Дәріс 6. Салыстырулар теориясы және оның қосымшалары

Жоспар:

1. Салыстырулар теориясы
2. Модульдік арифметика
3. Ең кіші ортақ бөлгішті есептеу
4. Қалындылардың толық және қысқартылған жүйесі
5. Эйлер функциясы
6. Қытай қалдық теоремасы

Салыстырулар теориясы

m натурал санды алайық, оны **модуль** деп атаймыз.

Анықтама 1. Егер $(a - b)$ айырма m $(m \mid a - b)$ бөлінетін болса, a және b бүтін сандары m салыстырмалы модуль деп аталады.

a, b және m арасындағы бұл қатынас қысқа түрде былай жазылады:

$$a \equiv b(mod\, m),$$

мұндағы a және b сәйкесінше салыстырудың сол және оң жақтары деп аталады.

1–анықтамадан шығатыны, егер a мәні m-ге бөлінетін болса, онда

$$a \equiv 0\, mod\, m.$$

Теорема 1. Егер a және b модулі m-ге бөлінгенде бірдей қалдықтар болса ғана a саны b санымен салыстырылады.

Дәлелдеу. Айталық

$$a \equiv b(mod\, m),$$

a және b түрінде көрсетейік

$$a = mq_1 + r_1,\ \ b = mq_2 + r_2,$$

мұндағы $0 \le r1 < m,\ \ 0 \le r\,2 < m$. Берілгеннен келесілерді аламыз

$$a - b = m(q_1 - q_2) + r_1 - r_2.$$

$(m \mid a - b)$ болғандықтан, одна m–ді $r_1 - r_2$. Бірақ келесілер орын алады

$$-m < r_1 - r_2 < m.$$

Осыдан $r_1 - r_2 = 0$, яғни $r_1 = r_2$.

Керісінше. a және b санын m–ге бөлудің қалдықтары тең болсын, яғни келесі орын алады

$$a = mq_1 + r,\ \ b = mq_2 + r,$$

онда $a - b = m(q_1 - q_2)$, яғни $m \mid a - b$.

1-теорема негізінде a және b сандарының салыстырмалылығының келесі анықтамасын беруге болады.

Анықтама 2. a және b бүтін сандар, егер бұл сандарды m-ге бөлген кездегі қалдықтар тең болса, m модулі бойынша салыстырылатын деп аталады.

Салыстыру қасиеттері:

Теорема 2. Салыстырмалы қатынастар рефлексивті, яғни $a \equiv a\ (mod\ m)$.

Салыстырудың сол және оң жақтарының тең қалдықтары бар екендігі дәлелденеді.

Теорема 3. Салыстырмалылық қатынастары симметриялы, яғни егер

$$a \equiv b\ (mod\ m),$$

онда

$$b \equiv a\ (mod\ m).$$

Дәлелдеу. Егер a мен b-ны m-ге бөлгенде тең қалдықтар болса, онда b мен a-ны m-ге бөлгендегі қалдықтар да тең болады.

Теорема 4. Салыстырмалылық қатынастары өтпелі, яғни егер

$$a \equiv b\ (mod\ m),\ \ b \equiv c\ (mod\ m),$$

онда

$$a \equiv c\ (mod\ m)$$

Дәлелдеу. Егер a және b сандары, сондай-ақ b және c сандары m-ге бөлінгенде бірдей қалдықтарға ие болса, онда a және c m-ге бөлгенде бірдей қалдық болады.

Теорема 5. Егер

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

және k кез келген бүтін сан болса, онда

$$ka \equiv kb(\ mod\ m)$$

Дәлелдеу. Егер $a \equiv b\ (mod\ m)$, то $m|a - b$. Онда $m|k(a - b)$ немесе $m|ka - kb$. Сәйкесінше, $ka \equiv kb(\ mod\ m)$.

Анықтама 2. a және b бүтін сандар болсын, және $b \neq 0$. b саны $a = kb$ болатындай k бүтін саны болса, a санының бөлгіші деп аталады.

Анықтама 3. a және b екі санының ортақ бөлгіші $k|a$ және $k|b$ болатын кез келген k бүтін сан болып табылады.

Анықтама 4. Екі a және b сандарының ең үлкен ортақ бөлгіші (ЕҮОБ) бұл сандардың кез келген басқа ортақ бөлгішіне бөлінетін оң ортақ бөлгіш k болып табылады. a және b сандарының ең үлкен ортақ бөлгіші былай белгіленеді:

$$(a, b) = k.$$

Анықтама 5. Егер осы сандардың ең үлкен ортақ бөлгіші 1 болса, a және b сандары қос жай сандар деп аталады, яғни. $(a, b) = 1$.

Теорема 6. Егер

$$ka \equiv kb(mod\ m)$$

және *(k,m)*=1, онда

$$a \equiv b(mod\ m).$$

Дәлелдеу. Егер $ka \equiv kb(mod\ m)$, онда $m|ka - kb$, яғни $m|k(a - b)$. Жоғарыдағы теоремалардың шарттары бойынша ең үлкен ортақ бөлгіш 1-ге тең болғандықтан, $m|k(a - b)$ шартынан $m|a - b$ шығады.

Теорема 7. Егер $a \equiv b(mod\ m)$ және k – ерікті бүтін натурал сан, онда $ka \equiv kb(mod\ m)$.

Дәлелдеу. Егер $m|a - b$, то $km|ka - kb$. Осыдан $ka \equiv kb(mod\ m)$ шығады.

Теорема 8. Егер $a \equiv b(mod\ m)$ $c \equiv d(mod\ m)$, онда $a + c \equiv (b + +d)\ (mod\ m)$ $a - c \equiv (b - d)\ (mod\ m)$.

Дәлелдеу. Егер $m|a - b$ и $m|c - d$, онда $m|(a - b) \pm (c - d)$. Осыдан келесіні аламыз $m|(a \pm c) - (b \pm d)$.

Теорема 9. Егер $a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$, онда $ac \equiv bd(mod\ m)$

Дәлелдеу. Егер $a \equiv b(mod\ m)$, және $c \equiv d(mod\ m)$, 5 теоремадан $ac \equiv bd(mod\ m)$ и $bc \equiv bd(mod\ m)$ алынады.

Онда транзивті салыстыру қасиетінен $ac \equiv bd(mod\ m)$ аламыз.

Теорема 10. Егер $a \equiv b(mod\ m)$ болғанда кез–келген $n \geq 0$ үшін $a^n \equiv b^n(mod\ m)$.

Дәлелдеу. $a \equiv b(mod\ m)$ және $a \equiv b(mod\ m)$ салыстыру үшін 9 теореманы n рет қолданып, 10–теореманың дәлелін аламыз.

n кез келген натурал сан болсын, $p(x)$ дәрежелі көпмүше n бүтін коэффициенттері бар. Онда 2 - 10 теоремаларынан келесі теорема шығады

Теорема 11. Егер $a \equiv b(mod\ m)$, онда $p(a) \equiv p(b)(mod\ m)$.

Модульдік арифметика

Модульдік арифметика немесе қалдық арифметикасы заманауи криптографияның негізі болып табылады. Бұл арифметикада тек бүтін

сандардан тұратын өрнектің нақты мәнін есептеудің орнына оның n бүтін санына бөлінуінің қалдығы анықталады.

Қалдықтардың арифметикасы әдеттегі арифметикаға ұқсас: ол коммутативтілік, ассоциативтілік және тарату қасиеттеріне ие. Сонымен қатар, n модулі бойынша аралық нәтижені есептеу бүкіл есептеуді орындау, содан кейін қалдықты табу сияқты нәтиже береді. Осылайша, 1.1-1.4 формулалары жарамды.

$$(a + b)\ mod\ n \equiv\ (\ (a\ mod\ n) + (b\ mod\ n)\ )\ mod\ n \quad (1.1)$$

$$(a - b) mod\ n \equiv\ \big(\ (a\ mod\ n) -\ (b\ mod\ n)\big) mod\ n \quad (1.2)$$

$$(a * b) mod\ n \equiv\ (\ (a\ mod\ n)\ *\ (b\ mod\ n)\ )\ mod\ n \quad (1.3)$$

$$\big(\ c(a + b)\big) mod\ n \equiv\ (\ ((ca)\ mod\ n) + ((cb)\ mod\ n)\ )\ mod\ n \quad (1.4)$$

Әзірге арифметикалық өрнектерді құрастыру кезінде тек қосу, көбейту және азайту амалдарын қолдануға болады. Болашақта біз үйренеміз санның кері мәнін, санның логарифмін және n квадрат түбір модулін есептейміз.

$a^x\ mod\ n$ есептейміз. Егер x көрсеткіші 2 дәрежесі болса, $a^x\ mod\ n$ есептеу үшін $x = 16$ келесі пішіні бар 3.5 формуланы қолдануға болады

$$a^{16} mod\ n\ =\ (\ (\ (a^2\ mod\ n)^2\ \ mod\ n\ )^2\ \ mod\ n\ )^2\ \ mod\ n \quad (1.5)$$

Егер x көрсеткіші 2-нің дәрежесі болмаса, онда бұл көрсеткішті екілік санау жүйесінде жазу арқылы x-ті 2 дәрежелерінің қосындысы ретінде көрсетуге болады, бұл көбейту амалдарының санын айтарлықтай азайтуға болады.

