7-ДӘРІС

МОДУЛЬДІК ДӘРЕЖЕ. ЭЙЛЕР ТЕОРЕМАСЫ

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Модульдік дәрежеге шығару ұғымын түсіну.

Үлкен дәрежелерді тікелей есептемей, тиімді есептеу тәсілдерін меңгеру.

Эйлердің φ-функциясын анықтау және әртүрлі n үшін есептеу.

Эйлер теоремасының шартын, мағынасын және қолданылуын түсіну.

Модульдік кері элемент пен RSA алгоритмімен байланысын көрсету.

Дәрістің құрылымы

1. Модульдік дәрежеге шығару
2. Квадраттау және көбейту әдісі
3. Эйлердің φ-функциясы
4. Эйлер теоремасы
5. Үлкен дәрежені қысқарту
6. Модульдік кері элемент
7. Криптографиядағы қолданылуы

1. Модульдік арифметиканы еске түсіру

$a \equiv b \pmod{m}$ жазуы a және b сандарының m-ге бөлгендегі қалдықтары бірдей екенін білдіреді.

Эквивалентті түрде: $m \mid (a - b)$.

Мысал: $17 \equiv 5 \pmod{12}$, себебі $17 - 5 = 12$.

Мысал: $29 \equiv 1 \pmod{7}$, себебі $29 = 7 \cdot 4 + 1$.

Модульдік дәрежеге шығару дегеніміз не?

Модульдік дәрежеге шығару — a^n санын толық есептемей, оның m модулі бойынша қалдығын табу.

Криптографияда $a^n \bmod m$ түріндегі есептеулер өте жиі кездеседі.

n үлкен болғанда a санын n рет көбейту тиімсіз.

Негізгі идея: әр аралық қадамда mod m бойынша қысқарту.

Қарапайым мысал: $7^4 \bmod 10$

$7^2 = 49 \equiv 9 \pmod{10}$

$7^4 = (7^2)^2 \equiv 9^2 = 81 \equiv 1 \pmod{10}$

Сондықтан $7^4 \bmod 10 = 1$.

Артықшылық: 2401 санын толық пайдаланудың қажеті жоқ.

Модульдік дәрежелеудің қасиеттері

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

$a^{k+l} \bmod m = [(a^k \bmod m)(a^l \bmod m)] \bmod m$

$(a^k)^l \bmod m = a^{kl} \bmod m$

Аралық нәтижені кішірейту есептеуді жеңілдетеді және үлкен сандардың өсуін шектейді.

Тікелей есептеу және тиімді есептеу

Көрсеткіш	Тікелей тәсіл	Квадраттау-көбейту
Негізгі әрекет	a санын көп рет көбейту	Қайталама квадраттау
Үлкен n кезінде	Тиімсіз	Тиімді
Аралық сандар	Өте үлкен болуы мүмкін	mod m арқылы кішірейеді
Криптографияда	Сирек қолданылады	Негізгі тәсіл

2. Квадраттау және көбейту әдісі

Үлкен дәрежені екілік жіктеуге негізделген тиімді алгоритм.

Дәреже n екілік түрде жазылады.

a^2, a^4, a^8, a^{16}, ... мәндері бірінен кейін бірі квадраттау арқылы табылады

n құрамына кіретін дәрежелер ғана көбейтіледі.

Әр қадамда mod m бойынша қалдық алынады.

Неліктен екілік жіктеу қолданылады?

$13 = 8 + 4 + 1 = 1101_2$

Сондықтан $a^{13} = a^8 \cdot a^4 \cdot a$.

a^8-ді алу үшін $a \rightarrow a^2 \rightarrow a^4 \rightarrow a^8$ түрінде тек квадраттау жеткілікті

Бұл тәсіл көбейту санын айтарлықтай азайтады.

Мысал: $5^{13} \bmod 23$

$5^2 = 25 \equiv 2 \pmod{23}$

$5^4 \equiv 2^2 = 4 \pmod{23}$

$5^8 \equiv 4^2 = 16 \pmod{23}$

$13 = 8 + 4 + 1$

$5^{13} \equiv 5^8 \cdot 5^4 \cdot 5 \equiv 16 \cdot 4 \cdot 5 = 320 \equiv 21 \pmod{23}$

Жауабы: 21.

$5^{13} \bmod 23$: қадамдық кесте

Қадам | Есептеу | mod 23 бойынша қалдық

1 | $5^2=25$ | 2

2 | $5^4=(5^2)^2$ | 4

3 | $5^8=(5^4)^2$ | 16

4 | $13=8+4+1$ | $5^8 \cdot 5^4 \cdot 5$

5 | $16 \cdot 4 \cdot 5=320$ | 21

Алгоритмнің жалпы сұлбасы

1) n дәрежесін екілік түрде жіктеу.

