

1.11 素数的故事

(1) 名不符实的冠名

素数并不素, 它的定义和名称似乎给人一种印象, 认为素数是质

朴简单的一种最基本的数,其实算术中麻烦事大都是由它惹起的。例如,我们知道的哥德巴赫猜想和孪生素数的黎曼猜想;1989年,Amdabl Six 小组在美国加利福尼亚圣克拉大学用 Amdabl 1200 超级计算机捕捉到一对孪生素数

$$1706595 \times 2^{11235} \pm 1$$

可见素数名不符实。

还有一个在数学史上贻笑大方的名不符实的故事是关于威尔逊定理的事。有一个关于素数的定理,用英国法官威尔逊(J. Wilson, 1741~1793)冠名。

威尔逊定理:若 p 为素数,则 p 可整除 $(p-1)! + 1$;若 p 为合数,则 p 不能整除 $(p-1)! + 1$ 。

事实上,这条定理是莱布尼茨首先发现,后经拉格朗日证明的;威尔逊的一位擅长拍马屁的朋友沃润(E. Waring)于 1770 年出版的一本书中却吹虚说是威尔逊发现的这一定理,而且还宣称这个定理永远不会被证明,因为人类没有好的符号来处理素数,这种话传到高斯的耳朵里,当时高斯也不知道拉格朗日证明了这一定理,高斯在黑板前站着想了 5 分钟,就向告诉他这一消息的人证明了这一定理,高斯批评威尔逊说:“他缺乏的不是符号而是概念。”

两百多年来,全世界的数论教科书上都照样把这一定理称为威尔逊定理,看来还历史以本来面貌,更换本定理的冠名已无必要,也不易纠正这么多年来文献与教材上的称呼了。

威尔逊定理应用很广,例如对较大的素数 p ,我们虽然无力算出 $(p-1)!$ 的值,但却知道 $(p-1)!$ 被 p 除的余数是 -1 或 $p-1$ 。事实上,由于 $(p-1)! + 1$ 可被 p 整除,则存在自然数 n ,使得 $(p-1)! + 1 = np$, $(p-1)! = np - 1 = (n-1)p + (p-1)$,所以 $(p-1)!$ 被 p 除的余数是 -1 或 $p-1$ 。

由于威尔逊定理戏剧性的冠名以及它的内容的重要性,难怪有

人戏称：“如果一个人不知道威尔逊定理，那他就白学了算术。”

下面介绍威尔逊定理的一种证明：

设 p 是素数， $p=2$ 时，定理成立不足道。对于奇素数，令 $a \in A = \{2, 3, \dots, p-2\}$ ，则 $B = \{a, 2a, 3a, \dots, (p-1)a\}$ 中不会有对于除数 p 同余的两个数；事实上，若 $\alpha a, \beta a \in B$ ， $\alpha a \equiv \beta a \pmod{p}$ ，则 $a|\alpha - \beta$ 可被 p 除尽，而 $|\alpha - \beta|a \in B$ ，但 B 中数不可能被 p 除尽。于是 B 中数被 p 除得到的余数形成的集合 $C = \{1, 2, \dots, p-1\}$ 。

设 B 中被 p 除余 1 的数是 γa ：

①若 $\gamma = 1$ ，则 $\gamma a = a$ ， γa 被 p 除余 a ，又 $a \geq 2$ ，与 $\gamma a \equiv 1 \pmod{p}$ 矛盾，故 $\gamma \neq 1$ 。

②若 $\gamma = p-1$ ，则 $\gamma a = pa - a$ ，它被 p 除余 a ，所以 $\gamma \neq p-1$ 。

③若 $\gamma = a$ ，则 $\gamma a = a^2$ ，由于 $a^2 \equiv 1 \pmod{p}$ ，故应有 $a^2 - 1 = (a+1)(a-1) \equiv 0 \pmod{p}$ ，这只能是 $a=1$ 或 $a=p-1$ ，此与 $a \in A$ 矛盾，故 $\gamma \neq a$ 。

