9-дәріс. Ферма теоремасы

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Нені үйренеміз?

Оқу нәтижелері

1. Жай сан, бөлінгіштік, қалдық, өзара жай сандар ұғымдарын ажырату.
2. Ферма теоремасының шартын және екі түрін тұжырымдау.
3. Теореманы дәлелдеп, үлкен дәрежелерді есептеу.
4. Кері элементті табу және криптографиялық қолданылуын түсіндіру.

Тарих: Пьер де Ферма

XVII ғасыр

Пьер де Ферма (1607–1665) — француз математигі, сандар теориясына зор үлес қосқан.

1640 жыл

Ферма теореманың тұжырымын Бернар Френикль де Бессиге жазған хатында хабарлаған.

Дерек

Ферма көптеген математикалық нәтижелерін хаттар мен жазбаларда қалдырған; оларды әрдайым толық дәлелдеп жарияламаған.

Тарих: Эйлер және «екі Ферма теоремасы»

Леонард Эйлер

XVIII ғасырда Эйлер Ферманың кіші теоремасының дәлелдерін беріп, оны жалпылауға үлес қосты.

Екі түрлі теорема

Ферманың кіші теоремасы: $a^{(p-1)} \equiv 1 \pmod{p}$.

Ферманың соңғы теоремасы: $n>2$ кезінде $x^n+y^n=z^n$ оң бүтін шешімдері жоқ.

Дерек

Соңғы теореманы Эндрю Уайлс 1990-жылдары дәлелдеді. Бұл — бүгінгі дәрістегі кіші теоремадан бөлек нәтиже.

Негізгі ұғым 1. Жай сан

Анықтама

Жай сан — 1-ден үлкен, тек 1-ге және өзіне ғана бөлінетін натурал сан.

Мысалдар

2, 3, 5, 7, 11, 13 — жай сандар.

1 — жай сан емес; $9 = 3 \times 3$ — құрама сан.

Неге маңызды?

Ферма теоремасының негізгі нұсқасында модуль p міндетті түрде жай сан.

Негізгі ұғым 2. Модуль бойынша салыстыру

Анықтама

$a \equiv b \pmod{n} \Leftrightarrow$ n саны $(a - b)$ айырмасын бөледі.

Мысал

$17 \equiv 5 \pmod{12}$, өйткені $17 - 5 = 12$.

$23 \bmod 7 = 2$, өйткені $23 = 7 \times 3 + 2$.

Есте сақтаңыз

«mod n» — n-ге бөлгендегі қалдық бойынша есептеу.

Негізгі ұғым 3. ЕҮОБ және өзара жай сандар

Анықтама

ЕҮОБ(a,b) — a мен b сандарының ең үлкен ортақ бөлгіші.

ЕҮОБ(a,b)=1 болса, олар өзара жай.

Мысал

ЕҮОБ(5,13)=1; ЕҮОБ(6,15)=3.

Ферма шартында

p жай және p ∤ a болса, автоматты түрде ЕҮОБ(a,p)=1.

Негізгі ұғым 4. Дәрежелер және кері элемент

Модульдік дәреже

$a^k \bmod n$ — a санының k-дәрежесін n-ге бөлгендегі қалдық.

Модульдік кері элемент

$a^{-1} \bmod n$ — $a \cdot x \equiv 1 \pmod{n}$ шартын орындайтын x саны.

Мысал

$3^{-1} \equiv 5 \pmod{7}$, өйткені $3 \times 5 = 15 \equiv 1 \pmod{7}$.

Ферманың кіші теоремасы — негізгі тұжырым

ТЕОРЕМА

Егер p — жай сан және $p \nmid a$ болса, онда:

Негізгі формула

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

Балама тұжырым

Кез келген бүтін a үшін: $a^p \equiv a \pmod{p}$.

Мысал

$p=7$, $a=2$: $2^6 = 64 \equiv 1 \pmod{7}$.

Неліктен екі шартты тексереміз?

1-шарт: p жай

$p=7$ — жарамды; $p=8$ — жарамсыз.

2-шарт: $p \nmid a$

$p=7, a=3$ — жарамды; $p=7, a=14$ — жарамсыз.

