալիս է 1 մնացորդ, 3-ի՝ 2, 4-ի՝ 3, 5-ի՝ 4, 6-ի՝ 5, 7-ի՝ 6, 8-ի՝ 7, 9-ի՝ 8 և 10-ի՝ 9 մնացորդ:

3.8 Գտնել ամենամեծ եռանիշ թիվը, որը 4-ի բաժանելիս տալիս է 3 մնացորդ, 5-ի բաժանելիս՝ 4, 6-ի բաժանելիս՝ 5:

3.9 Եթե $p>5$ պարզ թիվ է, ապա ցույց տալ, որ p^2 թիվը 30-ի բաժանելիս մնացորդը կարող է հավասար լինել միայն կամ 1, կամ 19:

3.10 Ապացուցել, որ եթե p-ն և q-ն պարզ թվեր են և մեծ են 3-ից, ապա p^2-q^2 թիվը բաժանվում է 24-ի:

3.11 Դիցուք $p>2$ պարզ թիվ է: Ապացուցել, որ $\frac{2}{p}$ կոտորակը միայն մեկ եղանակով կարելի է ներկայացնել $\frac{2}{p} = \frac{1}{x} + \frac{1}{y}$ տեսքով, որտեղ x և y իրարից տարբեր բնական թվեր են:

3.12 Ապացուցել հետևյալ տեսքի պարզ թվերի բազմության անվերջությունը.
1) 4m-1; 2) 6m-1:

3.13 Ապացուցել, որ եթե 2^n-1 պարզ թիվ է, ապա n-ը ևս պարզ թիվ է: Ճի՞շտ է արդյոք հակառակը:

3.14 Ապացուցել, որ հետևյալ թվերը միաժամանակ պարզ լինել չեն կարող՝
1) $5k-2$ և $5k+3$; 2) $7k, 7k+4, 7k+5$; 3) 2^k-1 և 2^k+1, երբ $k>2$:

4. ՎԵՐՋԱՎՈՐ ԱՆԸՆԴՀԱՏ (ՇՂԹԱՅԱԿԱՆ) ԿՈՏՈՐԱԿՆԵՐ

Յուրաքանչյուր $\frac{a}{b}$ սովորական անկրճատելի կոտորակ էվկլիդեսի ալգորիթմով կարելի է ներկայացնել հետևյալ տեսքով.

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \dots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}},$$

որտեղ q_i-ը ոչ բացասական ամբողջ թիվ է, $q_2, q_3, \dots, q_n$ դրական ամբողջ թվեր են: Այդ հավասարությունը կարճ գրում են հետևյալ տեսքով. $\frac{a}{b} = (q_1, q_2, q_3, \dots, q_n)$, իսկ աջ մասում գրված արտահայտությունը անվանում են վերջավոր անընդհատ կամ շղթայական կոտորակ:

$\frac{P_1}{Q_1} = \frac{q_1}{1}$, $\frac{P_2}{Q_2} = q_1 + \frac{1}{q_2}$, $\frac{P_3}{Q_3} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, \dots$ կոտորակները կոչվում են $\frac{a}{b}$ անընդհատ կոտորակների մերձավոր կոտորակներ:

Պարզ է, որ $\frac{P_n}{Q_n} = \frac{a}{b}$:

$S>1$ դեպքում P_S և Q_S հաշվում են հետևյալ անդրադարձ բանաձևերով.
$P_S = q_S P_{S-1} + P_{S-2}$, $Q_S = q_S Q_{S-1} + Q_{S-2}$, ընդունելով $P_0=1$, $Q_0=0$:
Հաշվարկները հարմար է կատարել աղյուսակով.

q_S		q_1	q_2	....	....	q_S	....	q_{n-1}	q_n
P_S	1	q_1	P_2	....	....	P_S	....	P_{n-1}	a
Q_S	0	1	Q_2	....	....	Q_S	....	Q_{n-1}	b

Մերձավոր կոտորակների հատկությունները.

ա) $S \geq 1$ դեպքում $P_S Q_{S-1} - Q_S P_{S-1} = (-1)^S$:

բ) $S \geq 2$ դեպքում $\frac{P_S}{Q_S} - \frac{P_{S-1}}{Q_{S-1}} = \frac{(-1)^S}{Q_S Q_{S-1}}$:

գ) $\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \dots < \frac{a}{b} < \dots < \frac{P_4}{Q_4} < \frac{P_2}{Q_2}$:

4.1 Հետևյալ սովորական կոտորակները վերածել վերջավոր անընդհատ կոտորակի.

1) $\frac{29}{37}$; 2) $\frac{163}{159}$; 3) $\frac{648}{385}$; 4) $\frac{571}{359}$; 5) $\frac{1882}{1651}$; 6) $\frac{2341}{1721}$:

4.2 Հետևյալ վերջավոր անընդհատ կոտորակներով գտնել նրանց համապատասխան սովորական անկրճատելի կոտորակները.

1) $\frac{a}{b} = (2,1,1,3,1,2)$; 2) $\frac{a}{b} = (1,1,2,3,4)$;

3) $\frac{a}{b} = (4,3,1,2)$; 4) $\frac{a}{b} = (2,5,3,2,1,4,2,3)$;

5) $\frac{a}{b} = (1,3,2,4,3,1,1,1,5)$; 6) $\frac{a}{b} = (1,2,3,1,2,3,1,2,3)$:

4.3 Օգտվելով անընդհատ կոտորակի վերլուծությունից, կրճատել հետևյալ սովորական կոտորակները.

1) $\frac{3587}{2743}$; 2) $\frac{1043}{3427}$; 3) $\frac{3653}{3107}$;

4) $\frac{11281}{6583}$; 5) $\frac{11111}{7093}$; 6) $\frac{85547}{87241}$:

4.4 Անընդհատ կոտորակների միջոցով լուծել հետևյալ անորոշ հավասարումները.

1) $38x+117y=209$; 2) $122x+129y=2$; 3) $119x-68y=34$;
4) $258x-175y=113$; 5) $41x+114y=5$:

5. ԹՎԱՅԻՆ ՖՈՒՆԿՑԻԱՆԵՐ

$\pi(x)$, $x \in N$ ֆունկցիան ներկայացնում է x-ին չգերազանցող պարզ թվերի քանակը: Մեծ x-երի համար $\pi(x)$-ը հաշվում են մոտավոր հետևյալ բանաձևերով.

$$\pi(x) \approx \frac{x}{\ln x} \text{ և } \pi(x) \approx \int_2^x \frac{dt}{\ln t}:$$

$[x]$ ֆունկցիան որոշված է բոլոր x իրական թվերի համար և ներկայացնում է x-ին չգերազանցող ամենամեծ ամբողջ թիվը: Այդ ֆունկցիան կոչվում է x թվի ամբողջ մաս: $\{x\}$ ֆունկցիան որոշված է բոլոր x իրական թվերի համար և կոչվում է x թվի կոտորակային մաս: Ունենք՝ $\{x\} = x - [x]$: $\sigma(a)$ և $\tau(a)$ ֆունկցիաները որոշված են բոլոր բնական a թվերի համար և ներկայացնում են տրված a թվի բոլոր բնական բաժանարարների համապատասխանաբար գումարը և քանակը: Այդ ֆունկցիաները հաշվում են հետևյալ բանաձևերով.

$$\sigma(a) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_n^{\alpha_n+1}-1}{p^n-1},$$

$$\tau(\alpha) = (\alpha_1+1)\cdot(\alpha_2+1)\ldots(\alpha_n+1),$$

որտեղ $p_1, p_2, \ldots, p_n$-ը a թվի պարզ բաժանարարներն են, իսկ $\alpha_1, \alpha_2, \ldots, \alpha_n$-ը a թվի $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ կանոնական վերլուծության մեջ պարզ բաժանարարների ցուցիչներն են:

$\varphi(a)$ էյլերի ֆունկցիան որոշված է բոլոր a բնական թվերի համար և ներկայացնում է a-ին չգերազանցող, a-ի հետ փոխադարձ պարզ

թվերի քանակը, ընդ որում, ընդունում են $\varphi(1) = 1$: Այդ ֆունկցիան հաշվում են հետևյալ բանաձևով.

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right) \text{ կամ}$$

$$\varphi(a) = p_1^{\alpha_1-1}\ldots p_n^{\alpha_n-1}(p_1-1)\ldots(p_n-1),$$

որտեղ $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ a թվի կանոնական վերլուծությունն է:

Մասնավորապես, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, $\varphi(p) = p-1$ որտեղ p-ն պարզ թիվ է:

Էյլերի ֆունկցիան արտադրյալային է՝

$$\varphi(a_1 \cdot a_2 \ldots \cdot a_n) = \varphi(a_1)\cdot\varphi(a_2)\ldots\varphi(a_n)$$

եթե $a_1, a_2, \ldots, a_n$ զույգ առ զույգ փոխադարձ պարզ են:

5.1 Գտնել ճշգրիտ արժեքները.

1) $\pi(4)$; 2) $\pi(7)$; 3) $\pi(8)$; 4) $\pi(12)$; 5) $\pi(25)$;
6) $\pi(37)$; 7) $\pi(50)$; 8) $\pi(100)$; 9) $\pi(200)$:

5.2 Գտնել մոտավոր արժեքները.

1) $\pi(50)$; 2) $\pi(100)$; 3) $\pi(500)$;
4) $\pi(1000)$; 5) $\pi(5000)$:

5.3 Գտնել. 1) $\left[\frac{8}{3}\right]$; 2) $\left[\frac{4}{5}\right]$; 3) $[2,8]$; 4) $[0,4]$; 5) $-\left[3\frac{1}{2}\right]$;
6) $[-2,3]$; 7) $[\sqrt{13}]$; 8) $[5]$; 9) $[\sqrt[3]{30}]$;
10) $[\sqrt[4]{200}]$; 11) $[\sqrt{715}+1]$; 12) $[\sqrt[4]{580}+1]$;
13) $\left[\frac{\sqrt{145}+2}{3}\right]$; 14) $\left[4+\cos\frac{101\pi}{205}\right]$; 15) $\left[\frac{17}{8}+\sin 1^0\right]$;
16) $[2+\lg 0,3]$; 17) $[1+\lg 12,5]$; 18) $[2-\lg 2512]$;

19) $[1+\ln 5]$; 20) $[1-\ln 50]$; 21) $\{2,6\}$;

22) $\left\{\frac{8}{3}\right\}$; 23) $\{6\}$; 24) $\{-4,35\}$; 25) $\{0,4\}$;

26) $\left\{-2\frac{1}{2}\right\}$; 27) $\{-4,8\}$; 28) $\{-0,5\}$:

5.4 Ապացուցել, որ $[x+y]\geq[x]+[y]$:

5.5 Լուծել $[ax]=m$ հավասարումը, որտեղ $a\neq 0$, x-ը իրական թիվ է:

5.6 Գտնել այն ցուցիչը, որով.
1) 3 թիվը մտնում է 100! թվի վերլուծության մեջ,
2) 11 թիվը մտնում է 1000! թվի վերլուծության մեջ,
3) 13 թիվը մտնում է 1000! թվի վերլուծության մեջ,
4) 17 թիվը մտնում է 1000! թվի վերլուծության մեջ:

5.7 Քանի՞ 0-ով են վերջանում հետևյալ թվերը.
1) 100!; 2) 125!; 3) 187!; 4) 200!:

5.8 Հետևյալ թվերը վերածել պարզ արտադրիչների.
1) 10!; 2) 15!; 3) 20!; 4) 25!; 5) 30!; 6) 50!:

5.9 Գտնել այն բնական թվերի քանակը, որոնք.
1) չեն գերազանցում 180-ին և չեն բաժանվում 5, 7, 11 պարզ թվերից ոչ մեկի վրա;
2) չեն գերազանցում 2311-ին և չեն բաժանվում 5, 7, 13, 17 պարզ թվերից ոչ մեկի վրա;
3) չեն գերազանցում 100-ին և փոխադարձ պարզ են 36-ի հետ;
4) չեն գերազանցում 12317-ին և փոխադարձ պարզ են 1575-ի հետ:

5.10 Գտնել հետևյալ թվերի բոլոր բնական բաժանարարների գումարը և քանակը.
1) 375; 2) 720; 3) 957; 4) 988; 5) 990; 6) 1200:

5.11 Գտնել հետևյալ թվերի բոլոր բնական բաժանարարները.

1) 360; 2) 375; 3) 957; 4) 988:

5.12 Գտնել այն բնական թիվը, որն ունի միայն երկու պարզ բաժանարար, բոլոր բաժանարարների քանակը 6 է, իսկ բոլոր բաժանարարների գումարը՝ 28:

5.13 $n=p^{\alpha}\cdot q^{\beta}$, որտեղ p, q պարզ թվեր են, $p\neq q$, n^2 թիվն ունի 15 տարբեր բաժանարարներ: Քանի՞ բաժանարար ունի n^3 թիվը:

5.14 Ստանալ բանաձև $a=p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ թվի բոլոր բաժանարարների k աստիճանների գումարի՝ $\sigma_k(a)$-ի համար և, օգտվելով այդ բանաձևից, գտնել.

1) $\sigma_2(12)$; 2) $\sigma_2(18)$; 3) $\sigma_3(36)$; 4) $\sigma_2(16)$;

5) $\sigma_3(8)$:

5.15 Ցույց տալ, որ 28, 496, 8128 թվերը կատարյալ թվեր են, այսինքն հավասար են իրենց բոլոր բաժանարարների կիսագումարին (կամ, որ նույնն է, հավասար են իրենցից տարբեր բոլոր բաժանարարների գումարին:)

5.16 Ցույց տալ, որ a թվի բոլոր բաժանարարների արտադրյալը հավասար է $a^{\frac{n}{2}}$, որտեղ $n=\tau(a)$: Օգտվելով ստացված բանաձևից, գտնել՝
1) այն a թիվը, որի բոլոր բաժանարարների արտադրյալը 5832 է,
2) այն a թիվը, որի բոլոր բաժանարարների արտադրյալը $3^{30}\cdot 5^{40}$ է:

5.17 Ապացուցել, որ $\tau(a)$-ն կենտ է միայն այն դեպքում, երբ a-ն բնական թվի քառակուսի է:

5.18 1) Գտնել բոլոր քառանիշ թվերը, որոնք ունեն 15 բնական բաժանարար;
2) Ապացուցել, որ 1234 .... 91011 ....133134135 թվի բաժանարարների քանակը հավասար չէ 357:

5.19 Գտնել էյլերի ֆունկցիան հետևյալ թվերի համար.

