1.3 算术的基因和基理

算术四则运算，人人都有体会，那就是加减法简单，乘法也不太难，有个“九九歌”，背熟了去乘就是了。除法里“事儿”多，除得尽还好，除不尽还要考虑约分与余数，等等，花样不少。例如：$100 \div 4$ 可以写成

$$\frac{100}{4}=\frac{2^2\times 5^2}{2^2}=5^2=25$$

我们看到，除法实质上是分子分母的约分，等到把分子分母的公共因子都约光了，剩下的就是既约分数，如果这时分母为 1，就除尽了。分子上的因子有两个 2，两个 5，这两个因子不能再变小，当然 4 和 25，或 20，也是 100 的因子，但它们还可以变小，那些不能再变小的因子，

即除了 1 与自身外，别的自然数除不尽的自然数，是最简单朴素的了，我们称这种数为素数（朴素的素）或质数（质朴的质），1 也是这类性质的数，但大家约定 1 不称为素数，因为如果让 1 取得素数资格，例如 100 则可以写成 $100=1\times1\times1\times1\times1\times\cdots\times1\times2\times2\times5\times5$，前方爱写几个 1 就写几个 1，这就很不妙，一个自然数写成素数之积的形式时，形状就不唯一了。经验表明，如果不让 1 参加，一个自然数若不是素数，例如 100，4 什么的，可以唯一地写成若干素数的积，这一结论可以用数学归纳法证明，这就是著名的算术基本定理。

大于 1 的不是素数的自然数称为合数，即由若干素数相乘而成的数。

素数是合数的基因，任给大于 1 的自然数 N，存在唯一的素数列 $P_1\leqslant P_2\leqslant\cdots\leqslant P_n$，使得 N 唯一地写成 $N=P_1P_2\cdots P_n$，此定理称为算术的基本定理，算术中很多证明，尤其是涉及除法时，主要靠这条结论去说理。

如果 N 是合数，则 $N=P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_m^{\alpha_m}$，$m\geqslant1$，$P_1, P_2, \cdots, P_m$ 是互异素数，$\alpha_1, \cdots, \alpha_m$ 是正整数，其中 $P_1<P_2<\cdots<P_m$，则显然 $P_1\leqslant\sqrt{N}$。据此，我们可以用下面的所谓“筛法”筛出不超过 N 的一切素数。这种筛法是希腊的埃拉托色尼（Eratosthenes）发明的，以 $N=30$ 为例，说明筛法的操作如下：

由于不超过 N 的合数的最小素因子不超过 $\sqrt{N}$，因此欲求不超过 N 的一切素数，只需把 $1, 2, \cdots, N$ 中不超过 $\sqrt{N}$ 的素数的倍数划去（筛除），剩下的就是素数。

$$1,\ \overset{\circ}{2},\ \overset{\square}{3},\ ④,\ \overset{\triangle}{5},\ ⑥,\ 7,\ ⑧,\ \boxed{9},\ ⑩,\ 11,\ ⑫,\ 13,\ ⑭,\ \boxed{15},\ ⑯,$$

$$17,\ ⑱,\ 19,\ ⑳,\ \boxed{21},\ ㉒,\ 23,\ ㉔,\ \triangle 25\ ㉖,\ \boxed{27},\ ㉘,\ 29,\ ㉚$$

$\sqrt{30}<6$，所以只考虑划去 2, 3, 5 的倍数，剩的是不超过 30 的那些素数：2, 3, 5, 7, 11, 13, 17, 19, 23, 29。

显然，这种方法只能写出不超过 N 的自然数中素数的清单，N 后面的自然数中还有不少素数，例如30之后的31就是。欧几里得第一个证明，素数的个数是无穷的。

事实上，若所有素数为 $P_1, P_2, \cdots, P_k$，取 $N = P_1 P_2 \cdots P_k + 1$，$N > 1$，设 N 本身是素数，N 能除尽 $P_1 P_2 \cdots P_k + 1$（商为1），又 $P_1, P_2, \cdots, P_k$ 是所有素数，则 N 是某个 P_i，$i \in \{1, 2, \cdots, k\}$，于是 N 能除尽 $P_1 P_2 \cdots P_k$，$P_1 P_2 \cdots P_k + 1$ 被 N 除余1，与 $N = P_1 P_2 \cdots P_k + 1$ 矛盾。若 N 是合数，则 N 有一个素数因子 P，于是 $P = P_i$，$i \in \{1, 2, \cdots, k\}$，$P$ 能除尽 $P_1 P_2 \cdots P_k$，不能除尽 $P_1 P_2 \cdots P_k + 1$，即 P 不能除尽 N，与 P 是 N 之因子矛盾，可见全体素数不是有限个。

