Math 321

Q/ 5.3 #5

a) $f(0)=2 \quad f(1)=3$ (basis)

→ $f(n) = f(n-1) - 1 \quad n=2,3,4,..$ open

2 | 3, 2, 1, 0, -1, -2, ..

0 ↑ (1 ↑ 2 ↑ 3)

closed formula

Forward.

$a_1 = 3$

$a_2 = a_1 - 1 = 3 - 1$

$a_3 = a_2 - 1 = 3 - 1 - 1 = 3 - 2$

$a_4 = a_3 - 1 = 3 - 1 - 1 - 1 = 3 - 3$

$a_5 = a_4 - 1 = 3 - 3 - 1 = 3 - 4$

!

$a_n = 3 - (n-1) = 4 - n$

$a_0 = 2, \quad a_n = 4 - n \quad n = 1, 2, 3, ...$

Q/ (basis) $f(0) = 1$

(Inductive) $f(n) = 9 f(n-2)$

$f(1) = 9 f(-1)$?

5.2 #11

Nim variation: (1) One pile
(2) take 1, 2, or 3

→ Lose if you take everything and have nothing.

→ win when other player loses.

n = pile

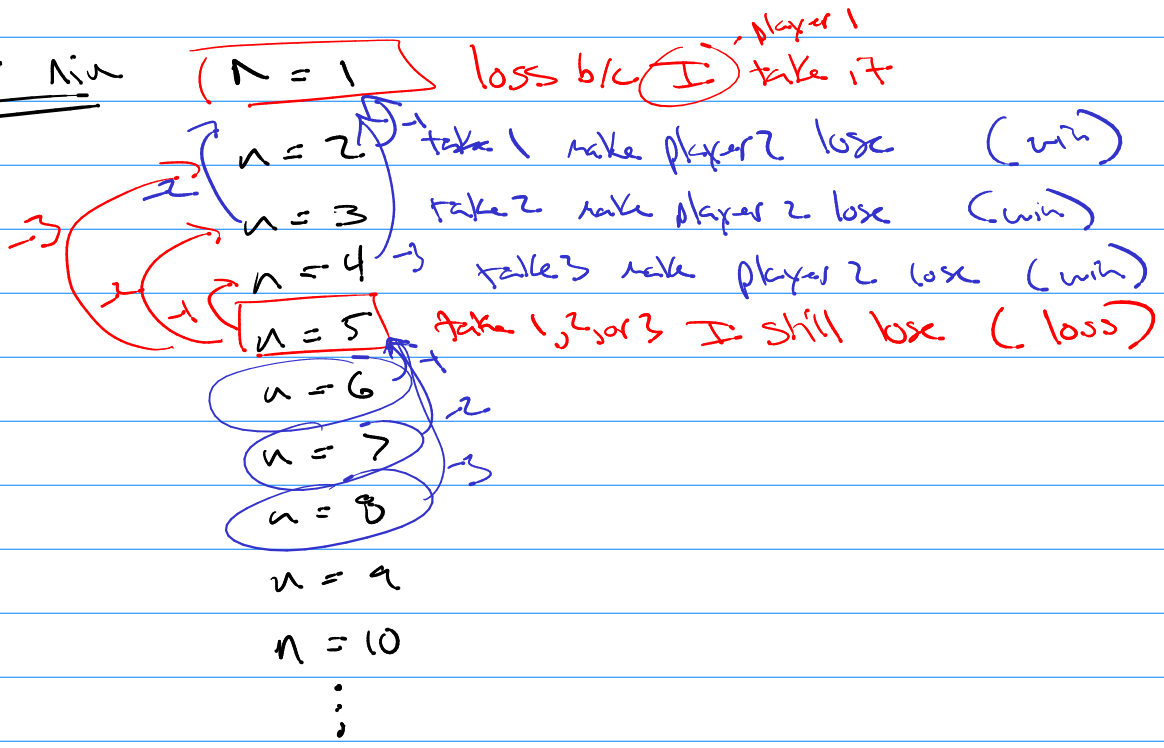
$n = 4j + 0$ → n is a mult. of 4 (win)

$n = 4j + 1$ → n mod 4 = 1 or 1 above a mult of 4 (loss)

$n = 4j + 2$ → n mod 4 = 2 or 2 above a mult. of 4 (win)

$n = 4j + 3$ → n mod 4 = 3 or 3 above a mult. of 4 (win)

play Nim



Conjecture: n mod 4 = 1 is a loss

n mod 4 = 0, 2, 3 is a win

PF (Basis) n=1, n=2, n=3, n=4 (use above game playing)

(Inductive) "Strong"

assume: $n=1, n=2, n=3, \dots, n=k$ follow our gameplay rules

show: $n=k+1 \rightarrow (k+1) \bmod 4$

Case 1 $(k+1) \bmod 4 = 1$

Subcase 1 take 1 $(k+1) \rightarrow k$

so $(k+1) \bmod 4 = 1$

player 2 $k \bmod 4 = 0$ sees a win (loss for me)

Subcase 2 take 2 $(k+1) \rightarrow (k-1)$

player 2 $(k-1) \bmod 4 = -1 \equiv_4 3$ see a win (loss for me)

etc

finish

Exam 3 11 probs @ 10pts

100pts = 100%

4.1 Divisible, div, mod, congruence (2 probs)

$a|b$ means $a \cdot n = b$, $n \in \mathbb{Z}$

(1) Prof involving divisibility. $a|b \wedge b|c \rightarrow a|c$

(2) use congruence. find div, mod

ex $-123 \bmod 4$, $123 \bmod 4$, etc

(ex) $(121^{1001} + 3^{3^3}) \bmod 2 = (1+1) \bmod 2$

$= 0$

(4.2) $(\ )_b$ representation (1 prob)

(1) $(\ )_b + (\ )_b$

$(\ )_b \cdot (\ )_b$

(4.3) Primes (3 prob)

(1) prove prims are infinite

(2) prime factors of a, b $\quad a = 2 \cdot 3^2 \cdot 5$

$\rightarrow \gcd(a,b) = 2^0 3^2 5^1 7^0 \quad b = 3^3 \cdot 5^2 \cdot 7$

$\rightarrow \text{lcm}(a,b) = 2^1 3^3 5^2 7^1$

(3) Euclidean Algorithm for $\gcd(a,b)$

(4.6) Crypto (2 probs)

(1) given Affine Encryption

$E(p) = (ap+k) \bmod n$

Find $E^{-1}(c) = (\ ?\ )$

(2) given $e =$, $n =$ & RSA/Cocks crypto

$E(p) = p^e \bmod n$

Find $E^{-1}(c) = c^{(d)} \bmod n$

5.1 | 5.2 | 5.3 Induction (3 probs)

(1) Weak Induction

(2) Strong Induction (Existence part of Fund. th^m)

(3) Weak Induction use fibonacci numbers

Ex

Prove $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$

using: $f_n = f_{n-1} + f_{n-2}$

$f_i = 0, 1, 1, 2, 3, 5, 8, \ldots$