1) 375; 2) 720; 3) 957; 4) 988; 5) 990; 6) 1200; 7) 1440; 8) 1500; 9) 1890; 10) 4320:

5. 20 Գտնել էյլերի ֆունկցիան հետևյալ պարզ թվերի և պարզ թվերի աստիճանների համար.

1) 17; 2) 31; 3) 43; 4) 71; 5) 83; 6) 3^5; 7) 5^4; 8) 11^3; 9) 17^2; 10) 23^2;

5.21 Գտնել էյլերի ֆունկցիան հետևյալ արտադրյալներից յուրաքանչյուրի համար, չհաշվելով արտադրյալները.

1) $5\cdot 11$; 2) $5\cdot 7\cdot 13$; 3) $12\cdot 17$; 4) $17\cdot 23$; 5) $14\cdot 15$; 6) $11\cdot 14\cdot 15$; 7) $32\cdot 81\cdot 49$ 8) $24\cdot 28\cdot 45$; 9) $720\cdot 957$; 10) $990\cdot 1890$:

5.22 1) Տրված է $\varphi(a)=3600$ և $a=3^{\alpha}\cdot 5^{\beta}\cdot 7^{\gamma}$: Գտնել a-ն:

2) Տրված է $\varphi(a)=120$ և $a=pq$, որտեղ p-ն և q-ն պարզ թվեր են, ընդ որում՝ $p-q=2$: Գտեք a-ն:

3) Տրված է $\varphi(a)=11424$ և $a=p^2q^2$, որտեղ $p\neq q$ պարզ թվեր են: Գտնել a-ն:

5.23 Ցույց տալ, որ m թվի հետ փոխադարձ պարզ և m-ից փոքր թվերի S գումարը հաշվվում է հետևյալ բանաձևով՝ $S=\frac{1}{2}m\cdot\varphi(m)$, և գտնել S-ը, եթե.

1) m=12; 2) m=15; 3) m=18; 4) m=28; 5) m=375; 6) m=720:

Այստեղից ստանալ, որ $m\geq 3$ դեպքում $\varphi(m)$-ը զույգ թիվ է:

5.24 Լուծել հավասարումը.

1) $\varphi(7^x)=294$; 2) $\varphi(7^x)=705894$;

3) $\varphi(5^x\cdot 7^y\cdot 11)=42000$:

5.25 Ապացուցել, որ $1+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^{\alpha})=p^{\alpha}$ որտեղ p-ն պարզ թիվ է:

5.26 Քանի՞ անկրճատելի կանոնավոր կոտորակ կա, որոնց հայտարարը հավասար է b: Գտնել այդպիսի կոտորակների քանակը, եթե՝

1) b=10; 2) b=16; 3) b=36; 4) b=17; 5) b=72:

5.27 Գտնել այն բնական թվերի քանակը, որոնք.

1) փոքր են 300-ից և նրա հետ ունեն 20 ամենամեծ ընդհանուր բաժանարարը;
2) փոքր են 1665-ից և նրա հետ ունեն 37 ամենամեծ ընդհանուր բաժանարարը;
3) փոքր են 1476-ից և նրա հետ ունեն 41 ամենամեծ ընդհանուր բաժանարարը;

5.28 Ստուգել $\sum_{d/a}\varphi(d)=a$ բանաձևի ճշտությունը a թվի հետևյալ արժեքների համար.

1) 72; 2) 80; 3) 360; 4) 375;

5.29 Գտնել x-ը, եթե .

1) $\varphi(x)=\frac{1}{2}x$; 2) $\varphi(x)=\frac{2}{3}x$; 3) $\varphi(x)=\frac{1}{3}x$;

4) $\varphi(x)=\frac{1}{4}x$; 5) $\varphi(x)=\frac{4}{5}x$:

6. ԲԱՂԴԱՏՈՒՄՆԵՐ

a և b ամբողջ թվերը կոչվում են բաղդատելի ըստ m մոդուլի (հենքի), որտեղ m>1 բնական թիվ է, եթե նրանք m թվի վրա բաժանելիս տալիս են նույն մնացորդը:

Եթե a և b թվերը բաղդատելի են ըստ m մոդուլի, ապա դա գրվում է այսպես՝

$$a \equiv b(\bmod m)$$

եթե $a,b \in Z$, $m \in N$, ապա հետևյալ պայմանները համարժեք են՝

1) $a \equiv b(\bmod m)$ 2) $(a-b) \vdots m$ 3) $a = b + mt$ որևէ $t \in Z$ թվի համար:

Բաղդատումների հիմնական հատկությունները, որոնք նման են հավասարությունների հատկություններին.

1.Բաղդատման հարաբերությունը համարժեքության հարաբերությունն է Z բազմության վրա, այսինքն $a,b,c \in Z$ համար $a \equiv a(\bmod m)$; եթե $a \equiv b(\bmod m)$, ապա $b \equiv a(\bmod m)$ և եթե $a \equiv b(\bmod m)$ և $b \equiv c(\bmod m)$, ապա $a \equiv c(\bmod m)$:

2. Ըստ նույն մոդուլի բաղդատումները կարելի է անդամ առ անդամ գումարել և հանել, այսինքն, եթե $a \equiv b(\bmod m)$ և $c \equiv d(\bmod m)$, ապա $a \pm c \equiv b \pm d(\bmod m)$:

2. ա) եթե $a + b \equiv c(\bmod m)$, ապա $a \equiv c - b(\bmod m)$:

բ) Բաղդատման յուրաքանչյուր մասի կարելի է գումարել կամ հանել մոդուլին բազմապատիկ ցանկացած թիվ, եթե $a \equiv b(\bmod m)$, ապա $a \pm mk \equiv b(\bmod m)$ և $a \equiv b \pm mk(\bmod m)$:

3. Ըստ նույն մոդուլի բաղդատումները կարելի է անդամ առ անդամ բազմապատկել, այսինքն, եթե $a \equiv b(\bmod m)$ և $c \equiv d(\bmod m)$, ապա $ac \equiv bd(\bmod m)$: Այս հատկությունը մնում է ճիշտ ցանկացած վերջավոր թվով բաղդատումների համար:

3. ա) եթե $a \equiv b(\bmod m)$ և $n \in N$, ապա $a^n \equiv b^n(\bmod m)$,

բ) եթե $a \equiv b(\bmod m)$ և $k \in Z$, ապա $ak \equiv bk(\bmod m)$;

4. Բաղդատման երկու մասը կարելի է բաժանել նրանց ընդհանուր բաժանարարի վրա, եթե այն փոխադարձ պարզ է մոդուլի հետ, այսինքն, եթե $ak \equiv bk(\bmod m)$ և $(k,m) = 1$, ապա $a \equiv b(\bmod m)$:

5. եթե $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_0$ ամբողջ ռացիոնալ ֆունկցիա է ամբողջ գործակիցներով, և $x \equiv x_1(\bmod m)$, ապա $f(x) = f(x_1)(\bmod m)$:

Բաղդատումների այլ հատկություններ

6. Բաղդատման երկու մասը և մոդուլը կարելի է բազմապատկել ցանկացած բնական թվով, այսինքն, եթե $a \equiv b(\bmod m)$ և $k \in N$, ապա $ak \equiv bk(\bmod mk)$:

7. Բաղդատման երկու մասը և մոդուլը կարելի է բաժանել նրանց ցանկացած ընդհանուր բաժանարարի վրա, այսինքն, եթե $a \equiv b(\bmod m)$ և $a = a_1d$, $b = b_1d$, $m = m_1d$, ապա $a_1 \equiv b_1(\bmod m_1)$:

8. եթե $a \equiv b(\bmod m_1)$, $a \equiv b(\bmod m_2)$, ... , $a \equiv b(\bmod m_k)$, ապա $a \equiv b(\bmod M)$, որտեղ $M = [m_1, m_2, \ldots, m_k]$:

9. եթե բաղդատումը տեղի ունի ըստ m մոդուլի, ապա այն տեղի ունի նաև ըստ d մոդուլի, որտեղ d-ն m-ի ցանկացած բնական բաժանարար է:

10. եթե բաղդատման մի մասը և մոդուլը բաժանվում են որևէ թվի վրա, ապա բաղդատման մյուս մասը ևս բաժանվում է այդ թվի վրա:

6.1 Գտնել բաժանումից ստացված մնացորդը.

1) 15^{231}-ը 14-ի; 2) 15^{231}-ը 16-ի; 3) $(12^{1231}+14^{4324})$-ը 13-ի;
4) 208^{208}-ը 23-ի; 5) 2^{15783}-ը 25-ի; 6) 3^{79824}-ը 17-ի;
7) 10^{2732}-ը 22-ի 8) 18^{2815}-ը 14-ի;
9) $(13^{1054}-23\cdot16^{285}+22^{17})$-ը 15-ի;
10) $(29^{2929}-34^{3434}+29\cdot41\cdot6^{231})$-ը 31-ի; 11) (1532^5-1)-ը 9-ի:

6.2 Ապացուցել, որ.

1) եթե $100a + 10b + c \equiv 0(\bmod 21)$,
ապա $a - 2b + 4c \equiv 0(\bmod 21)$;

2) եթե $a - 5b \equiv 0(\bmod 19)$, ապա $10a + 7b \equiv 0(\bmod 19)$;

3) Եթե $16a-11b+c\equiv 0(\mathrm{mod}\,21)$,

ապա $11a-b+2c\equiv 0(\mathrm{mod}\,21)$;

4) Եթե $\frac{11a+2b}{19}\in Z$, ապա $\frac{18a+5b}{19}\in Z$;

5) Եթե $\frac{a-5b}{17}\in Z$, ապա $\frac{2a+7b}{17}\in Z$;

6) Եթե $\frac{12a-7b}{16}\in Z$, ապա $\frac{4a+23b}{16}\in Z$;

7. ՄՆԱՑՔՆԵՐ ԵՎ ՄՆԱՑՔՆԵՐԻ ՀԱՄԱԿԱՐԳԵՐ

Բոլոր այն ամբողջ թվերի համախմբությունը, որոնք m բնական թվի վրա բաժանելիս տալիս են միևնույն r մնացորդը, կազմում են ըստ m մոդուլի բաղդատման հարաբերության նկատմամբ համարժեքության դաս: Այդ դասի բոլոր թվերի ընդհանուր տեսքը կլինի՝ mk+r, որտեղ k-ն ցանկացած ամբողջ թիվ է: Այդ դասերի թիվը հավասար կլինի m: Դասի ցանկացած թիվ կոչվում է ըստ տրված m մոդուլի մնացք (միևնույն դասի բոլոր թվերի նկատմամբ):

Յուրաքանչյուր դասից մեկական վերցրած ցանկացած թվերի համախմբության կոչվում է ըստ տրված m մոդուլի մնացքների լրիվ համակարգ: Հաճախ որպես մնացքների լրիվ համակարգ օգտագործվում է ըստ m մոդուլի փոքրագույն ոչ բացասական մնացքների լրիվ համակարգը՝ 0; 1; 2; ...; m-1: Երբեմն օգտագործվում է բացարձակ արժեքով փոքրագույն ոչ դրական մնացքների լրիվ համակարգը՝ -(m-1); -(m-2); ...; -2; -1; 0: Օգտագործվում է նաև ըստ մոդուլի բացարձակ փոքրագույն մնացքների լրիվ համակարգը, որը

կենտ m-ի դեպքում հետևյալն է՝ $-\frac{m-1}{2},\ldots,-1,\ 0,\ 1,\ldots,\frac{m-1}{2}$, իսկ

զույգ m-ի դեպքում՝ $-\frac{m}{2}+1,\ldots,-1,0,1,\ldots,\frac{m}{2}$ կամ՝

$-\frac{m}{2},\ldots,-1,0,1,\ldots,\frac{m}{2}-1$:

Այն թվերի համախմբությունը, որոնք վերցրված են մնացքների լրիվ համակարգից և փոխադարձ պարզ են m մոդուլի հետ, կոչվում է ըստ m մոդուլի մնացքների բերված համակարգ: Մնացքների բերված համակարգ կազմող թվերի քանակը հավասար է $\varphi(m)$:

Մնացքների լրիվ համակարգի նման օգտագործվում են բերված համակարգի տարբեր տեսակներ՝ փոքրագույն դրական, բացարձակ արժեքով փոքրագույն բացասական, բացարձակ փոքրագույն բերված համակարգեր: Ըստ p պարզ մոդուլի՝ այդ համակարգերը կլինեն՝

1, 2, 3, ..., p –1; -(p -1), -(p -2), ..., -2, -1; $\pm 1,\ \pm 2,\ \ldots,\ \pm\frac{p-1}{2}$:

- Եթե $x_1, x_2, \ldots, x_k$ թվերը ըստ m մոդուլի լրիվ (k=m) կամ բերված $(k=\varphi(m))$ համակարգեր են, ապա $ax_1, ax_2, \ldots, ax_k$ թվերը ևս, որտեղ (a, m)=1, կազմում են ըստ m մոդուլի համապատասխանաբար լրիվ կամ բերված համակարգ:

7.1 Գրել ըստ հետևյալ մոդուլների մնացքների լրիվ և բերված համակարգերի բոլոր երեք տեսակները.