Ең кіші ортақ бөлгішті есептеу

Ең үлкен ортақ бөлгішті есептеудің ең көне әдістерінің бірі Евклид алгоритмі болып табылады. Сонымен, екі натурал a және b саны берілсін. $a > b$ деп есептейік. Бұл жағдайда қатынас орындалатындай $q \neq 0$ және $r, 0 \leq r < b$, бүтін сандары бар.

$$a\ =\ bq\ +\ r.$$

Мұндағы q бөлінді, ал r мәні a санын b санына бөлудің қалдығы. Ең үлкен ортақ бөлгішті (ЕҮОБ) есептеудің евклидтік алгоритмі келесі фактіге негізделген. Егер a және b сандарының d бөлгіші болса, онда (1)-ден $d|r$ шығады, яғни келесі 1.6-формула әділ:

$$\text{НОД}(a, b) = \text{НОД}(b, r) = \text{НОД}(b, a\ mod\ b). \quad (1.6)$$

1.6 формула арқылы келесі схема арқылы ең үлкен ортақ бөлгішті анықтауға болады:

$$a\ =\ bq_1 + r_1,$$

$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$
$$\dots$$
$$r_{k-1} = r_k q_{k+1} + r_{k+1},$$
$$r_k = r_{k+1} q_{k+2} + r_{k+2},$$

мұндағы

$$b > r1 > r2 > \dots > 0.$$

i процесі кейбір қадамда бөлімнің қалған бөлігінен кейін аяқталады r нөлге айналады. Бұл жағдайда $r_{i-2} = r_{i-1} q_i$ теңдік ақиқат болады, одан r_{i-1} a және b сандарының ең үлкен бөлгіші болып шығады.

3.3 Класстар

6-Анықтама. Модульдік қалдық класы кейбір берілген a бүтін санымен салыстырылатын барлық бүтін сандар жиыны болып табылады. Мұндай класс $[a]_n$ арқылы белгіленеді.

Модульдің мәні біркелкі анықталған болса, класс белгілеуіндегі индексті өткізіп жібереміз деп келістік. Барлық қалдық кластарының модулі n жиынын Z / n деп белгілейміз. Анықтама a саны n модулінен үлкен болған жағдайды жоққа шығармайтынын ескеріңіз.

Теорема 12. a мен n модулімен салыстырылатын сандар класы $a + nk$ түріндегі сандар жиынымен сәйкес келеді, мұндағы k ерікті бүтін сан.

Дәлелдеу. Егер $x \in [a]$ бүтін сан болса, онда

$$x \equiv a(mod\ n),$$

яғни $x - a = nk$ немесе $x = a + nk$, мұндағы k – кез–келген бүтін сан. Сонымен бірге –ның кез келген мәні үшін бізде бар

$$a + nk \equiv a(mod\ n).$$

Осыдан $a + nk$ сандар жиыны $[a]$ класымен сәйкес келеді.

12-теоремадан әрбір класта шексіз сандар болатыны шығады.

Мысалы. Модуль n=7 болсын. Бұл жағдайда [18, 59 б.] клас келесі сандардан тұрады:

$$\dots, -12, -5, 2, 9, 16, 23, \dots,$$

Теорема 13. $[a] = [b]$ егер және тек егер

$$a \equiv b\ mod\ n.$$

Дәлелдеу. Егер $a \equiv b\ mod\ n$ болса, онда кез келген $x \in [a]$ үшін қатынас келесідей болады

$$x \equiv a(mod\ n).$$

Салыстырудың транзитивтілігінен мынау шығады

$$x \equiv b(mod\ n),$$

яғни $x \in [b]$. a және b симметриясының арқасында кез келген $x \in [b]$ үшін $x \in [a]$ орындалатыны шығады. Осылайша, $[a]$ және $[b]$ кластары бірдей.

Кері қарай. Егер $[a] = [b]$ болса, онда бұл дегеніміз

$$a \equiv b(mod\ n).$$

Теорема 14. Екі кластың кем дегенде бір ортақ элементі болса, онда олар сәйкес келеді.

Дәлелдеу. Егер $x \in [a]$ және $x \in [b]$, онда

$$x \equiv a(mod\ n), \qquad x \equiv b(mod\ n),$$

онда транзитивтілік қасиеті бойынша

$$a \equiv b(mod\ n),$$

Онда 13-теоремадан $[a] = [b]$ болады.

Теорема 15. Егер n модулінің кейбір саны n-ге бөлінгенде r-ге тең қалдық болса, онда кластағы барлық сандар n-ге бөлінгенде r қалдығы болады.

Дәлелдеу.

$$x = nk + r, 0 \leq r < n.$$

Сонда, 12-теорема бойынша, x жататын кластың барлық сандары келесідей болады:

$$x + nt = n(k + t) + r = ns + r,$$

мұндағы $s = k + t$ кез келген бүтін сан.

Теорема 16. Модуль кластарының саны ақырлы және n-ге тең.

Дәлелдеу. 15-теорема бойынша бір класстың барлық сандарын n–ге бөлгенде бірдей қалдық болады. Сондықтан модуль n кластары қалғандарға бір бірден сәйкес келеді. n-ге бөлгендегі қалдықтар $0,1,2,\dots,n-1$ сандары болып табылады.

Анықтама 7. Класс қалдығы берілген классқа жататын кез келген сан. Теріс емес (оң) класс қалдықтарының ішінде міндетті түрде ең кішісі болады, ол ең кіші оң класс қалдығы деп аталады.

Теорема 17. $[a]$ модулі n класының ең кіші теріс емес қалдығы –ны n– ге бөлудің қалдығына тең.

Дәлелдеу. a-ны n-ге бөлгенде r қалдық болсын, яғни $a = nq + r$. Сонда $a \equiv r(mod\ n)152$ және $[a] = [r]$. Бұл жағдайда $c \in [a]$ болса, онда

$$c = r + nt.$$

Егер $t < 0$, онда

$$r + nt \leq r - m < 0.$$

Нәтижесінде егер $t = 0$ болса, онда $c > 0$ болады.

Теорема 18. Берілген модуль үшін кластар жиыны аддитивтік топ болып табылады, яғни бір қосу амалы, нөлдік және қарама–қарсы элементтері бар жиын.

Теорема 19. Берілген модульге қатысты класстар жиыны коммутативті сақина болып табылады.

Қалындылардың толық және қысқартылған жүйесі

Анықтама 8. Белгілі бір модульге қатысты қалдықтардың толық жүйесі деп осы модульге қатысты әрбір кластан бірбірден алынған сандар жүйесі аталады.

Әрбір класс модулінен кез келген санды алсақ, қалдықтардың толық жүйесі алынады.

Мысал. 12, -23, 2, 63, -2, 5 сандары қалдықтардың толық жүйесін 6– модуль құрайды. Ескерту: -23 санын 6-ға бөлудің қалдығы қарапайым арифметика ережелері бойынша -5 тең. -23 саны қай класқа жататынын анықтау үшін қалған -5-ке 6 модулін қосу керек. -23 саны 1 санына сәйкес келетін класқа жататынын анықтаймыз. Егер біз қол жеткізетін болсақ, ұқсас нәтиже аламыз. бөлу кезінде оң қалдық. Бұл жағдайда -23 санының 6-ға бөлінетін бөлігі -4 тең болады, ал қалғаны 1-ге тең болады. Әдетте, сыныптардың өкілдері ретінде әрбір сыныптан ең кіші теріс емес сан алынады. Бұдан шығатыны, ең аз теріс емес қалдықтар жүйесі n модулі келесі сандар: $1,2,3, \dots, n$.

Теорема 20. Егер $(a, n) = 1$ (a, n – өзара жай), b ерікті бүтін сан және x модулі n қалдықтарының толық жүйесі арқылы өтетін болса, онда $ax + b$ сандары да мынадай мәндерді қабылдайды және осы модуль үшін қалдықтардың толық жүйесін құрайды.

Анықтама 9. Белгілі бір жүйе модуль бойынша қалдықтардың қысқартылған жүйесі деп әрбір класс қосындысынан модульге бір қабылданатын сандар жүйесі болып табылады.

Эйлер функциясы

Анықтама 10. Осы модульге тең болатын модуль n кластарының саны Эйлер функциясы $\varphi(n)$ деп аталады.

n модулімен салыстырылатын кластар саны –нен аспайтын бүтін сандар санына және n-ге тең болатындықтан, Эйлер функциясының келесі эквивалентті анықтамасын беруге болады.

Анықтама 11. n-ге тең және 1-ден аспайтын натурал сандар жиыны Эйлер функциясы $\varphi(n)$ деп аталады.

Мысал. $n = 1$ модулі үшін Эйлер функциясының мәні $\varphi(1) = 1$. Қалдықтардың келтірілген жүйесіндегі $n = 12$ модулі үшін 0,1,2,3,4,5,6,7,8,9, 10,11 тек 1,5,7,11 төрт саны ғана модулі 12-ге өзара жай сан. Сондықтан $\varphi(12) = 4$.

