Introduction to Cryptography

Veikko Keränen, Jouko Teeriaho (RAMK, 2006)

ELEMENTARY NUMBER THEORY AND ALGORITHMS

1. Integers and Division

1.4 Greatest Common Divisor and Least Common Multiple

We present central definitions: The *greatest common divisor* (GCD, *gcd*) and the *least common multiple* (LCM, *lcm*).

Definition 1.2
Let a and b be integers (a or $b \neq 0$). The *greatest common divisor* of a and b is a positive integer d such that

(1.1) d divides both integers a and b

and

(1.2) if f divides both a and b, then f divides also d.

The greatest common divisor of a and b is denoted by $gcd(a, b)$.

Definition 1.3
Let a and b be nonzero integers. The *least common multiple* of a and b is a positive integer m such that

(1.3) a and b divide m

and

(1.4) if a and b divide an integer n, then $n = k\,m$ with $k \in \mathbb{Z}$.

The least common multiple of a and b is denoted by $lcm(a, b)$.

Alternative definition for the *greatest common divisor* (*gcd*) and the *least common multiple* (*lcm*) of a and b can also be stated as follows:

gcd(a, b) is the greatest positive integer that divides both a and b;
lcm(a, b) is the least positive integer that is divisible by both a and b.

In order to show that the above mentioned *greatest common divisor*, i.e., gcd(a, b), is a well–definded concept, we show fistly the *existence* of it. Consider, for given a and b, the set consisting of *linear combinations* $x\,a + y\,b > 0$

$$U = \{x\,a + y\,b \mid x \in \mathbb{Z},\ y \in \mathbb{Z},\ x\,a + y\,b > 0\}.$$

Let m be a least (minimal) element of U (the existence of m is quaranteed by the Well–Ordering Axiom). We show that m satisfies conditions (1.1) and (1.2), so that m is, in fact, the desired integer syt(a, b). Obviously, if integer f divides both a and b, then f also divides m. Consequently, m satisfies condition (1.2). By Theorem 1 (*Division Algorithm*), the integer a can be written in the form $a = q\,m + r$, $0 \le r < m$. If $r \ne 0$, then $r \in U$ (because $m \in U$, we have $m = xa + yb$, and hence $r = a - q\,m = a - q(xa + yb) = (1 - qx)\,a + (-qy)\,b$). This is a contradiction with the fact that m is a least element of U. Thus $r = 0$, and therefore $m \mid a$. Analogously $m \mid b$. Consequently, m satisfies also condition (1.1).

The *uniqueness* of gcd(a, b) follows from (1.1) and (1.2). Indeed, if d and d' both satisfy (1.1) and (1.2), then $d \mid d'$ and $d' \mid d$. Both d and d' being positive integers, we obtain the equality $d = d'$.

The *existence* of lcm(a, b) can be justified as follows: Those positive integers that are divisible by both a and b, constitute a nonempty set V. By the Well–Ordering Axiom, the set V contains a least element which, in fact, is the lcm(a, b).

The *uniqueness* of gcd(a, b) can be proved by using the Fundamental Theorem of Arithmetic (Theorem 1.7). This Theorem says that a and b can always be uniquely represented (not taking the order into account) as a product of primes p_i in the form $a = \prod_i p_i^{e_i}, e_i \in \mathbb{N}$, and $b = \prod_i (p_i)^{f_i}, f_i \in \mathbb{N}$. Furthermore, it can be shown that

$$\gcd(a, b) = \prod_i p_i^{\min(e_i, f_i)}$$

$$\mathrm{lcm}(a, b) = \prod_i p_i^{\max(e_i, f_i)}$$

$$\gcd(a, b) \cdot \mathrm{pyj}(a, b) = a\,b.$$

We consider these product representations only shortly by looking at the following example.

Example 1.2

Let $a = 2^5 \cdot 3^2 \cdot 7^2$ and $b = 2^4 \cdot 3^3 \cdot 11^3$. In this setting

$$\gcd(a, b) = 2^{\min(5,4)} \cdot 3^{\min(2,3)} \cdot 7^{\min(2,0)} \cdot 11^{\min(0,3)} = 2^4 \cdot 3^2 \cdot 7^0 \cdot 11^0$$
$$\mathrm{lcm}(a, b) = 2^{\max(5,4)} \cdot 3^{\max(2,3)} \cdot 7^{\max(2,0)} \cdot 11^{\max(0,3)} = 2^5 \cdot 3^3 \cdot 7^2 \cdot 11^3$$
$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = (2^4 \cdot 3^2 \cdot 7^0 \cdot 11^0)\cdot(2^5 \cdot 3^3 \cdot 7^2 \cdot 11^3) = 2^{4+5} \cdot 3^{2+3} \cdot 7^{0+2} \cdot 11^{0+3} = ab.$$

The values of $\gcd(a, b)$ (GCD) and $\operatorname{lcm}(a, b)$ (LCM) can be computed by using *Mathematica* as follows:

```
a = 49; b = 35; GCD[a, b]
```

```
7
```

```
a = 49;  b = 35; LCM[a, b]
```

```
245
```

If the *greatest common divisor* of two given integers is = 1, we say that they are *coprimes*. As an important corollary of the considerations regarding the set U above, we obtain the following

Theorem 1.4
Let a and b be nonzero integers. Then there exist integers u and v such that

$$\gcd(a, b) = u\,a + v\,b.$$

In other words $\gcd(a, b)$ can be represented as a *linear combination* of a and b. In particular, if a and b are coprimes, there exist integers u and v such that

$$u\,a + v\,b = 1.$$

The following lemma is a very natural one.

Lemma 1.5
Let d be a factor of the product $a\,b$ and let $\gcd(d, a) = 1$. Then $d \mid b$.

Proof: Because $\gcd(d, a) = 1$, Theorem 1.4 implies $x\,d + y\,a = 1$ for some integers x and y. Multiplying both sides by b, we obtain $x\,d\,b + y\,a\,b = b$. Because $d \mid a\,b$ by assumption, it follows that $d \mid (x\,d\,b + y\,a\,b)$, i.e., $d \mid b$.

□

Corollary 1.6
Let p be a prime that divides $\prod_{i=1}^{k} a_i = a_1\,a_2 \cdots a_k$, where $a_i \in \mathbb{Z}$, $1 \le i \le k$.
Then p divides at least one of the factors a_i, $1 \le i \le k$.

Proof: Use Lemma 1.5 and mathematical induction with respect to k.

□