Discussion 3: Asymptotic Notation and Number Theory

- Asymptotic Notation
- Modular Arithmetic

Asymptotic Notation

Exponent rules

$$a^{x+y} = a^x \cdot a^y$$

$$a^{x-y} = \frac{a^x}{a^y}$$

$$a^{x \cdot y} = (a^x)^y$$

$$(a \cdot b)^x = a^x \cdot b^x$$

$$\left(\frac{a}{b}\right)^x = \frac{a^x}{b^x}$$

$$a^{-x} = \frac{1}{a^x}$$

Logarithm rules

$$\log_b(x \cdot y) = \log_b x + \log_b y$$

$$\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y$$

$$\log_b(x^y) = y \log_b x$$

$$\log_a x = \frac{\log_b x}{\log_b a}$$

Asymptotic Notation

1. Determine the asymptotic value using Θ notation for the following functions:

a. $n^3 + 2n^2 \log n + 16$

b. $\dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n$

c. $394n^2 + n^5 + 6n - 11$

d. $n^4 \log n + 8n^3 \log^5 n + 10n^3$

e. $n^6 2^n + 3^n + 43n^{11}$

f. $4n^2 \log n - n \log^2 n - 1$

g. $\dfrac{3}{n} + n^{-3} + \dfrac{2}{\log n}$

Asymptotic Notation

a. $f(n) = n^3 + 2n^2 \log n + 16$

Asymptotic Notation

a. $f(n) = n^3 + 2n^2 \log n + 16$

We have $n^3 + 2n^2 \log n + 16 \leq n^3 + 2\,n^2 \cdot n + 16\,n^3 = 19\,n^3$ for $n \geq 1$

Asymptotic Notation

a. $f(n) = n^3 + 2n^2 \log n + 16$

We have $n^3 + 2n^2 \log n + 16 \leq n^3 + 2\,n^2 \cdot n + 16\,n^3 = 19\,n^3$ for $n \geq 1$

We also have $n^3 + 2n^2 \log n + 16 \geq n^3$ for $n \geq 1$

Asymptotic Notation

a. $f(n) = n^3 + 2n^2 \log n + 16$

We have $n^3 + 2n^2 \log n + 16 \leq n^3 + 2\,n^2 \cdot n + 16\,n^3 = 19\,n^3$ for $n \geq 1$

We also have $n^3 + 2n^2 \log n + 16 \geq n^3$ for $n \geq 1$

Pick $c_1 = 1,\ c_2 = 19,\ n_0 = \max(1,1) = 1$

We have: $n^3 \leq f(n) \leq 19\,n^3$ for $n \geq 1 \Rightarrow f(n) = \Theta(n^3)$

Asymptotic Notation

b. $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n$

We have: $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n = n^2\sqrt{n} + 2n^2 \log^2 n$

Asymptotic Notation

b. $f(n) = \frac{n^3}{\sqrt{n}} + 2n^2 \log^2 n$

We have: $f(n) = \frac{n^3}{\sqrt{n}} + 2n^2 \log^2 n = n^2\sqrt{n} + 2n^2 \log^2 n$

Let show that: $f(n) = O(n^2\sqrt{n})$

Asymptotic Notation

b. $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n$

We have: $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n = n^2\sqrt{n} + 2n^2 \log^2 n$

Let show that: $f(n) = O(n^2\sqrt{n})$

We have:

$$
\begin{aligned}
f(n) &= n^2\sqrt{n} + 2n^2 \log^2 n \\
&= O(n^2\sqrt{n}) + n^2 \cdot O(\sqrt{n}) \quad \text{because } \log^2 n = O(n^{0.5}) \\
&= O(n^2\sqrt{n})
\end{aligned}
$$

Asymptotic Notation

b. $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n$

We have: $f(n) = \dfrac{n^3}{\sqrt{n}} + 2n^2 \log^2 n = n^2\sqrt{n} + 2n^2 \log^2 n$

Let show that: $f(n) = O(n^2\sqrt{n})$

We have:

$$
\begin{aligned}
f(n) &= n^2\sqrt{n} + 2n^2 \log^2 n \\
&= O(n^2\sqrt{n}) + n^2 \cdot O(\sqrt{n}) \quad \text{because } \log^2 n = O(n^{0.5}) \\
&= O(n^2\sqrt{n})
\end{aligned}
$$

We also have: $n^2\sqrt{n} + 2n^2 \log^2 n \geq n^2\sqrt{n}$ for $n \geq 1 \Rightarrow f(n) = \Omega(n^2\sqrt{n})$