Қарсы мысал

$a=2, p=8$: $2^7 = 128 \equiv 0 \pmod 8$, 1 емес.

$a=7, p=7$: $7^6 \equiv 0 \pmod 7$, 1 емес.

Дәлелдеу идеясы: қалдықтарды ауыстыру

Бастапқы жиын

1, 2, …, p−1 — p модулі бойынша нөл емес қалдықтар.

a санына көбейтеміз

a, 2a, …, (p−1)a (mod p).

Негізгі байқау

ЕҮОБ(a,p)=1 болғандықтан, бұл қалдықтар өзара әртүрлі және дәл сол 1,…,p−1 жиынын береді.

Ферма теоремасының дәлелдеуі

1-қадам. Көбейтінділер теңдігі

$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$.

2-қадам. a дәрежесін шығарамыз

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

3-қадам. Қысқартамыз

$(p-1)!$ саны p-ға бөлінбейді, сондықтан кері элементі бар.

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

Дәлелдеудің көрнекі мысалы: p=7, a=3

Қалдықтарды көбейту

$1 \to 3 \quad 2 \to 6 \quad 3 \to 2 \quad 4 \to 5 \quad 5 \to 1 \quad 6 \to 4$

Не өзгерді?

{1,2,3,4,5,6} жиыны тек басқа ретпен орналасты.

Қорытынды

$3^6 \cdot 6! \equiv 6! \pmod 7 \Rightarrow 3^6 \equiv 1 \pmod 7$.

Үлкен дәрежені қысқарту алгоритмі

Алгоритм

1. p санының жай екенін тексеріңіз.
2. $p \nmid a$ шартын тексеріңіз.
3. $k = q(p-1) + r$ деп бөліңіз.
4. $a^k \equiv a^r \pmod{p}$ түріне келтіріңіз.
5. Қалған шағын дәрежені есептеңіз.

Маңызды

Дәреже p бойынша емес, $p-1$ бойынша қысқартылады.

Мысал 1. $2^{100} \bmod 7$

Шарт

$p=7$ — жай, ЕҮОБ$(2,7)=1$.

Қысқарту

$2^6 \equiv 1 \pmod 7$. $100 = 6 \cdot 16 + 4$.

Есептеу

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

Жауап

2

Мысал 2. $5^{123} \bmod 13$

Шарт

13 — жай сан; ЕҮОБ(5,13)=1.

Қысқарту

$5^{12} \equiv 1 \pmod{13}$; $123 = 12 \cdot 10 + 3$.

Есептеу

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

Жауап

8

Мысал 3. $3^{222} \bmod 11$

Шарт

11 — жай; ЕҮОБ(3,11)=1.

Қысқарту

$222 = 10 \cdot 22 + 2$; $3^{10} \equiv 1 \pmod{11}$.

Есептеу

$3^{222} \equiv 3^2 = 9 \pmod{11}$.

Жауап

9

Дәрежелердің периодтылығы

Мысал: $2^k \bmod 7$

k:	1	2	3	4	5	6	7	8
$2^k \bmod 7$:	2	4	1	2	4	1	2	4

Түсінік

Бұл мысалда ең кіші период 3; ал Ферма теоремасы 6 қадамнан кейін міндетті түрде 1 алынатынын кепілдейді.

Назар аударыңыз

Нақты ең кіші период $p-1$-ден кіші болуы мүмкін.

Жылдам модульдік дәрежелеу алгоритмі

Square-and-multiply әдісі

Нәтиже = 1; негіз = a mod n.

Дәреже k > 0 болғанша:

- k тақ болса, нәтиже = нәтиже·негіз mod n;
- негіз = негіз² mod n;
- k = ⌊k/2⌋.

Ерекшелігі

Көбейту саны шамамен O(log k); үлкен дәрежені тікелей есептеу қажет емес.

Модульдік кері элемент: Ферма формуласы

Теоремадан шығару

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

Формула

$a^{-1} \equiv a^{(p-2)} \pmod{p}$, мұнда p — жай, $p \nmid a$.

Мысал

$3^{-1} \bmod 7 = 3^5 \bmod 7 = 5$.

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

Ферма және Эйлер теоремалары

Ферма

p — жай, ЕҮОБ(a,p)=1 ⇒ $a^{(p-1)} \equiv 1 \pmod{p}$.

