

剩余定理情未了

史定华 陈关荣

中国对数学基本理论的贡献不多，能让国人自豪并以“中国”命名的古老数学命题可能只有“中国剩余定理”一个，因而我们常常为之余情未了。本文回顾了剩余定理的简要历史和内容，并谈及其几个经典和最新应用。

同余的发现

古人为安排农事而编制历法，需要计算周期的起点。期间，数学同余概念的产生和利用反映了中国农耕文明的历史辉煌，而与之相应的诗情画意般的求解歌诀更体现了深厚的中华文化底蕴。

1 “物不知数”问题

这是中国古代一道著名算题。原载《孙子算经》，为卷下第二十六题。

“今有物，不知其数，三三数之，剩二，五五数之，剩三，七七数之，剩二。问：物几何？答曰：二十三”。

从这里引申出了一个重要的数学概念：同余。例如，“三三数之剩二”概括了多种“剩二”的情况，譬如5除以3余2，8除以3也余2，说明5和8除以3时有相同余数。进一步，还能观察到2、5、8、11、……除以3余2的周期现象，同时可将无限的自然数集合按周期的起点分成0、1、2三个不同的剩余类，等等。

上述“物不知数”问题用现代数学式子表达的话，可归结为求

$$x \equiv 2 \pmod{3} \equiv 3 \pmod{5} \equiv 2 \pmod{7}$$

这组一次同余式的整数解。

《孙子算经》是中国古代一部非常重要的数学著作，成书大约在公元四、五世纪的南北朝时期，也就是一千五百多年前，其作者生平和编写年代不详。传本的《孙子算经》共分三卷：卷上、卷中、卷下。“物不知数”问题也称“韩信点兵”问题（有多个版本）。其中一个版本如下：

传说刘邦建立汉朝之前有一大将韩信，计算士兵数目的方法十分特别。他不是五个五个或十个十个地数，也不要士兵“一、二、三、四、……”地报数，而是叫他们排成队伍，依次在他面前列队行进：先是每排三人，再是每排五人，然后是每排七人。他只将三次队列行进完后所余的士兵数目记下来，就知道了士兵的总数。据此有人认为《孙子算经》的作者是撰写《孙子兵法》的孙武。其实

不然，卷下“今有佛书”一问，说明《孙子算经》的作者和总结《孙子兵法》的孙子是不同时代的人。

我国古代天文历法资料表明，一次同余问题的研究受到天文和历法需求的推动，特别是和古代历法中所谓“上元积年”的计算密切相关。任何一部历法，都需要一个理想的时间起算点——这个起算点要从制定某部历法的当年往回逆推，所得起算点称为“上元积年”。在这个起算时刻，日、月、行星都恰好位于它们各自周期的起点，同时这一天的纪日干支又要恰好是“甲子”，如此等等，故上元积年的推算需要求解一组一次同余式。如南北朝时期祖冲之的《大明历》，要求上元积年必须是甲子年的开始，而且“日月合璧”、“五星联珠”（就是日、月、五大行星处在同一方位），同时月亮恰好行经它的近地点和升交点。在这样的约束条件下来推算上元积年，需要去解 10 个联立同余式，相当之不容易。

2 《孙子歌诀》解法

《孙子算经》解这道题目的“术文”是：“凡三三数之，剩一，则置七十，五五数之，剩一，则置二十一，七七数之，剩一，则置十五，一百六以上，以一百五减之；而三三数之，剩二，置一百四十；五五数之，剩三，置六十三；七七数之，剩二，置三十。并之，得二百三十三，以二百十减之，即得”。需要注意的是，古称“106”为“一百六”，而称“160”为“一百六十”。这里：被 3 除余 1，并能同时被 5、7 整除的最小数是 70 好理解；被 3 除余 2，并能同时被 5、7 整除的最小数是 35，为什么置一百四十？因为题目没有要求“最小”，“剩一，则置七十，剩二，置一百四十”，按同余运算顺理成章；但为了答案唯一，故最后都按“一百六以上，以一百五减之”直到最小。

