6-ДӘРІС
МАТЕМАТИКАЛЫҚ НЕГІЗДЕР: МОДУЛЬДІК АРИФМЕТИКА. ЕВКЛИД ЖӘНЕ КЕҢЕЙТІЛГЕН ЕВКЛИД АЛГОРИТМДЕРІ

Дәрістің мақсаты

Криптографияда қолданылатын бүтін сандар арифметикасының негізгі ұғымдарын түсіндіру, бөлінгіштік пен ең үлкен ортақ бөлгішті қарастыру, модуль бойынша салыстырулар мен арифметикалық амалдарды меңгерту, Евклид алгоритмі арқылы ЕҮОБ есептеуді және кеңейтілген Евклид алгоритмі арқылы Безу коэффициенттері мен модульдік кері элементті табуды мысалдармен көрсету.

Бүтін сандар және бөлінгіштік

Көптеген криптографиялық алгоритмдердің математикалық негізінде бүтін сандармен орындалатын амалдар жатыр. a саны b санына қалдықсыз бөлінсе, b саны a санының бөлгіші деп аталады және b | a түрінде жазылады. Егер b | a болмаса, a санын b-ға бөлгенде қалдық пайда болады.

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

Мұнда q – бөлінді, r – қалдық. Қалдықпен бөлу модульдік арифметиканың негізін құрайды.

Модуль бойынша салыстыру

Екі бүтін санның m модулі бойынша қалдықтары бірдей болса, олар m модулі бойынша салыстырмалы деп аталады. Бұл қатынас:

$$a \equiv b \pmod m$$

түрінде жазылады. Оның мағынасы – a−b айырмасы m санына бөлінеді. Мысалы, $17 \equiv 5 \pmod{12}$, себебі 17−5=12 және 12 саны 12-ге бөлінеді. Сондай-ақ $29 \equiv 5 \pmod{12}$.

Қалдықтар кластары

m модулі бойынша кез келген бүтін сан 0,1,…,m−1 қалдықтарының біріне сәйкес келеді. Сондықтан есептеулерді осы қалдықтар жиынында жүргізуге болады. Мысалы, mod 7 жағдайында 15 саны 1 қалдығына, 23 саны 2 қалдығына сәйкес келеді.

$$15 \bmod 7 = 1, \quad 23 \bmod 7 = 2$$

Модульдік қосу, азайту және көбейту

Модульдік арифметикада үлкен сандармен есептеуді жеңілдету үшін аралық нәтижелерді модуль бойынша қысқартуға болады.

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

Мысалы, $(17+19) \bmod 7 = 36 \bmod 7 = 1$. Ал $17 \bmod 7=3$ және $19 \bmod 7=5$, сондықтан $(3+5) \bmod 7=1$. Көбейту үшін $(13\cdot 11) \bmod 7 = 143 \bmod 7 = 3$.

Ең үлкен ортақ бөлгіш

a және b бүтін сандарының ең үлкен ортақ бөлгіші, ЕҮОБ(a,b), екі санды да қалдықсыз бөлетін ең үлкен оң бүтін сан. Егер ЕҮОБ(a,b)=1 болса, a және b өзара жай сандар деп аталады. Өзара жайлық криптографияда, әсіресе модульдік кері элементті анықтауда маңызды.

$$\gcd(a,b)=1 \Rightarrow \text{a және b өзара жай}$$

Евклид алгоритмі

Евклид алгоритмі екі бүтін санның ең үлкен ортақ бөлгішін қайталанатын қалдықпен бөлу арқылы табады. Негізгі қасиет: $\gcd(a,b)=\gcd(b,r)$, мұнда $r=a \bmod b$. Қалдық нөлге тең болғанша процесс жалғасады; соңғы нөлден өзге қалдық ЕҮОБ болады.

Мысал: $\gcd(252,105)$ табайық.

$252 = 105\cdot 2 + 42$

$105 = 42\cdot 2 + 21$

$42 = 21\cdot 2 + 0$

Соңғы нөлден өзге қалдық 21, сондықтан $\gcd(252,105)=21$.

