Math 321

Q's/ RSA/Locks Crypto $C = P^e \pmod n$

#25 $p = 53 \quad q = 61 \rightarrow n = 53 \cdot 61 = 3233$

$C = 13 \qquad M = 52 \cdot 60 = 3120$

Note: pick $e \not| 3120$

$C = P^{13} \pmod{3233}$

UPLOAD

2015 = 1909

$C_1 = (2015)^{13} \pmod{3233}$

by hand

by computer. ex)

Fund. th^m of Arith

$n \geq 2$, n can be written uniq. as a prod. of primes in non-dec. order.

To prove #1 $n =$ (prod. of primes) Existence part

#2 the prod of primes is unique.

by contradiction

assume not uniq: $n = (\text{prod. of primes \#1}) = (\text{prod of primes \#2})$

Cancel any common primes

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

all the p_i, q_j are primes and for all i,j $p_i \neq q_j$

$p_1 \mid p_1 p_2 \cdots p_k$

$p_1 \mid q_1 q_2 \cdots q_\ell$ by Lemma $\Rightarrow$ $p_1 \mid q_j$ one of the q's

!!!

F

#1 $n \geq 2$, n can be written as a prod. of primes.

pf Basis: $P(1^{st}\text{ case})$: "$n=2$" / $n=2$ it's prime so true

Inductive: (strong induction)

I.H. Assume $P(n=2) \wedge P(n=3) \wedge \cdots \wedge P(n=k)$ are true

Show $P(n=k+1)$ is true

Show: $(k+1)$ = prod. of primes ?

Consider $n = k+1$ gives two cases.

Case #1: $(k+1)$ is prime → $k+1$ is a prod. of primes is true.

Case #2: $(k+1)$ is Composite (not prime)

So $(k+1) = a \cdot b$ where $2 \le a \le k \rightarrow a$ = prod of primes
and $2 \le b \le k \rightarrow b$ = prod of primes

↑ by I.H.

$\therefore (k+1) = a \cdot b = (\text{prod of primes}) \times (\text{prod of primes}) =$ prod of primes ✓

5.3 Recursive Definitions

Open form & Seq's:

Basis: $a_0 = 2$

Recursive or Inductive: $a_n = 3a_{n-1} + 2$

Seq: 2, 8, 26, 80, ...

Strong Ind

$P(1^{st}\text{ case}) \wedge \forall k \left([P(1^{st}) \wedge P(2^{nd}) \wedge \dots \wedge P(k^{th})] \rightarrow [P(k+1^{st})] \right)$

Basis — Inductive or Recursive step

ex's $f_0 = 0$, $f_1 = 1$

recursive or Inductive def $f_n = f_{n-1} + f_{n-2}$

Seq: 0, 1, 1, 2, 3, 5, 8, ...

ex | of a set

Basis $5 \in S$

Inductive $a \in S \wedge b \in S \rightarrow (a+b) \in S$

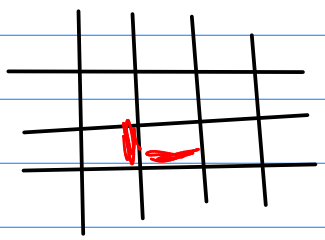
$S = \{ 5, 10, 15, 20, 25, \ldots \}$

(5+10, 15+10)

(5+5, 10+10)

Basis: v_1 , v_2 $\quad v_1 \in S \quad v_2 \in S$

Inductive: $\alpha v_1 + \beta v_2 \in S$



Know: $f_0 = 0 \quad f_1 = 1 \quad f_n = f_{n-1} + f_{n-2}$

Show: $\forall n$ if $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \rightarrow A^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$

Note: $\ldots, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, \ldots$

$\ldots, f_2, f_1, f_0, f_1, f_2, \ldots$

Base: $P(1^{st}\text{ case})$ ($n=1$): "$A^1 = \begin{bmatrix} f_2 & f_1 \\ f_1 & f_0 \end{bmatrix}$"

$= \text{"} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$" ✓

Inductive

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

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

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

Algebra → $= \ldots =$

Finish!