1) m=9; 2) m=8; 3) p=13; 4) m=12;
5) p=7; 6) m=10:

7.2 Ցույց տալ, որ

1) 25, -20, 16, 46, -21, 18, 37, -17 թվերը կազմում են ըստ m=8 մոդուլի մնացքների լրիվ համակարգ;
2) 21, 2, -18, 28, -19, 40, -22, -2, 15 թվերը կազմում են ըստ m=9 մոդուլի մնացքների բերված համակարգ;
3) 24, 18, -19, 37, 28, -23, -32, 5, 41, -35, -33 թվերը կազմում են ըստ m=11 մոդուլի մնացքների բերված համակարգ;
4) 32, -9, 15, 42, -18, 30, 6 թվերը կազմում են ըստ *p=7* մոդուլի մնացքների բերված համակարգ;
5) 11, -1, 17, -19 թվերը կազմում են ըստ *m=8* մոդուլի մնացքների բերված համակարգ;
6) 13, -13, 29, -9 թվերը կազմում են ըստ *m=10* մոդուլի մնացքների բերված համակարգ:

7.3 Փոխարինել բացարձակ փոքրագույն և փոքրագույն ոչ բացասական մնացքով.

1) 103-ը ըստ 87 մոդուլի, 2) 484-ը ըստ 15 մոդուլի
3) 185-ը ըստ 16 մոդուլի 4) 217-ը ըստ 19 մոդուլի
5) 153-ը ըստ 61 մոդուլի 6) 76499-ը ըստ 37 մոդուլի
7) 625-ը ըստ 25 մոդուլի 8) 624-ը ըստ 25 մոդուլի

8. ԷՅԼԵՐԻ ԵՎ ՖԵՐՄԱՅԻ ԹԵՈՐԵՄՆԵՐԸ

- ***Էյլերի թեորեմը:*** Եթե m>1, և (a, m)=1, ապա $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, որտեղ $\varphi(m)$-ը էյլերի ֆունկցիան է:
- ***Ֆերմայի թեորեմը:*** Եթե p-ն պարզ թիվ է, և (a,p)=1, ապա $a^{p-1} \equiv 1(\mathrm{mod}\, p)$:
- ***Հետևանք:*** Ցանկացած a ամբողջ դրական թվի համար.

$$a^p \equiv a(\mathrm{mod}\, p):$$

8.1 Գտնել a թիվը b թվի վրա բաժանելիս ստացվող մնացորդը, եթե.

1) $a=383^{175}$, b=45; 2) $a=109^{345}$, b=14; 3) $a=439^{291}$, b=60;
4) $a=293^{275}$, b=48; 5) $a=3^{80}+7^{80}$; b=11; 6) $a=3^{100}+5^{100}$,b=7;
7) $a=5^{70}+7^{50}$, b=12; 8) $a=2^{100}+3^{100}$, b=5;

8.2 Գտնել՝ 1) 2^{100} թվի վերջին երկու թվանշանները, 2) 2^{341} թվի վերջին երկու թվանշանները, 3) 243^{402} թվի վերջին երեք թվանշանները, 4) 289^{401} թվի վերջին երեք թվանշանները:

8.3 Ապացուցել, որ

1) եթե p-ն պարզ թիվ է, և $a^p \equiv \pm 1(\mathrm{mod}\, p)$, ապա
$a^p \equiv \pm 1(\mathrm{mod}\, p^2)$;
2) եթե p-ն և q-ն իրարից տարբեր պարզ թվեր են, ապա
$p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, pq)$;
3) p և $8p^2+1$ թվերը միաժամանակ պարզ լինել կարող են միայն p=3 դեպքում;

4) եթե p>3 և 2p+1 թվերը պարզ են, ապա 4p+1 թիվը բաղադրյալ է;
5) ցանկացած a ամբողջ թվի 100 աստիճանը 125-ի վրա բաժանելիս տալիս է 1 մնացորդ կամ բաժանվում է 125-ի վրա;
6) եթե (n, 6)=1, ապա $n^2 \equiv 1(\mathrm{mod}\, 24)$:

9. ՄԵԿ ԱՆՀԱՅՏՈՎ ԲԱՂԴԱՏՈՒՄՆԵՐ

x անհայտով բաղդատման ընդհանուր տեսքն է՝

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0(\mathrm{mod}\, m),$$

կամ ավելի կարճ՝ $f(x) \equiv 0(\mathrm{mod}\, m)$, որտեղ $a_0, a_1, \ldots, a_n$ ամբողջ թվեր են, իսկ n-ը ոչ բացասական ամբողջ թիվ է: Բաղդատումը կոչվում է n աստիճանի, եթե $a_0 \equiv \emptyset(\mathrm{mod}\, m)$: Լուծել բաղդատումը նշանակում է գտնել բաղդատմանը բավարարող՝ x-ի բոլոր արժեքները կամ ցույց տալ, որ այդ բաղդատումը լուծում չունի: Նույն x անհայտով, ըստ նույն մոդուլի, երկու բաղդատումներ կոչվում են համազոր, եթե նրանց բավարարում են x-ի միևնույն արժեքները: Եթե $f(x) \equiv 0(\mathrm{mod}\, m)$ բաղդատմանը բավարարում է որևէ $x = \alpha$ արժեք, ապա նրան բավարարում են նաև այն x թվերը, որոնց համար $x \equiv \alpha(\mathrm{mod}\, m)$, կամ՝ $x = mk + \alpha$ տեսքի թվերը, այսինքն՝ այն բոլոր թվերը, որոնք կազմում են ըստ m մոդուլի մնացքների մեկ դաս, որին պատկանում է α-ն: Յուրաքանչյուր դաս մեկ լուծում է: Հետևաբար, լուծել բաղդատումը նշանակում է գտնել բաղդատմանը բավարարող բոլոր դասերը: Սովորաբար որպես α վերցնում են փոքրագույն ոչ բացասական կամ բացարձակ փոքրագույն մնացքները՝ ըստ տրված m մոդուլի: Այսպիսով, բաղդատումը կունենա այնքան լուծում, որքան մնացք ըստ m մոդուլի մնացքների լրիվ համակարգից կբավարարի այդ բաղդատմանը:

9.1 Փոքրագույն ոչ բացասական մնացքների փորձարկման եղանակով գտնել հետևյալ բաղդատումների լուծումները.

1) $5x^2 - 15x + 22 \equiv 0(\mathrm{mod}\, 3)$; 2) $x^2 + 2x + 2 \equiv 0(\mathrm{mod}\, 5)$;
3) $3x \equiv 1(\mathrm{mod}\, 5)$; 4) $3x \equiv 1(\mathrm{mod}\, 13)$; 5) $8x \equiv 3(\mathrm{mod}\, 14)$;
6) $6x \equiv 5(\mathrm{mod}\, 9)$; 7) $x^2 - 2x + 2 \equiv 0(\mathrm{mod}\, 3)$;

8) $x^3 - 2 \equiv 0 (\mathrm{mod}\, 5)$;

9.2 Բացարձակ փոքրագույն մնացքների փորձարկման եղանակով լուծել հետևյալ բաղդատումները (նախօրոք կարելի է պարզեցնել բաղդատումները, օգտվելով նրանց հատկություններից).

1) $12x \equiv 1 (\mathrm{mod}\, 7)$;

2) $3x \equiv 13 (\mathrm{mod}\, 11)$;

3) $8x \equiv 1 (\mathrm{mod}\, 5)$;

4) $6x \equiv 3 (\mathrm{mod}\, 7)$;

5) $6x + 5 \equiv 6 (\mathrm{mod}\, 7)$;

6) $6x + 5 \equiv 1 (\mathrm{mod}\, 7)$;

7) $3x + 4 \equiv 2 (\mathrm{mod}\, 5)$;

8) $15x + 4 \equiv 7 (\mathrm{mod}\, 11)$;

9) $90x^{20} + 46x^2 - 52x + 46 \equiv 0 (\mathrm{mod}\, 15)$;

10) $25x^3 - 36x^2 + 18x + 13 \equiv 0 (\mathrm{mod}\, 12)$;

10. ԱՌԱՋԻՆ ԱՍՏԻՃԱՆԻ ԲԱՂԴԱՏՈՒՄՆԵՐ

Ընդհանուր տեսքով առաջին աստիճանի բաղդատումը գրվում է հետևյալ տեսքով՝ $ax \equiv b (\mathrm{mod}\, m)(1)$:

Այդ բաղդատման լուծման ժամանակ հնարավոր են հետևյալ երեք դեպքերը.

ա) եթե (a, m)=1, ապա բաղդատումն ունի միակ լուծում, այսինքն նրան բավարարում է ըստ m մոդուլի թվերի մեկ դաս,

բ) եթե (a, m)=d>1, իսկ b-ն չի բաժանվում d-ի, ապա բաղդատումը լուծում չունի,

գ) եթե (a,m)=d>1, և b-ն բաժանվում է d-ի, ապա բաղդատումն ունի d լուծում, որոնք գտնում են հետևյալ բանաձևով՝

$$x_{k+1} = m_1 k + \alpha (\mathrm{mod}\, m),$$

որտեղ k=0, 1, 2, ..., d-1; α -ն $a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$ բաղդատման լուծումն է, իսկ $m=m_1 d$: Այդ բաղդատումը ստացվում է (1)-ից, երբ կրճատում ենք նրա անդամները և մոդուլը d-ով:

$ax \equiv b (\mathrm{mod}\, m)$ բաղդատման լուծումը բավական է գտնել

ա) դեպքի համար, քանի որ գ) դեպքը հանգում է ա) -ին:

Կիրառվում են լուծման հետևյալ եղանակները.

ա) լուծումը գտնվում է ըստ m մոդուլի փոքրագույն ոչ բացասական կամ բացարձակ փոքրագույն մնացքների փորձարկման եղանակով,

բ) էյլերի եղանակով: Լուծումը գտնվում է $x \equiv b a^{\varphi(m)-1} (\mathrm{mod}\, m)$ բանաձևով, որտեղ $\varphi(m)$-ը էյլերի ֆունկցիան է,

գ) վերջավոր անընդհատ կոտորակների միջոցով, $x \equiv (-1)^n b P_{n-1} (\mathrm{mod}\, m)$ բանաձևով, որտեղ P_{n-1}-ը $\frac{m}{a}$ կոտորակը անընդհատ կոտորակի վերլուծության նախավերջին մերձավոր կոտորակի համարիչն է:

դ) օգտվում են բաղդատումների հատկություններից. եթե (a, m)=1, a-ն (b+sm)-ի բաժանարար է, ապա (1)-ի լուծումը կլինի՝ $x \equiv \frac{b + sm}{a} (\mathrm{mod}\, m)$:

10.1 էյլերի եղանակով լուծել հետևյալ բաղդատումները.

1) $43x \equiv 8 (\mathrm{mod}\, 34)$; 2) $3x \equiv 1 (\mathrm{mod}\, 5)$; 3) $5x \equiv 6 (\mathrm{mod}\, 7)$;

4) $5x \equiv 7 (\mathrm{mod}\, 10)$; 5) $3x \equiv 8 (\mathrm{mod}\, 13)$;

6) $25x \equiv 15 (\mathrm{mod}\, 17)$; 7) $29x \equiv 3 (\mathrm{mod}\, 12)$;

8) $5x \equiv 26 (\mathrm{mod}\, 12)$; 9) $4x \equiv 7 (\mathrm{mod}\, 8)$;

10.2 Անընդհատ կոտորակների միջոցով լուծել հետևյալ բաղդատումները.

1) $55x \equiv 7 (\mathrm{mod}\, 87)$; 2) $7x \equiv 4 (\mathrm{mod}\, 19)$;

3) $13x \equiv 1 (\mathrm{mod}\, 27)$; 4) $37x \equiv 25 (\mathrm{mod}\, 117)$;

5) $91x \equiv 143 (\mathrm{mod}\, 222)$; 6) $113x \equiv 89 (\mathrm{mod}\, 311)$;

7) $271x \equiv 25 (\mathrm{mod}\, 119)$; 8) $221x \equiv 111 (\mathrm{mod}\, 360)$;

9) $13x \equiv 178 (\mathrm{mod}\, 153)$;

10.3 Լուծել հետևյալ բաղդատումները, որոնցում (a, m)=d>1.

1) $12x \equiv 9 \pmod{18}$; 2) $12x \equiv 9 \pmod{15}$;

3) $20x \equiv 10 \pmod{25}$; 4) $10x \equiv 25 \pmod{35}$;

5) $39x \equiv 84 \pmod{93}$; 6) $90x + 18 \equiv 0 \pmod{138}$;

7) $375x \equiv 195 \pmod{501}$; 8) $78x \equiv 42 \pmod{51}$;

9) $114x \equiv 42 \pmod{87}$.

10.4 1) 523 թվի աջից կցագրել երեք թվանշան այնպես, որ ստացված վեցանիշ թիվը բաժանվի 7-ի, 8-ի և 9-ի:

2) 32 թվին աջից կցագրել երկու թվանշան այնպես, որ ստացված քառանիշ թիվը բաժանվի 3-ի և 7-ի:

11. ԱՌԱՋԻՆ ԱՍՏԻՃԱՆԻ ԲԱՂԴԱՏՈՒՄՆԵՐԻ ՀԱՄԱԿԱՐԳԵՐ

x փոփոխականից առաջին աստիճանի բաղդատումների համակարգի ընդհանուր տեսքը հետևյալն է.

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots\dots \\ a_nx \equiv b_n \pmod{m_n} \end{cases}$$

Նրանց լուծման ընդհանուր եղանակի էությունը հետևյալն է. նախ՝ գտնում են առաջին բաղդատման $x \equiv \alpha \pmod{m}$ լուծումը, որտեղ α-ն ըստ m_1 մոդուլի փոքրագույն ոչ բացասական կամ բացարձակ փոքրագույն մնացքն է, և վերցնում են թվերի $x = m_1t + \alpha$ դասը, որը բավարարում է առաջին բաղդատմանը: Այնուհետև՝ x-ի այդ արժեքը տեղադրում են երկրորդ բաղդատման մեջ՝ $a_2(m_1t + \alpha) \equiv b_2 \pmod{m_2}$, որտեղից գտնում են t-ն որպես թվերի $t = m_2t_1 + \beta$ դաս, որը տեղադրում են $x = m_1t + \alpha$ արտահայտության մեջ: Արդյունքում՝ ստանում են x-ի արժեքը որպես թվերի դաս, որը բավարարում է առաջին երկու բաղդատումներին: Այնուհետև՝ x-ի այդ արժեքը տեղադրում են երրորդ բաղդատման մեջ և շարունակում նույն ձևով:

11.1 Լուծել բաղդատումների հետևյալ համակարգերը.

