

### Евклид алгоритмі және арифметиканың негізгі теоремасы.

**Теорема** (қалдықпен бөлу туралы). Егер  $a, b \in Z (b \neq 0)$  болса. Онда

$$(*) \quad a = bq + r, \quad 0 \leq r < |b|$$

шарты орындалатындай бір ғана  $q, r \in Z$  сандары табылады.

Осы теореманың шартындағы  $a$  – бөлінгіш,  $b$  – бөлгіш,  $q$  – бөлінді, ал  $r$  – қалдық деп аталады.

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

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$$r_2 = r_3q_4 + r_4, \quad 0 \leq r_4 < r_3$$

$$\dots\dots\dots$$
$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}, \quad r_{n+1} = 0$$

$$b > r_1 > r_2 > \dots > r_n > 0,$$

**Мысал.**  $a = 525, b = 231$  сандары берілсін. Осы сандарға Евклид алгоритмін қолдану

$$525 = 231 \cdot 2 + 63,$$

$$231 = 63 \cdot 3 + 42,$$

$$63 = 42 \cdot 1 + 21,$$

$$42 = 21 \cdot 2.$$

Демек,  $(525, 231) = 21$ . Енді осы табылған ең үлкен ортақ бөлгіштің сызықты өрнектелуін келтіреміз.

$$21 = 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 = 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) = 525 \cdot 4 - 231 \cdot 9$$

Біздің іздеген сызықты коэффициенттер  $u$  және  $v$  сәйкес 4 және – 9 сандары болады.

2.  $(187, 221), (6188, 4709)$  және  $(314, 159)$  сандарын және олардың бастапқы сандар арқылы сызықты өрнектелуін табыңдар.

2.  $d = (317811, 196418)$  санын және оның  $d = 317811u + 196418v$  түріндегі сызықты өрнектелуін тап.

3.  $d = (81719, 52003, 33649, 30107) = ?$ .

2.1. Қалдықпен бөлу (алдымен біріншісін екіншісіне және керісінше): 1) 17 -ні 161-ге; 2) –17-ні 161-ге; в) 17-ні –161-ге; г) –17-ні –161-ге.

2.2. Ковбой барға кіріп, 3 долларлық бір стакан виски, 1 доллар 11 центтік Marlboro қорабын, алты патрон және 13 қорап шырпыға тапсырыс берді. Барлығына – 28 доллар 25 цент сұраған барменді ковбой сол заматта атып тастады. Не үшін?

2.3. Егер  $a = bc$  және  $(a, b) = 1$  болса, онда  $a$  саны  $c$  санына бөлінетінін дәлелде.

2.4. Кез келген  $n$  натурал саны үшін  $\frac{21n+4}{14n+3}$  бөлшегі қысқармайтынын дәлелде.

2.5. Кез келген  $a$ ,  $b$  және  $n$  натурал сандары үшін егер  $(m, n) = d$  болса, онда  $(a^n - 1, a^m - 1) = a^d - 1$  болатынын дәлелде.

2.4.

Бөлінгіштік қасиеттері.

3.1.  $a_n a_{n-1} \dots a_0$  – натурал санның ондық санау жүйесінде жазылуы болсын.

1) Берілген сан 3-ке бөлінеді сонда тек сонда ғана, егер оның цифрларының қосындысы 3-ке бөлінсе.

2) Берілген сан 9-ға бөлінеді сонда тек сонда ғана, егер оның цифрларының қосындысы 9-ға бөлінсе.

3) Берілген сан 11-ге бөлінеді сонда тек сонда ғана, егер оның тақ орындағы цифрларының қосындысы мен жұп орындағы цифрларының қосындысының айырымы 11-ге бөлінсе.

3.2. Бүтін санның ондық жүйедегі жазылуында 300 бірлік, ал қалған цифрлары нөлге тең болса, бұл сан толық квадрат болуы мүмкін бе?

