关于欧拉函数 ϕ 的一些结论和性质

本文内容选自《数论概论》(Joseph H.Silverman)

目录

1 问题的提出

为了提出这个问题，我们首先需要承认**费马小定理**：如果 p 是素数且 $p \nmid a$, 则 $a^{p-1} \equiv 1 \pmod{p}$. 定理的证明从略. 现在我们要问的是，是否有依赖模 m 的指数使得

$$a^{???} \equiv 1 \pmod{m}.$$

首先,观察到:如果 $\gcd(a,m) > 1$,则这是不可能的,因为若 $a^k \equiv 1 \pmod{m}$,则对某个整数 $y : a^k = 1+my$, 所以 $\gcd(a,m)$ 整除 $a^k - my = 1$，这得到了矛盾. 但这提示我们观察与 m 互素的数的集合：

$$\{a : 1 \le a \le m, \gcd(a,m) = 1\}.$$

现在我们记 $\phi(m) = \#\{a : 1 \le a \le m, \gcd(a,m) = 1\}$. 这个函数 ϕ 就叫做**欧拉函数**. 显然我们可以得到它的一条简单性质：

性质 1. *若 p 是素数，则 $\phi(p) = p - 1$.*

然后我们有下面非常重要的性质：

性质 2 (**欧拉公式**). *如果 $\gcd(a,m) = 1$, 则*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

为了证明这个结论，我们令

$$1 \le b_1 < b_2 < \cdots < b_{\phi(m)} < m$$

是 0 与 m 之间且与 m 互素的 $\phi(m)$ 个整数. 则我们可以证明下面的引理:

引理 1. 如果 $\gcd(a,m)=1$, 则数列

$$b_1 a, b_2 a, \cdots, b_{\phi(m)} a \pmod m$$

与数列

$$b_1, b_2, \cdots, b_{\phi(m)} \pmod m$$

相同，尽管它们次序不同.

注意到如果 b,m 互素，则 ab,m 互素，从而数列

$$b_1 a, b_2 a, \cdots, b_{\phi(m)} a \pmod m$$

中的每个数同余于数列

$$b_1, b_2, \cdots, b_{\phi(m)} \pmod m$$

中的一个数. 进而，每个数列都有 $\phi(m)$ 个数. 因此，如果能够证明第一个数列中的数对于模 m 不同，则就得到两个数列相同.

假设从第一个数列中取两个数 $b_j a, b_k a$，并且同余，

$$b_j a \equiv b_k a \pmod m.$$

则 $m \mid (b_j - b_k)a$. 但是 a,m 互素，从而 $m \mid b_j - b_k$. 另一方面，b_j, b_k 之差不超过 $m-1$，这说明只能是 $b_j = b_k$. 那也就是第一个数列中的数模 m 不同，这就完成了引理的证明.

使用上述引理可以完成欧拉公式的证明. 引理说明这两个数列是相同的，所以，第一个数列中的数的乘积等于第二个数列中的数的乘积：

$$(b_1 a)\cdot(b_2 a)\cdots(b_{\phi(m)} a) \equiv b_1 \cdot b_2 \cdots b_{\phi(m)} \pmod m.$$

于是得到

$$a^{\phi(m)} B \equiv B \pmod m, \quad B = b_1 b_2 \cdots b_{\phi(m)}.$$

最后由于每个 b_i 与 m 互素，于是 B 与 m 互素. 消去两边的 B 就得到了欧拉公式.

2 欧拉函数与中国剩余定理

下面给出欧拉函数的另外两个重要性质：

性质 3 (欧拉函数公式). *1.* 如果 p 是素数且 $k \geq 1$, 则 $\phi(p^k) = p^k - p^{k-1}$.

2. 如果 $\gcd(m,n)=1$, 则 $\phi(mn) = \phi(m)\phi(n)$.

考虑两个集合，第一个集合是

$$\{a : 1 \leq a \leq mn, \gcd(a, mn) = 1\}.$$

显然，这个集合包含 $\phi(mn)$ 个元素. 第二个集合是

$$\{(b,c) : 1 \leq b \leq m, \gcd(b,m)=1; 1 \leq c \leq n, \gcd(c,n)=1\}.$$

那么这个集合一共有 $\phi(m)\phi(n)$ 个元素.