1) $\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14} \end{cases}$ 2) $\begin{cases} x \equiv 13 \pmod{16} \\ x \equiv 3 \pmod{10} \\ x \equiv 9 \pmod{14} \end{cases}$ 3) $\begin{cases} x \equiv 1 \pmod{25} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{9} \end{cases}$

4) $\begin{cases} 4x \equiv 3 \pmod{7} \\ 5x = 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}$ 5) $\begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 3x \equiv 7 \pmod{31} \\ 14x \equiv 35 \pmod{19} \end{cases}$ 6) $\begin{cases} 4x \equiv 7 \pmod{13} \\ x \equiv 2 \pmod{17} \\ 5x \equiv 3 \pmod{9} \\ 8x \equiv 4 \pmod{14} \end{cases}$

7) $\begin{cases} 3x \equiv 7 \pmod{10} \\ 2x = 5 \pmod{15} \\ 7x \equiv 5 \pmod{12} \end{cases}$ 8) $\begin{cases} 4x \equiv 1 \pmod{9} \\ 5x = 3 \pmod{7} \\ 4x \equiv 5 \pmod{12} \end{cases}$ 9) $\begin{cases} 5x \equiv 1 \pmod{12} \\ 5x = 2 \pmod{8} \\ 7x \equiv 3 \pmod{11} \end{cases}$

11.2 Գտնել ամենափոքր բնական թիվը, որը.

1) 7-ի, 5-ի, 3-ի և 11-ի բաժանելիս տալիս է համապատասխանաբար 3, 2, 1 և 9 մնացորդ;

2) 11-ի, 7-ի և 5-ի բաժանելիս տալիս են համապատասխանաբար 2, 5, և 4 մնացորդ:

11.3 a-ի ինչպիսի՞ արժեքների դեպքում հետևյալ համակարգերը համատեղելի են.

1) $\begin{cases} x \equiv 5 \pmod{18} \\ x \equiv 8 \pmod{21} \\ x \equiv a \pmod{35} \end{cases}$ 2) $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 11 \pmod{20} \\ x \equiv 1 \pmod{15} \\ x \equiv a \pmod{18} \end{cases}$

11.4 Գտնել հետևյալ հավասարումների ամբողջ լուծումները.

1) 3x+4y=13, 2) 8x-13y=63, 3) 39x-22y=10,

4) 43x+37y=21, 5) 45x-37y=25, 6) 81x-48y=33:

12. ԲԱՐՁՐ ԱՍՏԻՃԱՆԻ ԲԱՂԱՏՈՒՄՆԵՐ ԸՍՏ ՊԱՐԶ ՄՈԴՈՒԼԻ

Այդպիսի բաղդատումների ընդհանուր տեսքը հետևյալն է.

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\, p) \qquad (1)$$

որտեղ p-ն պարզ թիվ է, $a_n \not\equiv 0 (\mathrm{mod}\, p)$, n-ը ամբողջ ոչ բացասական թիվ է, a_0, a_1, ... , a_n ամբողջ թվեր են: (1) տեսքի բաղդատումների տեսությունում տեղի ունեն հետևյալ թեորեմները.

ա) Թեորեմ բաղդատման աստիճանի վերաբերյալ.

(1) տեսքի բաղդատումը $n \geq p$ դեպքում կարելի է փոխարինել նրան համարժեք $R(x) \equiv 0 (\mathrm{mod}\, p)$ բաղդատումով, որի աստիճանը չի գերազանցում (p-1)-ին, և որտեղ R(x)-ը հանդիսանում է f(x)-ը (x^p-x)-ի վրա բաժանումից ստացված մնացորդը,

բ) Թեորեմ նույնական բաղդատման վերաբերյալ.

Եթե $n \leq p-1$ և (1) բաղդատմանը բավարարում են ըստ p մոդուլի իրար հետ ոչ բաղդատելի $\alpha_1, \alpha_2, \ldots, \alpha_k$ թվեր, ապա տեղի ունի հետևյալ նույնական բաղդատումը.

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k) f_k(x) (\mathrm{mod}\, p), \qquad (2)$$

այսինքն՝ (1) բաղդատումը համարժեք է հետևյալին.

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k) f_k(x) \equiv 0 (\mathrm{mod}\, p), \qquad (3)$$

որտեղ $f_k(x)$-ը n-k աստիճանի բազանդամ է:

(3) բաղդատման ձախ մասը անվանում են նաև f(x)-ի վերլուծություն բազմապատկիչների՝ ըստ p մոդուլի:

գ) Եթե k=n, (3) բաղդատումը համարժեք է հետևյալին.

$$a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \equiv 0 (\mathrm{mod}\, p) \qquad (4)$$

դ) Թեորեմ լուծումների քանակի վերաբերյալ.

(1) բաղդատումը, որտեղ $n \leq p-1$, չի կարող ունենալ n-ից շատ, ըստ p մոդուլի իրար հետ ոչ բաղդատելի լուծումներ, ընդ որում, դրանց որոշ մասը կարող են հանդիսանալ բազմապատիկ լուծումներ:

ե) Վիլսոնի թեորեմը.

Յուրաքանչյուր p պարզ թվի համար տեղի ունի հետևյալ բաղդատումը՝ $(p-1)!+1 \equiv 0 (\mathrm{mod}\, p)$, և հակառակը եթե $(p-1)!+1$ թիվը բաժանվում է p-ի վրա, ապա p-ն պարզ թիվ է:

12.1 Լուծել հետևյալ բաղդատումները, նախապես իջեցնելով նրանց աստիճանը.

1) $6x^{10} - 12x + 1 \equiv 0 (\mathrm{mod}\, 5)$; 2) $x^5 - 2x^3 + x^2 - 2 \equiv 0 (\mathrm{mod}\, 3)$;

3) $x^7 - x^6 + 5x^2 - 3 \equiv 0 (\mathrm{mod}\, 5)$; 4) $x^7 - 6 \equiv 0 (\mathrm{mod}\, 5)$;

5) $6x^4 + 17x^2 - 16 \equiv 0 (\mathrm{mod}\, 3)$;

6) $3x^7 - 2x^6 + 2x^2 + 13 \equiv 0 (\mathrm{mod}\, 5)$:

12.2 Հետևյալ բաղդատումները վերլուծել արտադրիչների՝ ըստ տրված մոդուլի.

1) $x^3 + 4x^2 - 3 \equiv 0 (\mathrm{mod}\, 5)$;

2) $x^4 + x + 4 \equiv 0 (\mathrm{mod}\, 11)$;

3) $3x^3 - 1 \equiv 0 (\mathrm{mod}\, 5)$;

4) $x^4 - 7x^3 + 13x^2 + 21x + 23 \equiv 0 (\mathrm{mod}\, 7)$;

5) $2x^3 + 5x^2 - 2x - 3 \equiv 0 (\mathrm{mod}\, 7)$;

6) $x^4 - 2x^2 + x + 4 \equiv 0 (\mathrm{mod}\, 7)$:

12.3 Ցույց տալ, որ եթե p-ն պարզ թիվ է, ապա՝

1) $(p-2)! \equiv 1 (\mathrm{mod}\, p)$;

2) $(p-3)! \cdot 2 + 1 \equiv 0 (\mathrm{mod}\, p)$;

3) $(p-4)! \cdot 3 - 1 \equiv 0 (\mathrm{mod}\, p)$:

13. ԵՐԿՐՈՐԴ ԱՍՏԻՃԱՆԻ ԲԱՂԴԱՏՈՒՄՆԵՐ: ԼԵԺԱՆԴՐԻ ՊԱՅՄԱՆԱՆՇԱՆԸ:

Դիտարկվում է $x^2 \equiv a(\mathrm{mod}\, p)$ (1) բաղդատումը, որտեղ $a \not\equiv 0(\mathrm{mod}\, p)$, իսկ p-ն կենտ պարզ թիվ է: Եթե (1) լուծում ունի, ապա a-ն կոչվում է քառակուսային մնացք ըստ p մոդուլի, հակառակ դեպքում a-կոչվում է քառակուսային ոչ մնացք ըստ p մոդուլի: Եթե a-ն քառակուսային մնացք է ըստ p մոդուլի, ապա (1) բաղդատումն ունի երկու լուծում:

Էյլերի հայտանիշը: a թիվը $(a, p)=1$ դեպքում հանդիսանում է քառակուսային մնացք ըստ p մոդուլի, եթե տեղի ունի $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$ (2) բաղդատումը: Եթե $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$, (3) ապա a-ն քառակուսային ոչ մնացք է ըստ p մոդուլի:

Լեժանդրի պայմանանշանը: (2)-ը և (3)-ը միավորելով մեկ բաղդատման մեջ, կարող ենք գրել

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(\mathrm{mod}\, p),$$

որտեղ $\left(\frac{a}{p}\right)$ կոչվում է Լեժանդրի պայմանանշան, և $\left(\frac{a}{p}\right)=1$, եթե a-ն քառակուսային մնացք է ըստ p մոդուլի, $\left(\frac{a}{p}\right)=-1$, եթե a-ն քառակուսային ոչ մնացք է ըստ p մոդուլի: a-ն կոչվում է Լեժանդրի պայմանանշանի համարիչ, b-ն՝ հայտարար:

Լեժանդրի պայմանանշանը կարելի է գտնել էյլերի հայտանիշով՝ $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \pm 1(\mathrm{mod}\, p)$:

Լեժանդրի պայմանանշանի հաշվումը պարզեցնում են հետևյալ հատկությունների կիրառմամբ:

ա) եթե $a \equiv b(\mathrm{mod}\, p)$, ապա $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$;

բ) $\left(\frac{1}{p}\right)=1$;

գ) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$;

դ) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$;

ե) $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_n}{p}\right)$, որտեղ $a_1, a_2, \ldots, a_n$ թվերը փոխադարձ պարզ են p-ի հետ: Մասնավորապես՝

$\left(\frac{a^n}{p}\right)=\left(\frac{a}{p}\right)^n$; $\left(\frac{a^2}{p}\right)=1$; $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$;

զ) Փոխադարձության օրենքը. եթե p-ն և q-ն իրարից տարբեր կենտ պարզ թվեր են, ապա

$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, կամ $\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$:

13.1 Էյլերի հայտանիշով գտնել ըստ p մոդուլի քառակուսային մնացքների դասերը, եթե.

1) p=11; 2) p=7; 3) p=13; 4) p=17:

13.2 Լուծում ունե՞ն արդյոք հետևյալ բաղդատումները.

1) $x^2 \equiv 68(\mathrm{mod}\, 113)$; 2) $x^2 \equiv 310(\mathrm{mod}\, 521)$;

3) $x^2 + 174 \equiv 0(\mathrm{mod}\, 619)$; 4) $x^2 \equiv 63(\mathrm{mod}\, 131)$;

5) $x^2 \equiv 47(\mathrm{mod}\, 73)$; 6) $x^2 \equiv 241(\mathrm{mod}\, 593)$;

7) $x^2 \equiv 251(\mathrm{mod}\, 577)$; 8) $x^2 \equiv 35(\mathrm{mod}\, 97)$;

9) $x^2 \equiv 29(\mathrm{mod}\, 383)$

13.3 Պարզել, թե հետևյալ բաղդատումներից որոնք լուծում ունեն և գտնել դրանց լուծումները.

1) $x^2 \equiv 2(\mathrm{mod}\,7)$; 2) $x^2 \equiv 4(\mathrm{mod}\,7)$; 3) $x^2 \equiv 3(\mathrm{mod}\,7)$;

4) $x^2 \equiv 6(\mathrm{mod}\,7)$; 5) $x^2 \equiv 5(\mathrm{mod}\,11)$; 6) $x^2 \equiv 12(\mathrm{mod}\,13)$:

13.4 Նախապես բերելով երկանդամ բաղդատումների, լուծել հետևյալ բաղդատումները.

1) $3x^2+7x+8 \equiv 0(\mathrm{mod}\,17)$; 2) $5x^2-11x+16 \equiv 0(\mathrm{mod}\,41)$;

3) $5x^2+x+4 \equiv 0(\mathrm{mod}\,13)$; 4) $3x^2+4x+7 \equiv 0(\mathrm{mod}\,31)$;

5) $12x^2+8x-15 \equiv 0(\mathrm{mod}\,47)$;

6) $4x^2-11x-3 \equiv 0(\mathrm{mod}\,23)$:

13.5 Ապացուցել, որ եթե p-ն $4k+3$ տեսքի պարզ թիվ է, իսկ a-ն քառակուսային մնացք է ըստ p մոդուլի, ապա $x^2 \equiv a(\mathrm{mod}\,p)$ բաղդատման լուծումներն են՝ $x \equiv \pm a^{k+1}(\mathrm{mod}\,p)$: Օգտվելով դրանից, լուծել հետևյալ բաղդատումները.

1) $x^2 \equiv 2(\mathrm{mod}\,311)$; 2) $x^2 \equiv 3(\mathrm{mod}\,47)$:

13.6 Ապացուցել, որ

1) $11y = 5x^2 - 7$ հավասարումն ամբողջ թվերով լուծում չունի,

2) երկու հաջորդական ամբողջ թվերի արտադրյալը 13-ի վրա բաժանելիս չի կարող տալ 1 մնացորդ:

13.7 Ցույց տալ, որ

1) եթե $p = 8k+7$ պարզ թիվ է, ապա $2^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\,p)$;

2) եթե $p = 8k+3$ պարզ թիվ է, ապա $2^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\,p)$:

14. ՆԱԽՆԱԿԱՆ ԱՐՄԱՏՆԵՐ ԵՎ ԻՆԴԵՔՍՆԵՐ

a թիվը կոչվում է ըստ m մոդուլի δ ցուցչին պատկանող, եթե $(a,m)=1$ և δ-ն $a^x \equiv 1(\mathrm{mod}\,m)$ ցուցչային բաղդատման փոքրագույն դրական լուծումն է: Նշենք δ ցուցիչի որոշ հատկություններ.

