2.3. Сандар теориясының элементтері

Көптеген криптографиялық Алгоритмдер нәтижелерге негізделген классикалық сандар теориясы. Біз қажетті минимумды қарастырамыз осы теориядан. Ферманың, Эйлердің және басқалардың классикалық теоремалары сандар теориясының нәтижелері дәлелсіз беріледі сандар теориясының кез-келген оқулығынан табуға болады (мысалы, [3] қараңыз). Сандар теориясымен таныс оқырмандар тікелей өтіңіз бөлім. 2.4

Анықтама 2.2. Бүтін оң Сан p деп аталады қарапайым, егер ол өзінен және бірлігінен басқа санға бөлінбесе Мысал 2.3. 11, 23 сандары — жай; 27, 33 сандары-құрама (27 3-ке және 9-ға, 33-ке 3-ке және 11-ге бөлінеді).

2.3 теоремасы (арифметиканың негізгі теоремасы). Кез келген бүтін оң санды жай сандардың көбейтіндісі ретінде және жалғыз түрде ұсынуға болады.

Мысал 2.4. $27 = 3 \cdot 3 \cdot 3$, $33 = 3 \cdot 11$.

Анықтама 2.3. Екі Сан өзара қарапайым деп аталады, егер оларда бірліктен басқа ортақ бөлгіш болмаса.

Мысал 2.5. 27 және 28 сандары өзара қарапайым (олардың ортақ белгілері жоқ бірліктен басқа бөлгіштер), 27 және 33 сандары жоқ (оларда ортақ бөлгіш 3).

2.4 анықтамасы(Эйлер функциясы). $N \geq 1$ бүтін сан берілсін. Эйлер функциясының мәні $\varphi(N)$ сандар санына тең 1, 2, 3 қатарында . . . , N-1, N-мен өзара қарапайым

Мысал 2.6.

$\varphi(10) = ?$ $\varphi(12) = ?$

1, 2, 3, 4, 5, 6 , 7, 8, 9, 1, 2, 3, 4, 5, 6 , 7, 8, 9, 10, 11

$\varphi(10) = 4$ $\varphi(12) = 4$

((мұнда аргументпен өзара қарапайым емес сандар сызылған).

Бекіту 2.4. Егер p жай сан болса, онда $\varphi(p) = p - 1$.

Дәлел. 1, 2, 3 қатарында . . . , p-1 барлық сандар өзара p - мен қарапайым, өйткені p-жай сан және анықтамасы бойынша бөлінбейді басқа сан жоқ.

Бекіту 2.5. P және q екі түрлі қарапайым болсын

сандар($p \neq q$). Содан кейін

$$\varphi(pq) = (p - 1)(q - 1).$$

Дәлел . 1, 2 қатарында . . . , pq-1 pq-мен өзара қарапайым емес сандар болады

Және

$$q, 2q, 3q, \cdot \cdot \cdot ,(p - 1)\, q.$$

Мұндай сандардың барлығы (q − 1) + (p − 1) болады. Демек, саны pq-мен өзара қарапайым сандар pq − 1 − (p − 1) − (q − 1) = pq − q − p + 1 = (p − 1) (q – 1) болады.

Теорема 2.6 (Ферма). P жай сан және 0 < a < p болсын.

Содан кейін

$$a^{p-1} \bmod p = 1.$$

Мысал 2.7.

$$p = 13,\ a = 2;$$

$$2^{12} \bmod 13 = (2^{2})^{2} \cdot (2^{2})^{2} \bmod 13 = 3 \cdot 9 \bmod 13 = 1,$$

$$10^{10} \bmod 11 = 10^{2} \cdot ((10^{2})^{2})^{2} \bmod 11 = 1 \cdot 1 = 1.$$

Теорема 2.7 (Эйлер). a және b өзара жай сандар болсын.

Онда

$$a^{\varphi(b)} \bmod b = 1.$$

Ферма теоремасы-Эйлер теоремасының ерекше жағдайы, егер в жай сан болса.