现在取第一个集合的每个元素，将它与第二个集合的序对对应. 这指的是取第一个集合的整数 a 并把它指派到序对 (b,c) 且满足：

$$a \equiv b \pmod m, a \equiv c \pmod n.$$

那么我们现在就要证明下面两个陈述是正确的：

1. 第一个集合的不同数对应第二个集合的不同序对 (单射)；
2. 第二个集合的每个序对适合第一个集合的某个数 (满射).

要验证 1，我们取第一个集合的两个数 a_1, a_2，假设它们在第二个集合中有相同的象. 这意味着

$$a_1 \equiv a_2 \pmod m, a_1 \equiv a_2 \pmod n.$$

因此 $a_1 - a_2$ 被 m, n 整除，而 m, n 互素，因此 $a_1 - a_2$ 一定被 mn 整除，即

$$a_1 \equiv a_2 \pmod{mn}.$$

这表明 a_1, a_2 是第一个集合中的相同元素.

要验证 2，需要证明对 b, c 的任何已知值，至少可求得一个整数 a 满足

$$a \equiv b \pmod m, a \equiv c \pmod n.$$

而实际上，这就是**中国剩余定理**的结论. 我们先来证之.

定理 1 (中国剩余定理)**.** *设 m, n 为互素的整数，b, c 为任意整数. 则同余式组*

$$a \equiv b \pmod m, a \equiv c \pmod n$$

恰有一个解 $0 \le x < mn$.

由解第一个同余式 $x \equiv b \pmod m$ 开始，其解由形如 $x = my + b$ 的所有数组成，代入第二个同余式得

$$my \equiv c - b \pmod n.$$

已知 $\gcd m, n = 1$，由线性同余式定理知恰有一个解 $y_1 : 0 \le y_1 < n$. 则

$$x_1 = my_1 + b$$

给出了原来同余式的解，这是唯一解 $0 \le x_1 < mn$. 从而完成了欧拉函数公式的证明.

3 欧拉函数与因数和

我们定义 $\sigma(n) = n$ 的所有因数之和 (包括 1 与 n). 仿照欧拉函数，可以证明若 $\gcd(m,n) = 1$, 则 $\sigma(mn) = \sigma(m)\sigma(n)$.

再定义 $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r), d_1, d_2, \cdots, d_r$ 为 n 的因数. 下面首先来证明一个引理：

引理 2. *如果 $\gcd(m,n) = 1$, 则 $F(mn) = F(m)F(n)$.*

设 $d_1, d_2, \cdots, d_r$ 为 n 的因数且 $e_1, e_2, \cdots, e_s$ 为 m 的因数.m, n 互素的事实揭示了 mn 的因数恰好是各种乘积 $d_ie_j, 1 \le i \le r, 1 \le j \le s$. 进而，每个 d_i 和每个 e_j 互素，所以 $\phi(d_ie_j) = \phi(d_i)\phi(e_j)$. 我们计算

$$F(mn) = \sum_{i=1}^{r}\sum_{j=1}^{s} d_ie_j = \sum_{i=1}^{r} d_i \cdot \sum_{j=1}^{s} e_j = F(m)F(n).$$

利用该引理，可以证明欧拉函数的下述求和公式：

定理 2 (欧拉函数求和公式)**.** 设 $d_1, d_2, \cdots, d_r$ 是 n 的因数，则

$$\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n.$$

设 $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$. 容易证明对素数 p 有 $F(p^k) = p^k$. 现在将 n 分解为素数幂的乘积，比如 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. 于是就有

$$\begin{aligned} F(n) &= F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) \\ &= F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) \\ &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= n. \end{aligned}$$

4 欧拉函数的其他性质

性质 4. 假设 $p_1, p_2, \cdots, p_r$ 是整除 m 的不同素数, 那么

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

对 m 进行分解：$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. 那么

$$\begin{aligned} \phi(m) &= \phi(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) \\ &= \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) \\ &= (p_1^{k_1} - p_1^{k_1 - 1}) \cdot (p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1}) \\ &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \end{aligned}$$

性质 5. 如果 n 是奇数，则 $\phi(2n) = \phi(n)$; 若 n 是偶数，则 $\phi(2n) = 2\phi(n)$.

性质 6. $\phi(mn) = \phi(m)\phi(n) \cdot \dfrac{d}{\phi(d)}, \quad d = \gcd(m, n).$

性质 7. $\phi(\operatorname{lcm}(m, n)) \cdot \phi(\gcd(m, n)) = \phi(m) \cdot \phi(n).$

5 参考文献

https://en.wikipedia.org/wiki/Euler%27s_totient_function