

1. BÖLÜM: İNTERPOLASYON

1) x 'in 1, 2, 3, 4 değerleri için $f(x) = \sqrt{x}$ fonksiyonu verilmiştir.

a) Lagrange İnterpolasyon polinomunu bulunuz.

b) Newton İnterpolasyon polinomunu bulunuz.

c) $x=5$ için İnterpolasyon hatasını bulunuz.

Çözüm.1.1:a)

$$P_3(x) = 1 \cdot \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 2 \cdot \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} \\ + 3 \cdot \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} + 4 \cdot \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}$$

b)

x	y	Δy	$\Delta^2 y$	$\Delta^3 y$
1	<u>1.0000</u>	<u>0.4142</u>		
2	1.4142	0.3178	<u>-0.0964</u>	
3	1.7321	0.2679	-0.0499	<u>0.0465</u>
4	2.0000			

Bu tabloda a_n değerleri altı çizili farklar olup;

$$P_3(x) = a_0 + a_1(x-1) + a_2(x-1)(x-2) + a_3(x-1)(x-2)(x-3)$$

$a_0 = y_0 = 1.0000$ ve $h = 1$ ise;

$$a_1 = \frac{\Delta y_0}{h} = 0.4142$$

$$a_2 = \frac{\Delta^2 y_0}{2! h^2} = \frac{-0.0964}{2}$$

$$a_3 = \frac{\Delta^3 y_0}{3! h^3} = \frac{0.0465}{3!}$$

$$P_3(x) = 1.0000 + 0.4142(x-1) - \frac{0.0964}{2}(x-1)(x-2) \\ + \frac{0.0465}{6}(x-1)(x-2)(x-3)$$

c)

$$|R_3(5)| \leq M_4(1; 5) \frac{|A_4(5)|}{4!},$$

$$A_4(5) = (5-1)(5-2)(5-3)(5-4) = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$f'(x) = \frac{1}{2}x^{-\frac{1}{2}}, f''(x) = -\frac{1}{4}x^{-\frac{3}{2}}, f'''(x) = \frac{3}{8}x^{-\frac{5}{2}}, f^{(iv)}(x) = -\frac{15}{16}x^{-\frac{7}{2}}$$

$$M_4(1; 5) = \max_{[1,5]} |f^{(iv)}(x)| = \frac{15}{16}$$

$$|R_3(5)| \leq \frac{15}{16} \cdot \frac{24}{4!} = \frac{15}{16} \cdot \frac{24}{24} = \frac{15}{16} = 0.9375$$

2) x'in 5, 6, 7, 8 değerleri için $f(x) = 2^x$ fonksiyonu verilmiştir.

a) Lagrange İnterpolasyon polinomunu bulunuz.

b) Newton İnterpolasyon polinomunu bulunuz.

c) x=2 için İnterpolasyon hatasını bulunuz.

Çözüm.1.2:a)

$$P_3(x) = 32 \cdot \frac{(x-6)(x-7)(x-8)}{(5-6)(5-7)(5-8)} + 64 \cdot \frac{(x-5)(x-7)(x-8)}{(6-5)(6-7)(6-8)} \\ + 128 \cdot \frac{(x-5)(x-6)(x-8)}{(7-5)(7-6)(7-8)} + 256 \cdot \frac{(x-5)(x-6)(x-7)}{(8-5)(8-6)(8-7)}$$

b)

x	y	Δy	$\Delta^2 y$	$\Delta^3 y$
5	<u>32</u>	<u>32</u>		
6	64	64	<u>32</u>	
7	128	128	64	<u>32</u>
8	256			

Bu tabloda a_n değerleri altı çizili farklar olup;

$$P_3(x) = a_0 + a_1(x-5) + a_2(x-5)(x-6) + a_3(x-5)(x-6)(x-7)$$

$$a_0 = 32$$

$$a_1 = \frac{\Delta y_0}{1} = 32$$

$$a_2 = \frac{\Delta^2 y_0}{2!} = 32$$

$$a_3 = \frac{\Delta^3 y_0}{3!} = 32$$

$$P_3(x) = 32 + 32(x-5) + 16(x-5)(x-6) + \frac{32}{6}(x-5)(x-6)(x-7)$$

c)

$$|R_3(2)| \leq M_4(2; 8) \frac{|A_4(2)|}{4!}, A_4(2) = (2-5)(2-6)(2-7)(2-8) = (-3)(-4)(-5)(-6) = 360$$

$$f^{(k)}(x) = (\ln 2)^k 2^x, \text{ türev kuralından ötürü } f^{(iv)}(x) = (\ln 2)^4 2^x$$

$$M_4(2; 8) = \max_{[2,8]} |f^{(iv)}(x)| = (\ln 2)^4 2^8 = 256(\ln 2)^4$$

$$|R_3(2)| \leq 256(\ln 2)^4 \cdot 15 = 3840(\ln 2)^4$$

$$\text{Hata} = (\ln 2)^4 \approx 0.2308 \Rightarrow |R_3(2)| \lesssim 3840 \cdot 0.2308 \approx 886$$

