8-ДӘРІС.
ҚЫТАЙ ҚАЛДЫҚТАРЫ ТЕОРЕМАСЫ

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Бірнеше модуль бойынша берілген салыстырулар жүйесінің мағынасын түсіну.

Қытай қалдықтары теоремасының шарттары мен тұжырымын меңгеру.

Конструктивті формула арқылы шешім табу алгоритмін қолдану.

Модульдік кері элементті есептеуді қайталау.

Теореманың криптографиядағы рөлін есептік мысалдар арқылы түсіндіру.

Дәрістің құрылымы

1. Модуль бойынша салыстыруды еске түсіру
2. Салыстырулар жүйесі
3. Қытай қалдықтары теоремасының тұжырымы
4. Теореманы қолдану алгоритмі
5. Толық есептік мысалдар
6. Формуланың жұмыс істеу себебі
7. Криптографиядағы қолданылуы

1. Модуль бойынша салыстыру

Егер a және b сандары m-ге бөлгенде бірдей қалдық берсе, олар m модулі бойынша салыстырмалы деп аталады.

$$a \equiv b \pmod{m} \iff m \mid (a-b).$$

Мысал: $17 \equiv 2 \pmod{5}$, себебі $17-2=15$ және 15 саны 5-ке бөлінеді.

Мысал: $29 \equiv 1 \pmod{7}$, себебі $29-1=28$.

Салыстыруды қалай оқимыз?

Жазылуы	Мағынасы	Мысал
$a \equiv b \pmod{m}$	a және b бірдей қалдық береді	$17 \equiv 2 \pmod{5}$
$m \mid (a-b)$	a−b саны m-ге бөлінеді	$5 \mid (17-2)$
$a \bmod m = r$	a-ны m-ге бөлгендегі қалдық r	$17 \bmod 5 = 2$

Өзара жай сандар

a және b сандарының ең үлкен ортақ бөлгіші 1 болса, олар өзара жай сандар деп аталады.

Белгіленуі: $\gcd(a,b)=1$.

Мысал: $\gcd(3,5)=1$; $\gcd(5,7)=1$.

Ал $\gcd(6,9)=3$, сондықтан 6 және 9 өзара жай емес.

Қытай қалдықтары теоремасының классикалық түрінде модульдердің жұп-жұбымен өзара жай болуы маңызды.

Модульдік кері элементті еске түсіру

a санының m модулі бойынша кері элементі a^{-1} — $a \cdot a^{-1} \equiv 1 \pmod{m}$ шартын қанағаттандыратын сан.

Кері элемент gcd(a,m)=1 болғанда бар.

Мысал: $3^{-1} \bmod 5 = 2$, себебі $3 \cdot 2 = 6 \equiv 1 \pmod{5}$.

ҚҚТ алгоритмінде кері элемент N_i мәндерін табу үшін қажет.

2. Салыстырулар жүйесі

Белгісіз x бір уақытта бірнеше модуль бойынша қалдықтарымен берілуі мүмкін.

Мысалы: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$.

Мақсат — екі салыстыруды да бір уақытта қанағаттандыратын x санын табу.

Мұндай есептерді салыстырулар жүйесі деп қарастырамыз.

Қарапайым жүйені алмастыру әдісімен шешу

$x \equiv 2 \pmod 3 \Rightarrow x=3k+2$.

Екінші шартқа қоямыз: $3k+2 \equiv 3 \pmod 5$.

$3k \equiv 1 \pmod 5$.

$3^{-1} \bmod 5 = 2 \Rightarrow k \equiv 2 \pmod 5$.

$k=5t+2 \Rightarrow x=3(5t+2)+2=15t+8$.

Жауабы: $x \equiv 8 \pmod{15}$.

Шешімнің мағынасы

$x \equiv 8 \pmod{15}$ бір ғана $x=8$ санын білдірмейді.

Барлық шешімдер: $x=8+15t$, $t \in Z$.

Мысалы: 8, 23, 38, 53, 68, ...

Олардың әрқайсысы 3-ке бөлгенде 2, 5-ке бөлгенде 3 қалдық береді.

