# 05 Elementary Number Theory

## 05_04 Algorithm _GCD

The Euclidean algorithm for computing the GCD of two positive integers is provided in this section. Suppose a and b are two positive integers such that $a \geq b$. By Division Algorithm, we have $a = b*q + r$, where $0 \leq r < b$. Then

**Theorem 1.** GCD(a, b) = GCD(b, r).

**[Proof]** Suppose s = GCD(a, b). Then $s \mid a$ and $s \mid b$. There are two integers u and v such that $a = s*u$ and $b = s*v$. Thus $r = a – b*q = s*(u – v*q)$. Therefore $s \mid r$. Hence s is a common divisor of b and r. So $s \leq$ GCD(b, r) := t. Since t = GCD(b, r). Then $t \mid b$ and $t \mid r$. There are two integers i and j such that $b = t*i$ and $r = t*j$. Thus $a = b*q + r = t*(i*q + j)$. Therefore $t \mid a$. Hence t is a common divisor of a and b. So $t \leq s$. Consequently, s = t. The proof of Theorem 1 is complete.

Example 1. Find GCD(57, 3).

[Solution] 57 = 3*19 + 0. Thus GCD(57, 3) = GCD(3, 0). Notice that GCD(3, 0) = 3. So GCD(57, 3) = 3.

In general, suppose a and b are two positive integers such that $a \geq b$ and $b \mid a$. Then GCD(a, b) = b.

Example 2. Find GCD(150, 9).

[Solution] 150 = 9*16 + 6,
9 = 6*1 + 3,
6 = 3*2 + 0.

Thus GCD(150, 9) = GCD(9, 6) = GCD(6, 3)
= GCD(3, 0) = 3.

Example 3. Find GCD(58, 5).

[Solution] 58 = 5*11 + 3,
5 = 3*1 + 2,
3 = 2*1 + 1,
2 = 1*2 + 0.

Thus GCD(58, 5) = GCD(5, 3) = GCD(3, 2)
= GCD(2, 1) = GCD(1, 0) = 1.

Notice that we have $0 \leq r < b$ in the division of a = b*q + r. The remainder will become a zero after a fixed number of divisions. We can write a recursive Java method for computing the GCD of two positive integers a and b with $a \geq b$ as follows.

```
public static int GCD(int a, int b) {
    if (a%b == 0)
            return b;
    else
            return GCD(b, a%b);
}
```

The iterative Java method for computing the GCD of two positive integers a and b with a ≥ b is as follows.

```
public static int GCD(int a, int b) {
     int c = 0;
      while (b != 0)
      {
             c = b;
             b = a%b;
             a = c;
       }
       return a;
 }
```