ա) եթե $(a,m)=1$, $(b,m)=1$, $a \equiv b(\mathrm{mod}\,m)$, ապա a-ն և b-ն պատկանում են ըստ m մոդուլի միևնույն δ ցուցչին;

բ) եթե a թիվը պատկանում է δ ցուցիչին և $a^k \equiv 1(\mathrm{mod}\,m)$, ապա δ / k;

գ) քանի որ, ըստ էյլերի թեորեմի, $a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$, ապա $\delta / \varphi(m)$;

դ) եթե a-ն պատկանում է δ ցուցչին, ապա $a^0 = 1, a^1, a^2, \ldots, a^{\delta-1}$ թվերն իրար հետ բաղդատելի չեն ըստ m մոդուլի և $x^\delta \equiv 1(\mathrm{mod}\,m)$ բաղդատման բոլոր լուծումները:

Եթե a թիվը պատկանում է $\delta = \varphi(m)$ ցուցչին, ապա a-ն կոչվում է նախնական արմատ ըստ m մոդուլի: Ըստ m բաղադրյալ մոդուլի՝ նախնական արմատներ կարող են գոյություն չունենալ, իսկ ըստ p պարզ մոդուլի՝ միշտ գոյություն ունեն նախնական արմատներ: Դրանք այն թվերն են, որոնք պատկանում են $\varphi(p) = p-1$ ցուցչին, ընդ որում, ըստ Գաուսի թեորեմի, նրանց քանակը հավասար է $\varphi(p-1)$: Ըստ p պարզ մոդուլի՝ նախնական արմատներ գտնելու ընդհանուր եղանակը հետևում է հետևյալ թեորեմից, եթե՝

$$g^{\frac{p-1}{p_1}} \not\equiv 1,\ g^{\frac{p-1}{p_2}} \not\equiv 1, \ldots,\ g^{\frac{p-1}{p_n}} \not\equiv 1(\mathrm{mod}\,p),$$

որտեղ $p_1, p_2, \ldots, p_n$ թվերը $p-1$ թվի պարզ բաժանարարներն են, ապա g-ն ըստ p մոդուլի նախնական արմատ է: Փորձարկման համար սովորաբար վերցնում են ըստ p մոդուլի մնացքների բերված համակարգի $2, 3, \ldots, p-1$ թվերը: Այս եղանակը հետևյալն է. եթե հայտնի է նախնական արմատի որևէ g արժեք, ապա մնացած նախնական արմատները գտնվում են որպես g^k աստիճանների փոքրագույն դրական մնացքների արժեքներ ըստ p մոդուլի, որտեղ

$(k, p-1)=1$ և $1<k<p-1$:
Յուրաքանչյուր a թվի համար, որը չի բաժանվում p պարզ թվի վրա, տեղի ունի $a \equiv g^k \pmod p$ բաղդատումը, որտեղ $0, 1, 2, \ldots, p-2$ թվերից որևէ մեկն է: Այդ դեպքում k-ն կոչվում է a թվի ինդեքս g հիմքով ըստ p մոդուլի և նշանակվում է $k = ind_g a$, կամ, ավելի հաճախ, առանց գրառելու հիմքը՝ $k = inda$:

Ինդեքսների համար տեղի ունեն հետևյալ հատկությունները.

ե) եթե $g^s \equiv g^t \pmod p$, ապա $s \equiv t \pmod{p-1}$;

զ) $ind1 = 0$, քանի որ միշտ $1 \equiv g^0 \pmod p$;

է) $ind(ab) = inda + indb \pmod{p-1}$;

ը) $inda^n \equiv ninda \pmod{p-1}$, որտեղ $n=0, 1, 2, \ldots$;

թ) $ind\dfrac{a}{b} \equiv inda - indb \pmod{p-1}$:

զ) – թ) հատկությունների կիրառումը կոչվում է ինդեքսավորում: Ինդեքսավորումը կատարվում է ինդեքսների միջոցով (տես հավելված):

14. 1 Գտնել այն ցուցիչները, որոնց ըստ m մոդուլի պատկանում են 2-ից $m-1$ բոլոր այն թվերը, որոնք փոխադարձ պարզ են m մոդուլի հետ.
1) m=5; 2)m=7; 3) m=8; 4) m=10; 5) m=11; 6) m=9:

14. 2 Գտնել ըստ հետևյալ մոդուլների նախնական արմատների քանակը և նրանցից փոքրագույնը.
1) 19; 2) 23; 3) 31; 4) 43; 5) 37; 6) 53:

14. 3 Գտնել δ ցուցիչը հետևյալ բաղդատումներում.

1) $5^\delta \equiv 1 \pmod 7$; 2) $5^\delta \equiv 1 \pmod{11}$; 3) $8^\delta \equiv 1 \pmod{13}$;

4) $12^\delta \equiv 1 \pmod{17}$; 5) $24^\delta \equiv 1 \pmod{31}$;

6) $10^\delta \equiv 1 \pmod{13}$; 7) $27^\delta \equiv 1 \pmod{17}$;

8) $18^\delta \equiv 1 \pmod{11}$; 9) $23^\delta \equiv 1 \pmod{41}$:

14.4 Լուծել հետևյալ ցուցչային բաղդատումները.

1) $2^x \equiv 7 \pmod{67}$; 2) $13^x \equiv 12 \pmod{47}$;

3) $16^x \equiv 11 \pmod{53}$; 4) $52^x \equiv 38 \pmod{61}$;

5) $12^x \equiv 17 \pmod{31}$; 6) $20^x \equiv 21 \pmod{41}$:

14. 5 Լուծել հետևյալ առաջին աստիճանի բաղդատումները.

1) $7x \equiv 23 \pmod{17}$; 2) $125x \equiv 7 \pmod{79}$;

3) $39x \equiv 84 \pmod{97}$; 4) $37x \equiv 25 \pmod{89}$;

5) $37x \equiv 5 \pmod{221}$; 6) $47x \equiv 13 \pmod{667}$:

14.6 Լուծել հետևյալ երկանդամ բաղդատումները.

1) $37x^{15} \equiv 62 \pmod{73}$; 2) $2x^8 \equiv 5 \pmod{13}$;

3) $27x^{15} \equiv 25 \pmod{31}$; 4) $23x^3 \equiv 15 \pmod{73}$;

5) $37x^8 \equiv 59 \pmod{61}$; 6) $11x^3 \equiv 6 \pmod{79}$:

14.7 Լուծել հետևյալ երկանդամ բաղդատումները.

1) $x^{12} \equiv 37 \pmod{41}$; 2) $x^{35} \equiv 17 \pmod{67}$;

3) $x^8 \equiv 23 \pmod{41}$; 4) $x^{27} \equiv 39 \pmod{43}$;

5) $x^2 \equiv 59 \pmod{67}$; 6) $x^2 \equiv -28 \pmod{67}$:

ՊԱՏԱՍԽԱՆՆԵՐ ԵՎ ՑՈՒՑՈՒՄՆԵՐ

1.1 *1) 134=26·5+4;* *2) 134=(-26) ·(-5)+4;* *3) –134=26·(-6)+22;*
4) –134= (-26) ·6+22;

1.2 *1) b=182, r=115;* *2) b=20, r=114;* *3) b=60,61 կամ 62*
r=15, 31 կամ 47;

1.3 Վերցնել $\frac{mn+pq}{m-p}=t$ ամբողջ թիվը և ցույց տալ, որ $\frac{mq+np}{m-p}-t$ ևս ամբողջ թիվ է:

1.4 եթե $N=\overline{abcde}\vdots 41$, ապա $N_1=\overline{bcdea}\vdots 41$:

1.5 $n(n^2+5)=n((n^2-1)+6)$;

2.1 *1) 21;* *2) 13;* *3) 119;*

2.2 *1) 2520;* *2) 138600;* *3) 99671;*

2.3 Ամենամեծ ընդհանուր բաժանարարը գտնել էվկլիդեսի ալգորիթմով:
1) 3276; *2) 1116;* *3) 67818;*

2.4 *1) x=3, y=150 և x=150, y=30;*

2) x_1=24, y_1=144; x_2=48, y_2=120; x_3=72, y_3=96 և հակառակը;

3) x=495, y=315;

4) x_1=4, y_1=180; x_2=20, y_2=36 և հակառակը:

2.5 *1) a_1=15, b_1=420; a_2=60, b_2=105 և հակառակը;*
2) a_1=15, b_1=420; a_2=60, b_2=105; a_3=60, b_3=168; a_4=84, b_4=120 և հակառակը;

3) a_1=5, b_1=260; a_2=20, b_2=65 և հակառակը;
4) a_1=232, b_1=435; a_2=115, b_2=552 և հակառակը;
5) a_1=6, b_1=84; a_2=12, b_2=42 և հակառակը;

2.6 1) Ըստ պայմանի, *a=899, b=493:* էվկլիդեսի ալգորիթմից կունենանք *a=b·1+406; b=406·1+87; 406=87·4+58; 87=58·1+29; 58=29·2:* Հետևաբար, *(a, b)=29:* Դիտարկելով այս հավասարությունները, սկսած նախավերջինից, կունենանք *29=87-58=87-(406-87·4)=87·5-406=(b-406) ·5-406=5b-406·6= =5b-(a-b) ·6=a·(-6)+b·11:* Հետևաբար *29=899x+493y*, որտեղ *x=-6* և *y=11:*
2) *17=a·(-10)+b·23;* 3) *43=a·(-4)+b·5;*
4) *47=a·2+b·(-5);* 5) *14=a·(-4)+b·67;*

2.7 $\frac{1}{a}+\frac{1}{a+b}=\frac{2a+b}{a(a+b)}$: Ցույց տալ, որ *(2a+b, a+b)=1*, և *(2a+b, a)=1* եթե *(a, b)=1:*

3.1 *1) 2333, 2339, 2341, 2347;*
2) 2647, 2657, 2659, 2663, 2671, 2677:

3.3 *3; 5; 7: p; p+2; p+4* թվերի մեջ վերցրեք *p=3q+r* և դիտարկեք *r*-ի հնարավոր արժեքները:

3.4 Ներկայացրեք *p*-ն *p=3q+r* տեսքով:

3.5 *1) p=3;* *2) p=3*
Բոլոր բնական թվերը կարելի է ներկայացնել $6k$, $6k\pm1$, $6k\pm2$, $6k+3$ տեսքով: 2 և 3 թվերից բացի, պարզ կարող են լինել $6k\pm1$ տեսքի թվերը:

3.6 *1) p=5;* *2) p=5*
Ներկայացրեք *p*-ն *p=5q+r* տեսքով:

3.7 *2519.* եթե n-ը անհայտ թիվ է, ապա *n+1* թիվը բաժանվում է *2*-ի, *3*-ի, *4*-ի, *5*-ի, *6*-ի, *7*-ի, *8*-ի, *9*-ի և *10*-ի, այսինքն *n+1=[2,3,4,5,6,7,8,9,10]:*

3.8 959:

3.9 $p=30k\pm1$, $30k\pm7$, $30k\pm11$, $30k\pm13$: Մնացածը պարզ է:

3.10 *(p-1)p(p+1)* բաժանվում է *3*-ի, բայց *p*-ն չի բաժանվում *3*-ի, ուրեմն *(p-1)(p+1)* բաժանվում է *3*-ի: Մյուս կողմից՝ *p-1* և *p+1* հաջորդական պարզ թվեր են (ինչու՞), ուրեմն *(p-1)(p+1)=p^2-1* բաժանվում է *8*-ի (ինչու՞): Բացի դրանից, *p^2-q^2=(p^2-1)-(q^2-1):*

3.11 $\frac{2}{p}=\frac{1}{x}+\frac{1}{y}$; $2xy=p(x+y)\Rightarrow p|2xy$ և քանի որ $p\nmid 2$, ապա կամ $p|x$ կամ $p|y$: Եթե $p|x$, ապա $x=ps$ և այլն:

3.12 1) Ենթադրենք, *4m-1* տեսքի պարզ թվերի բազմությունը վերջավոր է, և *a*-ն այդ բոլոր թվերի արտադրյալն է: Դիտարկենք *4a-1* թիվը: Այն պետք է ունենա *4m-1* տեսքի *q* պարզ բաժանարար, քանի որ *4m+1* տեսքի թվերի արտադրյալը ևս նույն տեսքի թիվ է: Հետևաբար, $q|a$ և $q|4a-1$, որը հնարավոր չէ, քանի որ *(a, 4a-1)=1*:

3.13 Ցուցում. կատարել հակասող ենթադրություն: Հակառակը ճիշտ չէ (բերել օրինակ):

3.14. Ցուցում. *k*-ն բաժանել 3-ի մնացորդով:

4.1 1) $\frac{29}{37}=(0,1,3,1,1,1,2)$:

4.2 1) $\frac{a}{b}=\frac{64}{25}$; 2) $\frac{a}{b}=\frac{73}{43}$; 5) $\frac{a}{b}=\frac{2633}{2041}$:

4.3 1) $\frac{17}{13}$; 3) $\frac{281}{239}$; 6) $\frac{101}{103}$:

4.4 1) Վերլուծելով $\frac{38}{117}$ կոտորակը անընդհատի, կստանանք $\frac{38}{117}=(0,3,12,1,2)$: Գտնել մերձավոր կոտորակները՝

q_s		0	3	12	1	2
P_s	1	0	1	12	13	38
Q_s	0	1	3	37	40	117

Այստեղ $P_{n-1}=13$, $Q_{n-1}=40$, $n=5$ և $x_2=(-1)^5\cdot 40\cdot 209=-8360$, $y_1=(-1)^4\cdot 13\cdot 209=2717$: Ընդհանուր լուծումը կլինի.

x=-8360-117t, y=2717+38t
3) *x=-2t4t, y=-4+7t, 5) x=-125-114t, y=45+41t*

5.1 *1) 2; 2) 4; 3) 4; 4) 5; 5) 9; 7) 15; 9) 46*

5.2 *1) ln50=3,9120;* $\pi(50)\approx\frac{50}{3,9120}\approx 13$;

