## CS1231 Review 13

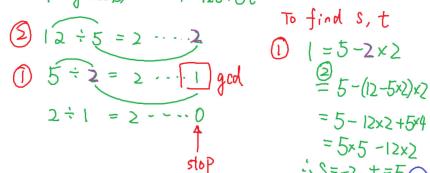
- 1. If n is composite, then it has a divisor d with  $1 < d \le \sqrt{n}$ .
- 2. If n does not have positive divisor d with  $1 < d \le \sqrt{n}$ , then  $\underline{N}$  is  $\underline{Prime}$ .
- 3. Two integers a, b are relatively prime (coprime) if  $\frac{2cd}{b} = \frac{1}{2cd} = \frac{1}{2c$
- 4. If  $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$  and  $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$ , then  $\gcd(a, b) = \frac{p_1^{b_1} (a_1, b_2)}{p_2^{b_2} \dots p_n^{b_n}}$ .
- 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

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

$$\textbf{e.g.} \quad \textbf{3} = | \textbf{x} \textbf{2}^1 + | \textbf{x} \textbf{2}^0 \quad \textbf{3} = (| \textbf{1} \textbf{1})_{\textbf{2}}$$
where  $k \in \mathbb{Z}^*$  and  $0 \le a_i < b$  for  $i = 0, \dots, k$  and  $a_k \ne 0$ .

The Base b Expansion of n is denoted as  $(A_k Q_{k-1} - \cdots Q_b)_b$ 

- 6. Binary Expansion: The base 2 expansion.
- 7. Modular Exponentiation. Find  $b^n \operatorname{Mod} m$ .
  - (1) compute  $n = (a_k \dots a_1 a_0)_2$ .
  - (2) Compute  $r_0 = b, r_1 = b^2, r_2 = b^4, \dots, r_k = b^{2^k} \text{ Mod } m$ .
  - (3)  $b^n \text{ Mod } m = r_0^{a_0} r_1^{a_1} \cdots r_k^{a_k} \text{ Mod } m$ .
- 8. (The Euclidean Algorithm) If  $a \mod b = r$ , then  $\gcd(a,b) = \gcd(b,r)$   $\gcd(a,b) = \gcd(b,r)$   $\gcd(a,b) = \gcd(a,b)$ . Then  $\gcd(a,b) = \gcd(a,b)$ . Then  $\gcd(a,b) = \gcd(a,b)$ .
- 1 = 900(12,5) 1 = 125 + 5t



an inverse of 12 is

LI Wei Email: matliw@nus.edu.sg