费马小定理及其欧拉推广

Alvin 2019/01/23
idealvin@qq.com

费马小定理是数论中的一个定理，最早由17世纪的法国“业余”数学家费马(Fermat)发现，从而得名。这个定理是说：

> 给定素数 p 与整数 a，p 与 a 互素(没有 1 之外的公约数)，则有:
>
> $$a^{p-1} \equiv 1 \pmod{p}$$

这里出现了一个同余符号≡，$a \equiv b \pmod{n}$ 表示 a、b 除以 n 的余数相同。因此，费马定理就相当于 a^{p-1} 除以 p 的余数是 1。可以找两个简单的数验证一下费马定理，如取 $p=7$，$a=2$，那么 $2^6-1=63$，确实是 7 的倍数。

同余

证明费马定理，需要用到同余的性质。同余只是简单的带余数除法，如 23 与 13 除以 5 的余数都是 3，即 23 与 13 关于 5 同余，用同余符号表示就是 $23 \equiv 13 \pmod{5}$。一个明显的结论是:

> $a \equiv b \pmod{n}$ 等价于 $a-b=kn$，k 是任意整数。

现在给定整数 a_1，a_2，b_1，b_2，若

$$\begin{aligned} a_1 &\equiv b_1 \pmod{n} \\ a_2 &\equiv b_2 \pmod{n} \end{aligned}$$

那么必定有:

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \pmod{n} \\ a_1 - a_2 &\equiv b_1 - b_2 \pmod{n} \\ a_1 \times a_2 &\equiv b_1 \times b_2 \pmod{n} \end{aligned}$$

上述 3 条性质很容易证明。同余意味着:

$$a_1 - b_1 = k_1 n$$
$$a_2 - b_2 = k_2 n$$

两式分别相加、相减容易得到:

$$(a_1 + a_2) - (b_1 + b_2) = (k_1 + k_2)n$$
$$(a_1 - a_2) - (b_1 - b_2) = (k_1 - k_2)n$$

从而证明了前两条性质(事实上证明费马定理用不到这两条，这里只是顺带证明一下)。而对于第 3 条，我们有:

$$a_1 \times a_2 = (b_1 + k_1 n)(b_2 + k_2 n)$$

简单的计算后得到:

$$a_1 \times a_2 - b_1 \times b_2 = (k_1 k_2 + k_1 b_2 + b_1 k_2)n$$

从而证明了第 3 条性质。

上述第 3 条性质，可以看作同余的乘法，很容易推广到多个同余式相乘的情况。特别的，有下面的结论:

> 若 $a \equiv b \pmod{n}$，则 $a^k \equiv b^k \pmod{n}$。

作为应用，可以用上面这条性质计算 23^{99} 除以 7 的余数:

$$23^{99} \equiv 2^{99} = 8^{33} \equiv 1^{33} = 1 \pmod{7}$$

所以结果是 1。

费马定理的证明

考虑 a，$2a$，$3a$ $\cdots$ $(p-1)a$ 这 $p-1$ 个数，由于 p 与 a，1，2，$\cdots$ $p-1$ 都互素，所以 p 不能整除这 $p-1$ 个数中的任何一个，即它们除以 p 的余数都不是 0，而只可能是 1 到 $p-1$ 中的一个。

另外，它们中的任意两个，除以 p 的余数不相同，否则令:

$$ia \equiv ka \pmod{p} \quad (i,\ k < p)$$

即 p 整除 $(i-k)a$，因为素数 p 与 a 是互素的，所以只可能 p 整除 $i-k$。但是 $i-k$ 的绝对值小于 p，所以必定有 $i=k$。从而证明上述 $p-1$ 个数除以 p 的余数各不相同，事实

上，恰好得到如下 $p-1$ 个不同的余数：

$$1, \ 2, \ 3, \ \cdots, \ p-1$$

根据同余的第3条性质，就得到:

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

即有:

$$1 \cdot 2 \cdot 3 \cdots (p-1) \cdot (a^{p-1}-1) = kp$$

因为 p 不能整除 $1, \ 2, \ 3 \ \cdots \ p-1$ 中的任何一个，所以必定有 p 整除 $a^{p-1}-1$，从而证明了费马定理。

费马定理的欧拉推广

欧拉(Euler)是 18 世纪的另一位数学天才，他证明了费马定理更一般的形式，即以其名字命名的**欧拉定理**:

> 给定正整数 n 与整数 a，a 与 n 互素，那么有:
>
> $$a^{\varphi(n)} \equiv 1 \pmod{n}$$

这里 $\varphi(n)$ 称为欧拉函数，它表示小于 n 且与 n 互素的正整数个数。由欧拉函数的定义，当 n 为素数 p 时，容易看出 $\varphi(p)=p-1$，将这个式子放到欧拉定理中，即得到费马定理。

欧拉定理的证明与费马定理是类似的，这里只给出证明思路。记 $\varphi(n)=k$，即小于 n 且与 n 互素的正整数有 k 个，设这 k 个数分别为 $x_1, \ x_2 \ \cdots \ x_k$，分别乘以 a 得到:

$$x_1a, \ x_2a \ \cdots \ x_ka$$

这 k 个数都与 n 互素(记得 a 也与 n 互素)。同时，这 k 个数除以 n 的余数恰好是 $x_1, \ x_2 \ \cdots \ x_k$ (为什么？)。所以像证明费马定理中一样，我们得到:

$$x_1 \cdot x_2 \cdots x_k \cdot a^k \equiv x_1 \cdot x_2 \cdot x_3 \cdots x_k \pmod{n}$$

由于 n 与 $x_1, \ x_2 \ \cdots \ x_k$ 互素，从而得到:

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

也就证明了欧拉定理。