3. Қытай қалдықтары теоремасы

$$x \equiv a_i \pmod{m_i},\ i=1,\ldots,k; \qquad M = \prod m_i$$

Егер $m_1, m_2, \ldots, m_k$ модульдері жұп-жұбымен өзара жай болса, жүйенің M модулі бойынша жалғыз шешімі бар.

«Жұп-жұбымен өзара жай» деген не?

Модульдер жұбы	gcd	Шарт орындала ма?
3 және 5	1	Иә
3 және 7	1	Иә
5 және 7	1	Иә
4 және 6	2	Жоқ

Теореманың негізгі шарты не үшін қажет?

m_i модульдері жұп-жұбымен өзара жай болса, $M_i=M/m_i$ саны мен m_i де өзара жай болады.

Сондықтан M_i санының m_i модулі бойынша кері элементі N_i міндетті түрде бар.

Бұл конструктивті формуланың әр мүшесін қажетті қалдықты «таңдап алатындай» етеді.

Егер модульдер өзара жай болмаса, қосымша үйлесімділік шарттары қажет.

Өзара жай емес модульдер: ескерту

Мысалы, 4 және 6 модульдері өзара жай емес: gcd(4,6)=2.

Сондықтан классикалық ҚҚТ формуласын автоматты түрде қолдануға болмайды.

Жүйенің шешімі болуы да, болмауы да мүмкін.

Бұл дәрісте жұп-жұбымен өзара жай модульдерге арналған классикалық жағдай қарастырылады.

4. ҚҚТ бойынша шешу алгоритмі

$$M \rightarrow M_i \rightarrow N_i \rightarrow \Sigma(a_i M_i N_i) \rightarrow \text{mod } M \rightarrow \text{тексеру}$$

Есепті осы ретпен орындау қателерді азайтады.

Алгоритмнің қысқаша кестесі

Қадам	Орындалатын әрекет	Формула
1	Жалпы модульді табу	$M=m_1m_2\ldots m_k$
2	Жеке көбейткіштерді табу	$M_i=M/m_i$
3	Кері элементті табу	$M_iN_i\equiv1 \pmod{m_i}$
4	Жалпы қосынды	$x\equiv\Sigma a_iM_iN_i \pmod{M}$
5	Тексеру	$x \bmod m_i=a_i$

Белгілеулерді түсіну

Белгі	Мағынасы	Мысал
m_i	Жеке модуль	3,5,7
a_i	Қажетті қалдық	2,3,2
M	Барлық модуль көбейтіндісі	105
M_i	M/m_i	35,21,15
N_i	M_i-дің m_i бойынша кері элементі	2,1,1

1-қадам: жалпы M модулін табу

Барлық модульдерді көбейтеміз:

$$M=m_1m_2\ldots m_k.$$

Мысалы, $m_1=3$, $m_2=5$, $m_3=7$ болса:

$M=3\cdot5\cdot7=105$.

Соңғы шешім M модулі бойынша жазылады.

2-қадам: M_i мәндерін табу

Әрбір модуль үшін сол модульді жалпы көбейтіндіден алып тастаймыз:

$$M_i = M/m_i.$$

M=105 болса: $M_1=105/3=35$; $M_2=105/5=21$; $M_3=105/7=15$.

M_i басқа барлық модульдерді көбейткіш ретінде қамтиды.

3-қадам: N_i кері элементтерін табу

N_i мына шарттан табылады: $M_iN_i \equiv 1 \pmod{m_i}$.

Мысал: $35N_1 \equiv 1 \pmod 3$.

$35 \equiv 2 \pmod 3 \Rightarrow 2N_1 \equiv 1 \pmod 3$.

$N_1=2$, себебі $2 \cdot 2=4 \equiv 1 \pmod 3$.

Шағын есептерде тікелей тексеруге, үлкендерде кеңейтілген Евклид алгоритмін қолдануға болады.

4-қадам: конструктивті формула

$$x \equiv \Sigma(a_i M_i N_i) \pmod{M}$$

Әрбір $a_i M_i N_i$ мүшесі бір модуль бойынша қажетті қалдықты, қалғандары бойынша 0 қалдығын береді.

5-қадам: mod M бойынша қысқарту және тексеру

Алынған үлкен қосындыны M модулі бойынша қысқартамыз.

Содан кейін $x \bmod m_i = a_i$ шарттарының әрқайсысын тексереміз.

