8-ДӘРІС
ҚЫТАЙ ҚАЛДЫҚТАРЫ ТЕОРЕМАСЫ

Дәрістің мақсаты

Бірнеше модуль бойынша берілген салыстырулар жүйесін шешудің математикалық негізін түсіндіру, Қытай қалдықтары теоремасының шарттары мен тұжырымын қарастыру, жүйенің шешімін конструктивті формула арқылы табу алгоритмін меңгерту, модульдік кері элементтерді есептеуді қайталау және теореманың криптографиядағы қолданылуын есептік мысалдар арқылы көрсету.

Негізгі ұғымдар

Қытай қалдықтары теоремасын түсіну үшін модуль бойынша салыстыру, өзара жай сандар және модульдік кері элемент ұғымдары қажет. a және b сандары m модулі бойынша бірдей қалдық берсе, олар m модулі бойынша салыстырмалы деп аталады:

$$a \equiv b \pmod{m}.$$

Бұл жазу $a-b$ айырмасының m санына қалдықсыз бөлінетінін білдіреді. Мысалы, $17 \equiv 2 \pmod 5$, себебі $17-2=15$ және 15 саны 5-ке бөлінеді.

Салыстырулар жүйесі

Кейбір есептерде белгісіз x саны бір ғана модуль бойынша емес, бірнеше модуль бойынша қалдықтарымен беріледі. Мысалы, x саны 3-ке бөлінгенде 2, ал 5-ке бөлінгенде 3 қалдық берсін:

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5.$$

Мұндай жүйенің мақсаты – барлық салыстыруларды бір уақытта қанағаттандыратын x мәнін табу. Бірінші салыстырудан $x=3k+2$ түрінде жазуға болады. Осы өрнекті екінші салыстыруға қоямыз:

$$3k + 2 \equiv 3 \pmod 5,$$
$$3k \equiv 1 \pmod 5.$$

3 санының 5 модулі бойынша кері элементі 2-ге тең, себебі $3\cdot 2=6 \equiv 1 \pmod 5$. Сондықтан:

$$k \equiv 2 \pmod 5.$$

Демек, $k=5t+2$. Оны $x=3k+2$ өрнегіне қойсақ:

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

Сондықтан жүйенің шешімі:

$$x \equiv 8 \pmod{15}.$$

Шынында да, 8 санын 3-ке бөлгенде қалдық 2, ал 5-ке бөлгенде қалдық 3 болады. Осы мысал бірнеше салыстыруды бір уақытта қанағаттандыратын санды табу идеясын көрсетеді.

Қытай қалдықтары теоремасының тұжырымы

$m_1, m_2, \ldots, m_k$ модульдері жұп-жұбымен өзара жай болсын, яғни кез келген $i \neq j$ үшін $\gcd(m_i,m_j)=1$. Онда келесі салыстырулар жүйесінің $M=m_1m_2\ldots m_k$ модулі бойынша жалғыз шешімі бар:

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

Теоремадағы «M модулі бойынша жалғыз шешім» дегеніміз x-тің тек бір ғана бүтін мәні бар деген сөз емес. Егер x_0 бір шешім болса, онда $x=x_0+tM$, мұндағы t – кез келген бүтін сан, түріндегі барлық сандар да шешім болады. Бірақ олардың барлығы M модулі бойынша бір қалдықтар класына жатады.

Мысалы, жоғарыдағы жүйеде $M=3\cdot5=15$ және $x \equiv 8 \pmod{15}$. Сондықтан 8, 23, 38, 53, … сандарының барлығы жүйені қанағаттандырады.

Теореманың негізгі шарты

Қытай қалдықтары теоремасының классикалық түріндегі маңызды шарт – модульдердің жұп-жұбымен өзара жай болуы. Мысалы, 3, 5 және 7 модульдері жұп-жұбымен өзара жай, себебі олардың кез келген екеуінің ең үлкен ортақ бөлгіші 1-ге тең.

$$\gcd(3,5)=1, \qquad \gcd(3,7)=1, \qquad \gcd(5,7)=1.$$

Осы шарт M_i санының m_i модулі бойынша кері элементінің бар болуын қамтамасыз етеді. Егер модульдер өзара жай болмаса, жүйе үшін қосымша үйлесімділік шарттарын тексеру қажет; сондықтан бұл дәрісте теореманың жұп-жұбымен өзара жай модульдерге арналған классикалық жағдайы қарастырылады.

Қытай қалдықтары теоремасы бойынша шешу алгоритмі

Салыстырулар жүйесі $x \equiv a_i \pmod{m_i}$, $i=1,\ldots,k$ түрінде берілсін. Жүйені конструктивті түрде шешу бірнеше кезеңнен тұрады.

