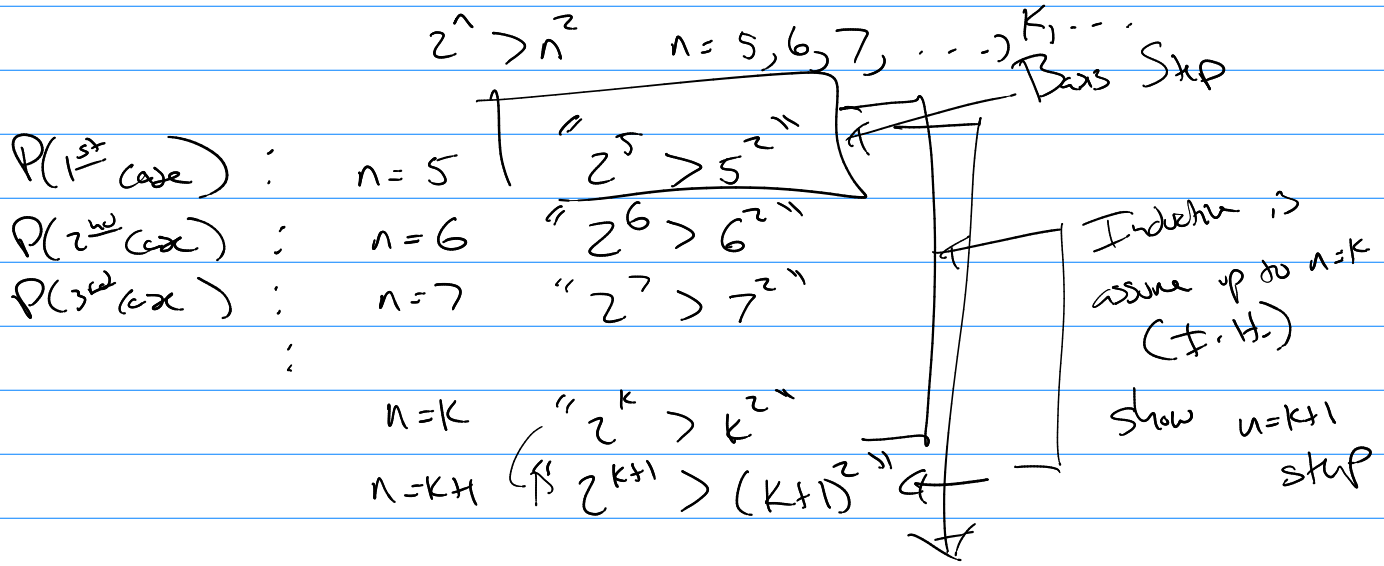
Math 321

Q's 5.1 #21 $\forall n\,[P(n)]$ $n =$ 1st case, 2nd case, ...

$2^n > n^2$ $n = 5, 6, 7, \ldots, k, \ldots$



Pf

Basis Step: for $n=5$ "$2^5 > 5^2$" **true** ($\because 32 > 25$)

Inductive Step: assume (I.H.) the inequality is true up to $2^k > k^2$

Show: $2^{k+1} \overset{?}{>} (k+1)^2$ (scratch work $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k$, $(k+1)^2 = k^2 + 2k + 1$)

start with $(k+1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1 < 2^k + 2k + k$ (I.H.; $\because 1 < k$; $\because 1 < k$)

$< 2^k + k^2 < 2^k + 2^k = 2^{k+1}$

$2^{k+1} \overset{?}{>} (k+1)^2$

$2^k > k^2$

$2 \cdot 2^k > 2k^2$

$2^{k+1} > 2k^2$

$2^{k+1} > k^2 + k^2$ $\quad k^2 + 2k + 1$

$2^k < k^2 + 1$

See Video

Note: H_k Harmonic Numbers

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$$

(a) Show $H_{2^n} \le 1 + n \quad n = 0, 1, 2, \ldots$

$P(1^{st}\text{ case})$: $n=0$ $\quad H_1 = "1 \le 1 + 0"$

$P(2^{nd}\text{ case})$: $n=1$ $\quad H_2 = "1 + \frac{1}{2} \le 1 + 1"$

$P(3^{rd}\text{ case})$: $n=2$ $\quad H_4 = "1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \le 1 + 2"$

