Jan 25th

Greatest common divisor

a, b integers

$\gcd(a,b) = d$ - largest natural number that divides both a & b.

if $\gcd(a,b)=1$ we call a, b relatively prime.

ex: $\gcd(6,4)=2$

$\gcd(9,20)=1$

Thm: if $a = p_1^{k_1} \cdots p_l^{k_l}$ be distinct primes.

$b = p_1^{m_1} \cdots p_l^{m_l}$

$\Rightarrow \gcd(a,b) = p_1^{\min(k_1,m_1)} \cdots p_l^{\min(k_l,m_l)}$

ex: $\gcd(30,24)$ ...

<u>Proof</u>: Let $d = p_1^{\min(k_1,m_1)} \cdots p_l^{\min(k_l,m_l)}$, then $d|a$ and $d|b$

if c is another number that divides both a and b.

$c = q_1^{t_1} \cdots q_s^{t_s}$ - prime factorization $q_i \neq q_j$

$a = cx = q_1^{t_1} \cdots q_s^{t_s} x = p_1^{k_1} \cdots p_l^{k_l}$ by the FTA the prime factorization is unique

$\Rightarrow$ the prime factorizations are the same

$\Rightarrow q_1$ should be one of the p_i's

say $p_1 = q_1$ and $t_1 \leq k_1$ and so on.

$\Rightarrow$ if $c|a \Rightarrow c = p_1^{t_1} \cdots p_l^{t_l}$

$t_1 \leq k_1, \cdots, t_l \leq k_l$ in the same way if $c|b \Rightarrow$

$t_1 \leq m_1, \cdots, t_l \leq m_l$

$\Rightarrow t_1 \leq \min(k_1,m_1), \cdots, t_l \leq \min(k_l, m_l)$

$t_i \leq \min(k_i, m_i)$

$\Rightarrow$ the largest common divisor $\gcd(a,b) = \cdots$

<u>Corallary</u>: if $c|a$ and $c|b$ then $c | \gcd(a,b)$

Proof: $\gcd(a,b) = p_1^{\min(k_1,m_1)} \cdots p_l^{\min(k_l,m_l)}$

if $c|a$, $c|b$ any $\Rightarrow c = p_1^{t_1} \cdots p_l^{t_l}$ $t_i \leq \min(k_i, m_i)$

ex: $\gcd(24,30)$

$24 = 2^3 \cdot 3^1 \cdot 5^0$ $\qquad c = 2^{t_1} 3^{t_2} 5^{t_3}$

$30 = 2^1 \cdot 3^1 \cdot 5^1$ $\qquad$ all common divisors $1, 2, 3, 6$

$1|6, 2|6, 3|6$

Recall: if $p|ab$ and $p \nmid a \Rightarrow p|b$, p is prime

need not be ture if p is not prime

ex: $p=4$, $4 | 2 \cdot 6$

$4 \nmid 2$ but $4 \nmid 6$

Let $a | bc$ and $\gcd(a, b) = 1 \Rightarrow a | c$

in particular if $a = p$ and $a \nmid b \Rightarrow a | b$
(p : prime)

$\gcd(a, b) = 1$

ex: $4 | 9 \cdot 12 = 108$ $\gcd(4, 9) = 1$

$\Rightarrow 4 | 12$, $a = 4$, $b = 9$, $c = 12$ 4 is not prime

if $\gcd(a, b) \neq 1$, this may fail

ex: $a = 4$, $b = 2$, $c = 6$

$4 | 12 = 2 \cdot 6$ and $4 \nmid 6$ cuz $(4, 2) \neq 1$

to use the formula for $\gcd(a, b)$ need to be able to factor #s into primes.

Ex: $\gcd(200381, 51176) =$?

Euclidean Algorithm

a, b divide a by b to the remainder

$a = bq + r$

$d | a$ & $d | b$ (a, b) (b, r)

$\Leftrightarrow d | b$ and $d | r$ in particular $\gcd(a, b) = \gcd(b, r)$

ex: $33 = 9 \times 3 + 6$

$\gcd(33, 9) = \gcd(9, 6) = 3$