نظریه اطلاعات

- میزان اطلاعات در هر پیام
  - حداقل تعداد بیت‌های مورد نیاز برای کدگذاری همه معانی آن پیام
  - مثال
    - خصیصه روز هفته در یک پایگاه داده
      - کدگذاری اطلاعات
        - شنبه ← 000
        - یک‌شنبه ← 001
        - دوشنبه ← 010
        - ...
      - میزان اطلاعات
        - سه بیت

نظریه اطلاعات

- آنتروپی (Entropy)
  - معیاری برای اندازه‌گیری میزان اطلاعات در هر پیام
  - با فرض این که تعداد معانی ممکن پیام M برابر با n باشد
    - آنتروپی پیام M
      - $\log_2 n$
  - مثال
    - آنتروپی یک پیام که جنسیت را نمایش می‌دهد
      - $\log_2 2 = 1$
    - آنتروپی یک پیام که روز هفته را نمایش می‌دهد
      - $\log_2 7 = 2.81$

نظریه اعداد

- با فرض این که a یک عدد صحیح و n یک عدد صحیح مثبت باشد
  - نماد $a \bmod n$
    - باقی‌مانده a در تقسیم بر n
      - عدد صحیح n
        - پیمانه
- دو عدد صحیح a و b همنهشت به پیمانه n نامیده می‌شوند اگر

$$(a \bmod n) = (b \bmod n)$$

  - نمایش همنهشتی
    - $a \equiv b \pmod{n}$

نظریه اعداد

- مثال
  - $21 \bmod 10 = -9 \bmod 10$
  - $21 \equiv -9 \pmod{10}$
- مجموعه اعداد صحیح از 0 تا $n-1$
  - مجموعه کامل باقی‌مانده‌ها به پیمانه n
- با فرض این که a و b دو عدد صحیح بوده و b صفر نباشد
  - b یک مقسوم علیه a نامیده می‌شود اگر عدد صحیحی مانند m وجود داشته باشد به گونه‌ای که $a = mb$

نظریه اعداد

- ویژگی‌های همنهشتی

$$\text{if } a \equiv b \pmod{n} \text{ then } b \equiv a \pmod{n}$$

$$\text{if } a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n} \text{ then } a \equiv c \pmod{n}$$

- عملیات حساب پیمانه‌ای

$$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$

$$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$

$$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

  - مثال

$$(11 \times 15) \bmod 8 = [(11 \bmod 8) \times (15 \bmod 8)] \bmod 8$$

نظریه اعداد

- مثال
  - $11^7 \bmod 13$

$$11^7 \bmod 13 = [(11 \bmod 13) \times (11^2 \bmod 13) \times (11^4 \bmod 13)] \bmod 13$$

$$11 \bmod 13 = 11$$

$$11^2 \bmod 13 = 121 \bmod 13 = 4$$

$$11^4 \bmod 13 = (11^2)^2 \bmod 13 = 4^2 \bmod 13 = 3$$

$$11^7 \bmod 13 = (11 \times 4 \times 3) \bmod 13 = 132 \bmod 13 = 2$$

نظریه اعداد

- ویژگی‌های حساب پیمانه‌ای
  - با فرض این که Z_n مجموعه اعداد صحیح غیرمنفی کوچک‌تر از n باشد

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

    - مجموعه کامل باقی‌مانده‌ها یا کلاس‌های باقی‌مانده به پیمانه n
  - قوانین

$$\text{if}\ \ (a+b) \equiv (a+c) \pmod{n}\ \ \text{then}\ \ b \equiv c \pmod{n}$$

    - با فرض این که $\gcd(a,n) = 1$

$$\text{if}\ \ (a \times b) \equiv (a \times c) \pmod{n}\ \ \text{then}\ \ b \equiv c \pmod{n}$$