素数既然是算术中的基因，几乎所有的算术命题当中，都有素数参与其中，有关素数的命题集中了算术学科的难点。广为人知的难题很多，例如下面两个就是算术中难题的代表。

(1) 关于孪生素数的黎曼猜想：孪生素数有无穷个

所谓孪生素数，即相差为2的一对素数，例如(3, 5)，(5,7)，(11,13)，(17,19)，等等。

至今无人能证明或反驳这一猜想。

(2) 哥德巴赫猜想

1742年6月7日，圣彼得堡中学教师，德国人哥德巴赫(Goldbach)给瑞士数学家欧拉写信提出如下猜想：

每个大于或等于6的偶数都是两个素数之和；每个大于或等于9的奇数都是三个素数之和。

两素数之和当然是偶数，但是事情让哥德巴赫反过来一提，可就给数学界惹来了天大的麻烦。欧拉给哥德巴赫的回函中说："我不能证明它，但是我相信这是一条正确的定理。"欧拉无能为力的问题，别人怕是很难解决了。在其后的150多年当中，多少专业的和业余的数论工作者，都兴趣盎然地冲击这一看似真实的命题，无奈人人不

得正果。1900年,数学界的领袖人物希尔伯特(Hilbert)在巴黎召开的世界数学家大会上向20世纪的数学家提出23个待解决的名题,其中哥德巴赫猜想列为第八问题。可惜20世纪的百年奋斗仍然辜负了希尔伯特的期望。

奉劝阅历尚浅、热情十足的年轻朋友,不可受某些不懂数学的记者们的误导,随便立志以攻克哥德巴赫猜想为己任,而应当从实际出发,打好坚实的数学理论基础,培养数学研究的能力,再来考虑攀登高峰的问题。

这里面对的是一个数学问题,不能沿用物理学家诉诸反复若干次实验来证实的办法,例如有人对不超过33×10^6的偶数逐一验证,哥德巴赫猜想都是成立的,但那仍然不能解决问题。

下面是近百年来关于哥德巴赫猜想的大事记。

1912年,数学家朗道提出相近的弱猜想:

存在一个自然数M,使得每个不小于2的自然数皆可表成不超过M个素数之和。

此猜想于1930年证明为真;如果$M\leqslant3$就好多了。

1937年,苏联数学家维诺格拉多夫证明了哥德巴赫猜想的后半句为真,即大于或等于9的奇数是三个素数之和,这是关于哥德巴赫问题的重大突破,引起了不小的轰动。但前半句至2000年基本上未被解决。

我们约定:命题"大于等于6的偶数可表成α个素数之积加上β个素数之积"记成$(\alpha+\beta)$,则哥德巴赫问题是:证明或反驳$(1+1)$。

1920年,朗道证明了$(9+9)$。

1924年,拉德马哈尔证明了$(7+7)$。

1932年,依斯特曼证明了$(6+6)$。

1938年,布赫塔布证明了$(5+5)$。

1938年,华罗庚证明了几乎所有的偶数都成立$(1+1)$。

1940 年，布赫塔布等证明了(4 + 4)。

1947 年，雷尼证明了($1+\alpha$)。

1955 年，王元证明了(3 + 4)。

1957 年，小维诺格拉多夫证明了(3 + 3)。

1957 年，王元证明了(2 + 3)。

1962 年，潘承洞证明了(1 + 5)。

1962 年，潘承洞、王元证明了(1 + 4)。

1965 年，布赫塔布、小维诺格拉多夫、邦比尼证明了(1 + 3)。

1966 年，陈景润证明了(1 + 2)，于 1973 年发表。

尽管(1 + 2)离(1 + 1)只“一步之遥”，但一步登天的事谈何容易！从陈景润搞出(1 + 2)至今已有 30 多年，一直没有人在这个阵地上前进半步，我国的陈景润仍然是此项世界纪录的保持者。

培养出如陈景润这样杰出的数学家，不但具有广深扎实的数学素质，而且具有全身心奉献科学事业的品质，乃是我们教育工作者的一项重要责任。