Бірінші кезеңде барлық модульдердің көбейтіндісі есептеледі:

$$M = m_1 m_2 \ldots m_k.$$

Екінші кезеңде әрбір m_i үшін қалған модульдердің көбейтіндісіне тең M_i саны табылады:

$$M_i = M / m_i.$$

Үшінші кезеңде M_i санының m_i модулі бойынша кері элементі N_i анықталады:

$$M_i N_i \equiv 1 \pmod{m_i}.$$

N_i мәнін кеңейтілген Евклид алгоритмі арқылы немесе шағын оқу есептерінде тікелей тексеру арқылы табуға болады.

Төртінші кезеңде барлық алынған мәндер жалпы формулаға қойылады:

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

Соңында алынған сан M модулі бойынша қысқартылады және нәтиже бастапқы салыстыруларға қою арқылы тексеріледі.

Алгоритмнің қысқаша кестесі

Қадам	Орындалатын әрекет	Формула
1	Жалпы модульді табу	$M=m_1 m_2 \ldots m_k$
2	Әрбір жеке көбейткішті табу	$M_i=M/m_i$
3	Кері элементті табу	$M_i N_i \equiv 1 \pmod{m_i}$
4	Жалпы қосындыны есептеу	$x \equiv \Sigma a_i M_i N_i \pmod{M}$
5	Нәтижені тексеру	$x \bmod m_i = a_i$

Толық есептік мысал

Келесі салыстырулар жүйесін шешейік:

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}.$$

3, 5 және 7 модульдері жұп-жұбымен өзара жай. Сондықтан Қытай қалдықтары теоремасын қолдануға болады. Алдымен жалпы модульді есептейміз:

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

Енді M_1, M_2 және M_3 мәндерін табамыз:

$$M_1 = 105/3 = 35, \qquad M_2 = 105/5 = 21, \qquad M_3 = 105/7 = 15.$$

Келесі қадамда әрбір M_i санының сәйкес m_i модулі бойынша кері элементін табамыз.

Бірінші жағдайда $35N_1 \equiv 1 \pmod 3$. $35 \equiv 2 \pmod 3$, сондықтан $2N_1 \equiv 1 \pmod 3$. $N_1=2$, себебі $2\cdot2=4 \equiv 1 \pmod 3$.

$$N_1 = 2.$$

Екінші жағдайда $21N_2 \equiv 1 \pmod 5$. $21 \equiv 1 \pmod 5$, сондықтан $N_2=1$.

$$N_2 = 1.$$

Үшінші жағдайда $15N_3 \equiv 1 \pmod 7$. $15 \equiv 1 \pmod 7$, сондықтан $N_3=1$.

$$N_3 = 1.$$

Барлық мәндерді жалпы формулаға қоямыз:

$$x \equiv 2\cdot35\cdot2 + 3\cdot21\cdot1 + 2\cdot15\cdot1 \pmod{105}.$$

$$x \equiv 140 + 63 + 30 = 233 \pmod{105}.$$

233 санын 105-ке бөлгендегі қалдық 23:

$$233 = 105\cdot2 + 23.$$

Демек:

$$x \equiv 23 \pmod{105}.$$

Нәтижені міндетті түрде тексереміз:

$$23 \bmod 3 = 2, \qquad 23 \bmod 5 = 3, \qquad 23 \bmod 7 = 2.$$

Барлық үш салыстыру орындалады. Сондықтан $x=23$ – ең кіші теріс емес шешім, ал барлық бүтін шешімдер $x=23+105t$, $t \in Z$ түрінде жазылады.

Екінші мысал

Келесі жүйені қарастырайық:

$$x \equiv 1 \pmod 4, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 3 \pmod 7.$$

4, 5 және 7 жұп-жұбымен өзара жай. Жалпы модуль $M=4\cdot5\cdot7=140$. Жеке көбейткіштер:

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

Кері элементтер: $35 \equiv 3 \pmod 4$, сондықтан $3N_1 \equiv 1 \pmod 4$ және $N_1=3$; $28 \equiv 3 \pmod 5$, сондықтан $N_2=2$; $20 \equiv 6 \pmod 7$, сондықтан $N_3=6$.

$$N_1=3, \qquad N_2=2, \qquad N_3=6.$$

Жалпы формула бойынша:

$$x \equiv 1\cdot35\cdot3 + 2\cdot28\cdot2 + 3\cdot20\cdot6 \pmod{140}$$

$$x \equiv 105 + 112 + 360 = 577 \equiv 17 \pmod{140}.$$

Тексеру: $17 \bmod 4=1$, $17 \bmod 5=2$, $17 \bmod 7=3$. Сондықтан жүйенің шешімі $x \equiv 17 \pmod{140}$.