明代著名的大数学家程大位，在他所著的《算法统宗》中，对于这种解“孙子问题”的方法，还编出了四句歌诀，名曰《孙子歌诀》：

“三人同行七十稀，五树梅花廿一枝，七子团圆正半月，除百零五便得知”。

从数学文化的角度，选择一个问题，离不开教学及历史、诗歌和绘画，特别是思想与创新。而“物不知数”问题就很符合这些条件。

以数糖果为例进行少儿教学，9 粒符合七七数之，剩二，但不符合五五数之，剩三；16 粒也如此。然而 23 粒符合七七数之，剩二；五五数之，剩三；三三数之，剩二。故 23 为一个答案，除法验证 128 也是答案。然而网上流传的“韩信点兵”问题（另一版本）：他带 1500 名士兵去打仗，战死四百多。余者，大刀队 3 人一排，多出 2 人；长矛队 5 人一排，多出 4 人；弓弩队 7 人一排，多出 6 人。问活着士兵人数？这个版本见图 1 左下，但这里的问题描述是不对的！正确描述应该是：余者，3 人一排，多出 2 人；5 人一排，多出 4 人；7 人一排，多出 6 人。问活着的士兵人数？在此基础上，有些小学生能够准确回答为 1049 人。

图 1 右图是上海行知小学四年级学生史佳妮按照《孙子歌诀》所作的画。它诗意盎然宛如一幅国画！据此“韩信点兵”问题中的

$$x = (2 \times 70 + 4 \times 21 + 6 \times 15) \pmod{105} = 104$$

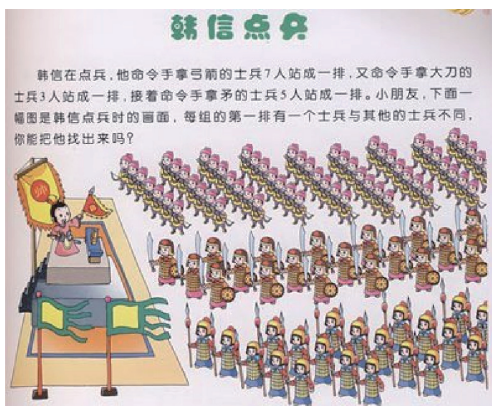
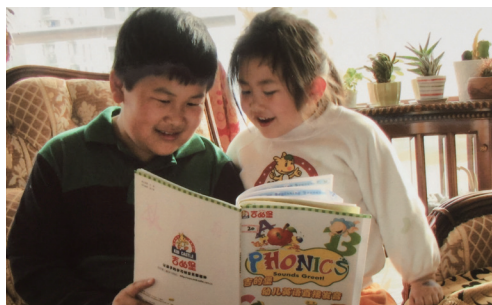


图1 有关教学的插图

容易接受；但对于 $104+9 \times 105 = 1049$ 小学生还得动动脑筋。

该问题的思想与创新将在后面的“同余的情缘”篇中进一步谈及。

3 “中国”剩余定理

《孙子歌诀》只能解答用 3、5、7 作除数的题目，遇到用其他数作除数的算题，它就行不通了。南宋数学家秦九韶将它推广，在《数书九章》中用大衍求一术给出了一个系统性解法。德国数学家高斯 (K. F. Gauss, 公元 1777-1855 年) 于 1801 年出版的《算术探究》中用现代数学语言把它明确地写成一个定理。

定理：设整数 $m_1, m_2, \dots, m_n$ 两两互质，则同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

有唯一解

$$x = \sum_{i=1}^n a_i t_i M_i \pmod{M},$$

其中

$$M = m_1 m_2 \cdots m_n, \quad M_i = M/m_i, \quad t_i M_i \equiv 1 \pmod{m_i}.$$