2) a^2, a^4, a^8, ... қалдықтарын есептеу.

3) n-нің екілік жазылуындағы 1-лерге сәйкес дәрежелерді таңдау.

4) Таңдалған қалдықтарды көбейту.

5) Әр әрекеттен кейін mod m бойынша қысқарту.

3. Эйлердің φ-функциясы

Эйлердің φ-функциясы φ(n) — 1-ден n-ге дейінгі аралықта n санымен өзара жай болатын оң бүтін сандардың саны.

Өзара жай сандар үшін gcd(k,n)=1.

Мысал: n=8.

8-мен өзара жай сандар: 1, 3, 5, 7.

Сондықтан φ(8)=4.

φ(n): бірнеше қарапайым мысал

n | n-мен өзара жай сандар | φ(n)

5 | 1, 2, 3, 4 | 4

6 | 1, 5 | 2

8 | 1, 3, 5, 7 | 4

9 | 1, 2, 4, 5, 7, 8 | 6

10 | 1, 3, 7, 9 | 4

Жай сан үшін φ(p)

$\varphi(p) = p - 1$

Егер p — жай сан болса, 1,2,…,p−1 сандарының барлығы p-мен өзара жай. Мысал: φ(7)=6.

Жай сан дәрежесі үшін $\varphi(p^k)$

$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$

Мысал: $\varphi(8)=\varphi(2^3)=8-4=4$; өзара жай сандар: 1,3,5,7.

Өзара жай көбейткіштер үшін

Егер gcd(m,n)=1 болса, онда Эйлер функциясы мультипликативті:

$\varphi(mn)=\varphi(m)\varphi(n)$

Мысал: $15 = 3\cdot5$ және $\gcd(3,5)=1$.

$\varphi(15)=\varphi(3)\varphi(5)=2\cdot4=8$.

15-пен өзара жай сандар: 1,2,4,7,8,11,13,14.

φ(n)-нің жалпы формуласы

$\varphi(n) = n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_r)$

Мұндағы $p_1, p_2, \ldots, p_r$ — n санының әртүрлі жай көбейткіштері.

Мысал: φ(20)

$20 = 2^2 \cdot 5$

$\varphi(20)=20(1-1/2)(1-1/5)$

$=20 \cdot 1/2 \cdot 4/5$

$=8$

Тексеру: 1,3,7,9,11,13,17,19 — барлығы 8 сан.

Қосымша мысалдар: φ(12), φ(18), φ(36)

n | Жай көбейткіштер | Есептеу | Нәтиже

12 | $2^2 \cdot 3$ | $12(1-1/2)(1-1/3)$ | 4

18 | $2 \cdot 3^2$ | $18(1-1/2)(1-1/3)$ | 6

36 | $2^2 \cdot 3^2$ | $36(1-1/2)(1-1/3)$ | 12

φ(n)-ді есептеу алгоритмі

1) n санын жай көбейткіштерге жіктеу.

2) Әртүрлі жай көбейткіштерді анықтау.

3) $\varphi(n)=n\prod(1-1/p)$ формуласын қолдану.

4) Нәтижені қажет болса өзара жай сандарды санап тексеру.

4. Эйлер теоремасы

Егер gcd(a,n)=1 болса, онда $a^{\varphi(n)} \equiv 1 \pmod{n}$

Бұл — модульдік арифметиканың негізгі теоремаларының бірі.

Теореманың негізгі шарты

Эйлер теоремасын қолданар алдында міндетті түрде gcd(a,n)=1 екенін тексеру керек.

Егер a мен n өзара жай болмаса, a^φ(n) ≡ 1 (mod n) формуласын тікелей қолдануға болмайды.

Мысал: a=2, n=4 → gcd(2,4)=2.

φ(4)=2, бірақ $2^2=4 \equiv 0 \pmod 4$, 1 емес.

Мысал: $3^{100} \bmod 10$

gcd(3,10)=1.

φ(10)=4.

Эйлер теоремасы: $3^4 \equiv 1 \pmod{10}$.

100 = 4·25.

$3^{100} = (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{10}$.

Жауабы: 1.

5. Дәрежені φ(n) арқылы қысқарту

$k = q \cdot \varphi(n) + r$ a^k $a^r \equiv a^{\square} \pmod{n}$

Шарт: gcd(a,n)=1. Яғни үлкен дәрежеден φ(n)-ге бөлгендегі қалдықты пайдаланамыз.

Мысал: $2^{100} \bmod 15$

gcd(2,15)=1.

$\varphi(15)=8$.

$100 = 8 \cdot 12 + 4$.

Сондықтан $2^{100} \equiv 2^4 \pmod{15}$.

$2^4=16 \equiv 1 \pmod{15}$.

Жауабы: 1.

