# CS1231 Review 13

1. If $n$ is composite, then it has a divisor $d$ with $1 < d \leq \sqrt{n}$.

2. If $n$ does not have positive divisor $d$ with $1 < d \leq \sqrt{n}$, then n is prime.

3. Two integers $a$, $b$ are **relatively prime (coprime)** if $\gcd(a,b) = 1$.

4. If $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$, then $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$.

5. Base $b$ Expansion of Integers Let $b(> 1)$ be an integer. If $n \in \mathbb{N}$, then it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_0 b^0$$

e.g. $3 = 1 \times 2^1 + 1 \times 2^0$ $\quad 3 = (11)_2$

where $k \in \mathbb{Z}^*$ and $0 \leq a_i < b$ for $i = 0, \ldots, k$ and $a_k \neq 0$.

The **Base** $b$ **Expansion of** $n$ is denoted as $(a_k a_{k-1} \cdots a_0)_b$

6. Binary Expansion: The base 2 expansion.

7. Modular Exponentiation. Find $b^n$ **Mod** $m$.

(1) compute $n = (a_k \ldots a_1 a_0)_2$.

(2) Compute $r_0 = b, r_1 = b^2, r_2 = b^4, \ldots, r_k = b^{2^k}$ **Mod** $m$.

(3) $b^n$ **Mod** $m = r_0^{a_0} r_1^{a_1} \cdots r_k^{a_k}$ **Mod** $m$.

8. (The Euclidean Algorithm) If $a$ **Mod** $b = r$, then $\gcd(a,b) = \gcd(b,r)$

12 Mod 5 = 2 $\quad \gcd(12,5) = \gcd(5,2)$

9. Let $a, b \in \mathbb{Z}^+$ and $d = \gcd(a,b)$. Then $d = as + bt$.

12, 5 $\quad 1 = \gcd(12,5)$ $\quad 1 = 12s + 5t$

② $12 \div 5 = 2 \cdots\cdots 2$

① $5 \div 2 = 2 \cdots \boxed{1}$ gcd

$2 \div 1 = 2 \cdots\cdots 0$

stop

To find s, t

① $1 = 5 - 2 \times 2$

② $= 5 - (12 - 5\times 2) \times 2$

$= 5 - 12 \times 2 + 5 \times 4$

$= 5 \times 5 - 12 \times 2$

$\therefore s = -2,\ t = 5$

an inverse of 12 mod 5 is $(-2)$