Анықтама 12. Натурал сандар жиынында анықталған f(n) функциясы, егер кез келген қосымша натурал сандар a және b үшін болса, мультипликативті деп аталады.

$$f(a,b) = f(a)f(b).$$

Теорема 21. Эйлер функциясы мультипликативті, яғни қатынасы бар

$$\varphi(ab) = \varphi(a)\,\varphi(b),$$

егер a және b сандары қос жай болса, яғни ең үлкен ортақ бөлгіші 1–ге тең немесе $(a,b) = 1$.

Теорема 22. p жай сан және α кез келген натурал сан болсын, онда $(p^{\alpha}) = p^{\alpha-1}(p-1)$. Жай p үшін Эйлер функциясы $\varphi(p) = p-1$ екенін ескеріңіз.

Теорема 23.

$$m = p_1^{a1}p_2^{a2}\ldots p_k^{ak}$$

мұндағы p_i – жай сан және $a, i \le k$, – кез–келген натурал сан. Онда $\varphi(\,p_1^{a1}p_2^{a2}\ldots p_k^{ak}) = p_1^{a1-1}(p_1-1)\,p_2^{a2-1}(p_1-1)\ \ldots\ p_1^{ak-1}(p_k-1)$.

Мысал. Сәйкесінше $n = 2$ және $n = 3$ модулі үшін $\varphi(2) = 1,\ \varphi(3) = 2$.

онда

$$\varphi(6) = \varphi(2\times 3) = \varphi(2)\varphi(3) = 2.$$

Сонымен бірге $\varphi(18) = \varphi(3\times 6) \neq \varphi(3)\varphi(6)$ 3 және 6 сандары салыстырмалы жай емес болғандықтан, бұл сандардың ең үлкен ортақ бөлгіші үш $(3,6) = 3$. Дегенмен

$$\varphi(18) = \varphi(2\times 9) = \varphi(2\times 3^2) =$$
$$= (2-1)\,3^{2-1}(3-1) = 3\times 2 = 6.$$

(Ферма) теоремасы. Кез келген жай p және p-ге бөлінбейтін кез келген a, $a \ge 1$ үшін салыстыру жарамды

$$a^{p-1} \equiv 1 \, mod \, p,$$

немесе

$$a^P \equiv a \, mod \, p.$$

Жай p үшін $p-1$ Эйлер функциясымен $\varphi(p) = p-1$ сәйкес келетінін ескеріңіз.

Сондықтан дәлелденетін Ферма теоремасын салыстыру түрінде жазуға болады

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \, mod \, p.$$

Соңғы салыстыру кез келген m модулі үшін $a, a \geq 1$ санына сәйкес келетіні белгілі болды. Соңғы факт Эйлердің келесі теоремасымен расталады.

(Эйлер) **теоремасы.** Кез келген m модулі үшін және кез келген $a \geq 1$, m-мен өзара жай сан, $a^{\varphi(p)} \equiv 1 \, mod \, p$ салыстыру айқын.

Ферма және Эйлер теоремалары берілген санның үлкен дәрежелерінің модуліне бөлу кезінде қалдықтарды табуға мүмкіндік береді. Егер сізге a^n модулін m модуліне бөлудің қалдығын табу керек болса, мұндағы $(a, m) = 1$ (a және m сандарының ортақ бөлгіші 1) және $\varphi(m) < n$, онда n саны болуы мүмкін. ретінде бейнеленген

$$n = q\varphi(m) + r,$$

мұндағы $0 \leq r < \varphi(m)$.

Егер a және m сандарының ең үлкен ортақ бөлгіші d болса, яғни $(m, a) = d$, онда $m = m_1 d$ және $a = a1d$, мұндағы $(m1, a1) = 1$. a^n–ның m бөлінуінің қалдығын r арқылы белгілейік. Содан кейін:

$$a^n = a^{n-1} \, a = a^{n-1} a_1 \, d \equiv r \, mod \, m \equiv r \, mod \, m_1 d.$$

Салыстыру қасиеті бойынша $r = r_1 d$ деп жазуға болады. Сондықтан

$$a^{n-1} a_1 \, d \equiv r \, mod \, m \equiv r_1 d \, mod \, m_1 d$$

немесе

$$a^{n-1} \, a \equiv r_1 \, mod \, m_1$$

a^n–ді m–ге бөлуден r_1 қалдығын есептеу a_1 және a^{n-1} сандарын m_1 модуліне бөлуден қалған қалдықты есептеуге келеді.

Мысал. 171^{2147} 52-ге бөлінгенде қалдықты табайық. Бөлу кезінде қалдықты анықтау үшін келесі қадамдарды орындаңыз.

52 модуль үшін Эйлер функциясының мәнін анықтаймыз, яғни

$$\varphi(52) = \varphi(4 \times 13) = \varphi(2^2 \times 13) = 2^{2-1}(2-1) \times (13-1) = 2 \times 12 = 24;$$

2147 дәрежесін 52 модулінің Эйлер функциясының мәніне бөлу нәтижесін анықтаймыз, бізде $\varphi(52) = 24$. Бөлудің бөлімі $q = 89$, ал қалған r 11–ге тең. Демек, біз жаза аламыз $2147 = q \times \varphi(52) + r = 89 \times 24 + 11;$

Бізде бар

$$171^{89\times24+11} = 171^{89\times24}171^{11} = (171^{24})^{89}171^{11} = (171^{\varphi(52)})^{89}171^{11}.$$

Эйлер теоремасы бойынша $171^{\varphi(52)} = 1$. Салыстыру қасиеті бойынша, егер дәреже $a > m$, m модуль және $a = qm + r$, мұндағы q түбірі, ал r a-ны m-ге бөлгендегі қалдық, онда $a^n \bmod m \equiv (qm + r)^n \bmod m \equiv r^n \bmod m$.

Түбірдің дәрежесі 171 саны 52 модульден көп болғандықтан, оны келесі түрде жазуға болады $171 = 3 \equiv 52 + 15$, мұндағы 3 – 52 модулі бойынша 171 санын бөлгендегі түбірі, ал 15 қалдық. Жүргізілген есептерді ескере отырып,

$$(171^{\varphi(52)})^{89}171^{11} \bmod 52 \equiv (1)891511 \bmod 52 \equiv \equiv 15^{11} \bmod 52 \equiv 15^8 15^3 \bmod 52.$$

Көрсеткіштерге формулаларды пайдалана отырып $a^8 \bmod n = ((a^2 \bmod n)^2 \bmod n)^2 \bmod n$, келесіні аламыз

$$15^2 \bmod 52 \equiv 225 \bmod 52 \equiv 17 \bmod 52,$$

әрі қарай

$$17^2 \bmod 52 \equiv 289 \bmod 52 \equiv 29 \bmod 52$$

Оны келесі түрде жазуға болады

$$15^8 \bmod 52 \equiv ((15^2 \bmod 52)^2 \bmod 52)^2 \bmod 52 \equiv \equiv 29^2 \bmod 52 \equiv 841 \bmod 52.$$

Ақырында $15^8 \bmod 52 \equiv 841 \bmod 52 \equiv 9 \bmod 52$ аламыз. Салыстыру қаситеі бойынша келесіні аламыз

$$15^8 15^3 \bmod 52 \equiv (15^8 \bmod 52)(15^2 \bmod 52)(15 \bmod 52) \equiv \equiv (9 \times 17 \times 15) \bmod 52.$$

Әрі қарай келесідей түрде жазамыз

$$(9 \times 17 \times 15) mod\ 52 \equiv (9 \times 17\ mod\ 52) \times 15\ mod\ 52 \equiv$$
$$\equiv (153\ mod\ 52) 15\ mod\ 52 \equiv (49\ mod\ 52) \times (15\ mod\ 52) \equiv$$
$$\equiv (49 \times 15)\ mod\ 52\ \equiv 735\ mod\ 52 \equiv 7\ mod\ 52.$$

Ақыры аламыз

$$171^{2147} \equiv (171^{\varphi(52)})^{89} 171^{11}\ mod\ 52\ \equiv\ 171^{11}\ mod\ 52\ \equiv$$
$$\equiv\ 15^{11}\ mod\ 52 \equiv 7\ mod\ 52.$$

171^{2147} санын 52 санына бөлгенде қалдықты есептеу тапсырмасы орындалды.

