Math 321

Q's: 3.7 (47)

$p = 43 \quad q = 59 \qquad n = 43 \cdot 59 = 2537$

$e = 13 \qquad M = 42 \cdot 58 = 2436$

$C_1 = 667 \qquad C_2 = 1947 \qquad C_3 = 671$

$M_1 = ?_6 \qquad M_2 = ?_6 \qquad M_3 = ?_6$

$$C = M^e \bmod n$$
$$M = C^d \bmod n$$

$\underline{d}$ is e's inverse mod M

$\gcd(\underline{M}, e) = 1 \qquad \gcd(2436, 13)$

$2436 = 187 \cdot 13 + 5$

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + \boxed{1}$ gcd

$2 = 2 \cdot 1 + 0$

$1 = 3 - (1) \cdot 2$

$1 = 3 - (1)(5 - 3)$

$= (-1)(5) + (2)(3)$

$1 = (-1)(5) + (2)(13 - 2 \cdot 5)$

$= (2)(13) + (-5)(5)$

$1 = (2)(13) + (-5)(2436 - 187 \cdot 13)$

$1 = (-5)(2436) + (937)(13)$

Mod 2436

$$\cancel{1}^{1} = \cancel{(-5)(2436)}^{0} + (937)(13)$$

$$1 \equiv [\underline{937} \cdot \underline{13}] \pmod{2436}$$

13's inv.

$d = 937$

$C_1 = 667$ $\quad C_2 = 1947$ $\quad C_3 = 671$

$M_1 = ?$ $\quad M_2 = ?$ $\quad M_3 = ?$

$$M = C^d \bmod n$$

$d = 937$ $\quad n = 2537$

$$M_1 = 667^{937} \bmod 2537 = \boxed{18}\boxed{08}$$

$$M_2 = 1947^{937} \bmod 2537 = \boxed{11}\boxed{21}$$

$$M_3 = 671^{937} \bmod 2537 = \boxed{04}\boxed{17}$$

to encrypt. $\boxed{e = 13 \quad n = 2537}$

3.6 (1) $(4532)_{10} =$

n		
$2^0 = 1$	9 - 512	
1	2	10 - 1024
2	4	11 - 2048
3	8	12 - 4096
4	16	13 - 8192
5	32	
6	64	
7	128	
8	256	

$4532 = 4096 + 256 + 180$

436

$180 + 52$

$32 \quad 20$

$16 \quad 4$

$$\begin{array}{r} 436 \\ 256 \\ \hline 180 \end{array}$$

$(1,0,0,0,1,1,0,1,1,0,1,0,0)_2$

4.2 Weak Induction.

$$\Big[\underbrace{P(1)}_{\text{Basis step}} \wedge \underbrace{\forall k\,(P(k) \to P(k+1))}_{\text{Weak Inductive step.}}\Big] \to \forall n\, P(n)$$

Strong Induction

$$\Big[\underbrace{P(1)}_{\text{Basis step}} \wedge \underbrace{\forall k\,(\{(P(1) \wedge P(2) \wedge \cdots \wedge P(k)\} \to P(k+1))}_{\text{Strong Inductive step.}}\Big] \to \forall n\, P(n)$$

---

ex 5

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = a_n$$

$n=1$ $\quad a_1 = 1/2$

$n=2$ $\quad a_2 = 1/2 + 1/6 = 3/6 + 1/6 = 4/6 = 2/3$

$n=3$ $\quad a_3 = \frac{1}{2} + 1/6 + 1/12 = 2/3 + 1/12 = 9/12 = 3/4$

$n=4$ $\quad a_4 = 1/2 + 1/6 + 1/12 + 1/20 = 3/4 + 1/20 = 16/20 = 4/5$

Conjecture.

$$a_n = 1/2 + 1/6 + \cdots + 1/n(n+1) = n/n+1$$

Th$^{\underline{m}}$: $\forall n\left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}\right)$

pf: $\boxed{\text{Basis Step.}}$ $P(1)$: let $n=1$

$$\left.\begin{array}{l}\text{left} = \frac{1}{1\cdot 2} = 1/2 \\ \text{right} = \frac{1}{2} = 1/2\end{array}\right\}\ \underline{\text{equal!}}\quad \underline{P(1)\text{ is true.}}$$

$\boxed{\text{Inductive Step}}$ $\forall k\,(P(k)\to P(k+1))$

$P(k)$: " $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k(k+1)}=\frac{k}{k+1}$ "

$P(k+1)$: " $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=\frac{k+1}{k+2}$ "

<u>assume</u>: $\frac{1}{1\cdot 2}+\cdots+\frac{1}{k(k+1)}=\frac{k}{k+1}$ is true

$$\frac{1}{1\cdot 2}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=\frac{(k)}{(k+1)}+\frac{1}{(k+1)(k+2)}$$

$$\to \frac{1}{1\cdot 2}+\cdots+\frac{1}{(k+1)(k+2)}=\frac{k(k+2)+1}{(k+1)(k+2)}=\frac{k^2+2k+1}{(k+1)(k+2)}$$

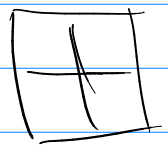
$$\to \frac{1}{1\cdot 2}+\cdots+\frac{1}{(k+1)(k+2)}=\frac{\cancel{(k+1)}(k+1)}{\cancel{(k+1)}(k+2)}=\frac{k+1}{k+2}$$

$$\to \frac{1}{1\cdot 2}+\cdots+\frac{1}{(k+1)(k+2)}=\frac{k+1}{k+2}$$

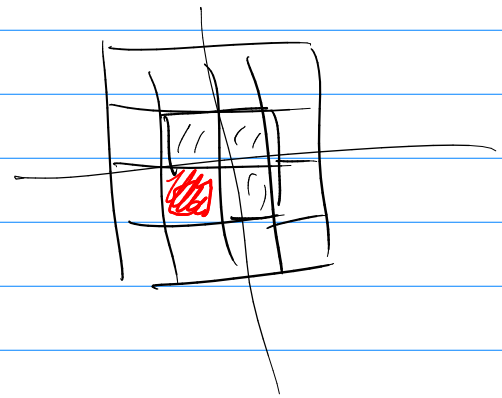
So inductive step is true.

$\therefore \forall n\, P(n)$ is True.

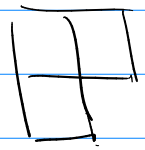
---

boards.  2×2 or 4×4 or 8×8 or $2^n \times 2^n$

if you remove 1 tile.



then the entire board can be tiled with

an L-  piece.