从数学的原子——素数谈起

古希腊时代，哲人留基波和德谟克里特推测世界由一种不可再分的最小的“原子”构成【1】。现代科学部分证实了他们的猜想：继道尔顿提出原子论后，布朗运动（Brownian motion）进一步证实了原子的存在性；现代科学也部分否证了“原子论者”的猜想：19 世纪末，约瑟夫·汤姆森（J. J. Thomson，1856-1940）在阴极射线的工作中发现了电子，从而原子是不可分的设想被打破[1]；而在“标准模型”（Standard Model）中“基本粒子”不只有一种，而是多种。

高斯（Carl Friedrich Gauss，1777-1855）曾说过：“数学是科学的皇后，数论是数学的皇冠。”【2】而素数，就是这顶皇冠上一颗璀璨的明珠，毋宁说素数就是数学的原子。

---

[1]尽管严格来说，这里的“原子”（道尔顿（John Dalton，1766-1844）提出的作为化学反应中不可再分的基本要素）与古希腊“原子论者”的作为基本粒子的“原子”并非同一个意思。古希腊者所谓原子，类似现代物理之基本粒子（Elementary particle），尽管在这里“基本粒子”之所以“基本”是因为要分割它们所需要的最小能量反而会形成一对新的“基本粒子”，因此它们不可再分。这也体现出，到了某一层面上之后，我们不能再将概念直接套用上去，而必须以崭新的目光来看东西，例如在现代物理中，温度达到某一级别后就不是通过感觉（有谁曾感受过几十亿度的高温？）或别的等等来定义的，而是通过光谱来定义的。在现代物理中，还有弦论（String theory）等“大一统理论”以及多种其他的理论可能有更基本的构成要素

素数是只有它自己和 1 是因数的数。素数在数学的地位在两个方面上符合“原子”的地位。一，在数学中有“算术基本定理”（Fundamental theorem of arithmetic）——任何一个自然数都可以唯一分解成一些素数的乘积，即任何一个自然数都可唯一地写成$p_1^{n_1} \times \ldots\ldots \times p_n^{n_n}$的形式，其中$\mathrm{p}_1$到$p_n$是素数，例如 6 可以写成 2*3，200 即$2^3 \times 5^2$。从这个意义上来说，素数是自然数的基本组成部分，素数是组成数学宇宙的原子；二，同时，我们知道，不仅有自然数，还有负数、有理数、实数等等等等，因此素数不能说是所有数论的核心要素，但是却是自然数论的基本组成部分，这也符合物理中原子并不是最基本的粒子但是却是化学反映中最基本的成分的特征。

那么除了唯一分解定理这一最基本的结果之外，素数在数论上还有什么用呢？那可真是数不胜数，我们提几个初等数论的例子吧。假如我们对一个正整数的因数感兴趣，那么我们怎么才能知道这个正整数的因数的数量呢？一个简单的方法就是如下的定理：

设 k 是一个正整数，$p_1 \ldots\ldots p_n$是互不相同的素数，k 的素因数分解的标准形式是$p_1^{n_1} \times \ldots\ldots \times p_n^{n_n}$，那么这个正整数的因数的数量正是$(n_1+1) \ldots\ldots (n_n+1)$。这是为什么呢？因为 k 的因数也是正整数，同时也是 k，即$p_1^{n_1} \times \ldots\ldots \times p_n^{n_n}$的因数，那么它们就可以分解成$p_1^{b_1} \times \ldots\ldots \times p_m^{b_m}$，其中 m 小于等于 n，$b_i$小于等于$n_i$。因为$b_1$可以取$n_1$+1 个不同的整数……$b_m$可以取$n_n+1$个不同的整数，所以所有 k 的因数的个数就是$(n_1+1) \ldots\ldots (n_n+1)$啦。一个正整数的所有因数之和（例如 18 的因数有 1，2，3，6，9，18，所以其因数之和为 1+2+3+6+9+18=39）也与素数有着密不可分的关系，我们有这样一个结果：若正整数 k 的标准素因数分解形式为$p_1^{n_1} \times \ldots\ldots \times p_n^{n_n}$，则 k 的所有因数之和为$\frac{{p_1}^{(n_1+1)}}{p_{1-1}} \ldots\ldots \frac{{p_1}^{(n_n+1)}}{p_{n-1}}$。

既然素数如此重要，同时它自身的特性又是如此之独特，涉及到它的相关理论又是如此是优美，素数本身自然也吸引了许多数学家的目光。一个最自然的问题就是，素数有多少个？答案是素数的数量是无限的，正像