    - مثال

$$(5+23) \equiv (5+7) \pmod{8}$$

$$23 \equiv 7 \pmod{8}$$

نظریه اعداد

- بزرگترین مقسوم علیه مشترک
  - عدد صحیح c بزرگترین مقسوم علیه مشترک اعداد صحیح a و b نامیده می‌شود اگر
    - c مقسوم علیه a و b باشد
    - هر مقسوم علیه a و b مقسوم علیه c باشد
  - نمایش بزرگترین مقسوم علیه مشترک a و b
    - $\gcd(a,b)$
  - ویژگی

$$\gcd(a,b)=\gcd(a,-b)=\gcd(-a,b)$$
$$=\gcd(-a,-b)=\gcd(|a|,|b|)$$

نظریه اعداد

- یافتن بزرگترین مقسوم علیه مشترک
  - با فرض این که a یک عدد صحیح غیرمنفی و b یک عدد صحیح مثبت باشد

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

  - الگوریتم اقلیدس

$$
\begin{array}{l}
\textbf{Euclid } (a,b) \\
1. \quad A \leftarrow a, B \leftarrow b \\
2. \quad \text{if } B = 0 \text{ return } A = \gcd(a,b) \\
3. \quad R = A \bmod B \\
4. \quad A \leftarrow B \\
5. \quad B \leftarrow R \\
6. \quad \text{goto } 2
\end{array}
$$

نظریه اعداد

- مثال

$$\begin{aligned}\mathbf{gcd}(\mathbf{55},\mathbf{22}) &= \mathbf{gcd}(\mathbf{22},\mathbf{55}\ \mathbf{mod}\ \mathbf{22}) = \mathbf{gcd}(\mathbf{22},\mathbf{11})\\ &= \mathbf{gcd}(\mathbf{11},\mathbf{22}\ \mathbf{mod}\ \mathbf{11}) = \mathbf{gcd}(\mathbf{11},\mathbf{0})\\ &= \mathbf{11}\end{aligned}$$

نظریه اعداد

- اعداد اول
  - عدد صحیح $p > 1$ اول نامیده می‌شود اگر و فقط اگر تنها مقسوم علیه‌های آن 1 و خودش باشد
  - هر عدد صحیح a را می‌توان به صورت حاصل ضرب اعداد اول نوشت
    - تجزیه به عوامل اول

$$a = \prod_{p \in P} p^{a_p}$$

  - مثال
    - $91 = 7 \times 13$
    - $3600 = 24 \times 32 \times 52$

نظریه اعداد

- **اعداد نسبت به هم اول**
  - **دو عدد صحیح a و b نسبت به هم اول نامیده می‌شوند اگر بزرگ‌ترین مقسوم علیه مشترک آن‌ها 1 باشد**

$$\gcd(a,b)=1$$

- **قضیه فرما (Fermat's Theorem)**
  - **با فرض این که p یک عدد اول، a یک عدد صحیح مثبت و $\gcd(a,p)=1$ باشد**

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

  - **با فرض این که p یک عدد اول و a یک عدد صحیح مثبت باشد**

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

نظریه اعداد

- تابع کامل اویلر $\varphi(n)$ (Euler's Totient Function)
  - تعداد اعداد صحیح مثبت کم‌تر از n که نسبت به n اول هستند
  - مثال
    - $\varphi(10) = 4$
  - با فرض این که p یک عدد اول باشد

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

  - با فرض این که p و q اعداد اول باشند

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

  - مثال
    - $\varphi(21) = (3-1)(7-1) = 2 \times 6 = 12$

نظریه اعداد

- با فرض این که n به عوامل اول خود تجزیه شده باشد

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_m^{e_m}$$

  - محاسبه تابع کامل اویلر

$$\varphi(n) = \prod_{i=1}^{m} (p_i^{e_i} - p_i^{e_i - 1})$$

- مثال
  - با فرض این که $n = 240$

$$n = 240 = 16 \cdot 15 = 2^4 \cdot 3 \cdot 5$$

$$\varphi(240) = (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0)$$
$$= 8 \cdot 2 \cdot 4 = 64$$

نظریه اعداد

- قضیه اویلر (Euler's Theorem)
  - با فرض این که $\gcd(a,n) = 1$

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

  - مثال
    - با فرض این که $a = 3$ و $n = 10$
      - $\varphi(10) = 4$
      - $3^4 \equiv 1 \pmod{10}$
    - با فرض این که $a = 2$ و $n = 11$
      - $\varphi(11) = 10$
      - $2^{10} \equiv 1 \pmod{11}$

