Math 321

Q's/ p. 308 #18

$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ th $A^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$ $n = 1, 2, 3, \ldots$

0	f_0
1	f_1
1	f_2
2	f_3
3	f_4
5	f_5

Pf: Basis: P(1) does equal

show $A^1 = \begin{bmatrix} f_2 & f_1 \\ f_1 & f_0 \end{bmatrix}$

$A^1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

$\begin{bmatrix} f_2 & f_1 \\ f_1 & f_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ equal.

True

Inductive: show $P(k) \to P(k+1)$ is true

assume P(k) is true and show P(k+1) is true.

P(k): $A^k = \begin{bmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{bmatrix}$

P(k+1): $A^{k+1} = \begin{bmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{bmatrix}$

Given $A^k = \begin{bmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{bmatrix}$ so $A^k \cdot A^1 = \begin{bmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

$$A^{k+1} = \begin{bmatrix} f_{k+1} + f_k & f_{k+1} \\ f_k + f_{k-1} & f_k \end{bmatrix} = \begin{bmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{bmatrix}$$

True

Exam 3 (10 probs + 1 extra credit)

ch 3 (Number theory)
ch 4 (Induction)

① (3.4) Divisibility Proof.

ex $a|b \wedge a|c \rightarrow a|b+c$

② (3.4) Know the Def and 2 th's for congruence.

$a \equiv b \pmod m$

Def: ① $m \mid (a-b)$

th's: ② $a \bmod m = b \bmod m$
③ $a = b + km$

③ Prove primes are infinite. (from 3.5)

④ base b operations (from 3.6)

ex $(3,2,1)_4 \overset{?}{+} (2,0,3)_4 =_6^?$ (base $b \geq 5$)

⑤ Find gcd(a,b) using Euclid's Algorithm.

ex ⓐ gcd(13, 28)

$28 = 2 \cdot 13 + 2$

$13 = 6 \cdot 2 + 1$ = gcd(13, 28)

$2 = 2 \cdot 1 + 0$

⑥ like #15 p. 244

⑦ Find e's inverse.

p, q are prime. → $n = pq$

→ $m = (p-1)(q-1)$

d was e's inverse mod m.

ex. $p = 7$ $q = 13$ $n = 91$

$m = 72$

let $e = 5$ ←

Use Euclid's Alg. to show gcd(5, 72) = 1

$72 = 14 \cdot 5 + 2$ → $1 = (1)5 - (2)(2)$

$5 = 2 \cdot 2 + 1$ ← $1 = (1)5 - 2[72 - 14 \cdot 5]$

$2 = 2 \cdot 1 + 0$ $(1 = (-2)(72) + 29 \cdot 5)$

Mod 72 $1 \equiv 29 \cdot 5 \pmod{72}$

your problem is $e = 5 \quad n = 91 = 7 \cdot 13$

Step 1

Find d.

Step 2 $M = 6 \cdot 12 = 72$

Step 3 $\gcd(5, 72) = 1$

use Euclid's Alg to find d.

---

(8) Weak Induction (numeric)

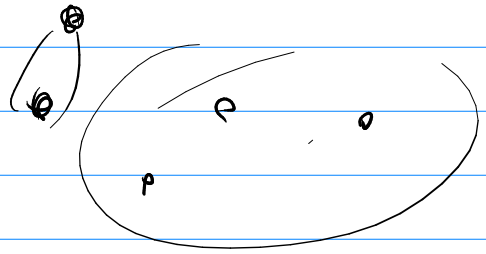
(9) Strong Induction

(10) $\forall n$ and weak induction

Extra Credit

p 276 Example 12

$P(2k+1)$



$P((2(k+1)+1)$

$2k+1+3$

$(2k+3)$