Мысал. 126^{1020} санын 138 санына бөлудің қалдығын табыңыз. 126 дәреженің негізі мен 138 модулінің 6 санына тең ең үлкен ортақ бөлгіші бар екенін ескеріңіз. Бөлудің қалған бөлігін анықтау үшін келесі қадамдарды орындаймыз. Дәреже мен модульді келесідей түрлендіреміз

$$126^{1020} = 126^{1019} \times 126 = 126^{1019} \times 21 \times 6,$$
$$138 = 23 \times 6$$

онда

$$126^{1020}\ mod\ 138\ \equiv\ 126^{1019} \times 21 \times 6\ mod\ (23 \times 6) \equiv$$
$$\equiv\ 126^{1019} \times 21\ mod\ 23$$

23 модуль үшін Эйлер функциясының мәнін анықтаймыз 23 - жай сан, онда $\varphi(23)\ =\ 23 - 1\ =\ 22$;

1019 дәрежесін 23 модулінің Эйлер функциясының мәніне бөлу нәтижесін анықтаймыз, яғни $\varphi(23) = 22$. Бөлудің бөлімі q=46, ал қалдық r бізде r=7 санына тең, сондықтан жаза аламыз

$$1019\ =\ q \times\ \varphi(23)\ +\ r\ =\ 22 \times 46\ +\ 7;$$

Келесідей қарым-қатынас бар

$$126^{1019} \times 21\ mod\ 23 \equiv (126^{22 \times 46 + 7} \times 21)\ mod\ 23 \equiv$$
$$\equiv\ ((126^{22})^{46} 126^{7} \times 21)\ mod\ 23.$$

Өйткені Эйлер теоремасы бойынша біз жаза аламыз

$$126^{\varphi(23)}\ mod\ 138\ \equiv\ 126^{22}\ mod\ 138\ \equiv 1\ mod\ 23,$$

Қорыта келе келесіні аламыз $126^{1020}\ mod\ 138\ \equiv 126^{7} \times 21\ mod\ 138$. 126 санын 23 модуліне бөлудің қалдығы 11 болатынын ескере отырып, салыстыру қасиеттерін пайдалана отырып, біз жаза аламыз

$$126^7 \times 21 \, mod \, 138 \equiv ((126 \, mod \, 23)^7 \times 21 \, mod \, 23) \equiv$$
$$\equiv 11^7 \, mod \, 23 \times 21 \, mod \, 23.$$

$11^7 \, mod \, 23$ есептейміз. Оны келесідей жазамыз

$$11^7 \, mod \, 23 \equiv 11^{6+1} \, mod \, 23 \equiv (11^6 \times 11) \, mod \, 23 \equiv$$
$$\equiv 11^6 \, mod \, 23 \times 11 \, mod \, 23$$ түрінде жазуға болады.

Әрі қарай

$$11^6 \, mod \, 23 \equiv (11^2 \, mod \, 23)^3 \, mod \, 23 \equiv (121 \, mod \, 23)^3 \, mod \, 23$$

121 санының 23 модулі 6-ға тең екенін ескере отырып, келесіні аламыз,

$$(121 \, mod \, 23)^3 \, mod \, 23 \equiv (6 \, mod \, 23)^3 \, mod \, 23.$$

Салыстыру қасиетін қолдана отырып,

$$(6 \, mod \, 23)^3 \, mod \, 23 \equiv 6^3 \, mod \, 23 \equiv 216 \, mod \, 23 \equiv 9 \, mod \, 23.$$

Сонымен, қорытындыда келесіні жазамыз

$$11^7 \, mod \, 23 \equiv 9 \, mod \, 23 \times 11 \, mod \, 23 \equiv$$
$$\equiv (9 \times 11) \, mod \, 23 \equiv 7 \, mod \, 23.$$

Әрі қарай келесіні аламыз

$$126^{1020} \, mod \, 138 \equiv 7 \, mod \, 23 \times 21 \, mod \, 23 \equiv (7 \times 21) \, mod \, 23 \equiv$$
$$\equiv 147 \, mod \, 23 \equiv 9 \, mod \, 23.$$

Қорыта келгенде, келесіні аламыз

$$126^{1020} \, mod \, 138 \equiv 6 \times 1 \, (26^{1019} \times 21 \, mod \, 23) \equiv$$
$$\equiv 6 \times 9 \, mod \, 138 \equiv 54 \, mod \, 138.$$

Осылайша, 126^{1020} санын 138 бөлгенде қалдық 54 болады. 126^{1020} санын 138 бөлгенде қалдықты есептеу тапсырмасы орындалды.

Сәйкесінше 1640 және 1760 жылдары алынған Ферма мен Эйлердің нәтижелері ашық кілтті RSA криптографиялық жүйесін құрудың негізі болды.

1977 жылы Американдық ғалымдар Рональд Ривест, Ади Шамир және Леонард Адлеман заманауи ақпараттық технологиялар үшін түбегейлі жаңа және маңызды жүйені бір уақытта ұсынды. Шын мәнінде, RSA жүйесі толығымен Эйлер теоремасына негізделген.

Бірінші дәрежелі салыстырулар

a және b бүтін сандар, ал m модуль деп аталатын бүтін сан болсын. Содан кейін өрнек

$$ax \equiv b \bmod m,$$

бірінші дәрежелі бір белгісізмен салыстыру деп аталады.

Салыстыруды шешу берілген салыстыруды қанағаттандыратын *x*-тің барлық мәндерін табуды білдіреді.

Теорема 24. Егер $(a, m) = d$ болса, яғни a саны мен m модулінің ортақ бөлгіші d бар, ал d саны b бөлмейді, онда салыстырудың

$$ax \equiv b \bmod m$$

шешімдері жоқ.

Теорема 25. Егер $(a, m) = d$ болса, яғни a және m сандары қос жай сан, содан кейін салыстыру

$$ax \equiv b \bmod m$$

бір және бір ғана шешімі бар.

Теорема 26. Егер $(a, m) = 1$ яғни a және b сандары қос жай болса, онда салыстыру шешімі

$$ax \equiv b \bmod m$$

класы болып табылады.

$$x \equiv ba^{\varphi(m)-1} \bmod m,$$

мұндағы $\varphi(m) - m$ модулі үшін Эйлер функциясының мәні.

Мысал. Салыстыруды шешу $3x \equiv 4 \bmod 34$.

Назар аударыңыз (3,4) = 1, яғни 3 және 4 сандары салыстырмалы жай сандар. Содан кейін формула бойынша анықталады

$$x \equiv 4 \times 3^{\varphi(34)-1} \bmod 34,$$

$\varphi(34) = \varphi(2 \times 17) = (2-1) \times (17-1) = 16$ Есептейміз.

Содан кейін ерітіндінің мәні 3.5–формула бойынша анықталады

$$x \equiv 4 \times 3^{16-1} \equiv 4 \times 3^{15} \bmod 34$$

Салыстыру қасиетін қолдана отырып, $3^{15} \bmod 34$ мәнін есептейміз. Келесіні аламыз

$$3^{15} = (3^4)^3 \times 3^3 \; mod\; 34 \equiv (81 \; mod\; 34)^3 \times 27 \; mod\; 34 \; \equiv$$
$$\equiv (13 \; mod\; 34)^3 \times 27 \; mod\; 34 \; \equiv (13^3 mod\; 34) \times 27 \; mod\; 34 \equiv$$
$$\equiv (2179 \; mod\; 34) \times 27 mod\; 34 \equiv mod\; (21 \; mod\; 34) \times 27 mod\; 34 \; \equiv$$
$$\equiv (21 \times 27) mod\; 34 \; \equiv 567 \; mod\; 34 \; \equiv 23 \; mod\; 34.$$

Қорытындылай салыстыруды шешу үшін келесі мәнді аламыз

$$x\, x \; \equiv \; 4 \times 23 \; mod\; 34 \; \equiv \; 92 \; mod\; 34 \; \equiv \; 24 \; mod\; 34.$$

Тексеру. Алынған шешімді тексерту үшін $x = 24 \; mod\; 34$ x мәнін бастапқы салыстыруға қоямыз $3x \equiv 4 \; mod\; 34$. Онда келесіні аламыз $(3 \times 24) \; mod\; 34 \equiv 72 \; mod\; 34 \equiv 4 \; mod\; 34,$ өйткені 72 санын модуль 34–ке бөлгенде бөлгіш 2, ал қалдық 4. Осы жерден табылған х шешімі бұл салыстыруды қанағаттандыратынын көреміз. $3x \equiv 4 \; mod\; 34$ салыстыруды шешу есебі аяқталды.

Егер m саны жеткілікті үлкен болса, оны жай көбейткіштерге бөлу қиынға соғады. Алайда, бұл ыдырау Эйлер функциясының мәнін $\varphi(m)$ есептеу үшін, сондай-ақ салыстыру шешімін табу үшін қажет.

$$ax \; \equiv \; b \; mod\; m$$

(3.7) формуласы бойынша

$$x \; \equiv \; ba^{\varphi(m)-1} \; mod\; m, \qquad (1.7)$$

қиын есеп болуы мүмкін. Салыстыру шешімін анықтау үшін әдетте (1.3) формула қолданылады

$$x \; \equiv \; (-1)^{k-1} b P_{k-1} \; mod\; m \qquad (1.8)$$

мұндағы

k – m/a жалғасатын бөлшекке ыдырауының қолайлы фракцияларының саны;

P_{k-1} – m/a кеңеюінің соңғыдан кейінгі қолайлы бөлігінің бөлгіші жалғастырылған бөлшек.

Еске салайық, жалғас бөлшектер теориясынан кез келген бөлшек болатыны белгілі

m/a, қолайлы фракциялар тізбегіне кеңейтілуі мүмкін

$$P_i/Q_i \; , i \; = \; 0, 1, \dots, k.$$

Сонымен қатар, P_i және $Q_i \; i \; = \; 0, 1, \dots, k,$ есептеу үшін қайталанатын қатынастар әділ болады.