由①，②，③知 $\gamma \neq a$ ，且 $\gamma \in A$ 。

a 不同时， γ 亦相异；若 $a_1 \neq a_2$ ， $a_1, a_2 \in A$ ，且 $\gamma a_1 \equiv \gamma a_2 \equiv 1 \pmod{p}$ ，因 $\gamma a_1, \gamma a_2 \in B$ ，而 B 中数关于 $\text{mod } p$ 不同余，可见 $a_1 \neq a_2$ ，则 $\gamma_1 \neq \gamma_2$ 。

依次取 a 为 $2, 3, \dots, \frac{p-1}{2}$ ；使 $\gamma a \equiv 1 \pmod{p}$ 的数 γ 分别为 $\frac{p-1}{2} + 1, \frac{p-1}{2} + 2, \dots, p-2$ ，即

$$\begin{aligned} 2 \times \left(\frac{p-1}{2} + 1 \right) &\equiv 3 \times \left(\frac{p-1}{2} + 2 \right) \equiv \dots \equiv \frac{p-1}{2} (p-2) \\ &\equiv 1 \pmod{p} \end{aligned}$$

从而

$$\begin{aligned} \left[2 \times \left(\frac{p-1}{2} + 1 \right) \right] \left[3 \times \left(\frac{p-1}{2} + 2 \right) \right] \dots \left[\frac{p-1}{2} (p-2) \right] \\ \equiv 1 \pmod{p} \end{aligned}$$

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

又 $p-1 \equiv -1 \pmod{p}$, 则

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

从而 $(p-1)! + 1$ 可被 p 除尽。

若 p 是合数, p 有因数 q , $1 < q \leq p-1$, 从而 $(p-1)!$ 可被 q 整除; $(p-1)! + 1$ 不能被 q 整除, 亦不能被 p 整除。

(2) 不能实施的素数判别法

威尔逊定理给出了一个判别法:

整数 $p \geq 2$ 是素数当且仅当 $(p-1)! + 1$ 可被 p 整除。

从字面上看, 这个定理已经明白无误地给出了一个简洁的 $+$ $-$ \times \div 算法, 可以判断任何一个正整数是不是素数。可惜 $(p-1)!$ 太无情了, 使得我们没有那么多时间和抄写空间(纸张或计算机内存)来弄清 $(p-1)!$ 是几! 例如 1876 年, 法国数学家卢卡斯(A. Lucas)用手和笔发现了一个 39 位的素数

$$p = 2^{127} - 1$$

$$= 170141183460469231731687303715884105727$$

即使有朝一日某国某人算出了 $[(2^{127} - 1) - 1]!$, 以每页书可排 2000 个阿拉伯数字计算, $[(2^{127} - 1) - 1]!$ 可以印成 500 页的书至少 2×10^{33} 本, 比全世界的总藏书量还多得多! 何况, 还有比 $2^{127} - 1$ 更大的素数待判定呢!

可见, 威尔逊定理只有理论的价值, 是一个无实施价值的判别法, 或者说, 它是一个无效的坏算法。

我们渴望设计出有效算法来判别任给的正整数是否是素数。这种迫切性从费马数和哥德巴赫猜想等问题上, 可以感觉到。

所谓费马数, 是指形如

$$F_n = 2^{2^n} + 1$$

的数,其中 $n = 0, 1, 2, \dots$

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537,$$

$$F_5 = 4294967297$$

F_0 到 F_4 容易判定它们都是素数, F_5 是 42 亿多的大数, 费马当年无力判断 F_5 是否素数, 他只是大胆猜想 F_n 每个都是素数。1732 年, 欧拉算出 $F_5 = 641 \times 6700417$, 从而否定了费马关于费马数素性的猜想。

1880 年, 法国数学家卢卡斯算出

$$F_6 = 274177 \times 67280421310721$$

1971 年, 有人对 F_7 得出素因子分解, 1981 年, 有人得出 F_8 的素因子分解。

1980 年, 有人得出 F_{9448} 的一个因子是

$$19 \times 2^{9450} + 1$$

1984 年, 有人得出 F_{23471} 的一个因子是

$$5 \times 2^{23473} + 1$$

1986 年, 有人用超级计算机连续运算十天得知 F_{20} 是合数。

至今知道的素费马数还只是 F_0, F_1, F_2, F_3, F_4 。

这个问题不能彻底解决的要害是今日没有搞出判别素数的有效算法, 也有一种潜在的厄运, 那就是判定一个数是否是素数和移动河内塔上的盘子一样, 本质上就不存在有效算法。

(3) 素数病毒越来越多

把 π 的小数点删去, π 就改写成了一个阿拉伯数字的无穷序列, 问: 长几的前缀是素数?