Тексеру есептеудегі кері элемент немесе арифметикалық қатені анықтауға көмектеседі.

Сондықтан тексеру — алгоритмнің міндетті бөлігі.

5. Толық мысал №1

Жүйе:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

3, 5 және 7 жұп-жұбымен өзара жай → ҚҚТ қолдануға болады.

Мысал №1: M және M_i

i	m_i	a_i	M=105	$M_i=M/m_i$
1	3	2	105	35
2	5	3	105	21
3	7	2	105	15

Мысал №1: N_i кері элементтері

i	Шарт	Қысқарту	N_i
1	$35N_1 \equiv 1 \pmod 3$	$2N_1 \equiv 1 \pmod 3$	2
2	$21N_2 \equiv 1 \pmod 5$	$N_2 \equiv 1 \pmod 5$	1
3	$15N_3 \equiv 1 \pmod 7$	$N_3 \equiv 1 \pmod 7$	1

Мысал №1: жалпы формула

$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$

$x \equiv 140 + 63 + 30$

$x \equiv 233 \pmod{105}$

$233 = 105 \cdot 2 + 23$

Жауабы: $x \equiv 23 \pmod{105}$.

Мысал №1: нәтижені тексеру

Тексеру	Есептеу	Нәтиже
mod 3	23 mod 3	2 ✓
mod 5	23 mod 5	3 ✓
mod 7	23 mod 7	2 ✓
Барлық шешім	$x=23+105t$	$t \in Z$

Толық мысал №2

Жүйе:

$x \equiv 1 \pmod 4$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

$M=4\cdot5\cdot7=140.$

$M_1=35,\ M_2=28,\ M_3=20.$

Мысал №2: кері элементтер

$35 \equiv 3 \pmod 4 \Rightarrow 3N_1 \equiv 1 \pmod 4 \Rightarrow N_1=3.$

$28 \equiv 3 \pmod 5 \Rightarrow 3N_2 \equiv 1 \pmod 5 \Rightarrow N_2=2.$

$20 \equiv 6 \pmod 7 \Rightarrow 6N_3 \equiv 1 \pmod 7 \Rightarrow N_3=6.$

Сондықтан $N_1=3$, $N_2=2$, $N_3=6$.

Мысал №2: шешім

$x \equiv 1 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 2 + 3 \cdot 20 \cdot 6 \pmod{140}$

$x \equiv 105 + 112 + 360 = 577 \pmod{140}$

$577 = 140 \cdot 4 + 17$

Жауабы: $x \equiv 17 \pmod{140}$.

Тексеру: 17 mod 4=1; 17 mod 5=2; 17 mod 7=3.

6. Неліктен формула жұмыс істейді?

$M_i = M/m_i$ саны m_i-ден басқа барлық модульдерді қамтиды.

Сондықтан $j \neq i$ болса, $M_i \equiv 0 \pmod{m_j}$.

N_i кері элемент болғандықтан, $M_i N_i \equiv 1 \pmod{m_i}$.

Осылай $a_i M_i N_i$ өз модулі бойынша a_i, ал қалған модульдер бойынша 0 береді.

Барлық мүшелер қосылғанда қажетті қалдықтар жеке-жеке қалпына келеді.

Формуланың логикасын кестемен көрсету

Мүше	mod m_1	mod m_2	mod m_3
$a_1M_1N_1$	a_1	0	0
$a_2M_2N_2$	0	a_2	0
$a_3M_3N_3$	0	0	a_3
Қосынды	a_1	a_2	a_3

ҚҚТ және модульдік кері элемент

ҚҚТ қадамы	Кері элементтің рөлі
$M_i = M/m_i$	M_i мен m_i өзара жай
$M_i N_i \equiv 1 \pmod{m_i}$	N_i қажетті қалдықты қалыптастырады
N_i табу	Тікелей тексеру немесе кеңейтілген Евклид алгоритмі
Нәтиже	Әр мүше өз модулі бойынша «1», қалғандары бойынша «0» сияқты жұмыс істейді

7. Криптографиядағы қолданылуы

- ✓ Үлкен модуль бойынша есептеуді бірнеше кіші модуль бойынша есептеулерге жіктеуге мүмкіндік береді.
- ✓ Қалдықтар жүйесі арқылы үлкен бүтін санды бірмәнді сипаттауға болады.
- ✓ Ашық кілтті криптографиядағы кейбір есептеулерді ұйымдастыруда қолданылады.
- ✓ RSA жүйесінде есептеулерді p және q модульдері бойынша бөлек орындау идеясымен байланысты.