2) ≈ 22; 3) ≈ 80; 4) ≈ 145

5.3 1) $2<\frac{8}{3}<3$, ուրեմն $\left[\frac{8}{3}\right]=2$; 2) 0; 3) 2; 4) 0; 5) –4;

6) –3; 8) 5; 10) 3; 12) 5; 14) $0<\cos\frac{101\pi}{205}<1$ և

$4<4+\cos\frac{101\pi}{205}<5$, ուրեմն $\left[4+\cos\frac{101\pi}{205}\right]=4$; 16) 1;

18) $-4<-\lg 2512<-3$, ուրեմն $[2-\lg 2512]=-2$; 20) -3;

21) {2,6}=2,6-2=0,6; 22) $\frac{2}{3}$; 23) 0; 24) 0,65; 26) $\frac{1}{2}$:

5.4 Ցուցում. Եթե $x=[x]+\alpha$, $y=y[y]+\beta$, որտեղ $0\le\alpha<1$, $0\le\beta<1$, ապա $x+y=[x]+[y]+(\alpha+\beta)$, որտեղ $0\le\alpha+\beta<1$ կամ $1\le\alpha+\beta<2$:

5.5 $x=\frac{m+\alpha}{a}$, որտեղ $0\le\alpha<1$:

5.6 Այն α ցուցիչը, որով *p* պարզ թիվը մտնում է *n!* թվի վերլուծության մեջ, գտնում են հետևյալ բանաձևով.

$$\alpha=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots\ldots;$$

1) 48; 2) 98; 3) 81:

5.7 1) 100! թիվը ավարտվում է այնքան 0-ով, քանի անգամ 5 թիվը մտնում է 100! թվի վերլուծության մեջ (ինչու՞): Ուրեմն՝

$$\left[\frac{100}{5}\right]+\left[\frac{100}{5^2}\right]+20+4=24$$ հատ 0; 2) 28:

5.8 1) $\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right]=5+2+1=8$; $\left[\frac{10}{3}\right]+\left[\frac{10}{3^2}\right]=3+1=4$;

$\left[\frac{10}{5}\right]=2$; $\left[\frac{10}{7}\right]=1$, ուրեմն՝ $10!=2^8\cdot 3^4\cdot 5^2\cdot 7$;

2) $2^{11}\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13$; 3) $2^{18}\cdot 3^8\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17$;

4) $2^{22}\cdot 3^{10}\cdot 5^6\cdot 7^3\cdot 11^2\cdot 13\cdot 17\cdot 19\cdot 23$;

5) $2^{26}\cdot 3^{14}\cdot 5^7\cdot 7^4\cdot 11^2\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29$;

5.9 Այն բնական թվերի քանակը, որոնք չեն գերազանցում n-ին և փոխադարձ պարզ են $p_1,p_2,\ldots,p_k$ թվերից յուրաքանչյուրի հետ, հաշվում են հետևյալ բանաձևով.

$$B(n;p_1;p_2,\ldots,p_k)=[n]-\left[\frac{n}{p_1}\right]-\ldots-\left[\frac{n}{p_k}\right]+\left[\frac{n}{p_1p_2}\right]+\ldots+\left[\frac{n}{p_{k-1}p_k}\right]-$$

$$\left[\frac{n}{p_1p_2p_3}\right]--\ldots-\left[\frac{n}{p_{k-2}p_{k-1}p_k}\right]+\ldots+(-1)^k\cdot\left[\frac{n}{p_1p_2\cdots p_k}\right]$$

$$B(180,5,7,11)=[180]-\left[\frac{180}{5}\right]-\left[\frac{180}{7}\right]-\left[\frac{180}{11}\right]+\left[\frac{180}{5\cdot 7}\right]+\left[\frac{180}{5\cdot 11}\right]+$$

$$+\left[\frac{180}{7\cdot 11}\right]-\left[\frac{180}{5\cdot 7\cdot 11}\right]=113$$

2) 1378; 3) B(100; 2, 3)=33; 4) 5634

5.10 1) 624; 8; 2) 2418; 30; 3) 1440; 8; 4) 1960; 12; 5) 2808; 24; 6) 3844; 30

5.11 1) $360=2^3\cdot 3^2\cdot 5$ և եթե $(1+2+2^2+2^3)(1+3+3^2)(1+5)$ արտահայտության մեջ բացենք փակագծերը, ապա ստացված գումարելիները կլինեն 360-ի բոլոր բնական բաժանարարները:

5.12 $n=p^\alpha q^\beta$, p և q պարզ են: $\tau(n)=(\alpha+1)(\beta+1)=6$ ուրեմն $\alpha=1,\ \beta=2$ (կամ $\alpha=2,\ \beta=1$): Հետևաբար. $n=pq^2$ և, ըստ պայմանի, $\sigma(n)=(1+p)(1+q+q^2)=28$, որտեղից՝ $1+q+q^2=7$, $1+p=4$ (ինչու՞): Հետևաբար, $q=2$, $p=3$ և $n=3\cdot 2^2=12$: Նույնը կստացվի, եթե $\alpha=2,\beta=1$:

5.13 $n=p^\alpha q^\beta$, $n^2=p^{2\alpha}q^{2\beta}$, $n^3=p^{3\alpha}q^{3\beta}$; $\tau(n)=(\alpha+1)(\beta+1)$, $\tau(n^2)=(2\alpha+1)(2\beta+1)$, $\tau(n^3)=(3\alpha+1)(3\beta+1)$: Ստացվում է $\tau(n^3)=28$:

5.14 Քանի որ $(p_1^{\alpha_1})^k\cdot(p_2^{\alpha_2})^k\ldots(p_n^{\alpha_n})^k=(p_1^k)^{\alpha_2}(p_2^k)^{\alpha_2}\ldots(p_n^k)^{\alpha_n}$, ապա $\sigma_k(a)$ գումարը կստացվի, եթե $\sigma(a)$-ի բանաձևի մեջ $p_1,p_2,\ldots,p_n$ թվերը փոխարինենք համապատասխանաբար $p_1^k,p_2^k,\ldots,p_n^k$ թվերով՝

$$\sigma_k(a)=\frac{p_1^{k(\alpha_1+1)}-1}{p_1^k-1}\cdot\frac{p_2^{k(\alpha_2+1)}-1}{p_2^k-1}\cdot\ldots\cdot\frac{p_n^{k(\alpha_n+1)}-1}{p_n^k-1}:$$

1) 210; 2) 455; 3) 341:

5.15 $28=2^2\cdot 7$; $\sigma(28)=\frac{2^3-1}{2-1}\cdot\frac{7^2-1}{7-1}=7\cdot 8=56=2\cdot 28$:

5.16 Գրենք a-ի բոլոր բաժանարարները՝ $1,\ a_1, a_2, \ldots, \frac{a}{a_2}, \frac{a}{a_1}, \frac{a}{1}$:

Յուրաքանչյուր a_i բաժանարարի համապատասխանում է $\frac{a}{a_i}$ բաժանարար, ուրեմն բաժանարարների թիվը զույգ է, բացառությամբ այն դեպքի, երբ $a=b^2$, այսինքն, երբ b բաժանարարին համապատասխանում է $\frac{a}{b}=\frac{b^2}{b}=b$ միևնույն բաժանարարը: Բազմապատկելով բաժանարարների յուրաքանչյուր զույգ, կստանանք $a_i \cdot \frac{a}{a_i} = a$, իսկ այդ զույգերի քանակը կլինի $\frac{n}{2}$, որտեղ $n=\tau(a)$: Այսպիսով, բոլոր բաժանարարների արտադրյալը՝ $P=\left(a_i \cdot \frac{a}{a_i}\right)^{\frac{n}{2}} = a^{\frac{n}{2}}$: Բանաձևը ճիշտ է նաև $a=b^2$ դեպքում՝ $P=\left(a_i \cdot \frac{a}{a_i}\right)^{\frac{n-1}{2}} \cdot b = a^{\frac{n-1}{2}} \cdot a^{\frac{1}{2}} = a^{\frac{n}{2}}$:

1) 18; 2) $3^3 \cdot 5^4 = 16875$:

5.17 Հետևում է $\tau(n)$-ի բանաձևից:

5.18 1) 5.17-ից՝ a-ն բնական թվի քառակուսի է և, քանի որ $\tau(a)=15=1\cdot 15=3\cdot 5$, ապա $a=p^{14}$ կամ $a=p^2q^4$ (p և q պարզ թվեր են): $a=p^{14}$ հնարավոր չէ (ինչու՞), իսկ $a=p^2q^4$ դեպքում $32 \le pq^2 \le 99$, իսկ այդ պայմանին բավարարում են $2\cdot 5^2$, $2\cdot 7^2$, $3\cdot 5^2$, $5\cdot 3^2$, $7\cdot 3^2$, $11\cdot 2^2$, $11\cdot 3^2$, $13\cdot 2^2$, $17\cdot 2^2$, $19\cdot 2^2$, $23\cdot 2^2$ թվերը, որոնց քառակուսիներն էլ կլինեն խնդրի պայմանին բավարարող քառանիշ թվերը;
2) Օգտվեք 5.17-ից:

5.19 1) $\varphi(375)=\varphi(3\cdot 5^3)=3\cdot 5^3\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)=200$; 2) 192;

4) 432; 6) 320; 8) 400; 10) 1152;

5.20 1) $\varphi(17)=17-1=16$; 2) 30; 4) 70; 6) $\varphi(3^5)=3^4\cdot 2=162$
6) 320; 8) 400; 10) 1152;

5.21 Պետք է օգտվել էյլերի ֆունկցիայի արտադրյալային լինելուց, իսկ դրա համար տվյալ արտադրյալները պետք է ներկայացնել կանոնական վերլուծությամբ: Օրինակ՝ $12\cdot 25\cdot 35=2^2\cdot 3\cdot 5^3\cdot 7$:
1) 40; 2) 288;
3) $\varphi(12\cdot 7)=\varphi(2^2\cdot 3\cdot 7)=\varphi(2^2)\cdot\varphi(3)\cdot\varphi(7)=24$;
6) 480; 10) 388800:

5.22 1) $\varphi(a)=3^{\alpha-1}\cdot 2\cdot 5^{\beta-1}\cdot 4\cdot 7^{\gamma-1}\cdot 6=2^4\cdot 3^{\alpha}\cdot 5^{\beta-1}\cdot 7^{\gamma-1}$ և
$\varphi(a)=3600=2^4\cdot 3^2\cdot 5^2$, ուրեմն
$\alpha=2, \beta=3, \gamma=1$, $a=3^2\cdot 5^2\cdot 7=7875$;
2) 143; 3) 14161;

5.23 Նախ՝ հակասող ենթադրությամբ ցույց տալ, որ եթե $(a,m)=1$, ապա $(a, m-a)=1$: Այժմ, եթե գրենք m-ից փոքր և նրա հետ փոխադարձ պարզ թվերն աճման կարգով՝ $1, a_1, a_2, \ldots, m-a_2, m-a_1, m-1$, նրանց քանակը կլինի $\varphi(m)$ և յուրաքանչյուր a_i-ի կհամապատասխանի $m-a_i$, ընդ որում, յուրաքանչյուր զույգի գումարը՝ $a_i+(m-a_i)=m$, այդ զույգերի քանակը $\frac{1}{2}\varphi(m)$ է և $S=\frac{1}{2}m\cdot\varphi(m)$:
2) 24; 3) 54; 5) 37500:

5.24 1) $x=3$; 3) $x=7$; 3) $x=3, y=2$:

5.26 $\varphi(b)$: 1) 4; 3) 12;

5.27 1) $(300, x)=20$ և $x<300$: Այստեղից՝ $(15, y)=1$, և $y<15$: Նրանց (y-ների, ուրեմն նաև x-երի) քանակը կլինի $\varphi(15)=8$;
2) $\varphi(45)=24$; 3) $\varphi(36)=12$:

5.28 1) $a=72=2^3\cdot 3^2$: Գտնում ենք a-ի բոլոր բաժանարարները՝ $(1+2+2^2+2^3)\cdot(1+3+3^2)$: Չբացելով փակագծերը, ընդունելով

$\varphi(1)=1$, վերցնում ենք բոլոր բաժանարարների էյլերի ֆունկցիան՝

$$\sum_{d/a}\varphi(d)=(\varphi(1)+\varphi(2)+\varphi(2^2)+\varphi(2^3))\cdot(\varphi(1)+\varphi(3)+\varphi(3^2))=$$
$$=(1+1+2+4)\cdot(1+2+6)=72=a$$

5.29 1) եթե $\varphi(x)=\frac{1}{2}x$, ապա x-ը զույգ թիվ է՝ 2/x և $x=2^{\alpha}\cdot n$, որտեղ n-ը կենտ թիվ է: Այդ դեպքում $\varphi(2^{\alpha}\cdot n)=\frac{1}{2}2^{\alpha}\cdot n$,

$2^{\alpha-1}\varphi(n)=2^{\alpha-1}\cdot n$, $\varphi(n)=n$, որը հնարավոր է միայն, եթե n=1, ուրեմն, $x=2^{\alpha}, \alpha\in\mathrm{N}$; 2) 3^{α}, $\alpha\in N$; 3) $2^{\alpha}\cdot 3^{\beta}$, $\alpha,\beta\in\mathrm{N}$; 4) լուծում չկա; 5) 5^{α}, $\alpha\in\mathrm{N}$:

6.1 1) 1; 2) 15; 3) 0; 4) 1; 5) 8; 6) 12; 7) 12; 8) 4; 9) 3; 10) 25; 11) 4: Լուծում՝ $1532\equiv 2(\mathrm{mod}\,9)$,

$1532^5\equiv 2^5=32\equiv 5(\mathrm{mod}\,9)$, և քանի որ $1\equiv 1(\mathrm{mod}\,9)$, ապա՝

$1532^5-1\equiv 4(\mathrm{mod}\,9)$ և պահանջվող մնացորդը հավասար է 4:

6.2 1) Ըստ պայմանի, $100a+10b+c\equiv 0(\mathrm{mod}\,21)$, ուրեմն՝

$400a+40b+4c\equiv 0(\mathrm{mod}\,21)$: Քանի որ $400a\equiv a(\mathrm{mod}\,21)$,

