CS5070 Mathematical Structures for Computer Science - Notes 7

José Garrido

Department of Computer Science
College of Computing and Software Engineering
Kennesaw State University

jgarrido@kennesaw.edu

Nov. 2021

Generating Functions (Chapter 5)

- A function that encodes a sequence as a series of coefficients
- For example: $2 + 3x + 5x^2 + 8x^3 + 12x^4 + \dots$
- An infinite power series is an infinite sum of terms of the form $c_n x^n$, where c_n is some constant
- Another way to denote this series is:

$$\sum_{k=0}^{\infty} c_k x^k$$

In expanded form:

$$c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + \cdots$$

The power series is known as a *generating series*.

More on Generating Functions

- The generating series produces the sequence of coefficients of the infinite polynomial.

$$c_0, c_1, c_2, c_3, c_4, c_5, \ldots$$

- The power series $1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \cdots + \frac{x^n}{n!} + \cdots$ converges to the function e^x
- This is the Taylor series for e^x.
- The generating series for $1, 1, 1, 1, 1, \ldots$ is $1 + x + x^2 + x^3 + x^4 + \cdots$
- To find the closed formula for this series, note that it is a *geometric series* with common ratio x.

$$1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1 - x}$$

Generating More Sequences

$$\frac{1}{1+x} = 1 - x + x^2 - x_3 + \cdots$$

generates $1, -1, 1, -1$

$$\frac{1}{1-3x} = 1 + 3x + 9x^2 + 27x^3 + \cdots$$

generates $1, 3, 9, 27, \ldots$

$$\frac{3}{1-3x} = 3 \times 1 + 3 \times 3x + 3 \times 9x^2 + 3 \times 27x^3 + \cdots$$

generates $3, 9, 27, 81, \ldots$

More Complex Series

Adding the sequences $1, 1, 1, 1, 1 \ldots$ and $1, 3, 9, 27, \ldots$

$$\begin{aligned}
2+4x+10x^2+28x^3+\cdots &= (1+1)+(1+3)x+(1+9)x^2+(1+27)x^3+\cdots \\
&= 1+x+x^2+x^3+\cdots+1+3x+9x^2+27x^3+\cdots \\
&= \frac{1}{1-x}+\frac{1}{1-3x}
\end{aligned}$$

Number Theory

- With integer numbers, the possible operations are addition, subtraction, multiplication.
- Division is possible with rational numbers
- For $a \div b$ or b *divides* a, we can use the notation $b|a$. If this results in a whole number, then b is a divisor or factor of a, and a is a multiple of b.
- if $b|a$ then $a = bk$ for some integer k
- **The Divisibility Relation**. For integers m and n, $m|n$ holds provided $n \div m$ results in an integer
- $m|n$ is a statement, it is true or false.

Division Algorithm

- Given any two integers a and b, there is an integer q such that

$$a = qb + r$$

  where r is an integer satisfying $0 \leq r < |b|$
- A large enough multiple of b would produce a *remainder* r as small as possible (including $r = 0$)
- There are only b possible remainders when dividing by b.
- Grouping integers by the remainder. Each group is known as a *remainder class modulo b* or *residue class*

Congruence Module n

- We say a is **congruent to** b **modulo** n

$$a \equiv b \pmod{n}$$

  provided a and b have the same remainder when divided by n

- **Congruence and Divisibility**. For any integers a, b, and n

  $a \equiv b \pmod{n}$, if and only if $n | a - b$

- This holds if and only if $a - b = kn$ for some integer k, and $a = b + kn$
- So, a and b are congruent modulo n

Congruence and Equality

- For any integers a, b, and n

  $a \equiv b \pmod{n}$ if and only if $a = b + bk$ for some integer k

- **Properties of Congruence**.
  Congruence Modulo n is an Equivalence Relation
  Given any integers a, b, and c, and any positive integer n:

  $a \equiv a \pmod{n}$

  If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$

  If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

  Thus, congruence modulo n is reflexive, symmetric, and transitive, so is an equivalence relation

Congruence and Arithmetic

For $a \equiv b \pmod{n}$ and $c \equiv d$ (mod n, then:

$a + c \equiv b + d \pmod{n}$

$a - c \equiv b - d \pmod{n}$

$ac \equiv bd \pmod{n}$

- We can replace any number in a congruence with any other number it is congruent to
- Any number is congruent to the sum of its digits, module 9.

Congruence and Division

- For $ad \equiv bd \pmod{n}$, then

$$a \equiv b \ (\bmod \frac{n}{\gcd(d, n)})$$

- If d and n have no common factors then

  $\gcd(d, n) = 1$, so $a \equiv b \pmod{n}$.