Эйлер

n ≥ 2, ЕҮОБ(a,n)=1 ⇒ a^φ(n) ≡ 1 (mod n).

Байланыс

p жай болса, φ(p)=p−1. Сондықтан Ферма — Эйлер теоремасының жеке жағдайы.

Мысал

φ(10)=4, ЕҮОБ(3,10)=1 ⇒ $3^4 \equiv 1 \pmod{10}$.

Криптографияда қолданылуы: негізгі бағыттар

1. Модульдік дәрежелеу

Ашық кілтті алгоритмдерде үлкен сандардың дәрежесін қалдық бойынша есептеу.

2. Кері элемент

Кілт есептеулерінде және ақырлы өріс арифметикасында бөлуді іске асыру.

3. Жай сандарды тексеру

Ферма тесті — ықтимал жай санды тексерудің қарапайым тәсілі; бірақ жеткіліксіз болуы мүмкін.

RSA архитектурасымен байланысы

Кілттерді құру

p, q жай сандар → $n=pq$ → $\varphi(n)=(p-1)(q-1)$.

e таңдалады; $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

Шифрлау / дешифрлау

Ашық кілт (n,e): $c \equiv m^e \pmod{n}$.

Жабық кілт (n,d): $m \equiv c^d \pmod{n}$.

Нақтылау

RSA дұрыстығын негіздеуде Эйлер теоремасы және жай модульдер бойынша Ферма теоремасы қолданылады; нақты жүйелерде қауіпсіз padding қажет.

RSA шағын оқу мысалы

Кілт генерациясы

$p=5$, $q=11 \rightarrow n=55$, $\varphi(n)=40$.

$e=3$; $d=27$, себебі $3 \cdot 27=81 \equiv 1 \pmod{40}$.

Шифрлау

$m=7 \rightarrow c=7^3 \bmod 55 = 13$.

Дешифрлау

$m=13^{27} \bmod 55 = 7$.

Ескерту

Бұл тек оқу мысалы. Мұндай кішкентай кілттер нақты жүйелер үшін қауіпсіз емес.

Ферма тесті: артықшылықтары мен шектеуі

Тест идеясы

Егер ЕҮОБ(a,n)=1 және $a^{(n-1)} \not\equiv 1 \pmod{n}$ болса, n — құрама сан.

Неліктен жеткіліксіз?

$a^{(n-1)} \equiv 1$ болуы n-нің жай екенін дәлелдемейді. Кейбір құрама сандар тесттен өтеді.

Мысал

$341 = 11 \cdot 31$ құрама, бірақ $2^{340} \equiv 1 \pmod{341}$.

Практика

Жай санды сенімді тексеру үшін Miller–Rabin сияқты күштірек тесттер пайдаланылады.

Жиі кездесетін қателер

Қате 1

p құрама болса да $a^{(p-1)} \equiv 1$ формуласын қолдану.

Қате 2

$p \mid a$ жағдайында негізгі формуланы қолдану.

Қате 3

k дәрежесін $p-1$ орнына p бойынша қысқарту.

Қате 4

Ферма тестінен өткен санды міндетті түрде жай деп есептеу.

Өзіндік тексеру: 4 тапсырма

Есептер

1. $4^{80} \bmod 11$ мәнін табыңыз.
2. $7^{100} \bmod 13$ мәнін табыңыз.
3. $5^{-1} \bmod 17$ кері элементін табыңыз.
4. $p=7$, $a=14$ үшін $a^{(p-1)} \equiv 1$ қолдануға бола ма? Неге?

Жауаптар

1) 1; 2) 9; 3) 7; 4) жоқ, себебі $7 \mid 14$.

Қорытынды және әдебиеттер

Негізгі тұжырым

Ферма теоремасы жай модульдегі үлкен дәрежелерді қысқартады; шарттары міндетті түрде тексеріледі. Ол кері элементтер мен криптографиялық есептеулердің маңызды құралы.

Дереккөздер

Ахметов және т.б. Қолданбалы криптология (2016).

Ахметов және т.б. Криптография негіздері (2020).

Васильева И.Н. Криптографические методы защиты информации (2024).

Омассон Ж.-Ф. О криптографии всерьез (2021).