Мысал 2.8.

$$\varphi(12) = 4,$$

$$5^{4} \bmod 12 = (5^{2})^{2} \bmod 12 = (1^{2})^{2} \bmod 12 = 1.$$

$$\varphi(21) = 2 \cdot 6 = 12,$$

$$2^{12} \bmod 21 = 2^{4} \cdot (2^{4})^{2} \bmod 21 = 16 \cdot 4 \bmod 21 = 1$$

Бізге Эйлер теоремасына жақын тағы бір теорема қажет болады.

Теорема 2.8. Егер p және q жай сандар болса, p 6= q және k —

ерікті бүтін сан, онда

$$a^{k\varphi(pq)+1} \bmod (pq) = a$$

Мысал 2.9. P = 5, q = 7 алайық. Содан кейін pq = 35, A функциясы

Эйлер-φ(35) = 4 · 6 = 24. K = 2 жағдайын қарастырайық, яғни.

сандарды дәрежеге көтеру 2 · 24 + 1 = 49. Шығады

$$9^{49} \bmod 35 = 9,\ 23^{49} \bmod 35 = 23.$$

Бұл таңқаларлық емес, өйткені 9 және 23 сандарының әрқайсысы өзара қарапайым 35 модулімен және Эйлер теоремасы бойынша $9^{24} \bmod 35 = 1$, $23^{24} \bmod 35 = 1$. Алайда, 2.8 теоремасы келесі сандар үшін де шындық болып қала береді:

$$10^{49} \bmod 35 = 10,\ 28^{49} \bmod 35 = 28$$

Эйлер теоремасы олар үшін қолданылмаса да (әрқайсысы 10 және 28 сандары 35 және $10^{24} \bmod 35 = 15$, $28^{24} \bmod 35 = 2$ модульдерімен өзара қарапайым емес

Анықтама 2.5.a және b екі натурал сан болсын сандар. a және b сандарының ең үлкен ортақ бөлгіші ең үлкен a мен екеуін бөлетін c саны.

$$c = \gcd(a,b)$$

(Ең үлкен ортақ бөлгіш үшін gcd белгісі орын алады ағылшын сөздерінен greatest common divisor және қазіргі заманда қабылданған әдебиет.)

Мысал 2.10. $\gcd(10, 15) = 5;\ \gcd(8, 28) = 4.$

Ең үлкен ортақ бөлгішті табу үшін Евклид алгоритмі деп аталатын келесі алгоритмді қолдануға болады.

Кіріс: A,b, A ≥ b жартылай Май сандары.

Шығу: ең үлкен gcd пайдаланушысы (a, b).

1. WHILE b6 = 0 дейін

2. r ← a mod b, a ← b, b ← r .

3. RETURN a.

Мысал 2.11. Евклид алгоритмін қалай қолдану керектігін көрсетейік gcd есептеледі (28, 8):

a : 28 8 4

b : 8 4 0

r : 4 0

мұнда әр баған алгоритмнің басқа итерациясын білдіреді. Процесс b тең болғанша жалғасады нөлге тең болғанша. Содан кейін a айнымалысының мәні жауап береді (4).

Келесі бөлімдер мен тарауларда қарастырылған көптеген криптографиялық жүйелер үшін жалпыланған деп аталатындар өзекті келесі теоремамен байланысты Евклид алгоритмі.

Теорема 2.9. a және b екі натурал сан болсын. Содан кейін бүтін сандар бар (міндетті түрде оң емес) x және y сандары осылай болады

$$ax + by = \gcd(a, b) .$$

(2.13)

Жалпыланған Евклид алгоритмі gcd(a, b) табуға қызмет етеді

және X , y қанағаттандырады (2.13). Біз үш жолды енгіземіз $U = (u_1, u_2, u_3)$,

$V = (v_1, v_2, v_3)$ және $T = (t_1, t_2, t_3)$. Содан кейін алгоритм келесідей жазылады.

Алгоритм 2.2. Евклидтің жалпыланған алгоритмі

INPUT: a,b, $a \geq b$ оң бүтін сандар.

ШЫҒЫС: gcd(a, b), x, y қанағаттандыратын (2.13).