$P(4^{th}\text{ case})$: $n=3$ $\quad H_8 = "1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \le 1 + 3"$

$\vdots$

$n=k$ $\quad H_{2^k} = "1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k} \le 1 + k"$

$n=k+1$ $\quad H_{2^{k+1}} = "1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{k+1}} \le 1 + (k+1)"$

$$\underbrace{1 + \frac{1}{2} + \cdots + \frac{1}{2^k}}_{\le 1+k} + \frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{k+1}} \le 1 + k + 1$$

$$\le (k+1) + \frac{1}{2^{k+1}} + \frac{1}{2^{k+2}} + \cdots + \frac{1}{2^{k+2^k}}$$

$$\le (k+1) + \underbrace{\frac{1}{2^k} + \frac{1}{2^k} + \cdots + \frac{1}{2^k}}_{2^k \text{ Sum}}$$

$$\le (k+1) + 2^k\left(\frac{1}{2^k}\right) = k + 2$$

Note: $\lim_{n \to \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}\right) = \infty$

(ex) Prove: $n \geq 2$, n is prime or a prod. of primes.

PF Basis: ($n=2$) 2 is prime so true (1st case)

Induction Step: assume 2, 3, 4, 5, ..., K each are prime or prod. of primes (I.H.)

show (K+1) is prime or a prod. of primes.

Now (K+1) is an integer. 2 cases for any integer → prime / → prime

case 1 (K+1) is prime. then statement is true.

case 2 (K+1) is not prime (composite)
says $(K+1) = a \cdot b$ where $2 \leq a < K$, $2 \leq b < K$

so a = (prime or prod. of primes)
b = (prime or prod. of primes)

thenfr $(K+1) = a \cdot b =$ (prime or prod. of primes)(prime or prod. of primes)
= prod. of primes
(true)

(ex) \$5 bills, \$7 bills you can give \$5, \$7, \$10, \$12, \$14, \$15, \$17, \$19, \$20, \$21, \$22, \$24, \$25, \$26, \$27, \$28 → all #

Basis: $\$24 = 2 \cdot \$7 + 2 \cdot \$5$
$\$25 = 0 \cdot \$7 + 5 \cdot \$5$
$\$26 = 3 \cdot \$7 + 1 \cdot \$5$
$\$27 = 1 \cdot \$7 + 4 \cdot \$5$
$\$28 = 4 \cdot \$7 + 0 \cdot \$5$

Induction: assume for \$24, \$25, \$26, \$27, \$28, ..., \$K
$\$(K+1) = \$(K-4) + 1 \cdot \$5$

Exam 12 probs 110pts = 100%

Number Theory 4.1 alg, thm's for <|b, mod., div, mod. arith.

(1) Division Alg (+) div, mod

$-21 \text{ div } 4$ vs $21 \text{ div } 4$

$a = qb + r$

(2) div. proofs

(3) mod. arith. (ex) $(7^{1024} + 71)^{1001} \pmod 3$

(4) congruence.

4.2 (1) $(\ )_b + (\ )_b$, $(\ )_b \cdot (\ )_b$ $b=3$ or $b=7$

4.3 Primes / gcd / lcm / Euclidean Alg. 2 probs

(1) gcd/lcm by prime factorization

(2) gcd by Euclidean Alg.

4.6 Crypto (2 probs)

(1) Affine shift given $f(p) \to$ find $f^{-1}(c)$

(ex) $f(p) = (3p+4) \bmod 11 = c$

$f^{-1}(c) = 3^{-1}(c-4) \bmod 11$

3^{-1} = inv. mod 11

② public key given (n, e) → find d

$f(p) = p^e \bmod n$

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

Step 1 $n = p \cdot q$

Step 2 $m = (p-1)(q-1)$

and $d \equiv e^{-1} \bmod m$

ch 5 Induction

① equality induction proof. (weak)

② inequality induction proof (weak)

③ If $n \geq 2$, n is prime or a prod. of primes.