$40b\equiv -2b(\mathrm{mod}\,21)$, $4c\equiv 4c(\mathrm{mod}\,21)$, ապա, գումարելով վերջին բաղդատումները, կստանանք՝

$400a+40b+4c\equiv a-2b+4c(\mathrm{mod}\,21)$ և հետևաբար՝

$a-2b+4c\equiv 0(\mathrm{mod}\,21)$:

7.1 1) Մնացքների լրիվ համակարգերը՝ 0, 1, 2, 3, 4, 5, 6, 7, 8; -8, -7, -6, -5, -4, -3, -2, -1, 0; -4, -3, -2, -1, 0, 1, 2, 3, 4;
Մնացքների բերված համակարգեր՝ 1,2, 4, 5, 7, 8; -8, -7, -5, -4, -2, -1, 1, 2, 4:

7.2 1) 25=8·3+1, -20=8·(-3)+4, 16=8·2+0, 46=8·5+6, -21=8·(-3)+3, 18=8·2+2, 37=8·4+5, -17=8·(-3)+7:

Բոլոր ստացված մնացորդներն իրարից տարբեր են, և կազմում են փոքրագույն ոչ բացասական մնացքների լրիվ համակարգ (0, 1, 2, 3, 4, 5, 6, 7), ուրեմն տրված թվերը ևս կազմում են մնացքների լրիվ համակարգ:

7.3 1) 16; 16; 2) 4; 4; 3) –7; 9; 4) 8; 8; 5) –30; 31; 6) –17; 20; 7) 0;0; 8) –1; 24:

8.1 1) Քանի որ $383\equiv 23(\mathrm{mod}\,45)$, ապա $383^{175}\equiv 23^{175}(\mathrm{mod}\,45)$;

Քանի որ $\varphi(45)=24$ և (23, 45)=1, ապա էյլերի թեորեմից՝

$23^{24}\equiv 1(\mathrm{mod}\,45)$, հետևաբար՝

$23^{175}=23^{24\cdot 7+7}=(23^{24})^7\cdot 23^7\equiv 1^7\cdot 23^7(\mathrm{mod}\,45)$: Բայց

$23^7=(23^2)^3\cdot 23=529^3\cdot 23\equiv 34^3\cdot 23=34^2\cdot 34\cdot 23=$

$=1156\cdot 782\equiv 31\cdot 17=527\equiv 32(\mathrm{mod}\,45)$:

Ուրեմն՝ $383^{175}\equiv 32(\mathrm{mod}\,45)$, և պահանջվող մնացորդը հավասար է 32:

2) 1, 3) 19, 4) 29, 5) քանի որ $\varphi(11)=10$ և (3, 11) =1, ապա

$3^{10}\equiv 1(\mathrm{mod}\,11)$ և $7^{10}\equiv 1(\mathrm{mod}\,11)$, հետևաբար՝

$3^{80}=(3^{10})^8\equiv 1(\mathrm{mod}\,11)$ և $7^{80}=(7^{10})^8\equiv 1(\mathrm{mod}\,11)$: Գումարելով այդ բաղդատումները, կստանանք՝ $3^{80}+7^{80}\equiv 2(\mathrm{mod}\,11)$, այսինքն պահանջվող մնացորդը հավասար է 2; 6) 6, 7) 2, 8) 2:

8.2 Թվի՝ վերջին երկու (երեք) թվանշաններով կազմված թիվն այդ թիվը՝ 100-ի (1000-ի) վրա բաժանելիս ստացված մնացորդն է:
1) 76, 2) 24, 3) 049, 4) 289:

8.3 1) $a^p-1=(a-1)(a^{p-1}+a^{p-2}+\ldots+a+1)\equiv 0(\mathrm{mod}\,p)$: Ֆերմայի թեորեմի հետևանքից՝ $a^p\equiv a(\mathrm{mod}\,p)$, ուրեմն՝

$a^p-1\equiv a-1(\mathrm{mod}\,p)$: Վերջին բաղդատումից՝

$a^{p-1}\equiv 1(\mathrm{mod}\,p),\ldots,a\equiv 1(\mathrm{mod}\,p)$, $1\equiv 1(\mathrm{mod}\,p)$, որոնք գումարելով, կստանանք՝ $a^{p-1}+\ldots+a+1\equiv p\equiv 0(\mathrm{mod}\,p)$ և

ուրեմն $a^p - 1 \equiv 0(\bmod p^2)$: Նույն ձևով, եթե $a^p + 1 \equiv 0(\bmod p)$, ապա $a^p + 1 \equiv 0(\bmod p^2)$:

2) Ֆերմայի թեորեմից՝ $p^{q-1} - 1 \equiv 0(\bmod p)$ և $q^{p-1} - 1 \equiv 0(\bmod p)$;

3) եթե $p=3$, ապա $8p^2+1=73$ պարզ է: Եթե $p \neq 3$, ապա $(p, 3)=1$ և կիրառելով Ֆերմայի թեորեմը, ստանում ենք՝ $8p^2 + 1 \equiv 9 \equiv 0(\bmod 3)$;

4) p և $2p+1$ պարզ են, ուրեմն $(2p+1)^2 \equiv 1(\bmod 3)$ և $p^2 \equiv 1(\bmod 3)$ (ըստ Ֆերմայի թեորեմի), որտեղից էլ ստանում ենք՝ $4p + 1 \equiv -3 \equiv 0(\bmod 3)$:

5) Դիտարկել երկու դեպք՝ a-ն բազմապատիկ է 5-ին և $(a, 5)=1$:

6) Եթե $(n, 6)=1$, ապա $(n, 2)=1$ և $(n, 3)=1$: Առաջինից կստանանք՝ $n^2 \equiv 1(\bmod 8)$, իսկ երկրորդից (Ֆերմայի թեորեմով)՝ $n^2 \equiv 1(\bmod 3)$:

9.1 1) $x \equiv 1(\bmod 3)$, $x \equiv 2(\bmod 3)$; 2) $x \equiv 1(\bmod 5)$, $x \equiv 2(\bmod 5)$; 3) $x \equiv 2(\bmod 5)$; 4) $x \equiv 9(\bmod 13)$;
5) լուծում չունի; 6) լուծում չունի; 7) լուծում չունի;
8) $x \equiv 3(\bmod 5)$:

9.2 1) $x \equiv 3(\bmod 7)$; 2) $x \equiv -3(\bmod 11)$; 3) $x \equiv 2(\bmod 5)$;
4) $x \equiv -3(\bmod 7)$; 6) $x \equiv -3(\bmod 7)$; 9) փոխարինելով գործակիցներն ըստ 15 մոդուլի փոքրագույն ոչ բացասական մնացքներով, կստանանք $x^2 - 7x + 1 \equiv 0(\bmod 15)$ բաղդատումը, որի լուծումն է $x \equiv -4(\bmod 15)$:

10.1 Որոշ դեպքերում բաղդատումը նախ պարզեցնել:
1) $43x \equiv 8(\bmod 34) \Leftrightarrow 9x \equiv 8(\bmod 34)$: Քանի որ (9,34)=1 և $\varphi(34) = 16$, ապա
$x \equiv 8 \cdot 9^{15} \equiv 8 \cdot 3^{30} \equiv 8 \cdot 3^{14} \equiv 8 \cdot (2187)^2 \equiv 8 \cdot 11^2 \equiv 16(\bmod 34)$;
4) լուծում չունի, քանի որ (5, 10)=5, իսկ 7-ը չի բաժանվում 5-ի;

5) $x \equiv 7(\bmod 13)$; 8) $x \equiv 10(\bmod 12)$; 9) լուծում չունի:

10.2 1) $\frac{87}{55}$ կոտորակը անընդհատ կոտորակի վերլուծելիս մերձավոր կոտորակների P_i համարիչների համար ստանում ենք աղյուսակ.

a_i	1	1	1	2	1	1	4
P_i	1	2	3	8	11	19	87

Այստեղ n=6 P_{n-1}=19 և բաղդատման լուծումը կլինի՝
$x \equiv (-1)^6 \cdot 7 \cdot 19 \equiv 46(\bmod 87)$;
2) $x \equiv 6(\bmod 19)$:

10.3 1) Լուծում չունի, քանի որ (12, 18)=6, իսկ 9-ը չի բաժանվում 6-ի;
3) Քանի որ (20, 10, 25)=5, ապա կրճատելով բաղդատման անդամները և մոդուլը 5-ով, կստանանք $4x \equiv 2(\bmod 5)$, կամ $2x \equiv 1(\bmod 5)$ բաղդատումը, որի լուծումն է $x \equiv 3(\bmod 5)$: Այժմ $x_{k+1} \equiv m_1 k + \alpha(\bmod m)$ բանաձևից՝ $x_1 \equiv 3$, $x_2 \equiv 8$, $x_3 \equiv 13$, $x_4 \equiv 18$, $x_5 \equiv 23(\bmod 25)$:

10.4 1) Կցագրվող թիվը նշանակենք x: Այդ դեպքում $523 \cdot 10^3 + x \equiv 0(\bmod 7 \cdot 8 \cdot 9)$, որտեղից՝ $x \equiv -5230000 \equiv 152(\bmod 504)$, այսինքն $x=504t+152$ դասն է: x-ի արժեքը եռանիշ կլինի $t=0$ և $t=1$ դեպքում՝ x_1=152, x_2=656:

11.1 1) $x=5t+4$; $5t+4 \equiv 1(mod12)$; $t \equiv 9(mod12)$; $t=12t_1+9$; $x=5(12t_1+9)+4=60t_1+49$; $60t_1+49 \equiv 7(mod14)$; $t_1 \equiv 0(mod7)$; $t_1=7t_2$; $x=60(7t_2+0)+49=420t_2+49$: Համակարգի լուծումը կլինի՝ x≡49(mod420):
3) $x \equiv 4126(mod6300)$; 5) $x \equiv 85056(mod130169)$;
6) $x \equiv 9573(mod13923)$:

11.2 1) 262; 2) 299;

11.3 1) Առաջին բաղդատումից՝ $x=18t+5$: Տեղադրելով երկրորդի մեջ, ստանում ենք t-ն՝ $t \equiv 6(mod7)$, կամ ավելի հարմար է $t \equiv -1(mod7)$, $t=7y-1$, և՝ $x=18(7y-1)+5=126y-13$: Տեղադրելով երրորդի մեջ, ստանում ենք. 21y≡a+13(mod35): Քանի որ $(21, 35)=7$, ապա վերջին

բաղդատումը, ուրեմն նաև տրված համակարգը կլինեն համատեղելի միայն այն դեպքում, երբ $a+13\equiv 0(mod7)$, կամ՝ $a\equiv 1(mod7)$:

2) $a\equiv 1(mod6)$:

11.4 Եթե $(a, b)=1$, ապա $ax+by=c$ հավասարումը (a, b, c ամբողջ թվեր են) ունի ամբողջ լուծումներ, որոնք ընդհանուր տեսքով գրվում են այսպես՝ $x=x_1+bt$, $y=y_1-at$ կամ, բացասական b-ի դեպքում հարմար է վերցնել $x=x_1-bt$, $y=y_1+at$. Այդ բանաձևերում x_1 և y_1 տրված հավասարմանը բավարարող x-ի և y-ի որևէ արժեքներ են, իսկ t-ն ցանկացած ամբողջ թիվ է: Եթե $(a, b)=d>1$ և d / c, ապա $ax+by=c$ հավասարումն ամբողջ թվերով լուծում չունի:

Բաղդատումներով x_1 և y_1 գտնում են այսպես.

$ax+by=c \Rightarrow ax\equiv c(modb)$, որտեղ b-ն վերցնում է + նշանով: Այդ բաղդատմանը բավարարող x-ի արժեքը վերցնում են որպես x_1, տեղադրում այն $ax+by=c$ հավասարման մեջ և վերցնում

$$y_1=\frac{c-ax_1}{b}:$$

1) $x=3+4t$, $y=1-3t$; 2) $x=3+13t$, $y=-3+8t$; 3) $x=20+22t$, $y=35+39t$;

4) $x=22-37t$, $y=-25+43t$; 5) $x=17+37t$, $y=20+45t$;

6) կրճատել գործակիցները 3-ով; $x=1+16t$, $y=1+27t$:

12.1 1) Բաղդատման գործակիցները արտաքսելով մոդուլին բազմապատիկ թվերը, կստանանք $x^{10}-2x+1\equiv 0(\mathrm{mod}\,5)$: Բաժանելով $x^{10}-2x+1$ բազմանդամը (x^5-x)-ի, մնացորդում կստանանք՝

x^2-2x+1, ուրեմն տրված բաղդատումը համարժեք է հետևյալին.

