6-ДӘРІС

МАТЕМАТИКАЛЫҚ НЕГІЗДЕР:

МОДУЛЬДІК АРИФМЕТИКА. ЕВКЛИД ЖӘНЕ КЕҢЕЙТІЛГЕН ЕВКЛИД АЛГОРИТМДЕРІ

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Бүтін сандар арифметикасының криптографияда қолданылатын негізгі ұғымдарын түсіну.

Бөлінгіштік, қалдықпен бөлу және модуль бойынша салыстыруды меңгеру.

Модульдік қосу, азайту және көбейтуді есептеу.

ЕҮОБ және өзара жай сандар ұғымдарын қолдану.

Евклид алгоритмімен ЕҮОБ табу.

Кеңейтілген Евклид алгоритмімен Безу коэффициенттері мен модульдік кері элементті табу.

Бүтін сандар және бөлінгіштік

$$a = bq + r, \quad 0 \le r < |b|$$

Егер a саны b санына қалдықсыз бөлінсе, b саны a санының бөлгіші деп аталады: b | a.

Егер қалдықсыз бөлінбесе, қалдықпен бөлу формуласы қолданылады.

q – бөлінді, r – қалдық; қалдық әрқашан $0 \le r < |b|$ шартын қанағаттандырады.

Қалдықпен бөлу модульдік арифметиканың негізін құрайды.

Мысал 1. Қалдықпен бөлу

a	b	q	r	Тексеру
29	7	4	1	$29=7\cdot4+1$
53	10	5	3	$53=10\cdot5+3$
100	12	8	4	$100=12\cdot8+4$

Қалдық r – санның mod b бойынша мәні.

Модуль бойынша салыстыру

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a-b)$$

Екі бүтін сан m-ге бөлгенде бірдей қалдық берсе, олар m модулі бойынша салыстырмалы.

$a \equiv b \pmod{m}$ жазуы $a-b$ айырмасының m санына бөлінетінін білдіреді.

Бір қалдықтар класына шексіз көп бүтін сан кіреді.

Мысал 2. Модуль бойынша салыстыру

$$17 \equiv 5 \pmod{12}$$

$17 - 5 = 12$, ал 12 саны 12-ге бөлінеді.

$$29 \equiv 5 \pmod{12}$$

$29 - 5 = 24 = 12 \cdot 2$

Сондықтан 5, 17, 29, 41, ... бір қалдықтар класына жатады.

Қалдықтар кластары

$$\mathbb{Z}_m = \{0,1,\ldots,m-1\}$$

m модулі бойынша кез келген бүтін сан $0,1,\ldots,m-1$ қалдықтарының біріне сәйкес келеді.

mod 7 үшін мүмкін қалдықтар: $\{0,1,2,3,4,5,6\}$.

$15 \bmod 7 = 1$, өйткені $15=7\cdot2+1$.

$23 \bmod 7 = 2$, өйткені $23=7\cdot3+2$.

Модульдік қосу және азайту

$$(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$$

Аралық нәтижені бірден модуль бойынша қысқартуға болады.

$(17+19) \bmod 7 = 36 \bmod 7 = 1$.

Бөлек қысқартсақ: $17 \bmod 7=3$, $19 \bmod 7=5$; $(3+5) \bmod 7=1$.

Азайтуда теріс нәтиже шықса, оған модульді қосып оң қалдыққа келтіруге болады: $-3 \bmod 7 = 4$.

Модульдік көбейту

$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

Көбейту кезінде де көбейткіштерді алдын ала модуль бойынша қысқартуға болады.

$(13 \cdot 11) \bmod 7 = 143 \bmod 7 = 3$.

$13 \bmod 7 = 6$ және $11 \bmod 7 = 4$; $6 \cdot 4 = 24$; $24 \bmod 7 = 3$.

Бұл қасиет үлкен сандармен есептеуді жеңілдетеді.

Мысал 3. Модульдік амалдар

Өрнек	Қарапайым есептеу	Нәтиже
$(25+18) \bmod 7$	$43 \bmod 7$	1
$(25-18) \bmod 7$	$7 \bmod 7$	0
$(13 \cdot 11) \bmod 7$	$143 \bmod 7$	3
$(8-15) \bmod 7$	$-7 \bmod 7$	0

Ең үлкен ортақ бөлгіш (ЕҮОБ)

gcd(a,b)=1 ⇒ a және b өзара жай

ЕҮОБ(a,b) – a және b сандарын қалдықсыз бөлетін ең үлкен оң бүтін сан.

Мысалы, 18 және 24 сандарының ортақ бөлгіштері: 1,2,3,6. Сондықтан gcd(18,24)=6.

Егер gcd(a,b)=1 болса, a және b өзара жай сандар деп аталады.

Өзара жайлық модульдік кері элементтің бар-жоғын анықтауда маңызды.

Евклид алгоритмінің идеясы

$$\gcd(a,b) = \gcd(b,r), \quad r = a \bmod b$$

Евклид алгоритмі ЕҮОБ-ты қайталанатын қалдықпен бөлу арқылы табады.

