7-ДӘРІС
МОДУЛЬДІК ДӘРЕЖЕ. ЭЙЛЕР ТЕОРЕМАСЫ

Дәрістің мақсаты

Модульдік дәрежеге шығару ұғымын түсіндіру, үлкен дәрежелерді тиімді есептеу тәсілін көрсету, Эйлердің φ-функциясын анықтау және есептеу ережелерін меңгерту, Эйлер теоремасының мазмұны мен шарттарын түсіндіру және оның криптографиялық алгоритмдердегі рөлін қарапайым есептер арқылы ашу.

Модульдік дәрежеге шығару

Криптографияда $a^n \bmod m$ түріндегі есептеулер жиі кездеседі. n дәрежесі үлкен болғанда a санын n рет тікелей көбейту тиімсіз. Сондықтан аралық нәтижелерді әр қадамда mod m бойынша қысқартып, жылдам дәрежеге шығару тәсілдері қолданылады.

$$a^n \bmod m$$

Мысалы, $7^4 \bmod 10$ есептейік. $7^2=49 \equiv 9 \pmod{10}$, ал $7^4=(7^2)^2 \equiv 9^2=81\equiv 1 \pmod{10}$. Үлкен сан 2401-ді толық есептемей-ақ соңғы қалдықты алуға болады.

Квадраттау және көбейту әдісі

Дәрежені екілік жіктеу арқылы есептеу квадраттау және көбейту әдісінің негізін құрайды. Мысалы, 13 саны екілік түрде 1101_2, яғни 13=8+4+1. Сондықтан $a^{13}=a^8 \cdot a^4 \cdot a$ түрінде жазылады. a^2, a^4, a^8 мәндері бірінен кейін бірі квадраттау арқылы табылады және әр қадамда mod m бойынша қысқартылады.

Мысал: $5^{13} \bmod 23$ есептейік.
$5^2 = 25 \equiv 2 \pmod{23}$
$5^4 \equiv 2^2 = 4 \pmod{23}$
$5^8 \equiv 4^2 = 16 \pmod{23}$
$5^{13} = 5^8 \cdot 5^4 \cdot 5 \equiv 16 \cdot 4 \cdot 5 = 320 \equiv 21 \pmod{23}$
Демек, $5^{13} \bmod 23 = 21$.

Эйлердің φ-функциясы

Эйлердің φ-функциясы φ(n) – 1-ден n-ге дейінгі аралықта n санымен өзара жай болатын оң бүтін сандардың санын көрсетеді. Дәлірек айтқанда, $1 \le k \le n$ және gcd(k,n)=1 шартын қанағаттандыратын k мәндерінің саны есептеледі.

Егер p – жай сан болса, 1,2,…,p−1 сандарының барлығы p-мен өзара жай. Сондықтан:

$$\varphi(p)=p-1$$

Мысалы, φ(7)=6.

Жай сан дәрежесі үшін φ-функция

Егер p – жай сан және $k \ge 1$ болса:

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

Мысалы, $\varphi(8)=\varphi(2^3)=8-4=4$. Шынында да 1,3,5,7 сандары 8-мен өзара жай.

Өзара жай көбейткіштер үшін

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

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

Мысалы, $15=3\cdot5$ және $\gcd(3,5)=1$. Сондықтан $\varphi(15)=\varphi(3)\varphi(5)=2\cdot4=8$.

Жалпы формула

Егер n санының жай көбейткіштерге жіктелуі $n=p_1^{a1}p_2^{a2}\dots p_r^{ar}$ болса, онда:

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

Мысалы, $n=20=2^2\cdot5$. Сонда $\varphi(20)=20(1-1/2)(1-1/5)=20\cdot1/2\cdot4/5=8$.

Эйлер теоремасы

Эйлер теоремасы модульдік арифметиканың негізгі нәтижелерінің бірі. Егер a және n өзара жай болса, яғни $\gcd(a,n)=1$, онда:

$$a^\varphi(n) \equiv 1 \pmod n$$

Теореманың маңызды шарты – a мен n өзара жай болуы керек. Бұл шарт орындалмаса, формуланы тікелей қолдануға болмайды.