例如, 3 与 31 是素数; 314159 是第三个素前缀; 1979 年美国数学家贝利(R. Baillie)等人发现 π 上的第四个素前缀

$$31415926535897932384626433832795028841$$

敢问： π 还有第五个素前缀吗？第六个，第七个……呢？

把 π 换成 e ，换成 $\sqrt{2}, \sqrt{3}, \dots, \sqrt[3]{2}, \sqrt[3]{3} \dots \lg 2, \lg 3 \dots$ 再问同类问题，又该怎么解答呢？

即使是温和一些的问题，例如下面问题仍然是悬案

$$\underbrace{11 \cdots 1}_{n \text{ 个 } 1} = 10^{n-1} + 10^{n-2} + \cdots + 10 + 1 = \frac{1}{9}(10^n - 1)$$

当 n 为素数时，例如 $\frac{1}{9}(10^{47} - 1)$ ， $\frac{1}{9}(10^{59} - 1)$ ， $\frac{1}{9}(10^{71} - 1)$ ， $\frac{1}{9}(10^{73} - 1)$ ， $\frac{1}{9}(10^{83} - 1)$ ， $\frac{1}{9}(10^{97} - 1)$ 等等，是否是素数？或更一般地，问 $\underbrace{11 \cdots 11}_{n \text{ 个 } 1}$ 是否是素数？

n 个 1

其中 n 为任意指定的自然数。

真是心血来潮，随便一问就会难倒人！这样提出问题会使人对素数产生一种反感。在形形色色应接不暇的问题当中，似应首选那些具有重要应用背景或理论背景，又有能力解决的问题去研究。

(4) 重要的问题是落实算术基本定理

算术基本定理告知，任一大于 1 的整数都可以唯一地表成某些素数的乘积，即 $n = p_1 p_2 \cdots p_m$ ，其中 n 是任意给定的大于 1 的整数， p_1, p_2, \dots, p_m 是被 n 唯一确定的素数。

问题是，如何由 n 具体地求出 p_1, p_2, \dots, p_m ？

这是一个有重要实用背景和计算机计算的时间复杂度理论背景的大问题。是数论的中心课题之一，也是计算机科学的主攻方向之一。

假设某年某人设计出了一个有效算法，能在多项式时间内求得 $n = p_1 p_2 \cdots p_m$ 中的 p_1, p_2, \dots, p_m 的值，那么当 n 是素数时， n 就是 p_1 ，即此算法可以有效地判定素数，从而可以在多项式时间内解决前面提出的诸多问题，例如费马数 F_n 是否素数 (n 是任意给定的自然数)，以

及无理数(例如 π)的前缀是否素数等问题。这里说的“多项式时间”是指对一个问题,存在一个多项式 $p(n)$, n 是要判定的整数的输入长,即它的位数的一个倍数。

在实用上,例如在保密通讯与密码破译当中,需要对大合数进行素因子分解,一般这种大合数有百位之大,所以目前各军事大国都集大量人力物力,研究这种合数素分解问题,但至今并未听说有明显进展。

素数判定和合数素分解,可能类似与求拉姆赛数那样,一个数一个搞法,不能形成普遍的有效算法,这就太不好办了。

如果真搞出素分解算法,则对任给定的大偶数,可以在多项式时间内表成两个素数之和或发现哥德巴赫猜想的反例。事实上,对于任意的 $2k$,表成 $1 + (2k - 1), 2 + (2k - 2), 3 + (2k - 3), \dots$,对这些和中的每对数加以判定,若都是素数,则可把 $2k$ 表成两素数之和,否则就反驳了哥德巴赫。

我们期望的这种素分解的有效算法能解决这么多非常之难的问题,可见设计出它的难度是诸多数论难题难度之集大成,即使这种算法存在,也是十分之难以设计出来,我们甚至还应想到它根本就不存在,以避免望梅止渴,水中索月。