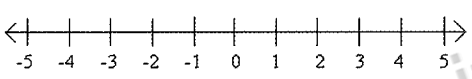
模算术 —内在美和人的好奇心的驱动

Richard Taylor

模算术作为数学家的主要关心对象至少已经有 250 年了，而且它仍是当前研究中的一个非常活跃的论题. 在本文中，我将会解释什么是模算术，说明它为什么对数学家们重要，并且讨论一下最近的一些突破.

对模算术的研究，在它几乎全部历史中，都由它的内在美和人类的好奇心所驱动. 但是，作为那些标志着人类知识进步的意外新发现之一，过去半个世纪里，模算术在“现实世界”中找到了重要应用. 今天，模算术理论 (如：Reed–Solomon 纠错码) 是 DVD 存储方式或者卫星无损传输大量数据的依据. 更进一步，例如保证我们银行交易安全的加密 (cryptographic) 码同样和模算术理论有紧密的联系.

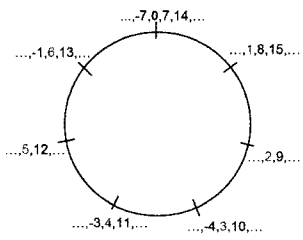
你可以将通常的算术看成是对沿着“数线”延伸的点的操作. 为了做 3 加 5, 你从 0 开始，向右数 3, 接着再向右数 5, 得到 8. 为了做 3 乘以 5, 你从 0 开始，向右数 5 次 3 就得到 15. 这类操作应该从小学就被大家所熟悉.



在模算术里，人们把整数排列在一个圆周上而不是沿着一条无限长的直线，就像小时排列在时钟上. 从一开始人们就需要决定我们的时钟上有多少“小时”. 它可以是任意的数，不一定是 12. 作为第一次说明，让我们假定我们的钟表上有 7“小时” —— 我们说我们在做 *模 7 算术*. 为了做 3 加 5 模 7, 你从 0 开始，顺时针数 3, 然后再顺时针数 5, 得到 1. 为了做 3 乘以 5 模 7, 你从 0 开始，顺时针数 5 次 3, 又得到 1. 我们可以写成

$$3+5 \equiv 1 \bmod 7 \quad \text{和} \quad 3\times 5 \equiv 1 \bmod 7.$$

模 7



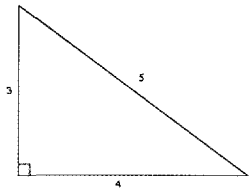
就如我们上面提到的，7 是没有什么特殊的. 我们可以把任意多个“小时”放在我们的时钟上和做模任意整数的算术. 我们通常的时钟可以用来做模 12 的算术. 如果你去看一场从 11 点开始的两小时长的电影，那么你将在 1 点看完. 这说明了在模 12 算术中的下述等式：

$$11+2 \equiv 1 \bmod 12.$$

这可以看作是对我们通常的算术的惯用变体，而且读者可以合理地想这会不会不仅仅是好奇而已. 我希望这篇文章能够让大家信服这点.

一个重要的观察是，在通常的算术里任何算术等式在任何整数模算术中也是成立的. 这可以通过如下观察得到：把通常的数线围着模钟的表面环绕，这就把通常的算术转化成了模算术.

为了说明数学家关心模算术的一个主要原因，让我从一个最古老的数学问题开始：找 Pythagoras (毕达哥拉斯) 三数组，即找方程



$$X^2 + Y^2 = Z^2$$

的整数解. 由 Pythagoras 定理，这相当于找所有的边 (在同一单位下测量) 是整数的直角三角形. 譬如

$$3^2 + 4^2 = 5^2,$$

这给出一个直角三角形.

