



## 费马数

当  $n=0, 1, 2, 3, \dots$  时,  $2^{2^n} + 1$  总是素数吗?

法国著名数学家费马(Pierre de Fermat, 1601 - 1665)的职业是律师,但他知识渊博,在语言学方面造诣颇深,精通法语、意大利语、西班牙语、拉丁语、希腊语,数学只是他的业余爱好.虽然他只能在闲暇思考和研究数学,却取得了惊人的成就,被誉为“业余数学之王”.他特别喜爱数论,曾提出过许多猜想,最著名的大概就是费马大定理了.另外,他还对微积分和概率论的创立做出了重要的贡献.

这个问题是费马在 1640 年给梅森(M. Mersenne, 1588 - 1648)的信中宣布的一个猜想.当时的背景是这样的:虽然欧几里得在公元前 300 年已经证明了素数有无穷多个,但素数的分布究竟有什么规律仍然是一个谜.特别地,人们致力于寻找这样一个公式  $f(n)$ ,使得当  $n$  取遍所有的正整数时,  $f(n)$  总能给出素数.现在,为了纪念费马,人们记  $F_n = 2^{2^n} + 1$ ,称  $F_n$  为费马数.通过简单的手算可知前 5 个费马数分别为:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3,$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5,$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17,$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257,$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537.$$

它们的确都是素数!费马由此推测所有的  $F_n$  也将都是素数,因

此他相信自己已经解决了那个古老的问题,即找到了一个总能给出素数的公式  $F_n$ . 他承认自己不能证明这个猜想,后来他又对这个猜想的正确性表示了怀疑.

到了 1732 年,大数学家欧拉(Euler, 1707 - 1783)终于发现下一个费马数  $F_5$  不是素数,从而否定了费马的猜想.事实上,欧拉找到了它的一个素因子 641,并且

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

按理说,费马数的研究应该到此为止了,但出人预料的是不少人仍然对它情有独钟.继欧拉之后,人们希望找到费马数为素数的情形,但奇怪的是至今还没有发现一个新的费马素数,也就是说,除了上述已知的五个费马数  $F_0, F_1, F_2, F_3, F_4$  为素数外,再也没有证明其他的某个  $F_n$  为素数.当然,困难在于这些费马数  $F_n$  随着  $n$  的递增会变得越来越大,超出了现代计算机所能处理的范围.人们猜测也许只有有限个  $F_n$  为素数,但目前这一猜想仍然无法证明.

另一方面,人们却发现了近 50 个费马数是合数.例如,1880 年兰德里(Landry)发现  $F_6$  为合数,有一个素因子为 274177.莫海德(Morehead)与外斯滕(Western)分别在 1905 年和 1909 年证明了  $F_7$  和  $F_8$  也是合数,但  $F_7$  的因子分解直到 1971 年才完成,而  $F_8$  的全部素因子也是在 1981 年使用计算机才得到的.

对费马数的理论研究也取得了一些有价值的结果.可以证明费马数具有以下性质:(1)  $F_n$  为素数当且仅当  $F_n$  整除  $3^{(F_n-1)/2} + 1$ ; (2) 当  $n > 1$  时,  $F_n$  的每个素因子必然形如  $2^{n+2}k + 1$ , 其中  $k$  为正整数; (3) 如果  $p$  为素数且  $p^2$  整除  $F_n$ , 则  $p^2$  也整除  $2^{p-1} - 1$ . 另外,有人猜测每个费马数  $F_n$  均无平方因子,但该猜想至今仍未得到解决.

总而言之,目前对费马数的研究分成了三种情形:(1)对少数

几个  $F_n$  人们得到了它的因子分解, 例如  $F_7$ ; (2) 对有些  $F_n$  目前仅知其为合数, 但尚未找到任何一个素因子, 如  $F_{14}$ ; (3) 对大部分已知的费马数  $F_n$  也只是发现了一部分素因子, 如  $F_9, F_{10}$ , 等等.

令人惊奇的是费马数不仅仅是一些神秘的大数, 而且出现在另外的数学领域中. 例如, 高斯在 1801 年证明: 一个正  $n$  边形可用直尺与圆规画出当且仅当  $n$  要么是 2 的方幂, 要么具有形式  $n = 2^k p_1 p_2 \cdots p_r$ , 其中  $k > 0$  且  $p_i$  恰好是两两不同的费马素数. 关于尺规作图的详细说明可参看后面的问题 065. 另外, 在近年来的数字信号处理中也用到了费马数.