Бұл жағдайда $m/a \; = \; P_k/Q_k,$, ал P_i және Q_i есептеу үшін $i \; = \; 0, 1, \dots, k,$ қайталану қатынастары жарамды (3.9), (3.10) формулаларда өрнектелген

$$P_i = q_i P_{i-1} + P_{i-2}, \quad (1.9)$$
$$Q_i = q_i Q_{i-1} + Q_{i-2}, \quad (1.10)$$

мұндағы q_i ең кіші ортақ бөлгішті есептеу кезінде Евклид алгоритміндегі үлестер болып табылады және P_0, P_1 және Q_0, Q_1 бастапқы мәндері келесідей көрсетіледі: $P_0 = 1, P_1 = q_1, Q_0 = 0, Q_1 = 1$.

Назар аударыңыз. Алгоритмнің бірінші қадамы т модулін салыстырудың сол жағына, яғни а санына бөлудің нәтижесі болып табылады.

Мысал. Салыстыруды шешу $37x \equiv 25 \, mod \, 107$.

Бұл салыстыруды шешу үшін біз келесі қадамдарды орындаймыз. $m = 107$ салыстыру модулін $a = 37$ санына бөлу арқылы q_1 бөлімі мен r_2 қалдығын есептейміз. $q_1 = 2$, ал қалған $r_2 = 33$ аламыз. Сонда анықтама бойынша бізде $P_1 = q_1 = 2$. $a = 37$ санын қалдыққа бөлу арқылы q_2 бөлімін және r_3 қалдығын есептейміз.

$r_2 = 33$ біз $q_2 = 2$, ал қалғанын $r_3 = 4$ аламыз. Формула арқылы P_2 есептейміз

$$P_2 = q_2 P_1 + P_0 = 1 \times 2 + 1 = 3.$$

$r_2 = 33$ санын қалдыққа бөлу арқылы q_3 бөлімін және $r_3 = 4$ қалдығын есептейміз. Біз $q_3 = 8$, ал қалғанын $r_4 = 1$ аламыз. Формула арқылы P_3 есептейміз

$$P_3 = q_3 P_2 + P_1 = 8 \times 3 + 2 = 26.$$

$r_3 = 4$ санын қалдыққа бөлу арқылы q_4 бөлімін және r_5 қалдығын есептейміз. $r_3 = 1$ біз $q_4 = 4$, ал қалғанын $r_5 = 0$ аламыз. Формула арқылы P_4 есептейміз

$$P_4 = q_4 P_3 + P_2 = 4 \times 26 + 3 = 107.$$

Соңында формула бойынша $37x \equiv 25 \, mod \, 107$ салыстыру шешімін анықтаймыз.

$$x \equiv (-1)^{k-1} b P_{k-1} \, mod \, m \equiv$$
$$\equiv (-1)^3 \times 26 \times 25 \, mod \, 107 \equiv -650 \, mod \, 107$$

немесе $x \equiv -8 \, mod \, 107 \equiv 99 \, mod \, 107$

$x \equiv 99 \, mod \, 107$ салыстыру үшін x ≡ 99 mod 107 шешімін тексеру: $(937x \equiv 25 \, mod \, 107$: $(99 \times 37) \, mod \, 107 \equiv 3663 \, mod \, 107 \equiv (34 \times 107 + 25) \, mod \, 107 \equiv 25 \, mod \, 107$.

$37x \equiv 25 \, mod \, 107$ салыстыруды шешу есебі аяқталды, (3.11) формула бойынша есептелінеді.

$$x \equiv (-1)^{k-1} b P_{k-1} \, mod \, m \qquad (1.11)$$

салыстыру $ax \equiv b \, mod \, m$ шешу үшін модульдік арифметика мағынасында a элементіне a^{-1} кері мәнін анықтау үшін пайдаланылуы мүмкін. a^{-1} есептеу үшін салыстыруды шешу арқылы x–ті анықтау керек

$$ax \equiv 1 \, mod \, m.$$

Бұл жағдайда

$$a^{-1} \equiv x \equiv (-1)^{k-1} b P_{k-1} \, mod \, m$$

Мысал. Салыстыруды есептеу

$$1181x \equiv 1 \, mod \, 1290816.$$

Бұл салыстыруды шешу үшін біз келесі қадамдарды орындаймыз.

$m = 1290816$ салыстыру модулін $a = 1181$ санына бөлу арқылы q_1 бөлімі мен r_2 қалдығын есептейміз. $q_1 = 1092$, ал қалған $r_2 = 1164$ аламыз. Сонда анықтама бойынша бізде $P_1 = q_1 = 1092$ болады.

$a = 1181$санын қалдыққа бөлу арқылы q_2 бөлімін және r_3 қалдығын есептейміз.

$r_2 = 1164$. Біз $q_2 = 1$, ал қалғанын $r_3 = 17$ аламыз. (3.4) формула арқылы P_2 есептейміз

$$P_2 = q_2 P_1 + P_0 = 1 \times 1092 + 1 = 1093.$$

$r_2 = 1164$ санын қалдыққа бөлу арқылы q_3 бөлімін және r_4 қалдығын есептейміз.

$r_3 = 17$. Біз $q_3 = 68$, ал қалған $r_4 = 8$ аламыз. (3.4) формула арқылы P_3 есептейміз

$$P_3 = q_3 P_2 + P_1 = 68 \times 1093 + 1092 = 75416.$$

$r_3 = 17$ санын қалдыққа бөлу арқылы q_4 бөлімін және r_5 қалдығын $r_4 = 8$ есептейміз. Біз $q_4 = 2$, ал қалғанын $r_5 = 1$аламыз. Формула арқылы P_4 есептейміз

$$P_4 = q_4 P_3 + P_2 = 2 \times 75416 + 1093 = 151925$$

$r_4 = 8$ санын қалдыққа бөлу арқылы q_5 бөлімін және r_6 қалдығын $r_5 = 1$ есептейміз. Біз $q_5 = 8$, ал қалғанын $r_6 = 0$ аламыз. (3.4) формула арқылы P_5 есептейміз

$$P_5 = q_5P_4 + P_3 = 8 \times 151925 + 75416 = 1290816$$

Соңында формула бойынша $1181x \equiv 1\, mod\, 1290816$ салыстыру шешімін анықтаймыз.

$$x \equiv (-1)^{k-1} bP_{k-1}\, mod\, m \equiv (-1)^4 \times 151925\, mod\, 1290816 \equiv$$
$$\equiv 151925\, mod\, 1290816.$$

Шешімді тексеру $1181x \equiv 1\, mod\, 1290816$ салыстыру үшін $1181x \equiv 1 mod\, 1290816$. Келесі түрде жазуға болады

$$(1181 \times 151925)\, mod\, 1290816 \equiv$$
$$\equiv 179423425\, mod\, 1290816 \equiv$$
$$(139 \times 1290816 + 1)\, mod\, 1290816 \equiv$$
$$\equiv 1\, mod\, 1290816.$$

$1181x \equiv 1\, mod\, 1290816$ салыстыруды шешу есебі аяқталды.

Теорема 27. Егер $(a, m) = d$ болса, яғни a саны мен m модулінің ортақ бөлгіші бар d және d саны b $(d|b)$ бөледі, содан кейін салыстыру $ax \equiv b\, mod\, m$ үшін d шешімдері бар.

Квадраттық қалдықтар есептейік. p тақ жай сан болсын.

Анықтама 1. Егер салыстыру орындалса, a бүтін саны p квадраттық қалдық модулі деп аталады.

$$x^2 \equiv a\, mod\, p$$

шешімі бар.

Анықтама 2. Егер $x^2 \equiv a\, mod\, p$ салыстыруының шешімі болмаса, a бүтін саны квадраттық p модулі қалдықсыз деп аталады.

a бүтін санының p квадраттық қалдық модулі болу немесе болмау қасиеті a санын p санына бөлгенде қалдықтың қасиеттерімен ғана анықталады. Сондықтан 1 және 2 анықтамаларын қанағаттандыратын сандар класы бар. Бұл сандар сәйкесінше квадраттық қалдық және қалдық емес модуль р класы деп аталады.

Теорема 1. a саны квадраттық қалдық модулі $p, p > 2, p$ салыстыру дұрыс болған жағдайда ғана a бөлмейді.

$$a^{(p-1)/2} \equiv 1\, mod\, p.$$

Теорема 2. Егер салыстыру орындалса ғана a саны квадраттық қалдықсыз модуль $p, p > 2, p$ a бөлмейді.

$$a^{(p-1)/2} \equiv -11\, mod\, p.$$

Теорема 3. $1^2, 2^2, \dots, [(p-1)/2]^2$сандары p модулі бойынша квадраттық қалдықтардың барлық кластарының өкілдерінің жүйесін құрайды p $(p > 2)$.