Conclusion $f(n) = \Theta(n^2\sqrt{n})$

Asymptotic Notation

c. $394n^2 + n^5 + 6n - 11$

d. $n^4 \log n + 8n^3 \log^5 n + 10n^3$

e. $n^6 2^n + 3^n + 43n^{11}$

f. $4n^2 \log n - n \log^2 n - 1$

g. $\dfrac{3}{n} + n^{-3} + \dfrac{2}{\log n}$

Asymptotic Notation

c. $394n^2 + n^5 + 6n - 11$ c. $\Theta(n^5)$

d. $n^4 \log n + 8n^3 \log^5 n + 10n^3$ d. $\Theta(n^4 \log n)$

e. $n^6 2^n + 3^n + 43n^{11}$ e. $\Theta(3^n)$

f. $4n^2 \log n - n \log^2 n - 1$ f. $\Theta(n^2 \log n)$

g. $\dfrac{3}{n} + n^{-3} + \dfrac{2}{\log n}$ g. $\Theta\left(\dfrac{1}{\log n}\right)$

Modular Arithmetic

Rules:

- $(a \pm b) \text{ rem } m \equiv (a \text{ rem } m \pm b \text{ rem } m) \pmod{m}$
- $(a \cdot b) \text{ rem } m \equiv (a \text{ rem } m \cdot b \text{ rem } m) \pmod{m}$
- $a^b \text{ rem } m \equiv (a \text{ rem } m)^b \pmod{m}$

Modular Arithmetic

1. Compute:

a. $(699 + 997)$ rem 3

b. 28^4 rem 13

Modular Arithmetic

1. Compute:

a. $(699 + 997) \text{ rem } 3$

b. $28^4 \text{ rem } 13$

a. $(699 + 997) \text{ rem } 3 \equiv (699 \text{ rem } 3 + 997 \text{ rem } 3) \equiv 1 \pmod 3$

Modular Arithmetic

1. Compute:

a. $(699 + 997)$ rem 3

b. 28^4 rem 13

a. $(699 + 997)$ rem $3 \equiv (699$ rem $3 + 997$ rem $3) \equiv 1 \pmod 3$

b. 28^4 rem $13 \equiv (28$ rem $13)^4$

$\equiv 2^4 \equiv 3 \pmod{13}$

Modular Arithmetic: Squaring Method

2. Compute 5^{117} rem 19

$$
\begin{aligned}
5^{117} &\equiv 5 \cdot (5^2)^{58} \\
&\equiv 5 \cdot (25 \text{ rem } 19)^{58} \quad \equiv 5 \cdot 6^{58} \\
&\equiv 5 \cdot (6^2)^{29} \quad \equiv 5 \cdot (17)^{29} \\
&\equiv 5 \cdot 17 \cdot (17^2)^{14} \quad \equiv 9 \cdot (4)^{14} \\
&\equiv 9 \cdot (4^2)^{7} \quad \equiv 9 \cdot 16 \cdot (16^2)^{3} \\
&\equiv 11 \cdot 9 \cdot 9^2 \quad \equiv 4 \cdot 5 \\
&\equiv 1 \pmod{19}
\end{aligned}
$$

Modular Arithmetic: Inverse

3. Find $2^{-1} \pmod 6$

Modular Arithmetic: Inverse

3. Find $2^{-1} \pmod{6}$

Since gcd$(2,6) = 2 \neq 1$, $2^{-1} \pmod{6}$ does not exist.

Modular Arithmetic: Inverse

4. Find $3^{-1} \pmod{7}$

Modular Arithmetic: Inverse

4. Find $3^{-1} \pmod 7$

$3^{-1} \pmod 7$ exists because gcd$(3,7) = 1$

We need to find α, β such that: $\alpha \cdot 3 + \beta \cdot 7 = 1$

Modular Arithmetic: Inverse

4. Find $3^{-1} \pmod{7}$

$3^{-1} \pmod{7}$ exists because gcd$(3,7) = 1$

We need to find α, β such that: $\alpha \cdot 3 + \beta \cdot 7 = 1$

multiples of 3	3	6	9	12	15
multiples of 7	7	14			

Modular Arithmetic: Inverse

4. Find $3^{-1} \pmod 7$

$3^{-1} \pmod 7$ exists because gcd$(3,7) = 1$

We need to find α, β such that: $\alpha \cdot 3 + \beta \cdot 7 = 1$

multiples of 3	3	6	9	12	15
multiples of 7	7	14			

So $\alpha = 5, \beta = -2 : \ 5 \cdot 3 + (-2) \cdot 7 = 1$

And this gives us that $3^{-1} \pmod 7 = 5.$

Linear Congruences

5. Solve $3x \equiv 4 \mod 7$

Linear Congruences

5. Solve $3x \equiv 4 \mod 7$

$$\implies 3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4 \mod 7$$
$$\implies x \equiv 3^{-1} \cdot 4 \mod 7$$

Linear Congruences

5. Solve $3x \equiv 4 \mod 7$

$$\implies 3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4 \mod 7$$
$$\implies x \equiv 3^{-1} \cdot 4 \mod 7$$

We have (from previous example): $3^{-1} \equiv 5 \mod 7$

$$\implies x \equiv 5 \cdot 4 \equiv 6 \mod 7$$