Негізгі қасиет: **gcd(a,b)=gcd(b, a mod b).**

Әр қадамда алдыңғы бөлгіш пен қалдық жаңа жұпқа айналады.

Қалдық нөлге тең болғанда процесс тоқтайды; соңғы нөлден өзге қалдық – ЕҮОБ.

Мысал 4. gcd(252,105)

$$252 = 105 \cdot 2 + 42$$

$$105 = 42 \cdot 2 + 21$$

$$42 = 21 \cdot 2 + 0$$

Соңғы нөлден өзге қалдық: 21

$$\gcd(252,105) = 21$$

Мысал 5. Өзара жай сандарды тексеру

$$35 = 12 \cdot 2 + 11$$

$$12 = 11 \cdot 1 + 1$$

$$11 = 1 \cdot 11 + 0$$

$$\gcd(35,12)=1$$

Демек, 35 пен 12 – өзара жай сандар.

Безу теңдігі

$$ax + by = d = gcd(a,b)$$

Егер d=gcd(a,b) болса, d санын a және b сандарының бүтін коэффициенттері бар сызықтық комбинациясы түрінде жазуға болады.

x және y – Безу коэффициенттері.

Кеңейтілген Евклид алгоритмі ЕҮОБ-пен бірге осы коэффициенттерді де табады.

Кеңейтілген Евклид алгоритмі: 35 және 12

Евклид алгоритмі:

$$35 = 12\cdot 2 + 11$$

$$12 = 11\cdot 1 + 1$$

Осыдан:

$$1 = 12 - 11$$

$$11 = 35 - 12\cdot 2$$

11-дің орнына қоямыз:

$$1 = 12 - (35 - 12\cdot 2)$$

$$1 = 12 - 35 + 12\cdot 2$$

$$1 = 3\cdot 12 - 35$$

Соңғы сандар қайдан шықты?

$$1 = 3\cdot 12 - 35$$

−35 санын көбейтінді түрінде жазамыз:

$$-35 = 35\cdot(-1)$$

Сондықтан:

$$1 = 35\cdot(-1) + 12\cdot 3$$

35x + 12y = 1 формуласымен салыстырамыз.

$$35\cdot x + 12\cdot y = 1$$

$$x = -1, \quad y = 3$$

Яғни −1 — 35-тің коэффициенті,
3 — 12-нің коэффициенті

Тексеру: $35\cdot(-1)+12\cdot 3=-35+36=1$

Модульдік кері элемент

Анықтама

a санының m модулі бойынша кері элементі a^{-1} деп белгіленеді және:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Кері элементтің бар болу шарты:

$$\gcd(a,m) = 1$$

яғни a мен m өзара жай болуы керек.

Есте сақтау:

a^{-1} — $1/a$ емес. Ол a-ға көбейткенде mod m бойынша 1 қалдығын беретін сан.

Мысал: $3^{-1} \bmod 7$ табайық

3-ті қандай санға көбейткенде 7-ге бөлгендегі қалдық 1 болады?

$$3 \cdot 5 = 15$$

$$15 = 7 \cdot 2 + 1$$

$$15 \equiv 1 \pmod{7}$$

Сондықтан:

$$3^{-1} \equiv 5 \pmod{7}$$

Тексеру: $3 \cdot 5 = 15 \equiv 1 \pmod{7}$

Шағын сандарда — таңдау арқылы; үлкен сандарда — кеңейтілген Евклид алгоритмі арқылы табылады.

Мысал 6. 5^{-1} mod 26 табу

$$26 = 5 \cdot 5 + 1$$

$$1 = 26 - 5 \cdot 5$$

$$-5 \equiv 21 \pmod{26}$$

$$5 \cdot 21 = 105 \equiv 1 \pmod{26}$$

Сондықтан $5^{-1} \equiv 21 \pmod{26}$

Мысал 7. Кері элемент бар ма?

a	m	gcd(a,m)	Кері элемент
5	26	1	Бар: 21
7	26	1	Бар
2	26	2	Жоқ
13	26	13	Жоқ

Шарт біреу: gcd(a,m)=1.

Аффиндік шифр және модульдік кері элемент

1. Шифрлау

Аффиндік шифрда әріптің сандық мәні x мына формуламен шифрланады:

$$E(x) = (ax + b) \bmod m$$

x – ашық мәтін символы; a, b – кілттер; m – әліпби өлшемі.

Мысал: m=26, a=5, b=8, x=7

$$E(7) = (5 \cdot 7 + 8) \bmod 26$$

$$= 43 \bmod 26 = 17$$

Демек: x=7 → y=17

2. Дешифрлау

Кері ашу үшін a-ға бөлмейміз. Оның модульдік кері элементін a^{-1} қолданамыз:

$$D(y) = a^{-1}(y - b) \bmod m$$

a=5 үшін: $5^{-1} \equiv 21 \pmod{26}$

себебі $5 \cdot 21 = 105 = 26 \cdot 4 + 1$

$$D(17) = 21(17 - 8) \bmod 26$$

$$= 189 \bmod 26 = 7$$

7 → 17 → 7

Шарт: gcd(a,m)=1. a=5 жарайды; a=2 жарамайды, өйткені gcd(2,26)=2.