2. BÖLÜM: RSA ŞİFRELEME

1) $p = 3, q = 11, e = 3, x = 5$ için şifreli metin nedir?

Çözüm: Modül: $n = 3 \cdot 11 = 33$

$$Z: Z(n) = (3-1)(11-1) = 2 \cdot 10 = 20$$

$$\text{Denklem: } d \cdot e \equiv 1 \pmod{z(n)}$$

$$d \cdot 3 \equiv 1 \pmod{20}$$

3 ile neyi çarparsam 20'ye bölümünden kalan 1 olur?

$$3 \cdot 7 = 21 \quad 21 \pmod{20} = 1 \quad (d): 7$$

Şifreleme: Formül: $y \equiv x^e \pmod{n}$

$$y \equiv 5^3 \pmod{33}$$

$$5^3 = 125$$

$$125 \pmod{33} \quad 125 = 3 \cdot 33 + 26 \Rightarrow y = 26$$

d'yi Kullanarak Geri Çözme: $x = y^d \pmod{n}$

$$x = 26^7 \pmod{33}$$

Hesap Kolaylığı (Üsleri

parçalayalım):

$$26^2 = 676 \pmod{33} = 16$$

$$26^4 = (26^2)^2 = 16^2 =$$

$$256 \pmod{33} = 25$$

$$26^7 = 26^4 \cdot 26^2 \cdot 26^1$$

$$26^7 = 25 \cdot 16 \cdot 26 \pmod{33}$$

$$25 \cdot 16 = 400 \pmod{33} = 4$$

$$\text{Kalan İşlem: } 4 \cdot 26 = 104$$

$$104 \pmod{33} = 5$$

Doğru! 5 sayısına geri döndük.

2) $p = 3, q = 5, e = 7, x = 2$ için şifreli metin nedir?

Çözüm: Modül: $n = 3 \cdot 5 = 15$

$$Z: Z(n) = (3 - 1)(11 - 1) = 2 \cdot 10 = 20$$

$$\text{Denklem: } d \cdot e \equiv 1 \pmod{Z(n)}$$

$$d \cdot 7 \equiv 1 \pmod{8}$$

7 ile neyi çarparsam 8'e bölümünden kalan 1 olur?

$$7 \cdot 7 = 49 \quad 49 \pmod{8} = 1 \quad (d) = 7$$

Şifreleme: Formül: $y \equiv x^e \pmod{n}$

$$y = 2^7 \pmod{15}$$

$$2^4 = 16 \cdot 16 \equiv 1 \pmod{15}$$

$$2^7 = 2^4 \cdot 2^3$$

$$2^7 = 1 \cdot 8 \pmod{15} \quad (d) = 8$$

d'yi Kullanarak Geri Çözme: $x \equiv y^d \pmod{n}$

$$x \equiv 8^7 \pmod{15}$$

Hesap Kolaylığı (Üsleri parçalayalım):

$$8^2 = 64 \cdot 64 \pmod{15}$$

$$8^4 = (8^2)^2 = 4^2 = 16 \equiv 1 \pmod{15}$$

$$8^7 = 8^4 \cdot 8^2 \cdot 8^1$$

$$8^7 = 1 \cdot 4 \cdot 8 \pmod{15}$$

$$4 \cdot 8 = 32$$

$$32 \pmod{15} = 2$$

Doğru! 2 sayısına geri döndük.