3.3. 1,2,3,4,5,6,7 сандары жазылған жеті жетон бар. Осы жетондар арқылы құрылған ешбір екі жетіорынды сан бір біріне бөлінбейтінін көрсет.

3.4.  $a_n a_{n-1} \dots a_0$  – натурал санның ондық санау жүйесінде жазылуы болсын. Енді  $a_n a_{n-1} \dots a_1 + 2a_0$  санын табайық. Егер табылған сан 19-дан үлкен болса, осы әрекетті алынған санға қайта қолданамыз. Бұл амалды табылған сан 19-дан кем болғанша жалғастырамыз. Онда бастапқы сан 19-ға бөлінуі үшін нәтиже санның 19-ға тең болуы қажетті және жеткілікті болатынын дәлелде.

3.5.  $a_n a_{n-1} \dots a_0$  – натурал санның ондық санау жүйесінде жазылуы болсын. Енді  $a_n a_{n-1} \dots a_1 - 2a_0$  санын табайық. Онда бастапқы сан 7-ге бөлінуі үшін алынған санның 7-ге бөлінуі қажетті және жеткілікті болатынын дәлелде.

3.6. Кез келген  $n$  натурал саны үшін  $7^{2n} - 5^{2n}$  санының 24-ке бөлінетінін дәлелде.

3.7. Кез келген  $n$  натурал саны үшін  $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$  саны бүтін болатынын дәлелде.

3.8. Қандай  $n$  натурал саны үшін  $20^n + 16^n - 3^n - 1$  саны 323 санына бүтін бөлінеді.

3.9.  $\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$  санының бүтін болмайтынын көрсет.

3.10. Кез келген  $k$  және  $n$  натурал сандары үшін  $\frac{1}{k} + \frac{1}{k+1} + \dots + \frac{1}{k+n}$  қосындысының бүтін сан болмайтынын көрсет.

3.11. Келесі сандар бүтін сан болатынын дәлелде.

1)  $\frac{(m+n)!}{m!n!}$ ,

2)  $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ ,

3)  $\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$ .

**Ең үлкен ортақ бөлгіш және ең кіші ортақ еселік.**

$a$  және  $b$  сандарының ең кіші ортақ еселігін  $[a, b]$  арқылы белгілейік.

**Теорема (Ең үлкен ортақ бөлгіштің сызықты өрнектелуі).**  $d = (a, b) \Leftrightarrow d = au + bv$  болатындай  $u$  және  $v$  бүтін сандары табылады.

4.1.  $(a_1, \dots, a_n)$  және  $[a_1, \dots, a_n] - a_1, \dots, a_n$  сандарының сәйкес ең үлкен ортақ бөлгіші мен ең кіші ортақ еселігін білдірсін. Онда

$$1) (a, b) = \frac{ab}{[a, b]}.$$

$$2) (a, b, c) = \frac{abc[a, b, c]}{[a, b][b, c][c, a]}.$$

4.2.  $(a, b, c) = (a, (b, c)) = ((a, b), c)$ .

4.3. Натурал сандар жиынында анықталған екі орынды  $f(a, b)$  функциясы келесі қасиеттерге ие:

1)  $f(a, a) = a$ ; 2)  $f(a, b) = f(b, a)$ ; 3)  $(a + b)f(a, b) = bf(a, a + b)$ .

Онда  $f(a, b) = [a, b]$  – ең кіші ортақ еселік болатынын дәлелде.

Қалдықтар.

5.1. Бүтін санның квадратын 1)3; 2) 4; 3) 5; 4) 5 сандарына бөлгенде қалдықтар қандай болады.

Тек екі бөлгіші болатын натурал сан *жай* сан деп аталады. Жай сан болмайтын натурал санды *құрама* сан деп атаймыз.

**Лемма.** Кез келген  $n$  – құрама санының  $\sqrt{n}$  -нен артпайтын жай бөлгіші болады.

**Теорема** (жай сандар жиынының ақырсыздығы). Жай сандар жиыны ақырсыз жиын болады.

**Теорема** (арифметиканың негізгі теоремасы). Кез келген натурал сан жай сандардың көбейтіндісіне жіктеледі.

**Жаттығулар.**

6.1. Айырымы 17-ге тең жай сандардың барлық пары табындар.

