密码学理论与实践

关于幻灯片 P21, CH8 中的错误

施劲松

跨媒体知识融合与工程应用研究所，西安交通大学

January 7, 2024

西安交通大學

XI'AN JIAOTONG UNIVERSITY

于 slide 的 p21, ch8 中，提到命题 1，

Proposition 1. 对任意正整数 a 和 n，都有 $a^{\varphi(n)+1} \equiv a \pmod{n}$。

这其实是错误的，首先，试考虑这样一种情况，此时 $a = 2, n = 4$，则有

$$\begin{aligned} a^{\varphi(n)+1} &\equiv 2^{2+1} \pmod{4} && (1)\\ &= 2^3 \pmod{4} && (2)\\ &\equiv 0 \pmod{4} && (3)\\ &\neq 2. && (4) \end{aligned}$$

正确的表述应为定理 1。

Theorem 1. 对正整数 a 和 n，$a^{\varphi(n)+1} \equiv a \pmod{n}$ 成立当且仅当 $(n/(a,n),(a,n)) = 1$。

为证明定理 1，首先提出如下之引理。

Lemma 1. 对于正整数 n，其任意之约数 x 满足 $x \mid n$，则有 $\varphi(x) \mid \varphi(n)$。

Proof. 根据算术基本定理，可设

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \tag{5}$$
$$x = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}. \tag{6}$$

其中，$p_1 < p_2 < \ldots < p_k$ 均为素数且对 $i = 1, 2, \ldots, k$ 均有 $0 \le \beta_i \le \alpha_i$。由 $\varphi(x)$ 为积性（可乘）函数知

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}), \tag{7}$$
$$\varphi(x) = \varphi(p_1^{\beta_1})\varphi(p_2^{\beta_2}) \dots \varphi(p_k^{\beta_k}). \tag{8}$$

注意到，对于素数 p 有

$$\varphi(p^\alpha) = \begin{cases} 1, & \text{if} \quad \alpha = 0, \\ p^{\alpha-1}(p-1), & \text{otherwise.} \end{cases} \tag{9}$$

由此可知，对于任意的 $\beta \le \alpha$，均有 $\varphi(p^\beta) \mid \varphi(p^\alpha)$。故对所有的 $i \in \{1, 2, \ldots, k\}$，均有 $\varphi(p_i^{\beta_i}) \mid \varphi(p_i^{\alpha_i})$，可知 $\varphi(x) \mid \varphi(n)$。 ■

Lemma 2. 对任意正整数 x, y，x 模 y 的乘法逆元存在的充分必要条件为 $(x, y) = 1$ 且 $y \neq 1$。

Proof. 显然 x 关于 y 乘法逆元若存在则 $y \neq 1$，考虑 $y > 1$ 的情况。

首先证明必要性，

注意到存在整数 u 使得

$$xu \equiv 1 \pmod{y}. \tag{10}$$

也即 $y \mid (xu - 1)$，故存在整数 v 使得

$$xu + yv = 1. \tag{11}$$

由式 (11) 知 $(x, y) \mid (xu + yv) = 1$，故得 $(x, y) \leq 1 \Rightarrow (x, y) = 1$。必要性得证。

再者证明充分性，

若 $(x, y) = 1$，由 Bézout's identity 知存在整数 u, v 使得

$$xu + yv = 1. \tag{12}$$

则 u 为 x 模 y 的乘法逆元。充分性亦得证。 ■

接下来证明定理 1。

Theorem 1's proof. 记 $d = (a, n)$，则 a 可表示为 $a'd$，同理有 $n = n'd$，且 $(a', n') = 1$。则有

$$a^{\varphi(n)+1} \equiv a \pmod{n} \tag{13}$$

$$\Leftrightarrow n \mid (a^{\varphi(n)+1} - a) \tag{14}$$

$$\Leftrightarrow n \mid a(a^{\varphi(n)} - 1) \tag{15}$$

$$\Leftrightarrow n' \mid a'(a^{\varphi(n)} - 1) \tag{16}$$

$$\Leftrightarrow n' \mid a^{\varphi(n)} - 1. \tag{17}$$

由 n', a 之关系进行分析，

若 $(n', a) = 1$，由欧拉定理知

$$n' \mid a^{\varphi(n')} - 1. \tag{18}$$

注意到 $n' \mid n$，由引理 1 知 $\varphi(n') \mid \varphi(n)$，故

$$(a^{\varphi(n')} - 1) \mid a^{\varphi(n)} - 1. \tag{19}$$

由式 (18)，式 (19) 及整除之传递性知

$$n' \mid a^{\varphi(n)} - 1. \tag{20}$$

故当 $(n', a) = 1$ 时，$a^{\varphi(n)+1} \equiv a \pmod{n}$ 成立。

若 $(n', a) \neq 1$，此时 $a \geq 2, n' \geq 2$ 且有 $\varphi(n) \geq \varphi(n') \geq 1$，故 $\varphi(n) - 1 \geq 0$。若此时能满足 $n' \mid a^{\varphi(n)} - 1$，则说明 $a^{\varphi(n)-1}$ 是 a 模 n' 的乘法逆元，由引理 2 知矛盾，故 $(n', a) \neq 1$ 时命题 1 不成立。

最后注意到

$$(n', a) = 1 \tag{21}$$

$$\Leftrightarrow (n', d) = 1 \tag{22}$$

$$\Leftrightarrow (n', (a, n)) = 1 \tag{23}$$

$$\Leftrightarrow \left(\frac{n}{(a, n)}, (a, n)\right) = 1. \tag{24}$$

这样就完成了定理 1 的证明。 ■