Эйлер теоремасына мысал

$3^{100} \bmod 10$ есептейік. $\gcd(3,10)=1$. $\varphi(10)=4$, себебі 1,3,7,9 сандары 10-мен өзара жай. Эйлер теоремасы бойынша $3^4\equiv1 \pmod{10}$.

$100 = 4\cdot25$

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

Демек, 3^{100} санының 10-ға бөлгендегі қалдығы 1.

Дәрежені қысқарту

Эйлер теоремасы үлкен дәрежелерді $\varphi(n)$ арқылы қысқартуға мүмкіндік береді. Егер $\gcd(a,n)=1$ және $k=q\varphi(n)+r$ болса, онда:

$$a^k \equiv a^r \pmod n$$

Мысалы, $2^{100} \bmod 15$ табайық. $\gcd(2,15)=1$ және $\varphi(15)=8$. $100=8\cdot12+4$, сондықтан $2^{100}\equiv2^4=16\equiv1 \pmod{15}$.

Эйлер теоремасы және модульдік кері элемент

$\gcd(a,n)=1$ болса, Эйлер теоремасынан $a^\varphi(n)\equiv1 \pmod n$ шығады. Осыдан:

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

Демек, теориялық түрде $a^{-1}\equiv a^(\varphi(n)-1) \pmod n$. Практикада кері элементті табу үшін кеңейтілген Евклид алгоритмі жиі тиімдірек, бірақ бұл байланыс модульдік арифметиканың құрылымын түсінуге маңызды.

Криптографиядағы рөлі

Модульдік дәрежеге шығару ашық кілтті криптографияда негізгі есептеу операцияларының бірі. Үлкен сандармен жұмыс істегенде квадраттау және көбейту тәрізді тиімді алгоритмдер қолданылады. Эйлер теоремасы белгілі бір модульдерде дәрежелердің периодтық қасиетін түсіндіреді және кейін RSA тәрізді жүйелердің математикалық дұрыстығын талдауға негіз болады.

Есептік мысал: $7^{222} \bmod 20$

Алдымен gcd(7,20)=1 екенін тексереміз. φ(20)=8. Эйлер теоремасы бойынша $7^8 \equiv 1 \pmod{20}$. 222=8·27+6, сондықтан:

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

$7^2 \equiv 49 \equiv 9, \quad 7^4 \equiv 9^2 \equiv 81 \equiv 1 \pmod{20}$

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

Жауабы: $7^{222} \bmod 20 = 9$.

Қорытынды

Модульдік дәрежеге шығару криптографиялық есептеулердің маңызды бөлігі. Үлкен дәрежелер квадраттау және көбейту арқылы тиімді есептеледі. Эйлердің φ-функциясы берілген модульмен өзара жай қалдықтардың санын анықтайды, ал Эйлер теоремасы gcd(a,n)=1 жағдайында a^φ(n)≡1 (mod n) қатынасын береді. Бұл нәтижелер кейінгі Ферма теоремасын және ашық кілтті криптожүйелерді түсінуге негіз болады.

Бақылау сұрақтары

1. Модульдік дәрежеге шығару дегеніміз не?
2. Үлкен дәрежені тікелей есептемей қалдықты қалай табуға болады?
3. Квадраттау және көбейту әдісінің негізгі идеясы қандай?
4. Эйлердің φ-функциясы нені көрсетеді?
5. p жай саны үшін φ(p) неге тең?
6. $\varphi(p^k)$ формуласы қалай жазылады?
7. Эйлер функциясының мультипликативті қасиеті қандай жағдайда орындалады?
8. Эйлер теоремасының тұжырымы және негізгі шарты қандай?
9. Эйлер теоремасы үлкен дәрежені қысқартуға қалай мүмкіндік береді?
10. Эйлер теоремасының криптографиядағы маңызы қандай?

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.