6.2. Жай санды 30-ға бөлгендегі табылған қалдықтың жа жай болатынын көрсет.

6.3.  $n > 2$  болса  $n$  және  $n!$  сандарының арасында ең болмағанда бір жай сан табылатынын дәлелде.

6.4. Егер  $n! + 1$  саны  $n + 1$  санына бөлінсе, онда  $n + 1$  жай сан болатынын дәлелде.

6.5.  $p^2 - 2q^2 = 1$  теңдігі орындалатындай  $p$  және  $q$  жай сандарының барлығын табындар.

6.6.  $p = 4k + 3$  түріндегі жай сандар жиынының ақырсыз болатынын көрсет.

6.7.  $p = 6k + 5$  түріндегі жай сандар жиынының ақырсыз болатынын көрсет.

6.8. 111, 1111, 11111, 111111, 1111111 сандарын жай көбейткіштерге жікте.

6.9. Қатарынан келетін 1000 құрама санның болатынын көрсет.

6.10. Кез келген  $n$  натурал саны үшін арасында бір ғана жай сан болатынын қатарынан келетін  $n$  натурал сан табылатынын дәлелде.

6.11. Тек жай сандардан тұратын арифметикалық прогрессия табыла ма?

6.12. Егер  $a^n - 1$  – жай сан болса, онда  $a = 2$  және  $n$  – жай сан болатынын көрсетіндер. Осы түрдегі жай сандарды Мерсенн сандары деп атайды.

6.13. . Егер  $a^n + 1$  – жай сан болса, онда  $a$  – жұп сан, ал  $n$  – 2-нің дәрежесі болатынын көрсетіндер.  $2^{2^k} + 1$  түріндегі жай сандарды Ферма сандары деп атайды.

## Салыстыру теориясы

### Анықтама және қарапайым қасиеттері.

Анықтама.  $a, b \in \mathbf{Z}$ ,  $m \in \mathbf{N}$ . Егер  $a$  және  $b$  сандарын  $m$ -ге бөлгенде, олардың қалдықтары бірдей болса, онда  $a$  және  $b$  сандарын  $m$  модулі бойынша салыстырымды деп айтып, бұл ұғымды  $a \equiv b(\text{mod } m)$  арқылы белгілейміз.  $a \equiv b(\text{mod } m) \Leftrightarrow m \mid (a - b)$ . Демек,  $a \equiv b(\text{mod } m)$  болуы үшін  $a = b + mt$  теңдігі орындалатындай  $t$  бүтін санының табылуы қажетті және жеткілікті.

**Қасиет 1.** Берілген модуль бойынша салыстыруларды мүшелеп қосуға болады.

**Қасиет 2.** Салыстырудың кез келген жағындағы қосылғышты, оның екінші жағына таңбасын өзгертіп көшіруге болады.

**Қасиет 3.** Салыстырудың кез келген жағына модульге еселі санды қосуға болады.

**Қасиет 4.** Берілген модуль бойынша екі салыстыруды мүшелеп көбейтуге болады, яғни  $a_1 \equiv b_1(\text{mod } m), a_2 \equiv b_2(\text{mod } m) \Rightarrow a_1 a_2 \equiv b_1 b_2(\text{mod } m)$ .

**Қасиет 5.** Салыстырудың екі жағын да бірдей дәрежеге шығаруға болады, яғни  $a \equiv b(\text{mod } m) \Rightarrow \forall n \in \mathbf{N}, a^n \equiv b^n(\text{mod } m)$

**Қасиет 6.** Егер  $a_0 \equiv b_0(\text{mod } m), a_1 \equiv b_1(\text{mod } m), \dots, a_n \equiv b_n(\text{mod } m), x \equiv y(\text{mod } m)$ , онда  $a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv b_0 y^n + b_1 y^{n-1} + \dots + b_n(\text{mod } m)$ .