Неліктен формула жұмыс істейді?

$M_i=M/m_i$ саны m_i-ден басқа барлық модульдерді көбейткіш ретінде қамтиды. Сондықтан $j \neq i$ болғанда $M_i \equiv 0 \pmod{m_j}$. Ал N_i кері элемент ретінде таңдалғандықтан $M_iN_i \equiv 1 \pmod{m_i}$. Демек, $a_iM_iN_i$ мүшесі өз модулі бойынша a_i қалдығын береді, ал қалған модульдер бойынша нөлге тең болады. Барлық осындай мүшелерді қосқанда әр салыстыру үшін қажетті қалдық жеке-жеке қалпына келеді.

Модульдік кері элементпен байланысы

Қытай қалдықтары теоремасының есептеу алгоритмінде модульдік кері элемент негізгі рөл атқарады. M_i және m_i өзара жай болғандықтан, M_i санының m_i модулі бойынша кері элементі міндетті түрде бар. Бұл 6-дәрісте қарастырылған кеңейтілген Евклид алгоритмінің осы тақырыппен тікелей байланысын көрсетеді.

Криптографиядағы қолданылуы

Қытай қалдықтары теоремасы үлкен модуль бойынша орындалатын кейбір есептеулерді бірнеше кіші модуль бойынша есептеулерге жіктеуге мүмкіндік береді. Бұл қасиет сандық алгоритмдерді ұйымдастыруда және ашық кілтті криптографияның математикалық есептеулерін түсіндіруде маңызды. Кейінгі дәрістерде қарастырылатын RSA жүйесінде де Қытай қалдықтары теоремасының идеясы есептеулерді жеке модульдер бойынша қарастыруға мүмкіндік беретін математикалық құрал ретінде кездеседі.

Сонымен қатар теорема қалдықтар жүйесі арқылы үлкен бүтін санды бірмәнді сипаттауға мүмкіндік береді. Егер модульдер жұп-жұбымен өзара жай болса, M аралығындағы әрбір қалдықтар комбинациясы M модулі бойынша бір ғана класқа сәйкес келеді.

Жиі жіберілетін қателер

Бірінші қате – модульдердің жұп-жұбымен өзара жай екенін тексермеу. Екінші қате – $M_i=M/m_i$ орнына басқа көбейтіндіні пайдалану. Үшінші қате – N_i кері элементін қате есептеу. Төртінші қате – соңғы қосындыны M модулі бойынша қысқартпау. Бесінші қате – алынған шешімді бастапқы салыстыруларға қойып тексермеу.

Сондықтан есепті орындағанда «модульдерді тексеру → M → M_i → N_i → жалпы формула → mod M → тексеру» ретін сақтау ұсынылады.

Қорытынды

Қытай қалдықтары теоремасы бірнеше модуль бойынша берілген қалдықтардан бір ортақ шешімді қалпына келтіруге мүмкіндік береді. Егер модульдер жұп-жұбымен өзара жай болса, салыстырулар жүйесінің олардың көбейтіндісі M модулі бойынша жалғыз шешімі бар. Шешімді табу үшін жалпы M модулі, M_i жеке көбейткіштері және олардың m_i модулі бойынша N_i кері элементтері есептеледі. Нәтиже $x \equiv \Sigma(a_iM_iN_i) \pmod M$ формуласы арқылы алынады және бастапқы салыстырулармен міндетті түрде тексеріледі.

Бақылау сұрақтары

1. Салыстырулар жүйесі дегеніміз не?
2. Қытай қалдықтары теоремасының негізгі шарты қандай?
3. «M модулі бойынша жалғыз шешім» дегенді қалай түсіндіруге болады?
4. Жалпы M модулі қалай есептеледі?
5. M_i мәні қалай анықталады?
6. N_i кері элементі қандай шартты қанағаттандырады?
7. Қытай қалдықтары теоремасының конструктивті формуласы қалай жазылады?
8. Модульдік кері элементті қандай алгоритм арқылы табуға болады?
9. Алынған шешімді қалай тексеруге болады?
10. Қытай қалдықтары теоремасының криптографиядағы маңызы неде?

Список источников

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016. – 500 б.
2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері: сандар теориясының, топтардың, өрістердің, сақиналардың элементтері. Алматы: АЭжБУ, 2020.
3. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024. – 474 с.
4. Рацеев С.М. Математические методы защиты информации и их основы. Сборник задач. Москва: Лань, 2023. – 140 с.