3800 多年前巴比伦的泥板 Plimpton 322 列了一些 Pythagoras 三数组. 该泥板的第 2 列列举了 X 的值，第 3 列列举了相应的 Z 的值，而 Y 的值没有列出来. 用现代的记号，Plimpton 322 列的是以下解答：

X	Y	Z
119	120	169
3367	3456	4825
4601	4800	6649
12709	13500	18541
65	72	97
319	360	481
2291	2700	3541
799	960	1249

X	Y	Z
481	600	769
4961	6480	8161
45	60	75
1679	2400	2929
161	240	289
1771	2700	3229
28	45	53

值得注意的是其中的一些解非常复杂，但我们却不知道他们是怎么生成的. 是通过反复试验还是巴比伦人知道一个算法？

能肯定的是 1500 年后，希腊人知道了一个能够生成这个方程所有整数解的算法. 我们知道这个是因为 Euclid (欧几里得) 在他著名的《 Elements (几何原本) 》的第 10 卷中解释了这个方法. 用现代的代数记号，Euclid 证明了方程 $X^2 + Y^2 = Z^2$ 的所有整数解有如下形式：

$$X = \frac{(a^2 - b^2)c}{2}, \qquad Y = abc, \qquad Z = \frac{(a^2 + b^2)c}{2},$$

其中 a, b, c 都是整数并且 a, b 是奇数 [1].

但如果我们把问题稍微变一下，会怎样呢？方程

$$X^2 + Y^2 = 2Z^2,$$

或者

$$X^2 + Y^2 = 3Z^2$$

的整数解是什么样的呢？会发现只要我们找到一个非零整数解，Euclid 的《几何原本》里的方法就能用，而且我们能够详细地描述所有的整数解. 例如方程

$$X^2 + Y^2 = 2Z^2$$

有一个解

$$X = 1, \ Y = 1, \ Z = 1 \ ,$$

那么我们可以推导出一般的整数解有如下形式

$$X = (a^2 + 2ab - b^2)c/2, \quad Y = (-a^2 + 2ab + b^2)c/2, \quad Z = (a^2 + b^2)c/2,$$

其中 a, b, c 是整数，并且 a, b 是奇数 [2].

1) 原文误为 "a, b, c 有相同的奇偶性". —— 译注
2) 原文误为 "a, b, c 有相同的奇偶性". —— 译注

但是如果你去找 $X^2+Y^2=3Z^2$ 的非零整数解，你将一无所获. $X^2+Y^2=Z^2$ 或者 $X^2+Y^2=2Z^2$ 与 $X^2+Y^2=3Z^2$ 之间有什么差别呢？答案来自于模算术.

假设 $X^2+Y^2=3Z^2$ 有一个解，且 X,Y,Z 是非零整数. 我们可以调整 X,Y,Z 的取值，使得没有大于 1 的整数整除所有的 X,Y,Z. (如果 X,Y,Z 有大于 1 的公因子，则把 X,Y,Z 同时除以这个公因子，它们仍然是原方程的一个解. 如果需要的话，我们重复这一过程. 注意到随着 X,Y,Z 的绝对值逐次递减，但依然保持是整数，这个过程最终会停止.) 然后原方程在模 3 算术上会有一个解. 但在模 3 算术上我们有

$$3\times Z^2\equiv 0\times Z^2\equiv 0 \bmod 3$$

和

$$0^2\equiv 0 \quad 和 \quad 1^2\equiv 1 \quad 和 \quad 2^2\equiv 1 \bmod 3,$$

即：

$$X^2\equiv 0 \text{ 或 } 1 \bmod 3 \quad 和 \quad Y^2\equiv 0 \text{ 或 } 1 \bmod 3.$$

我们能得到

$$X^2+Y^2\equiv 0 \bmod 3$$

的唯一途径是 $X^2\equiv Y^2\equiv 0 \bmod 3$. 这意味着 3 能整除 X 和 Y; 因此 9 整除 $X^2+Y^2=3Z^2$; 因此 3 整除 Z^2; 于是 3 也整除 Z. 这是不可能的，因为我们已经使得没有大于 1 的整数整除 X,Y,Z. 由于我们得到一个矛盾，所以唯一的可能是我们开始的假设是错的，即方程

$$X^2+Y^2=3Z^2$$

没有一个解使得 X,Y,Z 是非零整数.