无论我们写出多少正整数，我们都可以在我们写出的最大正整数后加 1 得到一个更大的新的正整数一样，无论我们写出多少个素数，我们总可以也通过令 a 等于所有这些素数的乘积再加 1，得到一个更大的而我们还未写下的素数，因而素数是无限的（至于为什么那样的数 a 是素数，这就留给读者回答）。在有的一些我们耳熟能详的自然的问题是：我们看到很多数都能分解成 2 个素数之和，例如 5 可以分解成 2+3，10 可以分解成 5+5，那么是否任何一个大于 2 的数都能分解成两个素数之和呢？这就是大名鼎鼎的哥德巴赫猜想（Goldbach's conjecture）；类似的问题还有，我们还发现了有这样“孪生”素数（twin prime）——只相差 2 的素数，例如 3 和 5，5 和 7 等，这样的“孪生素数”的对是否是无限的呢？虽然在这些问题上我们已经有了长足的发展，但都没有完全解决。我们看到，这些问题的表述都十分简单。数论就是这样，其中某些重要而回答起来非常难的问题，问起来却十分简单，也正是因为这表述形式的简单，不少数学爱好者都向这些问题发起了冲锋的号角，

只可惜用的都是初等数学的方法。在这里提醒一下，欧拉（Leonhard Euler，1707-1783）是初等数学的大师，也曾对这个问题刻加思考[3]，如果一个问题欧拉没有解决出来，那么很大概率它难以用初等方法解决。因此，与其“思而不学则殆”，不如去多学一些，尝试去获得足够的积淀和在学习和与之相伴的思考中享受乐趣。

数学家塞吉兰（Serge Lang，1927-2005）在巴黎向公众作数学科普演讲时曾问了听众一个问题：数学是什么？一个听众回答：数学就是研究数字的科学。而塞吉兰则说实际上我们可以完全不用数字做数学。[4]数学其实可以说是研究“结构”的科学（这里给读者留一个疑问：什么的“结构”？）。而代数正是这其中的代表。代数抛却“细微”[2]的各种具体情况，而研究普遍与抽象的结构。因此代数可以囊括从电路[3]到物理化学[4]的一切。

代数的一个重要分支是群论（Group Theory），群论的创立者是伽罗瓦（Évariste Galois，1811-1832）。群论的指导思想是：jump over calculations, group the

[2]这并不是说代数不能研究细微的结构
[3]例如可以用布尔代数表示电路
[4]例如物理和化学中研究粒子、物理现象或晶体的对称性时需要用到群论的知识

operations。一个“群”（Group）就是：一个集合，和集合上的一个操作 a，满足以下三个条件：

对于集合中的每个元素，都有一个恒等元，对集合中任何元素 b 和恒等元作操作 a 得到的还是元素 b；对集合中每个元素，都有一个逆元，对集合中任何元素和它的逆元作操作就会得到恒等元；同时该集合对操作 a 封闭，对集合中任二元素作操作 a 得到的元素还在集合中。

任何东西，只要满足以上三个条件，就是一个“群”。例如，一张桌子和把它旋转这个操作就构成了一个群。其中恒等元是不转动，而逆元即向相反的方向转动。魔方也是一个群。而更具“数学”意味的，整数和它的加法也是一个群，其中恒等元是 0，而任何一个元素 x 的逆元即-x。而同时，对于群论证明的任何一个定理和性质，都能套用到群的任何一个例子上。这也体现出了抽象代数的思想：重结构，普遍而抽象。而当附加了更多条件之后，我们就有了相应于有理数的加法和乘法的“环”（Ring）、相应于实数加法和乘法的“域”（Field）

等。而代数与数论的结合，就是代数数论。

我们知道，二次方程有根式解，16 世纪时，卡尔达诺（Girolamo Cardano，1501－1576）通过几何法找到了三次方程的根式解，而四次方程的求根公式也找到了，那么四次以上方程有没有根式解呢？数学家们一直为之不懈努力。直到了阿贝尔（Niels Henrik Abel，1802-1829）、伽罗瓦以崭新的目光开辟了抽象代数这一全新领域，这一问题才有了答案。伽罗瓦的伟大成果就是使用群论证明了 4 次以上的方程没有根式解。

素数与代数碰撞又产生了美妙的花火，这就是我们将要学习的东西了。怀抱着这样一种心情：即使发现不了星星，也能欣赏星星的美丽啊[5]，让我们踏开了脚步。

有人或许会问，尽管素数对于数学的结构如此之重要，可是它有什么“用”呢？确实，摆弄数字，看起来只是一种纯粹的智力游戏，或许最多也不过是加上了优美的成分。20 世纪早期的数论学家哈代（Thomas Hardy，1840-1928）就曾说过：

