9-ДӘРІС
ФЕРМА ТЕОРЕМАСЫ

Дәрістің мақсаты

Ферманың кіші теоремасының мазмұны мен қолданылу шарттарын түсіндіру, жай модуль бойынша үлкен дәрежелерді қысқарту тәсілін көрсету, Эйлер теоремасымен байланысын ашу және есептерде дұрыс қолдануды қалыптастыру.

Жай сандардың рөлі

Жай сан – 1-ден үлкен және тек 1 мен өзіне ғана бөлінетін оң бүтін сан. Жай сандар сандар теориясының негізгі объектілерінің бірі және ашық кілтті криптографияда ерекше орын алады.

Ферманың кіші теоремасы

Егер p – жай сан және a саны p-ға бөлінбесе, онда:

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

Теореманың эквивалентті түрі кез келген бүтін a үшін:

$$a^{p} \equiv a \pmod{p}$$

Эйлер теоремасымен байланысы

p жай болғанда $\varphi(p)=p-1$. Сондықтан Эйлер теоремасындағы $a^{\varphi(p)}\equiv 1 \pmod{p}$ формуласы дәл Ферманың кіші теоремасына айналады. Ферма теоремасын Эйлер теоремасының жай модульге арналған жеке жағдайы ретінде қарастыруға болады.

Қарапайым мысал

$2^{100} \bmod 7$ табайық. 7 – жай сан және $\gcd(2,7)=1$. Ферма теоремасы бойынша $2^{6}\equiv 1 \pmod{7}$. $100=6\cdot 16+4$.

$$2^{100} \equiv 2^{4} = 16 \equiv 2 \pmod{7}$$

Тағы бір мысал

$5^{123} \bmod 13$ есептейік. 13 – жай, 5 саны 13-ке бөлінбейді. Сондықтан $5^{12}\equiv 1 \pmod{13}$. $123=12\cdot 10+3$.

$5^{123} \equiv 5^{3} = 125 \equiv 8 \pmod{13}$

Модульдік кері элемент

a саны p-ға бөлінбесе, $a^{(p-1)}\equiv 1 \pmod{p}$. Осыдан $a\cdot a^{(p-2)}\equiv 1 \pmod{p}$, демек:

$$a^{-1} \equiv a^{(p-2)} \pmod{p}$$

Бұл формула жай модуль жағдайында кері элементті теориялық түрде табуға мүмкіндік береді.

Қолдану шектеулері

$a^{(p-1)}\equiv 1 \pmod{p}$ түрін қолдану үшін p жай және a саны p-ға бөлінбейтін болуы керек. Модуль құрама сан болса, Ферма теоремасын сол күйінде қолдануға болмайды; мұндай жағдайда Эйлер теоремасы немесе басқа әдістер қарастырылады.

Теореманың шарттарын түсіндіру

Ферманың кіші теоремасын қолданғанда модуль p жай сан болуы және a саны p-ға бөлінбеуі керек. Осы екі шарт орындалғанда a^(p−1) ≡ 1 (mod p). Балама түрде кез келген бүтін a үшін a^p ≡ a (mod p) қатынасы орындалады.

Толық есептік мысал

3^222 mod 11 табайық. 11 – жай сан, gcd(3,11)=1. Ферма теоремасы бойынша 3^10 ≡ 1 (mod 11). 222=10·22+2, сондықтан 3^222 ≡ 3^2 ≡ 9 (mod 11). Жауабы: 9.

Модульдік кері элемент

Жай p модулі үшін a^(−1) ≡ a^(p−2) (mod p). Мысалы, 3 санының mod 7 бойынша кері элементі 3^5 mod 7=5. Тексеру: 3·5=15 ≡ 1 (mod 7).

Эйлер теоремасымен байланысы

Ферма теоремасы Эйлер теоремасының жай модульге арналған жеке жағдайы. p жай болса, φ(p)=p−1, сондықтан a^φ(p)≡1 формуласы a^(p−1)≡1 түріне өтеді.

Жиі жіберілетін қателер

Құрама модульді жай деп қабылдау, gcd(a,p)=1 шартын тексермеу және дәрежені p−1 бойынша қате қысқарту жиі кездеседі. Әр есепте алдымен теореманың қолданылу шарттары тексерілуі тиіс.

Криптографиядағы маңызы

Ферма теоремасы модульдік дәрежелердің периодтылығын түсіндіреді, үлкен дәрежелерді қысқартуға мүмкіндік береді және жай сандармен байланысты криптографиялық конструкциялардың математикалық аппаратын қалыптастырады.

Қорытынды

Ферманың кіші теоремасы жай модуль бойынша дәрежелік есептеулерді ықшамдайды. Оның негізгі шарты – p жай сан болуы және a санының p-ға бөлінбеуі. Теорема Эйлер теоремасымен тікелей байланысты және модульдік арифметикадағы маңызды құрал болып табылады.

Бақылау сұрақтары

1. Жай сан дегеніміз не?
2. Ферманың кіші теоремасы қалай тұжырымдалады?
3. a^p≡a (mod p) формуласының мағынасы қандай?
4. Ферма теоремасының негізгі шарттары қандай?
5. Ферма және Эйлер теоремалары қалай байланысты?
6. Үлкен дәрежені p−1 арқылы қалай қысқартуға болады?
7. Жай модульде кері элементті Ферма теоремасы арқылы қалай өрнектеуге болады?
8. 2^{100} mod 7 есебінде дәреже қалай қысқарады?
9. Құрама модульде теореманы неге тікелей қолдануға болмайды?
10. Теореманың криптографиядағы рөлі 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. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024.

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