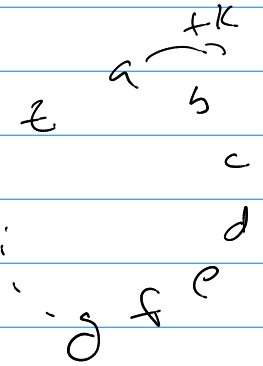
Math 321

Q's

4.6 #a ERC



shift $f(p) = (p+K) \bmod 26$

$f^{-1}(C) = (C-K) \bmod 26$

	ERC	MW
-1	DQB	LV
-2	CPA	KU
-3	DOZ	JT
-4	ANY	IS

$K=4$

$f(p) = (p+4) \bmod 26$

$f^{-1}(C) = (C-4) \bmod 26$

Finding K for $f(p) = (p+K) \bmod n$

use language study:

ex for "typical" messages find stats for characters.

a is X%

b is y%

etc

→ do stats for the encrypted text.

→ match % and use that to guess K.

Induction (weak / strong)

goal: prove for all "elements" a predicate holds.

$\forall n\ P(n)$ Book example

$\forall n_i\ P(n_i)$ cases: $n_1, n_2, \ldots$

till now: cases finite → proof by cases

Now

Induction: cases are infinite but cases are well ordered.

use proof by induction $\forall n, P(n)$

prove 1st — prove $P(1^{st}\ \text{case(s)})$ — Basis Step

also

prove 2nd — prove $P(k^{th}\ \text{case}) \rightarrow P(k+1^{st}\ \text{case})$ — Inductive Step

(weak induction)

or

prove $P(1^{st}) \wedge P(2^{nd}) \wedge \dots \wedge P(k^{th}) \rightarrow P(k+1^{st})$

(strong induction)

---

ex Prove: for all $n = 1, 2, 3, 4, \dots$

$$\forall n \left(1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2 \right)$$

1^{st} case: $1^3 = \left(\frac{1 \cdot 2}{2} \right)^2$ true

2^{nd} case: $1^3 + 2^3 = \left[\frac{2 \cdot 3}{2} \right]^2$ true

3^{rd} case: $1^3 + 2^3 + 3^3 = \left[\frac{3 \cdot 4}{2} \right]^2$ true

k^{th} case: $1^3 + 2^3 + \dots + k^3 = \left[\frac{k(k+1)}{2} \right]^2$

$k+1^{st}$ case: $1^3 + 2^3 + \dots + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2} \right]^2$ ✓ $\equiv P(k+1^{st})$

pf (by induction)

Basis Step (show true for 1^{st} case)

$1^3 \stackrel{?}{=} \left[\frac{1 \cdot 2}{2} \right]^2$ Yes

Inductive Step (weak) (show $P(k^{th}) \to P(k+1^{st})$)

Note: Direct Proof for $\square \to \Delta$ (assume $\square$, show Δ)

assume $1^3 + 2^3 + \cdots + k^3 = \left[\frac{k(k+1)}{2}\right]^2$ ← Inductive hypothesis (IH)

show $P(k+1^{st})$ ← see above to know what that is..

IH is $1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3$

$1^3 + 2^3 + \cdots + (k+1)^3 = (k+1)^2\left[\frac{k^2}{4} + \frac{(k+1)}{1}\right]$

$1^3 + 2^3 + \cdots + (k+1)^3 = (k+1)^2\left[\frac{k^2 + 4k + 4}{4}\right]$

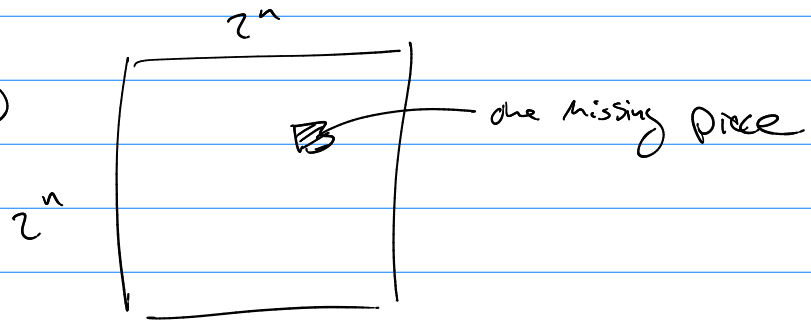
$1^3 + 2^3 + \cdots + (k+1)^3 = (k+1)^2\frac{(k+2)^2}{4}$

$P(k+1^{st})$ $\quad 1^3 + 2^3 + \cdots + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2}\right]^2$ ∎

---

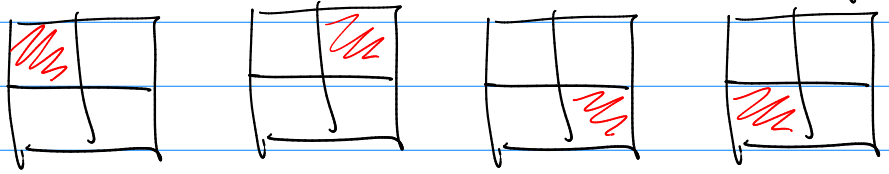
ex $2^n \times 2^n$ board

$n = 1, 2, 3, 4, \ldots$

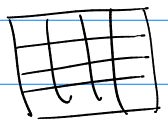


Predicate: these boards can be tiled by  piece

1st case: 2×2

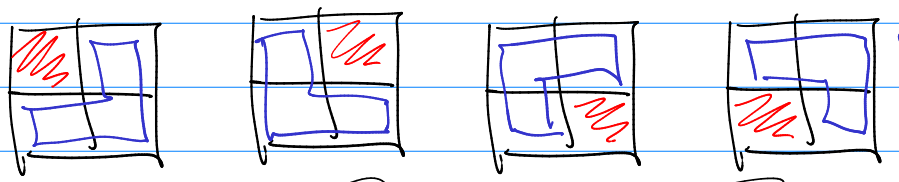


2nd case: 4×4



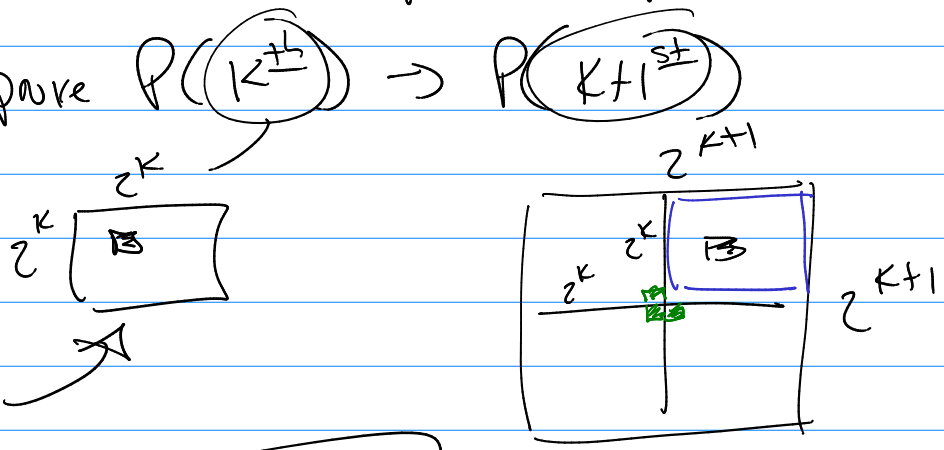
Induction

Basis Step — prove for 2×2 boards — 1st case



True!

Inductive Step — prove $P(k^{th}) \rightarrow P(k+1^{st})$



I.H.: I can tile

See video