$x^2-2x+1\equiv 0(mod5)$: Փորձարկելով ըստ 5 մոդուլի բացարձակ փոքրագույն մնացքները՝ 0; ±1; ±2, կգտնենք $x\equiv 1(mod5)$ լուծումը:

2) $x\equiv 2(mod3)$; 3) $x\equiv 3$, $x\equiv 4(mod5)$, 4) $x\equiv 1(mod5)$;
5) լուծում չունի; 6) $x\equiv 4(mod5)$:

12.2 1) Փորձարկելով 0; ±1; ±2 մնացքները, ստանում ենք լուծումներից մեկը՝ $x\equiv -1\equiv 4(mod5)$: Ուրեմն՝ $f(x)\equiv(x-4)f_1(x)(mod5)$: $f_1(x)$-ը գտնում ենք որպես $f(x)$-ը $(x-4)$-ի վրա բաժանելիս ստացված քանորդ՝ $f_1(x)=x^2+8x+32\equiv 0(mod5)$: Նրա լուծումը՝ $x\equiv -2\equiv 3(mod5)$ և՝

$f_1(x)\equiv(x-3)f_2(x)(mod5)$; $f_1(x)$-ը բաժանելով $(x-3)$-ի՝ քանորդում ստանում ենք՝ $f_2(x)=x+11\equiv 0(mod5)$ և $x\equiv 4(mod5)$, ուրեմն՝ $f_2(x)\equiv x-4(mod5)$: Վերջնականապես՝ $f(x)\equiv(x-3)(x-4)(mod5)$;

2) $f(x)\equiv(x-2)^2(x-3)(x-4)(mod11)$; 3) $f(x)\equiv(x-3)(3x^2+4x+2)(mod5)$, քանի որ $3x^2+4x+2\equiv 0(mod5)$ բաղդատումը լուծում չունի;

4) $f(x)\equiv(x-2)^2(x-5)^2(mod7)$; 5) լուծում չունի;

6) $f(x)\equiv(x-2)(x-3)(x^2-2x+3)(mod7)$:

12. 3 1) Վիլսոնի թեորեմից՝ $(p-1)!+1\equiv 0(modp)$, ուրեմն՝

$(p-2)!(p-1)+1=(p-2)!\cdot p-(p-2)!+1\equiv(p-2)!-1\equiv 0(modp)$:

13.1 1) $\frac{p-1}{2}=5$, $1^5\equiv 1$, $2^5\equiv -1$, $3^5\equiv 1$, $4^5\equiv 1$, $5^5\equiv 1$,

$6^5\equiv -1$, $7^5\equiv -1$, $8^5\equiv -1$, $9^5\equiv 1$, $10^5\equiv -1(\mathrm{mod}\,11)$,

հետևաբար, ըստ 11 մոդուլի քառակուսային մնացքների դասեր են՝ $\overline{1}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{9}$, իսկ քառակուսային ոչ մնացքների դասեր՝ $\overline{2}$, $\overline{6}$, $\overline{7}$, $\overline{8}$, $\overline{10}$:

2) Քառակուսային մնացքների դասեր՝ $\overline{1}$, $\overline{2}$, $\overline{4}$, ոչ մնացքների դասեր՝ $\overline{3}$, $\overline{5}$, $\overline{6}$:

13.2 1) 113-ը պարզ թիվ է և, հաշվելով Լեժանդրի պայմանանշանը, կունենանք.

$$\left(\frac{68}{113}\right)=\left(\frac{2}{113}\right)^2\left(\frac{17}{113}\right)=\left(\frac{113}{17}\right)=\left(\frac{11}{17}\right)=$$

$$=\left(\frac{17}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)-\left(\frac{3}{11}\right)=\left(\frac{11}{3}\right)=\left(\frac{2}{3}\right)=-1$$

ուրեմն տվյալ բաղդատումը լուծում չունի:

2)
$$\left(\frac{310}{521}\right)=\left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right)=\left(\frac{521}{5}\right)\left(\frac{521}{31}\right)=$$

$$=\left(\frac{1}{5}\right)\left(\frac{25}{31}\right)=\left(\frac{5^2}{31}\right)=1$$

ուրեմն տվյալ բաղդատումն ունի երկու լուծում:
3) ունի երկու լուծում; 4) ունի երկու լուծում;
5) լուծում չունի; 6) լուծում չունի;
7) ունի երկու լուծում; 8) ունի երկու լուծում;
9) ունի երկու լուծում:

13.3 1) $x \equiv \pm 3 (\mathrm{mod}\, 7)$; 2) $x \equiv \pm 2 (\mathrm{mod}\, 7)$; 3) լուծում չունի;
4) լուծում չունի; 5) $x \equiv \pm 4 (\mathrm{mod}\, 11)$; 6) $x \equiv \pm 5 (\mathrm{mod}\, 13)$:

13.4 1) Բազմապատկելով բաղդատման երկու մասը 12-ով, կստանանք. $36x^2 + 12 \cdot 7x + 96 \equiv 0 (\mathrm{mod}\, 17)$, $(6x+7)^2 \equiv 4 (\mathrm{mod}\, 17)$, և եթե նշանակենք 6x+7=y, կունենանք $y^2 \equiv 4 (\mathrm{mod}\, 17)$ բաղդատումը, որն ունի երկու լուծում՝ $y \equiv \pm 2 (\mathrm{mod}\, 17)$: Այժմ, տրված բաղդատումը լուծելու համար պետք է լուծել հետևյալ բաղդատումները. $6x + 7 \equiv 2 (\mathrm{mod}\, 17)$ և $6x + 7 \equiv -2 (\mathrm{mod}\, 17)$, որոնց լուծումներն են համապատասխանաբար $x \equiv 2 (\mathrm{mod}\, 17)$ և $x \equiv 7 (\mathrm{mod}\, 17)$;
2) լուծում չունի; 3) $x \equiv 2 (\mathrm{mod}\, 13)$, $x \equiv 3 (\mathrm{mod}\, 13)$:

13.5 Ըստ էյլերի հայտանիշի, եթե a-ն քառակուսային մնացք է ըստ p մոդուլի, ապա $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$: Ուրեմն՝ $a^{\frac{p+1}{2}} \equiv a (\mathrm{mod}\, p)$ և, քանի որ $p = 4k+3$, ապա $a^{2k+2} \equiv a (\mathrm{mod}\, p)$, կամ՝ $(a^{k+1})^2 \equiv a (\mathrm{mod}\, p)$, որտեղից՝ $x \equiv \pm a^{k+1} (\mathrm{mod}\, p)$:
1) $\left(\frac{2}{311}\right) = 1$, $p = 311 = 77 \cdot 4 + 3$, $k = 77$,
$x \equiv \pm 2^{k+1} = \pm 2^{78} \equiv \pm 66 (\mathrm{mod}\, 311)$;
2) $x \equiv \pm 12 (\mathrm{mod}\, 47)$:

13.6 1) Դիտարկել $5x^2 - 7 \equiv 0 (\mathrm{mod}\, 11)$ բաղդատումը;
2) Դիտարկել $x(x+1) \equiv 1 (\mathrm{mod}\, 13)$ բաղդատումը:

13.7 1) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8t+7)^2-1}{8}} = 1$, ուրեմն 2-ը քառակուսային մնացք է ըստ p մոդուլի;
2) 2-ը քառակուսային ոչ մնացք է ըստ p մոդուլի:

14.1 Ըստ գ) հատկության, ցուցիչները պետք է փնտրել $\varphi(m)$-ի բաժանարարների մեջ:
1) $a = 2$, $\delta = 4$; $a = 3$, $\delta = 4$; $a = 4$, $\delta = 2$;
3) $a = 3$, $\delta = 2$; $a = 5$, $\delta = 2$; $a = 7$, $\delta = 2$;
5) $a = 2, 6, 7, 8$, $\delta = 10$; $a = 3, 4, 5, 9$, $\delta = 5$; $a = 10$, $\delta = 2$:

14.2 1) $p = 19$, $\varphi(p) = 18$, 18-ի պարզ բաժանարարներն են 2-ը և 3-ը, փորձարկման համար բանաձևեր են $g^9 \not\equiv 1$, $g^6 \not\equiv 1 (\mathrm{mod}\, 19)$, քանի որ $2^9 \not\equiv 1$, $2^6 \not\equiv 1 (\mathrm{mod}\, 19)$, ապա 2-ը փոքրագույն նախնական արմատն է, իսկ ըստ 19 մոդուլի բոլոր նախնական արմատների քանակը հավասար է $\varphi(18) = 6$;
3) *8, g=3;* 4) *12, g=2:*

14.3 1) Ինդեքսավորելով բաղդատման ձախ և աջ մասերը, կստանանք $\delta ind 5 \equiv 0 (\mathrm{mod}\, 6)$: Ինդեքսների աղյուսակից՝ $ind 5 = 5$ և ստանում ենք $5\delta \equiv 0 (\mathrm{mod}\, 6)$, $\delta \equiv 0 (\mathrm{mod}\, 6)$, որտեղից էլ ստանում ենք δ-ի փոքրագույն արժեքը՝ $\delta = 6$;
3) $\delta = 4$; 5) $\delta = 30$; 7) $\delta = 16$:

14.4 1) Ինդեքսավորելով բաղդատման ձախ և աջ մասերը, կստանանք $x ind 2 \equiv ind 7 (\mathrm{mod}\, 66)$, $x \cdot 1 \equiv 23 (\mathrm{mod}\, 66)$, $x \equiv 23 (\mathrm{mod}\, 66)$:
3) $x ind 16 \equiv ind 11 (\mathrm{mod}\, 52)$, $x \cdot 4 \equiv 6 (\mathrm{mod}\, 52)$, $2x \equiv 3 (\mathrm{mod}\, 26)$: Քանի որ (2,26)=2 և 3-ը չի բաժանվում 2-ի, ապա վերջին բաղդատումը, ուրեմն նաև տրված բաղդատումը, լուծում չունեն; 5) $x \equiv 13 (\mathrm{mod}\, 30)$:

14.5 1) Ինդեքսավորելով բաղդատումը, կստանանք. $ind 7 + ind x \equiv ind 6 (\mathrm{mod}\, 16)$; $ind x \equiv ind 6 - ind 7 (\mathrm{mod}\, 16)$; $ind x \equiv 15 - 11 (\mathrm{mod}\, 16)$; $ind x \equiv 4 (\mathrm{mod}\, 16)$, և, ինդեքսների աղյուսակից՝ $x \equiv 13 (\mathrm{mod}\, 17)$;

2) $x \equiv 74(\mathrm{mod}\,79)$; 5) $x \equiv 30(\mathrm{mod}\,221)$: Քանի որ $221 = 13 \cdot 17$, ապա տրված բաղդատումը համարժեք է հետևյալ համակարգին՝ $\begin{cases} 37x \equiv 5(\mathrm{mod}\,13) \\ 37x \equiv 5(\mathrm{mod}\,17) \end{cases}$:

14.6 1) Ինդեքսավորելով բաղդատումը, կստանանք.
$15indx \equiv ind62 - ind37 = 19 - 64 \equiv 27(\mathrm{mod}\,72)$: Քանի որ վերջին բաղդատումը գծային է $indx$-ի նկատմամբ և (15,27,71)=3, ապա բաղդատումը, եթե համատեղելի է, ունի երեք լուծում: Կրճատելով վերջին բաղդատումը 3-ով, կստանանք՝
$5indx \equiv 9(\mathrm{mod}\,24)$, որտեղից՝ $indx \equiv 21(\mathrm{mod}\,24)$: Ուրեմն՝
$indx \equiv 24 \cdot 0 + 21 = 21(\mathrm{mod}\,72)$;
$indx \equiv 24 \cdot 1 + 21 = 45(\mathrm{mod}\,72)$;
$indx \equiv 24 \cdot 2 + 21 = 69(\mathrm{mod}\,72)$: Ինդեքսների աղյուսակից՝
$x \equiv 17,\ 63,\ 66(\mathrm{mod}73)$:
2) $x \equiv 2,\ 3, 10, 11(\mathrm{mod}13)$; 3) լուծում չունի;
4) $x \equiv 13,\ 29,\ 31(\mathrm{mod}73)$; 5) $x \equiv 25,\ 30, 31, 36(\mathrm{mod}61)$:

14.7 1) Ինդեքսավորելով բաղդատումը, կստանանք.
$12indx \equiv ind37(\mathrm{mod}\,40)$; $12indx \equiv 32(\mathrm{mod}\,40)$; (12, 32, 40)=4;
$3indx \equiv 8(\mathrm{mod}10)$; $indx \equiv 6, 16, 26, 36(\mathrm{mod}40)$,
$x \equiv 39, 18, 2, 23(\mathrm{mod}41)$;
2) $x \equiv 33(\mathrm{mod}\,67)$; 3) լուծում չունի; 4) $x \equiv 34, 32, 20(\mathrm{mod}43)$;
5) $x \equiv \pm 27(\mathrm{mod}\,67)$; 6) $x \equiv \pm 21(\mathrm{mod}\,67)$:

ԻՆԴԵՔՍՆԵՐԻ ԱՂՅՈՒՍԱԿՆԵՐ

p=3, p-1=2, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

p=5, p-1=2², g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

p=7, p-1=2·3, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

p=11, p-1=2·5, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

p=13, p-1=2²·3, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

p=17, p-1=2⁴, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

$p=19,\ p-1=2\cdot 3^2,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

$p=23,\ p-1=2\cdot 11,\ g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	18	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

$p=29,\ p-1=2^2\cdot 7,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

$p=31,\ p-1=2\cdot 3\cdot 5,\ g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	19
3	15									

$p=37,\ p-1=2^2\cdot 3^2,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

$p=41,\ p-1=2^3\cdot 5,\ g=6$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

$p=43,\ p-1=2\cdot 3\cdot 7,\ g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

$p=47,\ p-1=2\cdot 23,\ g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	6	15	24	13	43	41	23			

$p=53,\ p-1=2^2\cdot 13,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

$p=59,\ p-1=2\cdot 29,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

$p=67,\ p-1=2\cdot3\cdot11,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

$p=71,\ p-1=2\cdot5\cdot7,\ g=7$

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

$p=73,\ p-1=2^3\cdot3^2,\ g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

$p=79,\ p-1=2\cdot3\cdot13,\ g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

$p=83,\ p-1=2\cdot41,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

$p=89,\ p-1=2^3\cdot11,\ g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

$p=97,\ p-1=2^5\cdot3,\ g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

1812-ից փոքր պարզ թվերի և նրանց փոքրագույն նախնական արմատների աղյուսակ

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1383	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. Бухшаб А. А. Теория чисел. М., Просвещение, 1966
2. Виноградов И. М. Основы теории чисел. М., Наука. 1981
3. Куликов Л. Я. Алгебра и теория чисел. М., Высшая школа. 1979
4. Грибанов В. У., Титов П. И. Сборник упражнений по теории чисел. М., Просвещение. 1964
5. Шнеперман Л. Б. Сборник задач по альгебре и теории чисел. Минск. Вышэйшая школа. 1982
6. Մովսիսյան Յու. Մ. Հանրահաշիվ և թվերի տեսություն: Մաս Ա: Երևան, 2004

Պատվեր՝ 1087 Տպաքանակ՝ 100

Տպագրված է Հայաստանի Պետական Ճարտարագիտական Համալսարանի տպարանում

Երևան, Տերյան 105