1. $U \leftarrow (a, 1, 0)$, $V \leftarrow (b, 0, 1)$.

2. WHILE v1 6= 0 ЖАСАУ

3. $q \leftarrow u_1 \text{ div } v_1$;

4. $T \leftarrow (u_1 \bmod v_1, u_2 - qv_2, u_3 - qv_3)$;

5. $U \leftarrow V$, $V \leftarrow T$.

6. RETURN U = (gcd(a, b), x, y).

Нәтиже U жолында болады .

Алгоритмдегі div операциясы бүтін бөлу болып табылады

$$a \text{ div } b = [a/b].$$

Мысал 2.12. A = 28, b=19 болсын. Қанағаттандыратын x және y сандарын табыңыз (2.13).

U	*28*	*1*	*0*	
V U	*19*	*0*	*1*	
T V U	*9*	*1*	*−1*	*q = 1*

T V U 1 −2 3 q = 2

T V 0 19 −28 q = 9

Ұсынылған схеманы түсіндірейік. Алдымен U жолына жазылады сандар (28,1,0), ал V жолда сандар (19,0,1) (бұл алғашқы екі жол диаграммада). T жолы есептеледі (схемадағы үшінші жол). Кейін бұл U жолы ретінде тізбектегі екінші жол алынады, ал V-үшінші, және тағы да T жолы есептеледі (төртінші жол схема). Бұл процесс бірінші элемент болғанша жалғасады V жол нөлге тең болмайды. Содан кейін соңғы жол схемада жауап бар. Біздің жағдайда gcd (28, 19) = 1, x = -2, y = 3. Тексеруді аяқтайық: 28 · (-2) + 19 · 3 = 1.

Жалпыланған алгоритмнің бір маңызды қолданылуын қарастырыңыз Евклид. Берілген сандарға c,m арналған көптеген криптографиялық есептерде, d < M санын табу керек, бұл

$$cd \bmod m = 1.$$

Мұндай d сандар болған кезде ғана бар екенін ескеріңіз ,c және m өзара қарапайым.

Анықтама 2.6. (2.14) қанағаттандыратын d саны m модулі бойынша c инверсиясы деп аталады және көбінесе $c^{-1} \bmod m$ деп белгіленеді.

Инверсия үшін бұл белгі өте табиғи, өйткені біз қазір (2.14) түрінде қайта жаза аламыз.

$$cc^{-1} \bmod m = 1.$$

c^{-1}-ға көбейту арқылы есептеу кезінде c-ке модуль m бойынша бөлуге сәйкес келеді. Аналогия бойынша ерікті теріс енгізуге болады m модулін есептеу кезіндегі дәреже:

$$c^{-e} = (c^{e})^{-1} = (c^{-1})^{e} \pmod m.$$

Мысал 2.13. $3 \cdot 4 \bmod 11 = 1$, сондықтан 4 саны 11 модулі бойынша 3 санының инверсиясы болып табылады. $3^{-1} \bmod 11 = 4$ жазуға болады. $5^{-2} \bmod 11$ санын екі жолмен табуға болады:

$$5^{-2} \bmod 11 = (5^2 \bmod 11)^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4,$$

$$5^{-2} \bmod 11 = (5^{-1} \bmod 11)^{2} \bmod 11 = 9^2 \bmod 11 = 4.$$

Екінші әдісті есептеу кезінде біз теңдікті қолдандық

$5^{-1} \bmod 11 = 9$. Шынында да, $5 \cdot 9 \bmod 11 = 45 \bmod 11 = 1$.

Жалпыланған Евклид алгоритмі арқылы инверсияны қалай есептеуге болатынын көрсетейік. Теңдік (2.14) кейбір бүтін K үшін дегенді білдіреді.

$$cd - km = 1. \quad (2.15)$$

C және m өзара қарапайым екенін ескере отырып, біз (2.15) түрінде қайта жазамыз

$$m(-k) + cd = \gcd(m, c), \quad (2.16)$$

онда ол (2.13) толық сәйкес келеді, тек мұнда айнымалылар басқаша белгіленеді. Сондықтан есептеу үшін c^{-1}mod, яғни. Табу d саны, (2.16) теңдеуді шешу үшін жалпыланған Евклид алгоритмін қолдану қажет. Айнымалының мәнін ескеріңіз k бізді қызықтырмайды, сондықтан U , V , T жолдарының екінші элементтерін есептей алмаймыз. Сонымен қатар, егер d саны теріс болып шықса, оған m қосу керек, өйткені анықтамасы бойынша сана mod m {0, 1, жиынынан алынады. . . , m − 1}.