Мысал. $p = 7$ санын қарастырайық. Сонда:

$$1^2 = 1 \equiv 1 \, mod \, 7,$$
$$2^2 = 4 \equiv 4 \, mod \, 7$$
$$3^2 = 9 \equiv 2 \, mod \, 7$$
$$4^2 = 16 \equiv 2 \, mod \, 7$$
$$5^2 = 25 \equiv 4 \, mod \, 7$$
$$6^2 = 36 \equiv 1 \, mod \, 7$$

Жоғарыдағы қатынастардан $p = 7$ үшін тек 1, 2, 4 сандары болатыны анық квадраттық қалдықтар класының өкілдері болып табылады. Бұл қалдықтар $1^2, 2^2, 3^2$ сандары үшін әлдеқашан анықталған. 3, 5, 6 сандары квадраттық қалдық емес екенін ескеріңіз, сондықтан келесі теңдеулер:

$$x^2 \equiv 3 \, mod \, 7,$$
$$x^2 \equiv 5 \, mod \, 7,$$
$$x^2 \equiv 6 \, mod \, 7,$$

шешімі жоқ.

Анықтама 3. a – бүтін сан және $p, p > 2$ жай сан болсын. Лежандр символы $L(a, p)$ теңдігімен анықталады, егер $a \equiv 0 \, mod \, p$

Басқаша айтқанда $L(a, p) = 1$, егер а квадраттық қалдық $x^2 \equiv a \, mod \, p$ модулі болса, a болса p квадраттық қалдықсыз модуль болса келесідей:

$$L(a, p) = (\frac{a}{p})$$

Әрі қарай p бөлмейтін a жағдайды қарастырамыз, яғни $L(a, p) \neq 0$.

Мысалдар. $L(3, 11) = 1$, өйткені $x^2 \equiv 3 \, mod \, 11$ салыстыруында $x_1 \equiv 5 \, mod \, 11$ және $x_2 \equiv -5 \, mod \, 11$ екі шешімі бар. $L(6, 7) = -1$, өйткені салыстыру $x^2 \equiv 6 \, mod \, 7$ шешімдері жоқ. Леджендр символының негізгі қасиеттерін көрсетейік.

1) Егер $a \equiv b \, mod \, p$, онда $L(a, p) = L(b, p)$.

2) $L(a1 \times a2 \times \dots \times ak) = L(a1, p) \times L(a2, p) \times \dots \times L(ak, p)$.

3) $L(a^2, p) = 1$.

4) $L(1, p) = 1$.

5) $L(a, p) = a^{\frac{p-1}{2}} \, mod \, p$ (Эйлер критериясы).

6. $L(-1, p) = (-1)^{(p-1)/2} \, mod \, p$.

7) $L(2, p) = (-1)^{p-1/8}$.

8) $L(q, p) = -1^{[(p-1)/2][(q-1)/2]} L(p, q)$ – өзара келіскен қағида. Бұл

заңды осындай $L(q,p)L(p,q) = -1^{\left[\frac{p-1}{2}\right]\left[\frac{q-1}{2}\right]}$ түрде жазуға болады.

Көрсетілген қасиеттерге сүйене отырып, егер $a = a_1^{a1} \dots a_k^{ak}$ болса, $L(a,p) = L(a_1,p)^{a1} \dots L(a_k,p)^{ak}$ болатынын ескереміз.

Бұл теңдікте 3–қасиетті ескере отырып, a_j , $j \leq k$ көрсеткіші жұп сан болатын факторларды алып тастай аламыз. Егер кейбір $a_j = 2$, $j \leq k$ болса, онда 7 қасиет $L\left(a_j,p\right)^{aj} = L(2,p)^{aj}$ мәнін есептеуге мүмкіндік береді.

Жоғарыда айтылғандар Лежендр символын есептеу алгоритмін құрастыруға мүмкіндік береді. Егер a саны теріс болса, онда $L(-1,p)$ коэффициентін таңдаңыз; a санын p санына бөлудің қалдығымен ауыстырыңыз; a санын жай көбейткіштердің көбейтіндісіне кеңейтеміз

$$a = a_1^{a1} a_2^{a2} \dots a_k^{ak}$$

егер санды жай көбейткіштерге ыдырату мүмкін болмаса, онда 7-қадамға өтіңіз. Бөлуге көшіңіз

$$L(a,p) = L(a_1,p)^{a1} \dots L(a_k,p)^{ak}$$

a_j , $j \leq k$ көрсеткішінің жұп мәні бар факторларды алып тастаймыз a_j=2 үшін Legendre символын $L(a_j,p)^{aj}$ есептейміз. Егер барлық Лежандр таңбалары өрнекте болса

$$L(a,p) = L(a_1,p)^{a1} \dots L(a_k,p)^{ak}$$

есептеледі, содан кейін $L(a,p)$ есептеу алгоритмі аяқталады. Әйтпесе, $aj \neq 2$ болатын $L(a_j,p)^{aj}$ факторлары үшін өзара әрекет заңын қолданамыз.

$$L(q,p) = -1^{[(p-1)/2][(q-1)/2]} L(p,q)$$

$L(p,q)$ формуласы $p = a_j$ деп есептейді. 1–қадамға өтіңіз.

Назар аударыңыз. Әрбір қадамда Лежандр таңбасын есептеу процесі аяқталуы мүмкін. Алгоритмнің қандай да бір қадамында барлық a_j , $j \leq k$ сандары 1, 2 немесе –1–ге тең болса, бұл орын алады.

Мысал. $L(68,113)$ есептеңіз. Мұнда $a = 68$, ал $p = 113$ жай сан. $L(68,113)$ есептеу алгоритмі. $a > 0$ болғандықтан, $L(-1,113)$ факторы жоқ; $68 < 113$ болғандықтан, қалдық санның өзіне тең; $a = 68$ санын жай көбейткіштерге $68 = 2^2 \times 17$; Бізде бар:

$$L(68,113) = L(2^2 \times 17,113) = L(2^2,113)L(17,113) = \\ = [L(2,113)]^2 L(17,113);$$

$L(2^2,113) = 1$ (3 қасиетін қараңыз) мәнін қолдана отырып, онда

бөліктері

$$L(68,113) = [L(2,113)]^2 L(17,113)$$

Көбейту мәндері $[L(2,113)]^2$ орындалғаннан кейін 5-ші қадамды орындағанда келесі мәндер алынады

$$L(68,113) = L(17,113).$$

Алынған бөлінуде $L(2,113)$ көбейтіндісі жоқ;

L(17,113) көбейтіндісі үшін $a = 17$ және $p = 113$, үшін өзаралық заңын қолдану арқылы біз:

$$L(17,113) = (-1)^{8\times 56} L(113,17) = L(113,17).$$

Қорыта келе $L(68,113) = L(113,17)$ алынады.

Әрі қарай 1 қадамға барамыз және $L(113,17)$ есептейміз, мұндағы $a = 113$, ал $p = 17$ жай сан.

Есептеу алгоритмі $L(113,17)$.

$a > 0$ жоқ болғандықтан, көбейтіндісі болып табылады.

113 санын 17-ге бөлудің қалған бөлігі 11-ге тең, сондықтан біз аламыз:

$$L(113,17) = L(11,17);$$

11 саны көбейткіштерге жіктелмейтін жай сан;

11 жай сан болғандықтан, 7-қадамға көшеміз; $L(11,17)$ факторы үшін $a = 11$ және үшін өзара заңын қолдану $p = 17$, біз аламыз:

$$L(11,17) = (-1)^{5\times 8} L(17,11) = L(17,11).$$

Нәтижесінде бізде бар

$$L(113,17) = L(17,11).$$

Содан кейін 1-қадамға өтіп, $L(17,11)$ есептеуді бастаймыз, мұнда $a = 17, p = 11$ жай сан.

$L(17,11)$ есептеу алгоритмі. $a > 0$ болғандықтан, $L(-1,11)$ факторы жоқ; 17-ні 11-ге бөлгенде қалдық 6 болады. 6 санын жай көбейткіштерге 6 = 2×3 көбейтеміз. Бізде бар

$$L(6,11) = L(2,11)L(3,11)$$

Кеңейтуде дәреже көрсеткіштерінің жұп мәндері бар факторлар жоқ, сондықтан біз 6-қадамға өтеміз;

$L(2,11)$ мәнін есептейміз:

$$L(2,11) = [-1]^{(a-1)/8} = [-1]^{15} = -1,$$
$$a = p^2 = 11^2 = 121;$$

$L(3,11)$ факторы үшін $a = 3$ және $p = 11$ үшін өзара заңын қолдану арқылы, біз келесі мәндерді аламыз: $L(3,11) = (-1)^{1\times5}L(11,3) = -L(11,3)$. Нәтижесінде біз аламыз: $L(17,11) = (-1) \times [-L(11,3)] = L(11,3)$.

Содан кейін 1-қадамға өтіп, $L(11,3)$ есептеуді бастаңыз, мұнда $a = 11, p = 3$ - жай сан. $L(11,3)$ есептеу алгоритмі. $a > 0$ болғандықтан, $L(-1,3)$ факторы жоқ; 11 санын 3 санына бөлгенде қалғаны 2 болады, сондықтан келесіні аламыз: $L(11,3) = L(2,3)$.

