Math 321

Q2) 5.2 #11 **Nim**

$1, 2, \ldots, n$ — n matches. each time you play to take 1, 2, or 3. Take all that is left → you lose.

player 1 sees
$n = 4j$ to
$n = 4j + 2$
$n = 4j + 3$
player 1 wins

player 1 sees
$n = 4j + 1$
player 1 loses

if $n \bmod 4 \to 0, 2, 3 \to$ win
$n \bmod 4 = 1 \to$ lose

→ play:

- $n = 1 \to$ player 1 takes it and loses
- $n = 2 \to$ player 1 takes 1 → player 2 faces $n=1$ ∴ player 1 wins
- $n = 3 \to$ player 1 takes 2 → player 2 gets $n=1$ ∴ player 1 wins
- $n = 4 \to$ player 1 takes 3 → player 2 gets $n=1$ ∴ player 1 wins

- $n = 5 \to$ 3 cases
  - player 1 takes 1 → p_2 gets 4 → ∴ pl lose
  - player 1 takes 2 → p_2 gets 3 → pl lose
  - player 1 takes 3 → p_2 gets 2 → pl lose

Show: Nim by take 1, 2, or 3

$n \bmod 4 = \begin{cases} 1 \to \text{player 1 loses} \\ 0,2,3 \to \text{player 1 wins.} \end{cases}$

Pf Base: show formula works for $n=1,2,3,4$

Induction (strong)

Assume $P(n=1) \wedge P(n=2) \wedge \cdots \wedge P(n=k)$

show $P(n=k+1)$

$n=k+1 \to (k+1) \bmod 4$

Case #1 $(k+1) \bmod 4 = 0$

$(k-2) \bmod 4 = 1$

So player 1 takes 3 $\to$ "0"

$\to$ player 2 sees $((k+1)-3) \bmod 4$

$= (-3) \bmod 4 = 1$

$\therefore$ p2 loses

Case #2 $(k+1) \bmod 4 = 1$

(2a) take 1 $\to$ p2 $((k+1)-1) \bmod 4 = 0$

(2b) take 2 $\to$ p2 $(k+1-2) \bmod 4 > 3$

(2c) take 3 $\to$ p2 $(k+1-3) \bmod 4 = 2$

p2 wins $\to$ p1 loses

5.1 #29 H_n is the n^{th} harmonic number

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$$

$$\boxed{H_{2^n} \leq 1 + n}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n} \leq 1 + n$$

$n=0$ $\quad H_{2^0} = H_1 = 1$

$n=1$ $\quad H_2 = 1 + \frac{1}{2}$

$n=2$ $\quad H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}$

$n=3$ $\quad H_8 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}}$

$\vdots$

show $\boxed{H_{2^n} \leq 1 + n}$

PF Base $\quad P(1^{st}\text{ case}) = P(n=0)$: "$H_1 \leq 1 + 0$"

$\equiv$ "$1 \leq 1$" true

Inductive $\quad$ Assume $P(k^{th})$: "$n = k$"

$$\boxed{H_{2^k} \leq 1 + k}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k}$$

I.H.

show: $P(k+1^{st})$: "$n = k+1$"

$$H_{2^{k+1}} \leq 1 + (k+1)$$

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{k+1}} \leq \leq \ldots$$

2^k - terms $\qquad$ 2^k terms

take $H_{2^{k+1}} = \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k}\right| + \left|\frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{k+1}}\right|$

$\leq \left|(1+k)\right| + \left|\frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{k+1}}\right| \leq \frac{1}{2^k}$

$\leq (1+k) + \frac{1}{2^k} + \frac{1}{2^k} + \cdots + \frac{1}{2^k}$

$\leq (1+k) + 2^k\left(\frac{1}{2^k}\right) = 1 + k + 1$ ✓

Exam 3 $\qquad$ 11 probs

4.1 $\quad a \mid b$, $a \bmod m$, $a \equiv_m b$ $\qquad$ (2 probs)

(1) Divisibility proof

ex $\quad a \mid b \wedge b \mid c \rightarrow a \mid c$

$a \cdot k = b$ for an integer k

(2) find $\operatorname{div}, \bmod$, $\quad a = qb + r$

ex $\quad -21 \bmod 4$, $\quad 21 \operatorname{div} 6$,

$(32^{121})^{1027} \bmod 31$

4.2 $\quad$ Int. Reps and ops $\qquad$ (1 pr)

$b = 2, 5$ or 7

(1) $+\,(\ )_b \qquad \times\,(\ )_b$

4.3 Primes, GCD, LCM, Euclid's (3 probs)

(1) Prove Primes are infinite

(2) gcd, lcm using prime factors.

(3) Euclid's Alg. (+) Bézout's th^m

gcd(a,b) by euclid's

show $gcd(a,b) = s \cdot a + t \cdot b$

4.6 Crypto (2 probs)

(1) shift, Affine shift, and or One-time pad

plaintext ⇄ cypher text

(2) for RSA / locks crypto.

given $[e, n]$ + work the encryption and decryption functions

$$c = p^e \bmod n$$

$$p = c^d \bmod n$$

5.1-5.3 3 probs Induction

(1) Weak Ind. proof

(2) Strong Ind. proof

(3) Weak Ind. proof involving $f_0, f_1, \ldots$