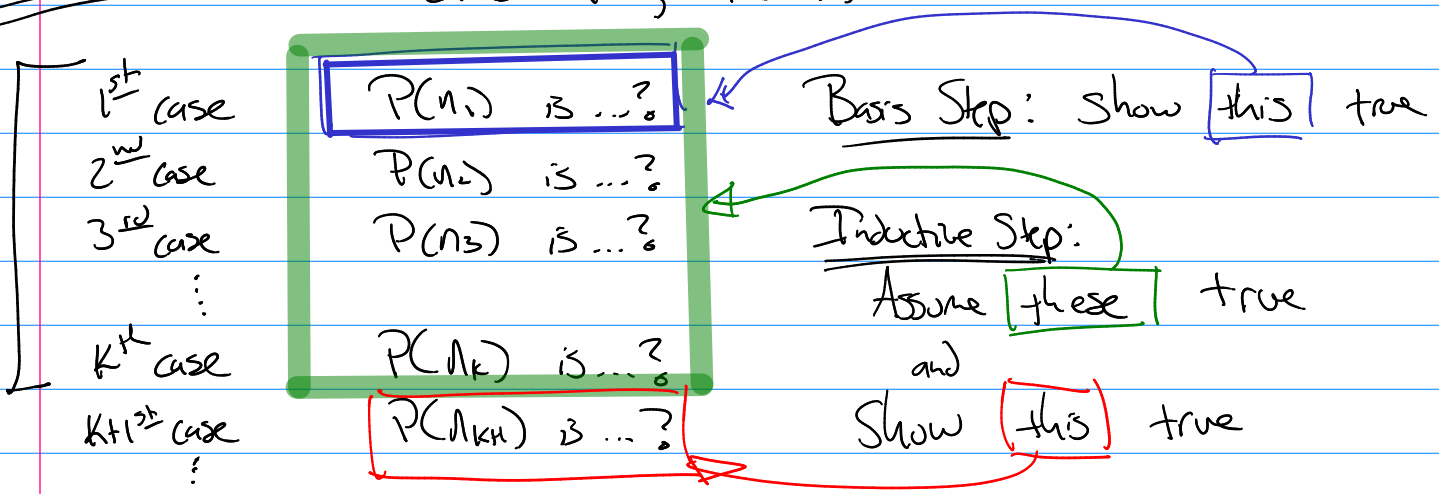
Math 321

Induction: for all cases n_i, $P(n_i)$ is true



Example **Know:** $f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, \ldots$

$f_n = f_{n-1} + f_{n-2}$

5.3 #15 **Show:** $(f_0 f_1 + f_1 f_2) + (f_2 f_3 + f_3 f_4) + \cdots + (f_{2n-2} f_{2n-1} + f_{2n-1} f_{2n}) = f_{2n}^2$

Assume true and show true:

- Case #1: $f_0 f_1 + f_1 f_2 = f_2^2$ ← show true for basis
- Case #2: $(f_0 f_1 + f_1 f_2) + (f_2 f_3 + f_3 f_4) = f_4^2$
- Case #3: $(f_0 f_1 + f_1 f_2) + (f_2 f_3 + f_3 f_4) + (f_4 f_5 + f_5 f_6) = f_6^2$
- ⋮
- Kth Case: $(f_0 f_1 + f_1 f_2) + \cdots + (f_{2K-2} f_{2K-1} + f_{2K-1} f_{2K}) = f_{2K}^2$
- K+1st case: $(f_0 f_1 + f_1 f_2) + \cdots + (f_{2K} f_{2K+1} + f_{2K+1} f_{2K+2}) = f_{2K+2}^2$

PF **Basis Step** is $f_0 f_1 + f_1 f_2 = f_2^2$ true?

$0 \cdot 1 + 1 \cdot 1 = 1^2$

So $1 = 1$ is true? yes

Inductive Step IH → assume $(f_0 f_1 + f_1 f_2) + \cdots + (f_{2k-2} f_{2k-1} + f_{2k-1} f_{2k}) = f_{2k}^2$

Start with $(f_0 f_1 + f_1 f_2) + \cdots + (f_{2k-2} f_{2k-1} + f_{2k-1} f_{2k}) + (f_{2k} f_{2k+1} + f_{2k+1} f_{2k+2})$

I.H. $= \left(f_{2k}^2 \right) + f_{2k} f_{2k+1} + f_{2k+1} f_{2k+2}$

$= f_{2k} f_{2k} + f_{2k} f_{2k+1} + f_{2k+1} f_{2k+2}$

$= f_{2k} (f_{2k} + f_{2k+1}) + f_{2k+1} f_{2k+2}$

$= f_{2k} f_{2k+2} + f_{2k+1} f_{2k+2}$

$= (f_{2k} + f_{2k+1}) f_{2k+2} = f_{2k+2}^2$ true

Q5 4.6 #25

UPLOAD

UP	LO	AD
2015	1114	0003

$e = 17$ $n = 53 \cdot 61 = 3233$

A=00
B=01
C=02
D=03
E=04
⋮
Z=25

$C_i = f(P_i) = P_i^e \bmod n$

$P_1 = 2015$ $C_1 = 2015^{17} \bmod 3233 = ?$

$C_2 = 1114^{17} \bmod 3233 = ?$

$C_3 = 3^{17} \bmod 3233 = ?$

$f(P) = P^{17} \bmod 3233$

---

on test (example) give $e=17$ $n=3233$

Find $f(P) = ?$ $f^{-1}(C) = ?$

Step 1 $n = pq$ $3233 = 53 \cdot 61$

Step 2 $M = (p-1)(q-1)$ $M = 52 \cdot 60 = 3120$

Step 3 find d = e's inv. mod M

gcd(3120, 17)

$3120 = ? \cdot 17 + ?$ — Euclid's

etc $=$

use to find $1 = s \cdot 17 + t \cdot 3120$

let $d = s$ & $s < 0$

$d = s \equiv_{3120} s + 3120$

RSA $f(p) = p^{17} \bmod 3233$

$f^{-1}(c) = c^{d} \bmod 3233$

Exam 11 pnts @ 10pts

4.1 (2 probs)

(1) divisible proof like 4.1 (3-8)

(2) div (mod) congruence for given numbers

(ex) $\text{div}(22, 7)$ $\text{mod}(22, 7)$ $7 \equiv_{11} ?$

$\text{div}(-22, 7)$ $\text{mod}(-22, 7)$

4.2 base-b (1 prob)

(1) $\begin{matrix} (\ \ )_b \\ +(\ \ )_b \\ \hline (\ \ )_b \end{matrix}$ $\begin{matrix} (\ \ )_b \\ \times(\ \ )_b \\ \hline (\ \ )_b \end{matrix}$ → convert ans into base 10

4.3 primes/gcd (3probs)

① prove primes are infinite
② find gcd, lcm using prime factors
③ gcd(a,b) and gcd(a,b) = sa + tb using Euclid's Algor.

4.6 Crypto (2probs)

① Affine Shift

given $f(p) = (a \cdot p + k) \bmod n$
find $f^{-1}(c) = (a^{-1}(c-k)) \bmod n$

② Public Key.

given $e, n \rightarrow$ show $f(p) = p^e \bmod n$
$f^{-1}(c) = c^d \bmod n$

5.1/5.2 Induction (2probs)

① weak induction
② strong induction

prove: $n \geq 2$, n is prime or a prod. of primes.

5.3 (1prob)

proof using Fibonacci numbers
↑ Induction