2 саны жай сан және көбейткіштерге бөлуге болмайды; Бізде бар $L(11,3) = L(2,3)$.

Ыдырауда көрсеткіштердің біркелкі мәндері бар факторлар жоқ, сондықтан біз 6-қадамға көшеміз; $L(2,3)$ мәнін есептеңіз

$$(2,3) = [-1]^{(a-1)/8} = [-1]1 = -1,$$
$$a = p^2 = 3^2 = 9.$$

Ақырында $L(68,113) = -1$ екенін аламыз.

Осылайша, Лежандр символының $L(68,113)$ есебі аяқталды. Лежандр символының мәні $L(68,13) = -1$ салыстыру туралы қорытынды жасауға мүмкіндік береді $x^2 \equiv 68 \, mod \, 113$ шешімдері жоқ.

Анықтама 4. Тақ p санының келесі жай көбейткіштерге жіктелуі болсын

$$p = p_1 p_2 \ldots p_k,$$

мұндағы $p_j, j \leq k$, жай сандар, олардың кейбіреулері бірдей болуы мүмкін. Якоби символы $J(a,p)$ теңдікпен анықталады:

$$J(a,p) = L(a,p_1)\, L(a,p_2) \ldots L(a,p_k).$$

Лежандр символы Якоби символының ерекше жағдайы екенін ескеріңіз. Оның үстіне, егер p жай сан болса, онда Якоби таңбасы анықтамасы бойынша Леджандр таңбасы болып табылады. Бұл ретте Якоби символы $J(a,p)$ 1–ге тең болуы мүмкін, яғни $J(a,p) =$ 1,ал салыстыру $x^2 \equiv a \, mod \, p$ шешімдері жоқ.

Мысал. Якоби символын $J(2,15)$ анықтайық. Анықтама бойынша $(2,15) = L(2,3)L(2,5)$. $L(2,3)$ есептейік

$$L(2,3) = [-1]^{(a-1)/8} = [-1] = -1 \, (a = p^2 = 3^2 = 9) \text{ және}$$
$$L(2,5)\, L(2,5) = [-1]^{(a-1)/8} = [-1]^3 = -1 \, (a = p^2 = 5^2 = 25).$$

Ақырында $J(2,15) = L(2,3)L(2,5) = (-1)(-1) = 1$ аламыз.

Сонымен, $J(2,15) = 1$, ал $x^2 \equiv 2 \, mod \, 15$ салыстыруының шешімі жоқ.

Якоби символының негізгі қасиеттерін көрсетейік.

1) Егер $a \equiv b \, mod \, p$, то $J(a,p) = J(b,p)$;

2) $J(a_1 \times a_2 \times \ldots \times a_k) = J(a_1,p) \times J(a_2,p) \times \ldots \times J(a_k,p)$;

3) $J(a^2,p) = 1$;

4) $J(1,p) = 1$;

5) $J(-1,p) = (-1)^{\frac{p-1}{2}} \, mod \, p$;

6) $J(2,p) = (-1)^{(p^2-1)/8}$;

7) $J(q,p) = (-1)^{\left[\frac{p-1}{2}\right]\left[q-\frac{1}{2}\right]} L(p,q)$ – өзара заң. Бұл заңды келесі формада да жазуға болады

$$J(q,p)J(p,q) = (-1)^{\left[\frac{p-1}{2}\right]\left[q-\frac{1}{2}\right]}$$

Якоби символын есептеу алгоритмі:

– Егер a саны теріс болса, $J(-1,p)$коэффициентін таңдаңыз;

– a санын p-ге бөлудің қалдығымен ауыстырыңыз;

– Егер a саны жұп болса, онда оны келесі түрде көрсетеміз

$$a = 2^t a_1,$$

мұндағы a_1 – тақ сан.

Декомпозицияға көшейік

$$J(a,p) = J(2,p)^t \, J(a1,p);$$

1) $J(2,p)^t$коэффициентін алып тастаймыз, егер t жұп сан болса;

2) Егер t тақ болса, онда Legendre символын $J(2,p)^t$ есептейміз;

3) $J(q,p)$ үшін өзара заңын қолданамыз.

$L(q,p) = (-1)^{\left[\frac{p-1}{2}\right]\left[q-\frac{1}{2}\right]} L(p,q)$ мұндағы $q = a_1$. 1–қадамға көшейік.

Мысал. $J(506,1103)$ есепте, мұндағы $a = 506, p = 1103$жай сан. 1103 жай сан болғандықтан, Якоби символының мәні Лежандр символының мәніне тең, яғни. $J(506.1103) = L(506.1103)$. Якоби таңбасын есептеу оңайлатылған, себебі а құрама сан болғанда, өзара заңның қолданылуы мүмкін [20]. Лежнадр таңбаларын қарастырғанда, құрама a санын жай көбейткіштердің көбейтіндісіне ыдырату керек, бұл оңай жұмыс емес.

$J(506,1103)$ есептеу алгоритміне мысал келтірейік:

1. $a > 0$ болғандықтан $J(-1,1103)$ коэффициенті жоқ;

2. $506 < 1103$ болғандықтан, қалдық санның өзіне тең;

3. $a = 506$ санын $506 = 2 \times 253$деп көрсетеміз;

4. $J(506.1103) = J(2.1103)J(253.1103)$ кеңеюіне көшеміз;

5. $J(2.1103)$ факторының $t = 1$ көрсеткіші тақ, сондықтан 6-қадамға өтіңіз;

6. Есептеңіз $J(2,1103) = [-1]^{(a-1)/8} = [-1]^{152076} = 1,$

мұндағы $a = p^2 = 1103^2$.

7. $J(253, 1103)$ коэффиценті үшін $a = 253$ және $p = 1103$ өзара заңын қолдана отырып. $J(53, 1103) = (-1)^{126\times551} J(1103, 253) = J(1103, 253))$ аламыз.

8. Нәтижесінде $J(506, 1103) = J(1103, 253$ аламыз. Содан кейін 1–қадамға өтіп, $J(1103{,}253)$ есептеуді бастаңыз, мұнда $a = 1103, p = 253$;

$J(1103{,}253)$ есептеу алгоритмі.

1. $a > 0$ болғандықтан $J(-1{,}253)$ коэффициенті жоқ;

2. 1103 санын 253 бөлгенде қалдық 91 тең, сондықтан $J(1103.253) = J(91.253)$;

3. $a = 91$ саны тақ, 7 қадамға өтіңіз;

4. Орындалмаған;

5. Орындалмаған;

6. Орындалмаған;

7. $J(91{,}253)$ Якоби символы үшін $a = 91$ және $p = 253$ үшін өзара заңын қолдана отырып. $J(91, 253) = (-1)^{45\times126} J(253{,}91) = J(253, 91)$ аламыз.

8. Нәтижесінде $J(1103.253) = J(253.91)$ болады. Содан кейін 1–қадамға өтіп, $J(253{,}91)$ есептеуді бастаңыз, мұнда $a = 253, p = 91$;

$J(253{,}51)$ есептеу алгоритмі.

1. $a > 0$ болғандықтан, $J(-1{,}91)$ факторы жоқ;

2. 253 санын 91–ге бөлгенде қалдық 71 болады, сондықтан $J(253, 91) = J(71, 91)$;

3. $a = 71$ саны тақ, 7-қадамға өтіңіз;

4. Орындалмаған;

5. Орындалмаған;

6. Орындалмаған;

7. Якоби символы $J(71{,}91)$ үшін $a = 71$ және $p = 91$ үшін өзара заңын қолдану. Бізде $J(71, 91) = (-1)^{35\times45} J(91, 71) = -J(91, 71)$ бар.

8. Нәтижесінде $J(253{,}91) = -J(91{,}71)$ аламыз. Содан кейін 1–қадамға өтіп, $J(91{,}71)$ есептеуді бастаңыз, мұнда $a = 91, p = 71$;

$J(91{,}71)$ есептеу алгоритмі.

1. $a = 91 > 0$ болғандықтан, $J(-1{,}71)$ факторы жоқ;

2. 91 санын 71 бөлгенде қалдық 20 болады, сондықтан $J(91, 71) = J(20, 71)$;

3. $a = 20$ санын $a = 22 \times 5$түрінде көрсетейік;

4. $J(20, 71) = J(2, 71)2\,J(5, 71)$ кеңеюіне көшейік:

5. $J(2, 71)$ $t = 2$коэффициентінің көрсеткіші жұп, демек $J(2, 71)^2 = 1$. 7-қадамға өтіңіз;

6. Орындалмаған;

7. Якоби символы $J(5{,}71)$ үшін $a = 5$ және $p = 71$ үшін өзара заңын қолдана отырып. Бізде $J(5, 71) = (-1)^{2\times35} J(71, 5) = J(71, 5)$.

8. Нәтижесінде $-J(91, 71) = -J(71, 5)$ аламыз. Содан кейін 1–қадамға өтіп, $-J(71, 5)$ есептеуді бастаңыз, мұндағы $a = 71, p = 5$;

$J(71, 5)$есептеу алгоритмі.

