Properties of gcd

November 22, 2009

First, recall the definition:

Definition 1. *Let a, b be integers, not both zero. The largest integer that divides both a and b is called the greatest common divisor of a and b. Notation:* $\gcd(a, b)$.

Next, give a native generation:

Definition 2. *Let $a_1, a_2, \ldots, a_k$ be integers, not both zero. The largest integer that divides $a_1, a_2, \ldots, a_k$ is called the greatest common divisor of $a_1, a_2, \ldots, a_k$. Notation:* $\gcd(a_1, a_2, \ldots, a_k)$.

For greatest common divisor, there are many properties:

1. $\gcd(a, b) = \gcd(b, a)$, and $\gcd(\cdots, a_i, \cdots, a_j, \cdots) = \gcd(\cdots, a_j, \cdots, a_i, \cdots)$ for all $i, j \in \{1, 2, \ldots, k\}$.

2. $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$, and $\gcd(\cdots, a_i, \cdots) = \gcd(\cdots, -a_i, \cdots)$ for all $i \in \{1, 2, \ldots, k\}$.

3. $\gcd(a, b) = \gcd(a, b + an)$ for all $n \in \mathbb{Z}$, and $\gcd(\cdots, a_i, \cdots, a_j, \cdots) = \gcd(\cdots, a_i, \cdots, a_j + a_i n, \cdots)$ for all $i, j \in \{1, 2, \ldots, k\}$ and $n \in \mathbb{Z}$.

4. If $m | \gcd(a_1, \cdots, a_k)$, then

$$m \cdot \gcd\left(\frac{a_1}{m}, \cdots, \frac{a_k}{m}\right) = \gcd(a_1, \cdots, a_k).$$

   Specially, we have

$$\gcd\left(\frac{a_1}{\gcd(a_1, \cdots, a_k)}, \cdots, \frac{a_k}{\gcd(a_1, \cdots, a_k)}\right) = 1.$$

5. $d = \gcd(a, b)$ if and only if $\begin{cases} d|a \text{ and } d|b; \\ \text{for all } n \in \mathbb{N}, \text{ if } n|a, n|b, \text{ then } n|d. \end{cases}$

   $d = \gcd(a_1, \cdots, a_k)$ if and only if $\begin{cases} d|a_1, \cdots, d|a_k; \\ \text{for all } n \in \mathbb{N}, \text{ if } n|a_1, \cdots, n|a_k, \text{ then } n|d. \end{cases}$

6. $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$.

7. $m > 0$, then $\gcd(ma_1, \cdots, ma_k) = m\gcd(a_1, \cdots, a_k)$.

8. $\gcd(a, m) = 1$, then $\gcd(m, ab) = \gcd(m, b)$.

9. $\gcd(a, m) = 1$, if $m|(ab)$, then $m|b$.

10. $\gcd(m_1, m_2) = 1$, $m_1|n$, $m_2|n$, then $(m_1m_2)|n$.

11. $\gcd(a, b)$ is the smallest positive linear combination of a and b.

Proof. Properties 1, 2, 3 are very easy.

4. Let $d = \gcd\left(\frac{a_1}{m}, \cdots, \frac{a_k}{m}\right)$ and $D = \gcd(a_1, \cdots, a_k)$.
   Since $d|\frac{a_i}{m}$, we have $(md)|a_i$ for all $i \in \{1, 2, \ldots, k\}$. Hence, $md \leq D$.
   Since $D|a_i$ and $m|D$, we have $m|a_i$ for all $i \in \{1, 2, \ldots, k\}$. Therefore, $\frac{D}{m}|\frac{a_i}{m}$ for all i. Hence, $\frac{D}{m} \leq d$.
   Therefore $md = D$.

5. In textbook.

6. By part 5, we know that the set of common divisors of a and b equals to the set of divisors $\gcd(a, b)$. Hence, The set of common divisors of $a, \gcd(b, c)$ equals to the set of of common divisors of a, and b, c.

7. By part 4.

8. $\gcd(m, b) = \gcd(m, b\gcd(a, m)) = \gcd(m, \gcd(ba, bm)) = \gcd(m, ba, bm) = \gcd(m, ab)$.

9. By part 8, $\gcd(m, b) = \gcd(m, ab) = |m|$, therefore $m|b$.

10. By part 9 or part 11.

11. In textbook.

□