RSA-дағы ҚҚТ идеясы

RSA-да $n=pq$, мұндағы p және q — үлкен жай сандар.

n модулі бойынша кейбір есептеулерді p және q модульдері бойынша бөлек есептеуге болады.

Содан кейін екі нәтиже Қытай қалдықтары теоремасы арқылы біріктіріледі.

Бұл тәсіл үлкен сандармен есептеуді тиімді ұйымдастыруға мүмкіндік береді.

Бұл слайд математикалық идеяны түсіндіреді; нақты қауіпсіз RSA параметрлері әлдеқайда үлкен.

ҚҚТ қолданудың артықшылықтары

Артықшылық	Түсіндіру
Декомпозиция	Үлкен есепті бірнеше кіші модульге бөлу
Бірмәнді қалпына келтіру	Қалдықтар жиыны M модулі бойынша бір класқа сәйкес келеді
Параллель есептеу идеясы	Кіші модульдер бойынша есептеулерді бөлек орындауға болады
Криптография	RSA сияқты жүйелердегі модульдік есептеулермен байланысты

Жиі жіберілетін қателер

1. Модульдердің жұп-жұбымен өзара жай екенін тексермеу.

2. $M_i = M/m_i$ орнына қате көбейтінді алу.

3. N_i кері элементін қате есептеу.

4. Соңғы қосындыны M модулі бойынша қысқартпау.

5. Алынған шешімді бастапқы салыстыруларға қойып тексермеу.

Есте сақтау реті: шарт → M → M_i → N_i → формула → mod M → тексеру.

ҚҚТ есептерін шешудің қысқа жадынамасы

1) gcd → 2) M → 3) M_i → 4) N_i → 5) Σ → 6) mod M → 7) тексеру

Алдымен шартты тексеріңіз; соңында әр бастапқы салыстыруды міндетті түрде тексеріңіз.

Қорытынды

Қытай қалдықтары теоремасы бірнеше модуль бойынша берілген қалдықтардан ортақ шешімді қалпына келтіреді.

Классикалық шарт: модульдер жұп-жұбымен өзара жай.

Жалпы шешім $M=m_1m_2…m_k$ модулі бойынша бірмәнді.

Конструктивті шешім M_i және N_i мәндері арқылы есептеледі.

Нәтижені бастапқы салыстырулармен міндетті түрде тексеру қажет.

Теорема криптографиялық есептеулерді ұйымдастыруда маңызды математикалық құрал.

Бақылау сұрақтары

1. Салыстырулар жүйесі дегеніміз не?
2. ҚҚТ-ның негізгі шарты қандай?
3. «M модулі бойынша жалғыз шешім» нені білдіреді?
4. M және M_i қалай есептеледі?
5. N_i қандай шартты қанағаттандырады?
6. Конструктивті формула қалай жазылады?
7. Кері элементті қандай алгоритммен табуға болады?
8. Шешімді қалай тексереміз?
9. Модульдер өзара жай болмаса не өзгереді?
10. ҚҚТ криптографияда не үшін маңызды?

Өзіндік тексеруге арналған есептер

1) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$ жүйесін шешіңіз.

2) $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$ жүйесін шешіңіз.

3) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 5$ жүйесін ҚҚТ арқылы шешіңіз.

4) 11 санының 7 модулі бойынша кері элементін табыңыз.

5) 6 және 9 модульдеріне классикалық ҚҚТ-ны неге тікелей қолдануға болмайтынын түсіндіріңіз.

Список источников

1. Ахметов Б.С. және т.б. Қолданбалы криптология: шифрлау әдістері. Алматы: ҚазҰТЗУ, 2016.

2. Ахметов Б.С. және т.б. Криптография негіздері. Алматы: АЭжБУ, 2020.

3. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024.

4. Рацеев С.М. Математические методы защиты информации и их основы. Сборник задач. Москва: Лань, 2023.