1. $a = 71 > 0$болғандықтан $J(-1,71)$ коэффициенті жоқ;

2. 71 санын 5–ке бөлгенде қалдық 1 болады, сондықтан $J(71,5) = J(1,5)$;

3. $a = 1$ саны тақ, 7-қадамға өтіңіз;

4. Орындалмаған;

5. Орындалмаған;

6. Орындалмаған;

7. Якоби символын есептеңдер $J(1,5) = 1$;

8. Нәтижесінде $-J(71,5) = -1$ аламыз. Якоби символының $J(1103,253)$ есебі аяқталды. Соңында $J(1103,253) = -1$ аламыз. Якоби символының $J(506,1103) = -1$ мәні $x^2 \equiv 506\ mod\ 1103$салыстыруының шешімі жоқ деген қорытынды жасауға мүмкіндік береді.

Қытай қалдық теоремасы

Сандар теориясының маңызды нәтижелерінің бірі қытай қалдық теоремасы (ҚҚТ) деп аталады [18, 59 б.]. Негізінде, бұл теорема кейбір жұптық тең жай сандар жиынынан сандарға бөлу арқылы оның қалдықтары жиынынан бүтін санды қайта құруға болатынын айтады. Бұл теорема біздің эрамызға дейінгі 100 жылдар шамасында дәлелденген. Қытайлық қалдық теоремасының бірнеше тұжырымдары бар. Олардың кейбіреулерін осы жерде ұсынайық. Қалдықтар сақинасын Z_n арқылы n модулімен белгілейік.

Теорема (ҚҚТ). Егер

$$n = n_1 n_2 \dots n_k,$$

мұндағы $n_i, 1 \le i \le k$,салыстырмалы жай сандар, онда Z_n сақинасы Z_{ni} сақиналарының тура қосындысы.

Теорема (ҚҚТ). Айталық $n_i, 1 \le i \le k$, болсын қарапайым сандарды көбейтіңіз және a_j бүтін сандар болсын. Сонда x саны бар, ондай

$$\begin{gathered} x \equiv a_1\ mod\ n_1, \\ x \equiv a_2\ mod\ n_2, \\ \dots \\ x \equiv a_k\ mod\ n_k, \\ x \equiv a_1\ mod\ n_1, \\ x \equiv a_2\ mod\ n_2, \\ \dots \\ x \equiv a_k\ mod\ n_k, \end{gathered}$$

Теорема (ҚҚТ). Сызықтық салыстыру жүйесінің модульдері салыстырмалы жай болсын. Бұл n_i және n_j екі санның ортақ бөлгіші біреуге тең екенін білдіреді, яғни $(n_i, n_j) = 1$ үшін $1 \le i, j \le k$. Бұл жағдайда шартты қанағаттандыратын Z_{ni} қалдық класы бар

$$Z_{ni} \equiv 0 \, mod \, n_j.$$

Соңында, осы оқулықта кейінірек қолданатын теореманың басқа тұжырымын қарастырайық.

Теорема (ҚҚТ). m_j, $1 \leq i \leq k$ өзара жай сандар болсын, ал $M = m_1, m_2 \ldots m_k$ болсын.

$a_j, 0 \leq a_j \leq m_i$, бүтін сандар болсын. $M_i = M/m_i$ белгісін енгізейік. $M_i N_i \equiv 1 \, mod \, m_i$ салыстыруын қанағаттандыратын сан болсын. Осы шарттарда салыстыру

$$x \equiv a_i \, mod \, m_i$$

формуласымен анықталатын $[0, M-1]$ интервалында бірегей шешімі бар

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + \ldots + a_k N_k M_k.$$

Теореманың шарттары ішінде қытай қалдық теоремасы бүтін сандар мен кейбір бүтін сандар жиыны арасында бір–бірден сәйкестік бар екенін айтады. Басқаша айтқанда, әрбір B бүтін саны үшін оған сәйкес келетін $b_1, b_2, \ldots, b_k$, сандарының бірегей жиыны бар, ал, керісінше, $b_1, b_2, \ldots, b_k$ сандарының әрбір жиыны үшін осы жиынға сәйкес келетін бірегей B саны.

Мысал. Салыстыру жүйесін шешу

$$\begin{aligned} x &\equiv a_1 \, mod \, 4, \\ x &\equiv a_2 \, mod \, 5, \\ x &\equiv a_3 \, mod \, 7, \end{aligned}$$

мұндағы $m_1 = 4, m_2 = 5, m_3 = 7$. $M = m_1 m_2 m_3 = 4 \times 5 \times 7 = 140.$ санын анықтаймыз.

Есептеп көрейік

$$\begin{aligned} M_1 &= \frac{M}{m_1} = \frac{140}{4} = 35 \\ M_2 &= \frac{M}{m_2} = \frac{140}{5} = 28 \\ M_3 &= \frac{M}{m_3} = \frac{140}{7} = 20. \end{aligned}$$

Келесі салыстырулардан $N_1, N_2,$ және N_3 есептейік

$$\begin{aligned} N_1 M_1 &= 35 N_1 \equiv 1 \, mod \, 4, \\ N_2 M_2 &= 28 N_2 \equiv 1 \, mod \, 5, \\ N_3 M_3 &= 20 N_3 \equiv 1 \, mod \, 7. \end{aligned}$$

1–ші салыстыруды $35N_1 \equiv 1 \, mod \, 4$ шешеміз. Эйлер функциясын $\varphi(4) = \varphi(2^2) = 2^{2-1}(2-1) = 2$ анықтаймыз.

Сонда Ферма теоремасынан $N1 = 35^{\varphi(4)-1} \, mod \, 4 = 35^{2-1} \, mod \, 4 = 35 \, mod \, 4 = 3$ шығады. 1–ші салыстырудың шешімін тексеру $35N_1 \equiv 1 \, mod \, 4$, $35N_1 \equiv 1 \, mod \, 4$ салыстыруында $N_1 = 3$ мәнін ауыстырамыз, біз $35 \times 3 \, mod \, 4 \equiv 105 \, mod \, 4 \equiv 1 \, mod \, 4$ аламыз.

Біз 2–ші салыстыруды шешеміз $28N_2 \equiv 1 \, mod \, 5$. Эйлер функциясын анықтаймыз $\varphi(5) = 5 - 1 = 4$. Сонда Ферма теоремасынан келесідей болады.

$N_2 = 28^{\varphi(5)-1} \, mod \, 5 = 28^{4-1} \, mod \, 4 = 28^3 \, mod \, 5 = 112 \, mod \, 5 = 2 \, mod \, 5.$

2–ші салыстырудың шешімін тексеру $28N_2 \equiv 1 \, mod \, 5$. $N_2 = 2$ мәнін $28N_2 \equiv 1 \, mod \, 5$ салыстыруына ауыстырсақ, аламыз $28 \times 2 \, mod \, 5 \equiv 56 \, mod \, 5 \equiv 1 \, mod \, 5$

3–ші салыстыруды $20N_3 \equiv 1 \, mod \, 7$ шешеміз.

Эйлер функциясын $\varphi(7) = 7 - 1 = 6$ анықтаймыз. Сонда Ферма теоремасынан шығады

$$N_3 = 20^{\varphi(7)-1} \, mod \, 7 = 20^{6-1} \, mod \, 7 = 20^5 \, mod \, 7 = 20 \, mod \, 7 = 6 \, mod \, 7 .$$

3–ші салыстыру $20N_3 \equiv 1 \, mod \, 7$ шешімін тексеру. $20N_2 \equiv 1 \, mod \, 7$ салыстыруында $N_3 = 6$ мәнін ауыстырсақ, бізде $20 \times 6 \, mod \, 7 \equiv 120 \, mod \, 7 \equiv 1 \, mod \, 7$ болады.

Соңында біз салыстыру жүйесінің шешімін аламыз

$$x \equiv a_1 \, mod \, 4,$$
$$x \equiv a_2 \, mod \, 5,$$
$$x \equiv a_3 \, mod \, 7,$$

(3.12) формуласымен анықталады:

$$x = (a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 = (35 \times 3a_1 + 28 \times 2a_2 + 20 \times 6a_3) \, mod \, 140. \quad (3.12)$$

Бұл маңызды математикалық нәтиже сызықтық салыстыру жүйелерін шешудің тиімді әдісін ұсынады, ол әртүрлі салаларда, соның ішінде криптография, кодтау, тіпті информатиканың кейбір салаларда қолданылады. Қытай қалдық теоремасы модульдік арифметиканың күшін және оның практикалық қосымшалардағы әртүрлі есептерді шешудегі маңыздылығын көрсетеді.

Қолданылған әдебиеттер тізімі

1. Белларе М., Рогауэй П. (1993). Аутентификация объекта и распределение ключей. / Белларе М. – CRYPTO, 2020. – 249 с.

2. Шуп, В. Практические пороговые подписи. – М.: Триумф, 2023. – 556 с.

3. Diffie W, Hellman ME. Multiuser cryptographic techniques. In: Proceedings of the June 7-10, 1976, national computer conference and exposition. ACM Digital Library; 1976. pp. 109-112