**Қасиет 7.** Салыстырудың екі жағын да модульмен өзара жай болатын олардың ортақ бөлгішіне қысқартуға болады.

**Қасиет 8.** Салыстырудың екі жағы мен модульді бірдей санға көбейтуге және олардың ортақ бөлгішіне бөлуге болады.

**Қасиет 9.** Егер  $a \equiv b$  салыстыруы бірнеше әртүрлі модуль бойынша орындалса, онда бұл салыстыру аталған модульдердің ең кіші ортақ еселігі үшін де орындалады.

**Қасиет 10.** Егер салыстыру  $m$  модуль бойынша орындалса, онда ол осы  $m$  саныны кез келген бөлгіші  $d$  модуль үшін де орындалады.

**Қасиет 11.** Егер салыстырудың бір жағы мен модуль қандай да бір санға бөлінсе,

**Мысал.** Кез келген  $n$  натурал саны үшін  $37^{n+2} + 16^{n+1} + 23^n$  саны 7-ге бөлінетінін дәлелде.

**Шешуі.**  $37 \equiv 2(\text{mod } 7), 16 \equiv 2(\text{mod } 7), 23 \equiv 2(\text{mod } 7)$ . Енді бірінші салыстыруды  $n+2$ , екіншіні  $n+1$ , ал үшіншіні  $n$  дәрежеге шығарып, мүшелеп қосамыз. Онда  $37^{n+2} + 16^{n+1} + 23^n \equiv 2^{n+2} + 2^{n+1} + 2^n \equiv 7 \cdot 2^n \equiv 0(\text{mod } 7)$ . Демек берілген сан 7-ге бөлінеді.

**Есептер**

1.  $3^{105} + 4^{105}$  саны 181-ге бөлінетінін дәлелде.

2. Кез келген  $n$  натурал саны үшін  $5^{2n-1} \cdot 2^{n+1} + 3^{n+1} \cdot 2^{2n-1}$  саны 9-ға

	<p>бөлінетінін дәлелде.</p> <p><b>3.</b> <math>(9674^6+28)^{15}</math> санын 39-ға бөлгендегі қалдықты тап.</p> <p><b>4.</b> <math>N</math> натурал санын 3-ке және 37-ге бөлгендегі қалдықтар сәйкес 1 және 33 сандары болады. Осы санды 111-ге бөлгендегі қалдықты тап.</p> <p><b>5.</b> <math>n</math> санының барлық оң тақ мәндерінде <math>S_m=1^n+2^n+3^n+\dots+m^n</math> саны <math>1+2+3+\dots+m</math> санына бөлінетінін көрсет.</p> <p><b>6.</b> <math>20^{15}-1</math> саны <math>11 \cdot 31 \cdot 61</math> көбейтіндісіне бөлінетінін дәлелде.</p> <p><b>7.</b> <math>p</math> және <math>q</math> – 3-тен артық жай сандар болса, онда <math>p^2 - q^2</math> санының 24-ке бөлінетінін дәлелде.</p> <p><b>8.</b> Егер натурал сан 99-ға бөлінсе, онда оның цифрларының қосындысы 18-ден кем болмайды.</p> <p><b>10.</b> Ешбір натурал <math>n</math> және <math>k</math> (<math>k &gt; 1</math>) сандары үшін <math>3^{nk}</math> санының 5-ке бөлінбейтінін дәлелде.</p>
--	--

### Қалындылардың толық және келтірілген жүйелері.

Осының алдында  $\equiv_m$  қатынасы бүтін сандар жиынын өзара қиылыспайтын кластарға бөледі. Барлық кластар саны  $m$  -ге тең. Әрбір класта  $m$  –ге бөлгенде қалдықтары бірдей болатын бүтін сандар жатады.