3. BÖLÜM: ÇİN KALAN TEOREMİ

- 1) 2'ye bölündüğünde 1, 5'e bölündüğünde 2, 7'ye bölündüğünde 3 kalanını veren x sayısı kaçtır

Çözüm: $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}$

Adım 1: M değerini bulalım $\rightarrow M=2.5.7=70$

Adım 2: m_k ve terslerini (y_k) bulalım.

$$m_1 = \frac{70}{2} = 35 \quad 35.y_1 \equiv 1 \pmod{2} \Rightarrow 1.y_1 \equiv 1 \Rightarrow y_1 = 1$$

$$m_2 = \frac{70}{5} = 14 \quad 14.y_2 \equiv 1 \pmod{5} \Rightarrow 4.y_2 \equiv 1 \Rightarrow y_2 = 4$$

$$m_3 = \frac{70}{7} = 10 \quad 10.y_3 \equiv 1 \pmod{7} \Rightarrow 3.y_3 \equiv 1 \Rightarrow y_3 = 5$$

Adım 3: Genel Çözüm: $x = \sum (a_k.y_k.m_k) \pmod{M} \rightarrow$

$$x = (1.35.1) + (2.14.4) + (3.10.5)$$

$$x = 35 + 112 + 150 \Rightarrow x = 297$$

Mod 70'e göre sadeleştirme: $297 = 4.70 + 17$ sonuç : $x = 17$

- 2) 2'ye bölündüğünde 1, 3'e bölündüğünde 2, 5'e bölündüğünde 4 kalanını veren x sayısı kaçtır?

Çözüm: $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 4 \pmod{5}$

Adım 1: M değerini bulalım $\rightarrow M=2.3.5=30$

Adım 2: m_k ' e terslerini ve (y_k) bulalım.

$$m_1 = \frac{30}{2} = 15 \rightarrow 15.y_1 \equiv 1 \pmod{2} \Rightarrow 1.y_1 \equiv 1 \Rightarrow y_1 = 1$$

$$m_2 = \frac{30}{3} = 10 \rightarrow 10.y_2 \equiv 1 \pmod{3} \Rightarrow 1.y_2 \equiv 1 \Rightarrow y_2 = 1$$

$$m_3 = \frac{30}{5} = 6 \rightarrow 6.y_3 \equiv 1 \pmod{5} \Rightarrow 1.y_3 \equiv 1 \Rightarrow y_3 = 1$$

Adım 4: Genel çözüm: $x = \sum (a_k.y_k.m_k) \pmod{M} \rightarrow x = (1.15.1) +$

$$(2.10.1) + (4.6.1) \quad x = 15 + 20 + 24 = 59 \quad x = 59$$

Mod 30'e göre sadeleştirme: $x = 29$ Sonuç: $x = 29$

4. BÖLÜM: REKÜRANS BAĞINTILARI

- 1) $a_n = 3a_{n-1} - 2a_{n-2}$ ve $a_0 = 3, a_1 = 4$ olan bağıntıyı bulup a_7 'yi hesaplayınız.

Çözüm: Karakteristik denklem: $r^2 - 3r + 2 = 0$ $(r - 2)(r - 1) = 0 \Rightarrow r_1 = 1, r_2 = 2$

$$\text{Genel çözüm: } a_n = c_1(1)^n + c_2(2)^n = c_1 + c_2 2^n$$

Katsayıları Bulma:

$$n = 0: c_1 + c_2 = 3$$

$$n = 1: c_1 + 2c_2 = 4$$

$$\text{Taraf tarafa çıkarma: } c_2 = 1, \text{ buradan } c_1 = 2$$

$$\text{Özel Çözüm: } a_n = 2 + 2^n$$

$$\text{Sonuç}(a_7): a_7 = 2 + 2^7 = 2 + 128 = 130$$

- 2) $a_n = 6a_{n-1} - 9a_{n-2}$ ve $a_0 = 2, a_1 = 9$ olan bağıntıyı bulup a_9 'u hesaplayınız.

Çözüm: Karakteristik denklem:

$$r^2 - 6r + 9 = 0 \Rightarrow (r - 3)^2 = 0 \text{ Çakışık kök var: } r_1 = r_2 = 3$$

$$\text{Genel Çözüm (Çakışık Kök): } a_n = 3^n(c_1 + c_2 n)$$

Katsayılar:

$$n = 0: 3^0(c_1) = 2 \Rightarrow c_1 = 2$$

$$n = 1: 3^1(2 + c_2) = 9 \Rightarrow 3(2 + c_2) = 9 \Rightarrow 2 + c_2 = 3 \Rightarrow c_2 = 1$$

$$\text{Özel Çözüm: } a_n = 3^n(2 + n)$$

$$\text{Sonuç } (a_9): a_9 = 3^9(2 + 9) = 11 \cdot 3^9 = 11 \cdot 19683 = 216.513$$

