Дәріс 6: Салыстырулар Теориясы және Қолданылуы

Бұл дәрісте біз салыстырулар теориясының негіздерін, модульдік арифметиканы, Эйлер функциясын және Қытай қалдық теоремасын қарастырамыз. Бұл ұғымдар криптография мен ақпараттық технологияларда маңызды рөл атқарады.

Салыстырулар Теориясының Негіздері

Салыстырулар теориясы сандар арасындағы қатынастарды модуль бойынша зерттейді. Егер **(a – b)** айырмасы **m** санына бөлінсе, **a** және **b** сандары **m** модулі бойынша салыстырмалы деп аталады.

- **Анықтама 1:** $a \equiv b \pmod{m}$ жазбасы **a** мен **b** арасындағы қатынасты білдіреді.
- **Теорема 1:** **a** және **b** сандары **m**-ге бөлінгенде бірдей қалдықтар берсе ғана салыстырылады.

Салыстыру Қасиеттері

Салыстырулар қатынасы бірнеше маңызды қасиеттерге ие, олар оны математикалық есептеулерде ыңғайлы етеді.

Рефлексивтілік

$a \equiv a \pmod{m}$

Симметриялылық

Егер $a \equiv b \pmod{m}$ болса, онда $b \equiv a \pmod{m}$.

Өтпелілік

Егер $a \equiv b \pmod{m}$ және $b \equiv c \pmod{m}$ болса, онда $a \equiv c \pmod{m}$.

Модульдік Арифметика

Модульдік арифметика — заманауи криптографияның негізі. Ол бүтін сандардың нақты мәнін емес, олардың **n** бүтін санына бөлінуінің қалдығын анықтайды.

1. Қосу

   (a + b) mod n ≡ ((a mod n) + (b mod n)) mod n

2. Азайту

   (a - b) mod n ≡ ((a mod n) - (b mod n)) mod n

3. Көбейту

   (a * b) mod n ≡ ((a mod n) * (b mod n)) mod n

Ең Үлкен Ортақ Бөлгіш (ЕҮОБ)

ЕҮОБ есептеудің ең көне әдістерінің бірі — Евклид алгоритмі. Ол **НОД(a, b) = НОД(b, a mod b)** қатынасына негізделген.

> Егер **a** және **b** сандарының **d** бөлгіші болса, онда **d** **r**-ді де бөледі, яғни `НОД(a, b) = НОД(b, r)`.

Бұл алгоритм қалдық нөлге айналғанша қайталанады, соңғы нөл емес қалдық ЕҮОБ болады.

Қалдық Кластары

Модульдік қалдық класы — берілген **a** бүтін санымен салыстырылатын барлық бүтін сандар жиыны. Ол [a]n арқылы белгіленеді.

- **Теорема 12:** **a** мен **n** модулімен салыстырылатын сандар класы a + nk түріндегі сандар жиынымен сәйкес келеді.
- **Теорема 16:** Модуль кластарының саны ақырлы және **n**-ге тең.

Әрбір класта шексіз сандар болады, бірақ олардың барлығы **n**-ге бөлгенде бірдей қалдық береді.

Эйлер Функциясы (ϕ(n))

Эйлер функциясы ϕ(n) — **n**-нен аспайтын және **n**-мен өзара жай натурал сандар саны. Бұл функция криптографияда, әсіресе RSA жүйесінде маңызды.

- **Анықтама 10:** ϕ(n) — **n** модуліне қатысты қалдықтардың қысқартылған жүйесіндегі кластар саны.
- **Теорема 21:** Эйлер функциясы мультипликативті: егер **(a, b) = 1** болса, $\varphi(ab) = \varphi(a)\varphi(b)$.

Мысалы, $\varphi(12) = 4$, себебі 12-мен өзара жай сандар: 1, 5, 7, 11.

Ферма және Эйлер Теоремалары

Бұл теоремалар үлкен дәрежелердің модуль бойынша қалдықтарын табуға мүмкіндік береді.

> **Ферма теоремасы:** Кез келген жай **p** және **p**-ге бөлінбейтін кез келген **a ≥ 1** үшін $a^{(p-1)} \equiv 1 \mod p$.

> **Эйлер теоремасы:** Кез келген **m** модулі үшін және кез келген **a ≥ 1**, **m**-мен өзара жай сан, $a^{\varphi(m)} \equiv 1 \mod m$.

Бұл теоремалар RSA криптографиялық жүйесінің негізі болып табылады.

Бірінші Дәрежелі Салыстырулар

ax ≡ b mod m түріндегі салыстырулардың шешімдерін табу.

- **Теорема 24:** Егер (a, m) = d және **d b**-ны бөлмесе, шешімі жоқ.
- **Теорема 25:** Егер (a, m) = 1 болса, бір ғана шешімі бар.
- **Теорема 26:** Егер (a, m) = 1 болса, шешімі x ≡ b * a^(φ(m)-1) mod m арқылы табылады.

Мысалы, 3x ≡ 4 mod 34 салыстыруының шешімі x ≡ 24 mod 34.

Қытай Қалдық Теоремасы (ҚҚТ)

ҚҚТ — бірнеше салыстырулар жүйесінің шешімін табуға мүмкіндік беретін маңызды теорема.

> **Теорема (ҚҚТ):** Егер $n = n1 * n2 * ... * nk$ және **ni** өзара жай сандар болса, онда $x \equiv ai \mod ni$ жүйесінің шешімі бар.

Бұл теорема криптография, кодтау және информатика салаларында кеңінен қолданылады.

Ұсынылатын әдебиеттер тізімі

- 1. Гольдвассер С., Беллар М. Достижения в криптологии / Гольдвассер С. – М.: Триумф, 2016. – 513 с.
- 2. Шнайер, Брюс. Криптографическая методы защиты информации, 26-я ежегодная международная конференция по криптологии, Санта-Барбара, Калифорния, США, 20–24 августа 2022 г.
- 3. Фергюсон Н., Шнайер Б., Коно Т. Криптографическая инженерия: принципы проектирования и практическое применение. / Фергюсон Н. – М.: Пресс, 2022. – 416 с.