نظریه اعداد

- معکوس ضربی پیمانه‌ای
  - معکوس ضربی عدد صحیح a به پیمانه n یک عدد صحیح مانند x است به گونه‌ای که $a \times x \equiv 1 \pmod{n}$
  - نمایش معکوس ضربی عدد صحیح a
    - a^{-1}
  - عدد صحیح a به پیمانه n دارای معکوس ضربی است اگر و فقط اگر a و n نسبت به هم اول باشند
  - مثال
    - معکوس ضربی عدد صحیح 3 به پیمانه 7
      - 5

نظریه اعداد

- محاسبه معکوس ضربی پیمانه‌ای با استفاده از قضیه اویلر
  - با فرض این که $\gcd(a,n) = 1$

$$a^{\varphi(n)} \bmod n = 1$$
$$x = a^{\varphi(n)-1} \bmod n$$

- مثال
  - معکوس ضربی عدد صحیح 3 به پیمانه 7

$$\varphi(7) = 6$$
$$\begin{aligned} x &= 3^{6-1} \bmod 7 \\ &= 3^5 \bmod 7 \\ &= 5 \end{aligned}$$

نظریه اعداد

- مولدها (Generators)
  - عدد صحیح g یک مولد به پیمانه p است اگر برای هر b از 1 تا $p-1$ عدد صحیحی مانند a وجود داشته باشد به گونه‌ای که

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

  - مثال
    - عدد صحیح 3 یک مولد به پیمانه 7 است

$$3^6 = 729 \equiv 1 \pmod{7}$$
$$3^2 = 9 \equiv 2 \pmod{7}$$
$$3^1 = 3 \equiv 3 \pmod{7}$$
$$3^4 = 81 \equiv 4 \pmod{7}$$
$$3^5 = 243 \equiv 5 \pmod{7}$$
$$3^3 = 27 \equiv 6 \pmod{7}$$

نظریه اعداد

- قضیه باقی‌مانده چینی (Chinese Remainder Theorem)
  - با فرض این که اعداد صحیح n_1 تا n_k دو به دو نسبت به هم اول باشند
    - تنها یک عدد صحیح مثبت کوچک‌تر از $n = n_1 \times \cdots \times n_k$ وجود دارد که در دستگاه معادلات زیر صدق می‌کند

$$\begin{gathered} x \bmod n_1 = a_1 \\ x \bmod n_2 = a_2 \\ \cdots \\ x \bmod n_k = a_k \end{gathered}$$

  - هر عدد صحیح را می‌توان از روی باقی‌مانده‌هایش به پیمانه یک مجموعه از اعداد صحیح دو به دو نسبت به هم اول شناسایی کرد

نظریه اعداد

- مثال
  - با فرض این که

$$x \bmod 3 = 2$$
$$x \bmod 5 = 4$$

  - تنها یک عدد صحیح کوچک‌تر از $3 \times 5 = 15$ وجود دارد که دارای باقی‌مانده‌های فوق است
    - $x = 14$
  - هر جواب دیگر برای دستگاه معادلات فوق به پیمانه 15 با 14 همنهشت است
    - $x = 29$
    - $x = 44$

نظریه اعداد

- حل دستگاه معادلات
  - با فرض این که

$$m_i = n/n_i \text{, for } 1 \le i \le k$$

$$c_i = m_i \times (m_i^{-1} \bmod n_i) \text{, for } 1 \le i \le k$$

  - m_i نسبت به n_i اول است
    - m_i دارای معکوس ضربی به پیمانه n_i است
  - محاسبه مقدار x

$$x \equiv \left(\sum_{i=1}^{k} a_i c_i\right) \pmod n$$

نظریه اعداد

- **مثال**
  - **با استفاده از قضیه باقی‌مانده چینی مقدار x را محاسبه کنید**

$$x \bmod 3 = 2$$

$$x \bmod 5 = 4$$

  - **جواب**

$$n_1 = 3$$
$$n_2 = 5$$

$$m_1 = 15/3 = 5$$
$$m_2 = 15/5 = 3$$

$$m_1^{-1} = 2 \bmod 3$$
$$m_2^{-1} = 2 \bmod 5$$

$$x = (2 \times 5 \times 2 + 4 \times 3 \times 2) \bmod 15 = 14$$