这类论证并不只是对这个特殊的方程适用. Hermann Minkowski (闵科夫斯基) (1890) 和 HelmutHasse (哈塞) (1924) 的一个漂亮的定理说：任给一个任意元的整系数二次齐次多项式 $Q(X_1,\ldots,X_d)$, 则

$$Q(X_1,\ldots,X_d)=0$$

有一个非零整数解当且仅当它在实数中有一个非零解和在所有的模正整数 m 的算术中有一个本源 (primitive) 解. (我们称 $(X_1,\ldots,X_d)$ 是一个模 m 本源 解是指：

$$Q(X_1,\ldots,X_d)\equiv 0 \bmod m,$$

但是没有大于 1 的整数整除所有的 X_i.) 这实际上是一个非常实用的判别法. 表面上可能看来人们需要对无穷多个 m 验证原方程在模 m 时候的解. 但是，人们可以找到一个整数 m_0 (依赖于多项式 Q) 具有如下性质：如果 $Q(X_1,\ldots,X_d)=0$ 模 m_0 有一个本源解，那么对任意其他的正整数 m, 它都有一个模 m 的本源解.

然而，对于高次方程，相应的定理不成立. 例如

$$3X^3+4Y^3+5Z^3=0$$

对模任意的正整数都有非零解 (并且在实数中也有解), 但是它没有一个整数解. (这个著名的例子是被高等研究院 (IAS) 前成员 Emst Selmer (塞尔默) 发现的.) 尽管如此，在研究任意多项式方程整数解的时候，研究模 m 的解经常是一个关键工具.

早在 1800 多年前，中国的《孙子算经》记载了一个现在被称为中国剩余定理的命题. 这个定理给出了一个非常有效的算法，该算法将研究一个多项式方程模 m 的整数解

化为研究该方程在模 m 的 p^a 形式的因子的解，其中 p 是一个素数，a 是一个正整数．事实上，可以发现考虑的最关键的情况是当 m 是一个素数的时候．因此，在本文的剩下部分中，我们将只考虑模一个素数 p 的情况．

回忆一下，一个素数是一个只能被 1 和它本身整除且大于 1 的整数．例如 2, 3, 5, 7, 11, 13, 17, 19 都是素数，但 15 就不是了，它可以被 3 和 5 整除．每个正整数都可以被唯一地 (不考虑顺序) 写成素数的乘积．某种意义上，素数有些像原子，其他所有的整数都可以由它们合成．

模算术研究的第一个真正伟大的成就是 Carl Friedrich Gauss (高斯) 在 1796 年证明的早先由 Leonhard Euler (欧拉) 和 Joseph Lagrange (拉格朗日) 猜想的著名的 *二次互反律*. 这被认为是 Gauss 最喜欢的定理，在他的一生中，他经常返回去思考它，并且给出了 8 个不同的证明．该定理陈述如下：

如果 p 是一个素数，则一个整数 n 模 p 的平方根的个数仅依赖于 p 模 $4n$.

表面上看来，这似乎并不惊人，但我想强调的是，并没有明显的理由说明为什么解方程

$$X^2 \equiv n \bmod p$$

应该和 $p \bmod 4n$ 有联系．从我第一次学会证明这个定理后的 30 年间，它对我来说还是不可思议的．

Gauss 的定理也提供了一个决定一个整数模一个素数 p 的平方根个数的有效方法．例如，人们可以问在模素数 20132011 的算术中 3 有多少个平方根．理论上，你可以验证 20132011 种可能并且得到答案，但是 (不用计算机) 这会花很长时间．另一方面，

$$20132011 = 1677667 \times 12 + 7,$$

因此 3 在模素数 20132011 的平方根个数与它在模 7 时的平方根个数一样．而列出模 7 的平方数是很快的：

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1 \bmod 7.$$

因此，3 在模 7 的算术中没有平方根，于是由 Gauss 定理它没有模 20132011 的平方根．(一件好事是我们没有浪费时间去验证所有 20132011 种可能 !)