**Анықтама.**  $\equiv_m$  арқылы анықталған эквиваленттік кластың кез келген элементін  $m$  модулі бойынша қалынды деп атаймыз. Әрбір кластан бір-бір элементтен алынып құрылған қалындылар жүйесін  $m$  модулі бойынша *қалындылардың толық жүйесі* (толық жүйеде дәл  $m$  бүтін сан болады) деп атайды. Ал тек  $m$  –ге бөлгенде пайда болған қалдықтардан құрылған жүйе – ең кіші теріс емес қалындылар деп аталады. Егер  $|p|$  модульдері бойынша ең кіші болса, онда  $p$  қалындысы абсолютті кіші қалынды делінеді:

**Мысал :**  $m = 5$ . Онда:

0, 1, 2, 3, 4 - ең кіші теріс емес қалындылар;

-2, -1, 0, 1, 2 - абсолютті кіші қалындылар.

Келтірілген екі қалындылар жүйесі де толық жүйе болады.

**Лемма 1.** 1)  $m$  модулі бойынша өзара салыстырымды болмайтын  $m$  сан  $m$  модулі бойынша қалындылардың толық жүйесі болады.

2) Егер  $a$  және  $m$  сандары өзара жай, ал  $x$  санының мәндері  $m$  модулі бойынша толық жүйеден таңдалса, онда кез келген  $b$  саны үшін  $ax+b$  түріндегі сандар да  $m$  модулі бойынша толық жүйе құрады.

**Анықтама.** Қалындылардың толық жүйесінен алынған,  $m$  модулімен ең үлкен ортақ бөлгіші 1-ге тең қалындылар жүйесін  $m$  модулі бойынша келтірілген қалындылар жүйесі деп атайды.

Келтірілген қалындылар жүйесін әдетте ең кіші оң қалындылар ішінен таңдайды.

Олардың санын  $\varphi(m)$  – Эйлер функциясының мәніне тең деп есептейді. Яғни  $\varphi(m) – m$  модулі бойынша келтірілген қалындылар жүйесіндегі сандардың санын білдіреді.

**Мысал.**  $m = 42$  болсын. Онда осы модуль бойынша келтірілген қалындылар жүйесі төмендегідей: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

**Лемма 2.** 1)  $m$  модулі бойынша екеуара салыстырымды болмайтын  $\varphi(m)$  сан  $m$  модулі бойынша келтірілген қалындылар жүйесін құрады.

2) Егер  $(a, m) = 1$  және  $x$  саны қандай да  $m$  модулі бойынша келтірілген қалындылар жүйесінен мәндер таңдаса, онда  $ax$  сандар да  $m$  модулі бойынша келтірілген қалындылар жүйесінен мәндер таңдайды.

**Лемма 3.**  $m_1, m_2, \dots, m_k$  – екеуара жай сандар тізімі және  $m_1 m_2 \dots m_k = M_1 m_1 = M_2 m_2 = \dots = M_k m_k$  болсын. Мұндағы  $M_j = m_1 \dots m_{j-1} m_{j+1} \dots m_k$

1) Егер  $x_1, x_2, \dots, x_k$  сандары сәйкес  $m_1, m_2, \dots, m_k$  модулдері бойынша қалындылардың толық жүйесін қабылдаса, онда  $M_1 x_1 + M_2 x_2 + \dots + M_k x_k$  сызықты өрнегінің мәндері де  $m = m_1 m_2 \dots m_k$  модулі бойынша қалындылардың толық жүйесінің мәндерін қабылдайды.

2) ) Егер  $x_1, x_2, \dots, x_k$  сандары сәйкес  $m_1, m_2, \dots, m_k$  модулдері бойынша қалындылардың келтірілген жүйесін қабылдаса, онда  $M_1 x_1 + M_2 x_2 + \dots + M_k x_k$  сызықты өрнегінің мәндері де  $m = m_1 m_2 \dots m_k$  модулі бойынша қалындылардың келтірілген жүйесін құрады.