有人认为纯数学家以其工作的无用性为荣，并宣称他们的工作没有实际应用价值。这种念头是基于高斯的一句不谨慎的话，其大意是：如果数学是科学中的皇后，那么数论由于其极端无用性而成为数学中的皇后——我从没能找到这话的确切引用。我敢肯定高斯的原话(如果真的是他说的)被很粗鲁地曲解了。如果数论能够被应用于任何实用的、显赫的目的，如果它能像物理甚至化学那样直接增加人类的欢乐和减少人类的痛苦，那么高斯或其他数学家决不会愚蠢到为这种应用哀叹或后悔。但是科学可为善服务，也可为恶助纣(特别是在战争时期)，这样高斯和另一些数学家就应该庆幸有一种科学，就是他们的科学，由于其远离人类日常的活动而保留了其纯洁性。[6]

可是他也没想到，他的研究在几十年后的密码学（Cryptography）、信息论（Information theory）等学科里大派用场。

例如密码学，传统的密码，如对字符作替换（比如

说将“a”替换成“g”、“b”替换成“f”等，当然还有更复杂的但也类似的），是很容易破解的，因为只要一个密码需要被使用的次数足够多，我们就可以对密码中的字符作频率统计，例如我们知道英文中最常使用的一个字母是“e”，比率达$\frac{1}{16}$，因此我们就可以合理地推断，密码中出现最多的字符就代表的是“e”，再根据上下文，再根据正确率比对，我们很容易就作出破解。而在现代，我们的一切几乎都跟密码有关：我们的储蓄、网络支付、账户等等，每天密码被使用的次数数以亿计。而我们的信息和财富安全就需要密码学来保护。要算出两个素数的成绩比较简单，可是对一个大数作素因数分解却十分困难，以至于靠暴力运算即使 1 亿年也不能找到正确答案。现代密码学的一个基本方法，就是将两个素数的乘积作为公匙，要破解一个密码，实际上也就是将一个大数作素因数分解。我们的密码及信息安全，正是建立在与之相关的数论结果之上。[7] 这只是数论应用的其中一个例子。

这正是“无用之用”的一种可能诠释。我们现在凭

着我们的兴趣与对知识的渴望而得到的东西，尽管现在看似没用，却可能在某一天大派用场。就像据说法拉第（Michael Faraday，1791-1867）在电刚刚能够利用起来的时候回答电的用处时对女王说的：一个婴儿对您有什么用呢？[8]我们不可能等到需要用时再去发展，一来在没有原先的结果的指引的情况下，我们可能根本就不知道要发展什么；而反过来说，现代数学的发展推动了现代物理中弦论的创立与发展，这体现了纯粹的知识作为指引与引导的作用；二来，假使我们真的到时候再去发展相关所需的知识，那我们的创新和得用可能晚上相当长的一段时间。例如，假如没有黎曼（Bernhard Riemann，1826-1866）和希尔伯特（David Hilbert，1862-1943）对几何学的发展，爱因斯坦（Albert Einstein，1879-1955）要创立和发展相对论就不会那么顺利；而中国大陆社会今天对芯片技术发展的需要也体现了基础科学的积累与沉淀的重要性。

参考文献

【1】 The atomists, Leucippus and Democritus: fragments, a text and translation

with a commentary by C.C.W. Taylor, University of Toronto Press Incorporated 1999, ISBN 0-8020-4390-9, pp. 157-158.

【2】 Waltershausen, Wolfgang Sartorius von (1965) [1856]. Gauss zum Gedächtniss. Sändig Reprint Verlag H. R. Wohlwend. ISBN 978-3-253-01702-5, p. 79.

【3】 潘承洞，潘承彪. 哥德巴赫猜想[M]. 北京：科学出版社. 1981.，引言

【4】 塞吉·兰. 做数学之美妙[M]. 李德琅 译. 四川：四川大学出版社. 2001.，p. 4.

【5】 结城浩. 数学女孩 2[M]. 丁灵 译. 北京：人民邮电出版社. 2015.，p. 297.

【6】 哈代. 一个数学家的自白[M]. 王希勇 译. 北京：商务印书馆. 2007.，pp. 85-86.

【7】 吴军. 数学之美[M]. 人民邮电出版社. 2012.， pp. 155-162.

【8】 COHEN, I. BERNARD (1946). Authenticity of Scientific Anecdotes. Nature, 157(3981), 196–197.