我们可以寻求一个类似的方法，它能对任意多个变量的给定的任意多个多项式帮助我们确定这些方程在算术模素数 p (p 可变动) 下解的数目．这些结果就是所谓的 “互反律”. 在 20 世纪 20 年代，Emil Artin (阿廷) 给出了在当时被认为是能得到的最一般的互反律 —— 他的交换互反律．但是，Artin 的互反律仍然只适用于非常特殊的方程 —— 有 “交换 Galois (伽罗瓦) 群” 的单变量方程．

令人震惊的是在 1954 年，Martin Eichler (艾克勒) (高等研究院前成员) 发现了一个未包含在 Artin 的定理里的全新互反律．(这类互反律通常所谓 “非交换的”.) 更精确地，他发现了二元方程

$$Y^2 + Y = X^3 - X^2$$

的一个互反律．他证明了这个方程模素数 p 的解的个数与 p 只差以下形式无穷乘积中的 q^p 的系数：

$$q(1-q)^2(1-q^{11})^2(1-q^2)^2(1-q^{22})^2(1-q^3)^2(1-q^{33})^2(1-q^4)^2\cdots$$
$$=q-2q^2-q^3+2q^4+q^5+2q^6-2q^7-2q^9-2q^{10}+q^{11}-2q^{12}+\cdots$$

例如，你看到 q^5 的系数是 1，所以，Eichler 的定理告诉我们

$$Y^2+Y=X^3-X^2$$

在模 5 的算术中应该有 $5-1=4$ 个解．你可以通过验证 (X,Y) mod 5 的 25 种可能来验证这个，而且你的确会找到恰好 4 个解

$$(X,Y)\equiv(0,0),(0,4),(1,0),(1,4) \text{ mod } 5.$$

在不到 3 年之内，Yutaka Taniyama (谷山丰) 和 Goro Shimura (志村五郎) (高等研究院前成员) 提出把 Eichler 的互反律大胆地推广到所有二元三次方程．10 年后，André Weil (韦伊)(高等研究院前教授) 把这个猜想变得更加精确，而且找到很强的启发性的迹象支持志村－谷山互反律．这个猜想完全改变了数论的发展．

在 20 世纪 80 年代中期，Gerhard Frey (弗雷)，Jean–Pierre Serre (塞尔) (高等研究院前成员) 和 Kenneth Ribet (高等研究院前成员) 指出如果志村－谷山猜想是正确的，它将蕴含 Fermat (费马) 大定理．出于这个想法，在 1995 年，Andrew Wiles (怀尔斯)(高等研究院前成员) 部分地与本文作者合作，建立了许多情形下的志村－谷山互反律，而且因此最终证明了 Fermat 大定理．

同时，在 20 世纪 70 年代中期，Robert Langlands (朗兰兹) (高等研究院数学学部的荣誉退休教授) 超常地洞察到 Eichler，谷山和志村的想法是一个大得多的蓝图中的一小部分．他能够提出对最终的互反律的猜想 —— 对以往发展的一个巨大的推广，适用于任意多变量的任何次数的任何数量的方程．在过去的 10 年里，用 Wiles 引进的想法，在 Langlands 的互反猜想上有很多的进展，但更多的仍待解决．

所有非交换互反律都具有的一个显著特征是，解的个数的公式是由弯曲空间的对称性 —— 在解代数方程和几何对称之间的一种意想不到的联系 —— 给出来的．在志村－谷山互反律的情形，相关的对称是 “双曲平面” 的对称．双曲平面可以被想象成一个 (无边界的) 圆盘，但是带了一个特别的距离．对于接近圆盘中心的两点，他们的 “双曲” 距离和通常的距离近似，但在靠近边界的时候距离是急速扭曲的．在 Escher (埃舍尔)[1] 的一些木刻中描述了双曲平面和它的对称性，就好像下面这张图 (因版权原因此图略去 —— 编注)．在双曲世界里，Escher 的图案中的所有鱼被认为有相同的大小．

我将以讨论关于最近有所发展的模算术的一个进一步的问题来结束本文．

我们可以用寻求当素数变化时模素数解的个数的统计行为，去代替寻求一条能预测当模变化的素数 p 的时候一个方程的解的个数的法则．追溯到单变元二次方程这一简单情形，Lejeune Dirichlet(狄利克雷) 在 1837 年证明了：对一个固定的非完全平方的整数 m，方程

