# Introduction to Cryptography

Veikko Keränen, Jouko Teeriaho (RAMK, 2006)

# ELEMENTARY NUMBER THEORY AND ALGORITHMS

## 4. Euler's and Fermat's Theorems

### ■ 4.4 Euler's Totient Function and Preservation of Multiplication

**Definition 4.4**
A function $f : \mathbb{N} \longrightarrow \mathbb{N}$ *multiplicative*, if for every pair of integers $(m, n)$ it holds that

$$\gcd(m, n) = 1 \implies f(m \cdot n) = f(m) \cdot f(n).$$

**Theorem 4.6**
Euler's Totient Function $\varphi(m)$ is *multiplicative*.

□

**Proof of Theorem 4.6 (2nd way):** Let $\gcd(m, n) = 1$. Remainders mod $(mn)$ are as follows:

$$\begin{array}{cccccc}
 & \multicolumn{5}{c}{n \text{ colums}} \\
 & \hline
 & 0 & 1 & 2 & \cdots & n-1 \\
 & n & n+1 & n+2 & \cdots & n+(n-1) \\
m \text{ rows} \left\{ \right. & 2n & 2n+1 & 2n+2 & \cdots & 2n+(n-1) \\
 & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & (m-1)n & (m-1)n+1 & (m-1)n+2 & \cdots & (m-1)n+(n-1) \\
 & \uparrow & \uparrow & \uparrow & \cdots & \uparrow \\
 & \equiv 0 \pmod{n} & \equiv 1 \pmod{n} & \equiv 2 \pmod{n} & \cdots & \equiv (n-1) \pmod{n}
\end{array}$$

**Proof (1st way):**
Let $\gcd(m, n) = 1$, $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ and also $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ are Reduced Residue Systems modulo $m$ ($n$ correspondingly). It suffices to show that $\varphi(m) \cdot \varphi(n)$ and the integers $n \cdot a_i + m \cdot b_j$, $1 \le i \le \varphi(m)$ and $1 \le j \le \varphi(n)$, form a Reduced Residue System modulo $m \cdot n$. It is relatively easy to see, that all the integers $n \cdot a_i + m \cdot b_j$,

$1 \le i \le \varphi(m)$ and $1 \le j \le \varphi(n)$, are different modulo $m \cdot n$, and that they are coprimes with $m \cdot n$. (See Lemma 3.2 and Implication (3.2)).

It should be also proved that $k$, with $\gcd(k, m \cdot n) = 1$, is congruent to $n \cdot a_i + m \cdot b_j$ with mod ( $m \cdot n$), when $1 \le i \le \varphi(m)$ and $1 \le j \le \varphi(n)$. Since $\gcd(k, m) = 1$ and $\gcd(k, n) = 1$, it follows by Lemma 4.2 that there are integers $i$ and $j$, $1 \le i \le \varphi(m)$ and $1 \le j \le \varphi(n)$, such that

$$k \equiv n \cdot a_i \pmod{m} \quad \text{and} \quad k \equiv m \cdot b_i \pmod{n}.$$

It follows that both $m$ and $n$ divide the number $k - n \cdot a_i - m \cdot b_j$, i.e., $k - n \cdot a_i - m \cdot b_j = m \cdot m_1$ and $k - n \cdot a_i - m \cdot b_j = n \cdot n_1$ for some $m_1, n_1 \in \mathbb{Z}$. Because $m \cdot m_1 = n \cdot n_1$ and $\gcd(m, n) = 1$, we can conclude by using Lemma 1.5 that $m \mid n_1$ and $n \mid m_1$, i.e., $m \cdot n \mid m \cdot m_1 = n \cdot n_1$. This means that $m \cdot n$ is a divider of $k - n \cdot a_i - m \cdot b_j$, i.e., $k \equiv (n \cdot a_i + m \cdot b_j) \bmod (m \cdot n)$.

□

By using mathematical induction we can prove that if integers $m_1, m_2, \ldots, m_k$ are pairwise coprimes, then $\varphi(m_1 \cdot m_2 \cdots m_k) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_k)$.

**Example 4.1** (Exercise 28)
Fill completely the table below, that is, find all the coprime residue classes (representatives of them) of 120. Pass through the proof of Theorem 4.6 once again in the special case of $\varphi(120) = \varphi(8 \cdot 15) = \varphi(8) \cdot \varphi(15) = 4 \cdot 8 = 32$. The first relevant column has been presented as an example. Indicate also the coprime residue classes of the selected integers (denote them by a square) modulo 8 and modulo 15.

```
Table[Range[0, 7] + i * 8, {i, 0, 14}]
```

$$\begin{pmatrix} & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \boxed{1} & 2 & 3 & 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & \boxed{17} & 18 & 19 & 20 & 21 & 22 & 23 \\ 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \\ 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \\ 40 & \boxed{41} & 42 & 43 & 44 & 45 & 46 & 47 \\ 48 & \boxed{49} & 50 & 51 & 52 & 53 & 54 & 55 \\ 56 & 57 & 58 & 59 & 60 & 61 & 62 & 63 \\ 64 & 65 & 66 & 67 & 68 & 69 & 70 & 71 \\ 72 & \boxed{73} & 74 & 75 & 76 & 77 & 78 & 79 \\ 80 & 81 & 82 & 83 & 84 & 85 & 86 & 87 \\ 88 & \boxed{89} & 90 & 91 & 92 & 93 & 94 & 95 \\ 96 & \boxed{97} & 98 & 99 & 100 & 101 & 102 & 103 \\ 104 & 105 & 106 & 107 & 108 & 109 & 110 & 111 \\ 112 & \boxed{113} & 114 & 115 & 116 & 117 & 118 & 119 \end{pmatrix}$$

**Theorem 4.7**
Let $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ be the representation of $m$ as a product of different primes $p_1, p_2, \ldots, p_r$. Then

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right),$$

In other words

$$\varphi(m) = m \prod_{p \text{ is prime},\, p|m} \left(1 - \tfrac{1}{p}\right)$$

**Proof:** Combine Theorem 1.7 (Fundamental Theorem of Arithmetic), Theorem 4.5 and Theorem 4.6. Details are left as an Exercise.

□

**Example 4.2**
Let us compute $\varphi(3000)$. Because $3000 = 2^3 \cdot 3 \cdot 5^3$, we obtain by Theorem 4.7 that

$$\varphi(3000) = 3000 \cdot (1 - \tfrac{1}{2}) \cdot (1 - \tfrac{1}{3}) \cdot (1 - \tfrac{1}{5}) = 3000 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 800.$$

Thus, out of integers 0, 1, 2, ..., 2999 there are 800 coprimes with respect to 3000. Therefore, there are also 800 Coprime Residue Classes (mod 3000).

*In Mathematica* we can test Theorem 4.7 as follows:

```
m = 100;
Length[CoPrimes[m]]
EulerPhi[m]

m * Apply[Times,
  Table[If[PrimeQ[i] && IntegerQ[m/i], 1 - 1/i, 1], {i, 2, m}]]
```

```
40
```

```
40
```

```
40
```