МЫСАЛ 2.14. 7^{-1} мод 11 есептеңіз . Біз де солай қолданамыз 2.12 мысалдағыдай есептеу схемасы:

11	0	
7	1	
4	−1	q = 1
3	2	q = 1
1	−3	q = 1
0	11	q = 3.

Біз d = -3 және D mod 11 = 11 − 3 = 8 аламыз, яғни 7^{-1} мод 11 = 8. Нәтижені тексерейік: 7 * 8 модуль 11 = 56 модуль 11 = 1.

Ашық криптографиядағы маңызды операциялардың бірі кілттер-бұл модуль дәрежесін көтеру операциясы. Идея тиімді құрылыс алгоритмін құру дәрежесі бұрын болған (2.5) және (2.6) көмегімен суреттелген. Қарастырылған алгоритмді бірқатар сандарды жадта сақтамай-ақ жүзеге асыруға болады (2.5). Біз бұл алгоритмнің сипаттамасын тікелей бағдарламалық жасақтаманы іске асыруға жарамды түрде береміз. Алгоритм

атауында көрсетілген көрсеткіш биттері оңнан солға қарай, яғни кішіден үлкенге қарай қаралатындығы.

Алгоритм 2.3. Экспоненциация (оңнан солға қарай)

INPUT: бүтін сандар a, x = (xtxt−1 . . . . . x0)2, p.

ШЫҒЫС: y = a саны

xmodb.

1. y ← 1, s ← a.

2. FOR i = 0, 1, . . . , t DO

3. ЕГЕР x_i = 1 болса, онда y ← y s mod p;

4. s ← s s modp.

5. RETURN y .

Ұсынылған алгоритм бойынша y (2.6) бойынша есептелетінін көрсету үшін айнымалылардың дәрежелерін жазамыз циклдің әр қайталануынан кейін. X = 100 = (1100100)2 болсын 2.1 мысалында, содан кейін:

$i: 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

$x_i: 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1$

$y: 1 \quad 1 \quad a^4 \quad a^4 \; a^4 \quad a^{36} \quad a^{100}$

$s: a^2 \quad a^4 \quad a^8 \; a^{16} \; a^{32} \quad a^{64} \quad a^{128}$

Кейбір жағдайларда келесі алгоритм тиімдірек болады, онда көрсеткіш биттері солдан оңға қарай, яғни үлкеннен кішіге қарай қаралады.

Алгоритм 2.4. Экспоненциация (солдан оңға қарай)

INPUT: бүтін сандар a, x = $(x_t x_{t-1} . . . . . x_0)_2$, p.

ШЫҒЫС: y = a^x саны

x modb.

1. y ← 1.

2. FOR i = t, t − 1, . . . , 0 DO

3. y ← y y mod p;

4. ЕГЕР x_i = 1 болса, онда y ← y a mod p.

5. RETURN y .

Ұсынылған алгоритм бойынша y (2.6) бойынша есептелетінін көрсету үшін айнымалылардың дәрежелерін жазамыз циклдің әр қайталануынан кейін. X = 100 = $(1100100)_2$ болсын 2.1 мысалында, содан кейін:

i:	*6*	*5*	*4*	*3*	*2*	*1*	*0*
x_i *:*	*1*	*1*	*0*	*0*	*1*	*0*	*0*
y:	a	a^3	a^6	a^{12}	a^{25}	a^{50}	a^{100}

Бұл бөлімде сандар теориясынан алынған мәліметтер болады

негізгі криптографиялық алгоритмдерді сипаттау үшін жеткілікті

және әдістері.