Мысал 8. Аффиндік шифрдағы бір символ

m=26, a=5, b=8, A=0,…,Z=25

C → x=2

E(2)=(5·2+8) mod 26 = 18 → S

$a^{-1}=21$

D(18)=21·(18−8) mod 26 = 210 mod 26 = 2 → C

Кері элемент бастапқы символды қалпына келтіруге мүмкіндік береді.

Криптографиядағы маңызы

- ✓ Модульдік арифметика классикалық шифрлардан ашық кілтті криптографияға дейін қолданылады.
- ✓ Евклид алгоритмі сандардың өзара жайлығын жылдам тексереді.
- ✓ Кеңейтілген Евклид алгоритмі Безу коэффициенттері мен кері элементтерді есептейді.
- ✓ Бұл аппарат Эйлер және Ферма теоремаларын түсінуге негіз болады.
- ✓ Кейін асимметриялық алгоритмдердің математикалық есептерінде осы ұғымдар қайта қолданылады.

СІЗ БІЛЕСІЗ БЕ?

Евклид алгоритмі: ежелгі математикадан қазіргі криптографияға дейін

1

2300 жылдан астам тарихы бар

Евклид алгоритмі шамамен б.з.д. 300 жылдары Евклидтің «Бастамалар» еңбегінде сипатталған. Ол адамзатқа белгілі ең көне алгоритмдердің бірі.

2

ЕҮОБ-ты өте тиімді табады

Негізгі идея: үлкен санды кіші санға бөліп, есептеуді бөлгіш пен қалдық арқылы қайталау. Соңғы нөлден өзгеше қалдық — ЕҮОБ.

3

Кеңейтілген Евклид көбірек ақпарат береді

Ол тек gcd(a,b)-ті емес, ax + by = gcd(a,b) теңдігін қанағаттандыратын x және y коэффициенттерін де табады.

4

Модульдік кері элементті табуға мүмкіндік береді

Егер gcd(a,m)=1 болса, кеңейтілген Евклид алгоритмі $a^{-1} \bmod m$ мәнін есептеуге қолданылады.

5

RSA-мен тікелей байланысты

RSA-да жабық көрсеткіш d: $ed \equiv 1 \pmod{\varphi(n)}$ шартымен анықталады. Яғни d — e санының $\varphi(n)$ модулі бойынша кері элементі.

Евклид → ЕҮОБ → кеңейтілген Евклид → кері элемент → RSA

Сабақта орындауға арналған есептер

1. 73 mod 9 және 125 mod 11 мәндерін табыңыз.

2. 38 ≡ ? (mod 7) үшін ең кіші теріс емес қалдықты жазыңыз.

3. (45+29) mod 8 және (17·23) mod 9 есептеңіз.

4. Евклид алгоритмімен gcd(414,662) табыңыз.

5. 55 және 34 сандарының өзара жай екенін тексеріңіз.

6. Кеңейтілген Евклид алгоритмімен 7^{-1} mod 26 табыңыз.

7. Неліктен 6 санының mod 26 бойынша кері элементі жоқ екенін түсіндіріңіз.

1. $73 \bmod 9$

$$73 = 9 \times 8 + 1$$

Қалдық **1**, сондықтан:

$$\boxed{73 \bmod 9 = 1}$$

2. $125 \bmod 11$

$$125 = 11 \times 11 + 4$$

Қалдық **4**, сондықтан:

$$\boxed{125 \bmod 11 = 4}$$

Жауабы: 1 және 4.

Өзін-өзі тексеру

Сұрақ	Жауап
17 mod 12	5
$29 \equiv 5 \pmod{12}$?	Иә
gcd(252,105)	21
gcd(35,12)	1
$5^{-1} \bmod 26$	21
$2^{-1} \bmod 26$	Жоқ

Қорытынды

Модульдік арифметика бүтін сандарды қалдықтар кластары арқылы қарастырады.

Модуль бойынша қосу, азайту және көбейту аралық нәтижелерді қысқартуға мүмкіндік береді.

Евклид алгоритмі екі санның ЕҮОБ-ын есептейді және өзара жайлықты тексереді.

Кеңейтілген Евклид алгоритмі Безу коэффициенттерін табады.

gcd(a,m)=1 болса, a санының mod m бойынша кері элементі бар.

Модульдік кері элемент аффиндік шифр сияқты криптографиялық алгоритмдерде дешифрлау үшін қажет.

Бақылау сұрақтары

1. Модуль бойынша салыстыру дегеніміз не?
2. $a \equiv b \pmod{m}$ жазуы қандай шартты білдіреді?
3. Модульдік қосу мен көбейту қалай орындалады?
4. ЕҮОБ дегеніміз не?
5. Қандай сандар өзара жай деп аталады?
6. Евклид алгоритмінің негізгі идеясы қандай?
7. Безу теңдігі қалай жазылады?
8. Кеңейтілген Евклид алгоритмі қандай қосымша нәтиже береді?
9. Модульдік кері элемент қандай жағдайда бар?
10. Модульдік кері элемент аффиндік шифрда не үшін қажет?