费马小定理

费马小定理是数论中的一个定理.在信中,费马还提出 a 是一个质数的要求.这个要求实际上不存在.其内容为:

假如 a 是一个整数,p 是一个质数的话,那么

$$a^p \equiv a \pmod{p}.$$

假如 a 不是 p 的倍数的话,那么这个定理也可以写成

$$a^{p-1} \equiv 1 \pmod{p}.$$

费马于 1636 年发现了这个定理,在一封 1640 年 10 月 18 日的信中他第一次使用了上面的书写方式.

证明:

因为 $(a,p)=1$,则 $a,2a,\cdots,(p-1)a$ 分别按某个重排顺序,模 p 同余于 $1,2,\cdots,p-1$.故有 $a^{p-1}\cdot(p-1)!\equiv(p-1)!\pmod{p}$.因为 p 是素数,因此 p 与 $(p-1)!$ 互素,因此,$a^{p-1}\equiv 1\pmod{p}$.