1) Maurits Cornelis Escher, 1898—1972, 荷兰版画家，因其作品中的数学性而著名．他的主要创作方式包括木刻，铜版印刷画，素描等．在他的作品中可以看到对分形，对称，密铺平面，双曲几何和多面体等数学概念的形象表达以及建筑学上办不到的 “结构”．本刊 2003 年第 1 期有介绍 Escher 的文章：“M. C. Escher: 比眼睛看到的要更多的数学”.—— 编注

$$X^2 \equiv m \bmod p$$

对一半的素数 p 有两个解和对一半的素数 p 没有解. 这似乎是一个自然的答案, 但是 Dirichlet 的证明非常巧妙, 它把 Gauss 的互反律和来自复分析的想法结合了起来. 1880 年, Ferdinand Frobenius (弗罗贝尼乌斯) 把 Dirichlet 的定理推广到一元的任意方程. 对其他的方程, 正确的答案也许更加难以猜测. 例如, 方程

$$X^4 \equiv 2 \bmod p$$

对所有素数的 5/8 没有解; 对所有素数的 1/4 有 2 个解; 对所有素数的 1/8 有 4 个解.

对于多于一个变元的方程, 这种密度定理是什么样的呢, 如:

$$Y^2 + Y = X^3 - X^2?$$

在这种情形, Hasse 在 1933 年证明了: 模 p 的解的个数, 我们记成 N_p, 和 p 的数量的阶一样. 更准确地, 他证明了 N_p 与 p 至多差 $2\sqrt{p}$. 他对所有的二元三次方程证明了这个结论.

1949 年, Weil 提出将 Hasse 的界推广到任意多变量任意次的任意多个方程的猜想. 这个著名的猜想引起了算术代数几何的革命. Weil 的猜想最终被 Pierre Deligne (德利涅) (高等研究院数学学部的荣誉退休教授) 在 1974 年证明了.

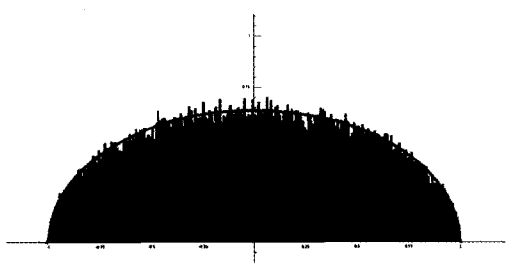
回到方程

$$Y^2 + Y = X^3 - X^2,$$

Hasse 的定理告诉我们, 寻找这个方程的素数比率 —— 例如求这个方程算术模 p 有 10 个解的那些素数在所有素数中有多大比率是没有意义的: 答案永远是 0. 更自然的问题是考虑规范化的误差项

$$\frac{N_p - p}{\sqrt{p}}.$$

根据 Hasse 的定理, 这是一个在 -2 到 2 之间的 (实) 数, 而且人们可以问它在这个区间里是如何分布的. 误差经常像 Hasse 的定理允许的那么大, 还是它通常较小而且很罕见地取其极吗? 1963 年, Mikio Sato (佐藤干夫) 和 John Tate (泰特) (都是高等研究院前成员) 独立地猜想了正确的密度定理 —— 误差分布应该像 $\frac{1}{2\pi}\sqrt{4-t^2}$, 一个 "压扁的半圆".



对于 Δ 和 $p < 1,000,000$ 的 Sato–Tate 分布
(由 William Stein 画)

Sato–Tate 密度定理最近已经被 (Laurent Clozel 和 Michael Harris (哈里斯), 都是高等研究院前成员; 以及 Nicholas Shepherd-Barron 和本文作者) 证明, 不仅仅是对这个方程, 而是对所有的二元三次方程. 证明结合了 Dirichlet 和 Frobenius 的论证和一个无穷列的 Langlands 的互反律的新情形. 当然, 应该有任意多个变量任意次的任意多个方程的密度定理, 但是这些仍然是非常猜想性的. 故事仍在继续 ...

(王章结 译　舒杰 李艳芳 校)

阅读此文的还阅读了：