Кешенді мысал: $7^{222} \bmod 20$

$\gcd(7,20)=1$, $\varphi(20)=8$.

$222 = 8 \cdot 27 + 6$.

$7^{222} \equiv 7^6 \pmod{20}$.

$7^2 \equiv 9 \pmod{20}$.

$7^4 \equiv 9^2 = 81 \equiv 1 \pmod{20}$.

$7^6 = 7^4 \cdot 7^2 \equiv 1 \cdot 9 \equiv 9 \pmod{20}$.

Жауабы: 9.

6. Эйлер теоремасы және модульдік кері элемент

$a^{-1} \equiv a^{(\varphi(n)-1)} \pmod{n}$

Себебі $a^{\varphi(n)} \equiv 1 \Rightarrow a \cdot a^{(\varphi(n)-1)} \equiv 1$. Шарт: $\gcd(a,n)=1$.

Кері элементке мысал

$3^{-1} \bmod 10$ табайық.

$\gcd(3,10)=1$, $\varphi(10)=4$.

Эйлер бойынша: $3^{-1} \equiv 3^{\wedge}(4-1)=3^3=27 \equiv 7 \pmod{10}$.

Тексеру: $3 \cdot 7=21 \equiv 1 \pmod{10}$.

Практикада үлкен сандар үшін кеңейтілген Евклид алгоритмі жиі тиімдірек.

7. Криптографиядағы рөлі

Ұғым | Криптографиядағы рөлі | Мысал

Модульдік дәрежелеу | Ашық кілтті алгоритмдердің негізгі операциясы | RSA

φ(n) | Кілт параметрлерін байланыстырады | RSA: φ(pq)

Эйлер теоремасы | Дәрежелердің периодтылығын түсіндіреді | Дұрыстықты негіздеу

Кері элемент | Жабық кілт параметрін есептеуде қажет | $d=e^{-1} \bmod \varphi(n)$

RSA-мен байланысы: шағын оқу мысалы

$p=3$, $q=11 \rightarrow n=pq=33$.

$\varphi(n)=(p-1)(q-1)=2\cdot 10=20$.

$e=3$ таңдайық, $\gcd(3,20)=1$.

d саны $3d \equiv 1 \pmod{20}$ шартын қанағаттандыруы керек $\rightarrow d=7$.

Ашық кілт: $(e,n)=(3,33)$, жабық кілт: $d=7$.

Бұл мысал тек математикалық байланысты көрсетуге арналған; нақты RSA әлдеқайда үлкен жай сандарды қолданады.

Әдістерді салыстыру

Әдіс | Қашан қолданамыз? | Негізгі идея | Артықшылығы

Тікелей mod | Кіші дәреже | Әр қадамда қалдық алу | Қарапайым

Квадраттау-көбейту | Үлкен дәреже | n-ді екілік жіктеу | Жылдам

Эйлер теоремасы | gcd(a,n)=1 | Дәрежені φ(n) арқылы қысқарту | Өте үлкен n үшін ыңғайлы

Кеңейтілген Евклид | Кері элемент керек | ax+ny=1 | Практикада тиімді

Жиі жіберілетін қателер

gcd(a,n)=1 шартын тексермеу.

φ(n)-ді n−1 деп алу: бұл тек n жай сан болғанда дұрыс.

Дәрежені φ(n)-ге қысқартқанда қалдықты қате есептеу.

Квадраттау кезінде әр қадамда mod m бойынша қысқартуды ұмыту.

φ(mn)=φ(m)φ(n) формуласын m және n өзара жай емес кезде тікелей қолдану.

Қорытынды

Модульдік дәрежелеу — криптографиялық есептеулердің негізгі операцияларының бірі.

Квадраттау және көбейту әдісі үлкен дәрежелерді тиімді есептейді.

φ(n) берілген модульмен өзара жай қалдықтардың санын сипаттайды.

gcd(a,n)=1 болса, a^φ(n) ≡ 1 (mod n).

Эйлер теоремасы дәрежелерді қысқартуға және кері элементті түсіндіруге мүмкіндік береді.

Бұл идеялар RSA сияқты ашық кілтті криптожүйелердің математикалық негізіне кіреді.

Бақылау сұрақтары

1. Модульдік дәрежеге шығару дегеніміз не?
2. Квадраттау және көбейту әдісінің идеясы қандай?
3. φ(n) нені көрсетеді?
4. p жай сан болса, φ(p) неге тең?
5. $\varphi(p^k)$ формуласы қандай?
6. φ(n)-нің жалпы формуласы қалай жазылады?
7. Эйлер теоремасының негізгі шарты қандай?
8. Үлкен дәрежені φ(n) арқылы қалай қысқартамыз?
9. Модульдік кері элементпен қандай байланыс бар?
10. Бұл ұғымдар RSA-да не үшін маңызды?