CS 200, CS210

if left is T, then right naturally should be T, they are equivalent statements

If 2nd propos is T, if P(x) is T for all x then 1st prop is T, if not, then P(x) fails for some x, but for this x there must be y such that P(x) ∨ Q(y) is T, so Q(y) must be T, thus 1st proposition is T

(4.3) 5, 11, 19, 25, 37

prime, composite

$$9 \to 3 \cdot 3 \qquad 23 \to 1 \cdot 23 \text{ prime}$$

every + int greater than 1 can be written uniquely as prime or product of

(5) Find prime factorization of 10! ?

!10 ~~[illegible]~~ multiplication of numbers from 2 to 10

$$!10 = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 =$$
$$= 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 =$$
$$= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

(11) $\log_2 3$ is irrational number, real num x that cannot be written as ratio of 2 integers

$\log_2 3 = p/q$, p and q are integers

$\log_2 3 > 0$, then $p, q > 0$

exponential equivalence of $\log_2 3 = p/q$

$\Rightarrow 3 = 2^{p/q}$ | q^{th}

$3^q = 2^p \Rightarrow \log_2 3$ is irrational

(19) If $2^n - 1$ is prime then n is prime

$2^{ab} - 1 = \underbrace{(2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots 2^a + 1)}$

$2^{ab} - 1$

$n = ab$ for int's > 1

$a > 1$, $2^a - 1 > 1$

$2^n - 1 = 2^{ab} - 1$, is product of 2 int's each greater than 1, so it's not prime

(25) Greatest common divisor?

(a) $3^7 \cdot 5^3 \cdot 7^3$, $\cancel{2^{11}} \cdot 3^5 \cdot 5^9$

prime prime prime

Common prime factor 3, 5

smallest power 3^5

smallest power 5^3

$GCD = 3^5 * 5^3$

$3^5 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 243$

$5^3 = 5 \cdot 5 \cdot 5 = 125$ $\}$ $\times$

$= GCD = 30,375$

(b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

No common prime factor

$= GCD = 1$

(c) $23^{31}, 23^{17} \Rightarrow GCD = 23^{17} = 141,050,039_{\dots}$

(d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
GCD = $41 \cdot 43 \cdot 53$, bc all prime nums and have no divisors other than 1 and themselve
GCD = 1
(e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
$\Rightarrow$ No prime factors, so gcd = 1
(f) 1111, 0
GCD = 1111, bc gcd of any positive int and 0 is that int
(37) positive integers a and b
(36) $2^a - 1 \Rightarrow 2^b - 1$ divides $2^{kb} - 1$
$2^b - 1$
(1) $\Rightarrow 2^{kb} - 1 = (2^b - 1)(2^{(k-1)b} + 2^{(k-2)b} + ... + 2^b + 1)$
$\Rightarrow 2^{kb} \equiv 1 \mod (2^b - 1)$

(2) let R = remainder when a/b
$a = qb + R$, q = quotient $0 \leq R < b$
$2^a = 2^{qb+R} = 2^{qb} \times 2^R$
(3) $2^{qb} \equiv 1 \mod (2^b - 1) = 2^a \equiv 2^R \mod (2^b - 1)$
where $R = a \mod b$
(4) $2^a - 1 \equiv 2^R - 1 \mod (2^b - 1)$
$\Rightarrow (2^a - 1) \mod (2^b - 1) = 2^{a \mod b} - 1$
(37)
$d = \gcd(a, b)$, there exist x and y ints
$\Rightarrow d = xa + yb$, d is largest int to divide a, b
$2^a - 1$ and $2^b - 1$

$\gcd(2^a-1, 2^b-1)$ must divide $2^{\gcd(a,b)} - 1$

Let $d = \gcd(a,b)$, $\Rightarrow 2^a - 1 \equiv 2^{a \bmod b} - 1$
$\equiv 2^a - 1 \pmod{2^b - 1}$

$2^b - 1 \equiv 2^{b \bmod a} - 1$
$\equiv 2^b - 1 \pmod{2^a - 1}$

$\Rightarrow 2^{\gcd(a,b)} - 1$ divides both

$\Rightarrow \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$
for any positive int a and b