Lecture 18

$\boxed{Ex}$ $f_n = \underbrace{f_{n-1} + 2f_{n-2}}_{f_n^{(h)}} + \underbrace{n^2 2^n}_{f_n^{(p)}}$

1. $f_n^{(h)}$:

$$f_n - f_{n-1} - 2f_{n-2} = 0$$

$$x^2 - x - 2 = 0$$

$$(x-2)(x+1) = 0$$

$$x_1 = 2 \ , \ x_2 = -1$$

general Solution:

$$f_n = A(2)^n + B(-1)^n$$

2. solve $f_n^{(p)}$

↳ we can see the root is 2.

↳ but there are three roots : $x_1 = 2$, $x_2 = 2$, $x_3 = 2$ in $f_n^{(p)}$

↳ so in total we have four 2's total.

↳ general solution $f_n = \underbrace{A(2)^n + B(-1)^n}_{f_n^{(h)}} + \underbrace{Cn(2)^n + Dn^2(2)^n + En^3(2)^n}_{f_n^{(p)}}$

Integer Properties

- Discrete Logarithm → Current digital signatures in cryptocurrency.
- Integer Factorization → Current digital signatures in web browsers.
- Approximate GCD → Advanced cryptography that is obsolete now

Integer Division :

- For any integers a and d, when we do $a \div d$ in the integer domain :
  - $a = dq + r$
  - q can be any integer, called quotient
  - r has to be a positive integer, $0 \leq r < d$, called remainder
  - d is called the dividend

Modular arithmetic :

$(7 \times 3) \bmod 5 \longleftrightarrow (7 \bmod 5)(3 \bmod 5) \bmod 5$

$= 1$

$2(3) \bmod 5$

$6 \bmod 5 = 1$

so $abcd \ldots \bmod 5$

$(a \bmod 5)(b \bmod 5) \ldots \bmod 5$

- Integer ring $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-2, n-1\}$
  - ↳ This is the outcome of mod applied to $\mathbb{Z}$