Өзара жай сандарды тексеру

Мысалы, 35 және 12 сандары үшін Евклид алгоритмін қолданамыз: $35=12\cdot 2+11$; $12=11\cdot 1+1$; $11=1\cdot 11+0$. Соңғы нөлден өзге қалдық 1 болғандықтан $\gcd(35,12)=1$. Демек, 35 пен 12 өзара жай.

Безу теңдігі

Егер $d=\gcd(a,b)$ болса, онда d санын a және b сандарының бүтін коэффициенттері бар сызықтық комбинациясы ретінде жазуға болады:

$ax + by = d$

Мұндағы x және y – Безу коэффициенттері. Оларды кеңейтілген Евклид алгоритмі арқылы табуға болады.

Кеңейтілген Евклид алгоритмі

Кеңейтілген Евклид алгоритмі ЕҮОБ-ты ғана емес, $ax+by=\gcd(a,b)$ теңдігін қанағаттандыратын x және y коэффициенттерін де есептейді. Мысал ретінде $a=35$ және $b=12$ алайық.

$35 = 12\cdot 2 + 11$

$12 = 11\cdot 1 + 1$

Кері қойсақ: $1=12-11$. Ал $11=35-12\cdot 2$. Сондықтан:

$1 = 12 - (35 - 12\cdot 2) = 3\cdot 12 - 35$

Демек, $35\cdot(-1)+12\cdot 3=1$. Безу коэффициенттері $x=-1$ және $y=3$.

Модульдік кері элемент

a санының m модулі бойынша кері элементі a^{-1} деп аталады, егер:

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

Мұндай кері элемент тек $\gcd(a,m)=1$ болғанда бар. Кеңейтілген Евклид алгоритмі оны есептеудің негізгі тәсілдерінің бірі.

Мысалы, 5 санының mod 26 бойынша кері элементін табайық. Евклид алгоритмі бойынша $26=5\cdot 5+1$, сондықтан $1=26-5\cdot 5$. Демек, -5 саны 5-тің mod 26 бойынша кері коэффициенті. Оң қалдыққа келтірсек $-5 \equiv 21 \pmod{26}$.

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

Сондықтан $5^{-1} \equiv 21 \pmod{26}$. Бұл нәтиже аффиндік шифр сияқты алгоритмдерде дешифрлау коэффициентін есептеу үшін қолданылады.

Аффиндік шифрмен байланысы

Аффиндік шифрда $E(x)=(ax+b) \bmod m$ түрлендіруі қолданылады. Дешифрлау үшін a коэффициентінің m модулі бойынша кері элементі болуы тиіс. Сондықтан $\gcd(a,m)=1$ шарты міндетті.

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

Мысалы, m=26 кезінде a=5 таңдауға болады, себебі gcd(5,26)=1 және $5^{-1}=21$. Ал a=2 жарамсыз, өйткені gcd(2,26)=2 және 2 санының mod 26 бойынша кері элементі жоқ.

Криптографиядағы маңызы

Модульдік арифметика классикалық шифрлардан бастап ашық кілтті криптографияға дейін кең қолданылады. Евклид алгоритмі сандардың өзара жайлығын жылдам тексереді, ал кеңейтілген Евклид алгоритмі кері элементтерді есептеуге мүмкіндік береді. Кейінгі дәрістерде бұл аппарат Эйлер және Ферма теоремаларын, сондай-ақ асимметриялық алгоритмдердің математикалық негіздерін түсіндіру үшін қажет болады.

Қорытынды

Модульдік арифметика бүтін сандарды қалдықтар кластары арқылы қарастыруға мүмкіндік береді. Криптографиялық есептерде қосу, азайту, көбейту және кері элементті табу mod m кеңістігінде орындалады. Евклид алгоритмі ЕҮОБ есептейді, кеңейтілген Евклид алгоритмі Безу коэффициенттерін және өзара жай сандар үшін модульдік кері элементті табады.

Бақылау сұрақтары

1. Модуль бойынша салыстыру дегеніміз не?
2. $a \equiv b \pmod m$ жазуы қандай шартты білдіреді?
3. Модульдік арифметикада 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?

Әдебиеттер тізімі

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. Васильева И.Н. Криптографические методы защиты информации. Москва: Юрайт, 2024.

4. Омассон Ж.-Ф. О криптографии всерьез. Практическое введение в современное шифрование. Москва: ДМК Пресс, 2021.