Some applications

I. The factorization of numbers give another way to find gcd. This may not be efficient but useful.

Example: find gcd (700, 360)

$$700 = 2^2 \cdot 5^2 \cdot 7 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1$$

$$360 = 2^3 \cdot 3^2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^0$$

Find the smaller power in each prime

$$\gcd(700, 360) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0$$

$$= 2^2 \cdot 5^1 = 20.$$

Observation: Let m, n be two integers.

$\gcd(m, n) = 1$ is equivalent to

m, n have no common primes.

II. A useful lemma.

Lemma: Let m, n be integers such that $\gcd(m,n) = 1$. Then for any integers α, β, $\gcd(m^\alpha, n^\beta) = 1$.

Proof: $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$n = q_1^{\beta_1} \cdots q_s^{\beta_s}$

$\gcd(m,n) = 1 \Rightarrow \{p_1, \cdots p_r\} \cap \{q_1, \cdots q_s\} = \phi$.

$m^\alpha = p_1^{\alpha_1 \alpha} \cdots p_r^{\alpha \alpha_r}$

$n^\beta = q_1^{\beta_1 \beta} \cdots q_s^{\beta_s \beta}$

m^α, n^β have no common primes.

and hence $\gcd(m^\alpha, n^\beta) = 1$ $\square$

III. Proposition: Let n be an integer and p a prime. Then we can find an integer $\alpha \geq 0$ and an integer m such that

$$n = p^{\alpha} m$$

and $\gcd(p, m) = 1$.

Proof: When $p \nmid n$, $\alpha = 0$, $m = n$.

When $p \mid n$, by the factorization

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

One of $p_1, \cdots p_r$ must be p; say p_1,

then $\alpha = \alpha_1$ $\quad m = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

We can show:

$$\gcd(p,m) = \gcd\left(p,\ p_2^{\alpha_2}\cdots p_r^{\alpha_r}\right) = 1. \square$$

Definition: Let n be an integer and p a prime. Then we can find $\alpha \geq 0$ and m such that $n = p^\alpha m$ with $(p,m) = 1$.

We write: $\text{ord}_p(n) = \alpha$.

We also write $p^\alpha \| n$

read: p^α exactly divides n.

Example: $48 = 2^4 \cdot 3$

$$\Rightarrow \text{ord}_2(48) = 4$$

$$2^4 \| 48.$$