**Лемма 4.**  $x_1, x_2, \dots, x_k, x$  және  $\xi_1, \xi_2, \dots, \xi_k, \xi$  сандары  $i \neq j \Rightarrow (m_i, m_j) = 1$  болғанда, сәйкес  $m_1, m_2, \dots, m_k$  және  $m = m_1 m_2 \dots m_k$  модулдері бойынша толық және келтірілген қалындылар жүйелерін аралап шықсын, онда  $\{x_1/m_1 + x_2/m_2 + \dots + x_k/m_k\}$  бөлшектері  $\{x/m\}$  бөлшектерімен, ал  $\{\xi_1/m_1 + \xi_2/m_2 + \dots + \xi_k/m_k\}$  бөлшектері  $\{\xi/m\}$  бөлшектерімен бірдей болады.

### Эйлер және Ферма теоремалары.

**Теорема (Эйлер).**  $m > 1$ ,  $(a, m) = 1$ , ал  $\varphi(m)$  – Эйлер функциясы болсын. Онда:

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

**Теорема (Ферма).**  $p$  – жай сан және ол  $a$  санының бөлгіші болмаса, онда

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

**Салдар 1.** Кез келген  $a \in Z$  саны мен  $p$  жай саны үшін  $a^p \equiv a \pmod{p}$ .

**Салдар 2.** Кез келген  $a, b \in Z$  сандары үшін  $(a+b)^p \equiv a^p + b^p \pmod{p}$ .

**Мысал 1.** Бір орынды санның тоғызыншы дәрежесі 7-ге аяқталады.

**Шешуі.** Берілгені бойынша  $a^9 \equiv 7 \pmod{10}$ . Сонымен бірге,  $(7, 10)=1$  және  $(a, 10)=1$ . Эйлер теоремасы бойынша  $a^{\varphi(10)} \equiv 1 \pmod{10}$ . Демек  $a^4 \equiv 1 \pmod{10}$ . Оны квадраттасақ,  $a^8 \equiv 1 \pmod{10}$ . Онда  $a^9 = a^8 \cdot a \equiv 1 \cdot a \equiv a \equiv 7 \pmod{10}$ . Яғни  $a = 7$ .

**Жаттығу.**

1. Дәлелде  $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1 \pmod{7}$

2.  $7^{402}$  санын 101-ге бөлгендегі қалдықты тап.

3.  $243^{402}$  санының соңғы екі цифрын тап.

**Жаттығу.**  $(73^{12} - 1)$  саны 105-ке бөлінетінін дәлелде.

<b>Есептер</b>	<p>1. а) <math>13^{176} - 1</math> саны 89-ға; б) <math>52^{60} - 1</math> саны 385-ке бөлінетін дәлелде.</p> <p>2. <math>3^{100} - 3^{60} - 3^{40} + 1</math> саны 77-ге бөлінеді.</p> <p>4. Дәлелде:</p> <p>а) <math>1^{19} + 2^{19} + 4^{19} + 5^{19} + 7^{19} + 8^{19} \equiv 0 \pmod{9}</math>;</p> <p>б) <math>1^{14} + 3^{14} + 7^{14} + 9^{14} \equiv 0 \pmod{10}</math>.</p> <p>5. Келесі сандардың соңғы екі цифрын тап:</p> <p>а) <math>19^{321}</math>; б) <math>131^{161}</math>.</p> <p>6. Қалдықты тап:</p> <p>а) <math>3^{200} + 7^{200}</math> санын 101-ге; б) <math>7^{65} + 11^{65}</math> санын 80-ге бөлгенде.</p> <p>7. Соңғы 1000 цифры бірден және екіден тұратын 2 санының дәрежесі болатынын көрсет.</p> <p>8. Бірінші мүшесі мен айырымы натурал сандар болатын <math>a, a+d, a+2d, \dots</math> – ақырсыз арифметикалық прогрессиясы берілсін. Осы прогрессияда канондық жіктеулерінде бірдей жай сандар кездесетіндей (әрине әртүрлі дәрежемен) мүшелер саны ақырсыз болатынын дәлелде.</p>
----------------	---