定理中的 m_i 称为模数, a_i 称为余数, M 是模数的最小公倍数, 而 M_i 称为衍数, 即局部(除 m_i 外的)公倍数, t_i 称为乘率, $t_i M_i \equiv 1 \pmod{m_i}$ 称为“求一术”。可见大衍求一术是将求解一组一次同余式问题简化为求解单个同余式问题。

下面以“物不知数”问题为例来解释大衍求一术。

衍数 $M_1 = 5 \cdot 7 = 35$, 寻找乘率 t_1 ? 因为模数 $m_1 = 3$, 采用“求一术”公式 $t_1 35 \equiv 1 \pmod{3}$, 得 $t_1 = 2$ 。衍数 $M_2 = 3 \cdot 7 = 21$, 寻找乘率 t_2 ? 因为模数 $m_2 = 5$, 采用“求一术”公式 $t_2 21 \equiv 1 \pmod{5}$, 得 $t_2 = 1$ 。类似地, 可得 $t_3 = 1$ 。于是

$$x = (2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15) \pmod{105} = 23.$$

而歌诀关键数“七十稀、廿一枝、正半月”则是 $t_i M_i$ 所得数值。

目前解一组一次同余式最有效的是 Garner 算法。

仍以同一“物不知数”问题为例来解释 Garner 算法。

式中唯一未知数 x 的混合基数表示有形式: $x = v_0 + v_1 \cdot 3 + v_2 \cdot 3 \cdot 5$, 其中 v_0 、 v_1 、 v_2 分别是除以 3、5、7 的余数。因此, 确定了整数 v_0 、 v_1 、 v_2 后就能找到解 x 。由 $x \equiv 2 \pmod{3}$, 得 $v_0 + v_1 \cdot 3 + v_2 \cdot 3 \cdot 5 \equiv 2 \pmod{3}$, 推出 $v_0 = 2$ 。现在 $x = 2 + v_1 \cdot 3 + v_2 \cdot 3 \cdot 5$, 由 $x \equiv 3 \pmod{5}$, 得 $2 + v_1 \cdot 3 + v_2 \cdot 3 \cdot 5 \equiv 3 \pmod{5}$, 推出 $3v_1 \equiv 1 \pmod{5}$, 于是 $v_1 = 2$ 。现在 $x = 2 + 2 \cdot 3 + v_2 \cdot 3 \cdot 5$, 由 $x \equiv 2 \pmod{7}$, 得 $2 + 2 \cdot 3 + v_2 \cdot 3 \cdot 5 \equiv 2 \pmod{7}$, 推出 $1 + v_2 \equiv 2 \pmod{7}$, 于是 $v_2 = 1$ 。因此答案是 $x = 2 + 2 \cdot 3 + 1 \cdot 3 \cdot 5 = 23$ 。

公元 1852 年, 英国基督教士维里 (A. Wylie, 1815-1887) 将《孙子算经》中“物不知数”问题的解法传到欧洲, 随后公元 1874 年马蒂生 (L. Mathiesen) 指出其解法符合高斯的定理, 从而西方的数学史将这一个定理称为“中国剩余定理” (Chinese Remainder Theorem)。此后, 剩余定理、威尔逊定理、欧拉定理、费马小定理并称为初等数论的四大基本定理。

同余的发展

剩余定理在科技领域中最成功的应用是实现通讯保密。为此需要推广同余的概念。从同余到平方剩余, 从无限数域到有限域, 再到椭圆曲线, 同余的发展和运用反映了西方工业文明过程中的科学探索精神。

1 RSA 算法

密码学的公钥系统是将密钥一分为二: 加密公钥和解密私钥。虽加密公钥对外公开, 然解密私钥难以破解。为此需要设计一个好的 Trapdoor-Oneway-Function (天窗单向陷门函数), 它的计算在一个方向 (由 x 算 y) 容易, 在另一方向 (由 y 算 x) 极其困难 (但知道私钥时, 计算它也相当容易)。两者难度差别越大, 该公钥系统就越安全。例如, 计算两个已知素数乘积容易, 而通过大整数分解去找出两个素数因子却难得多。

基于大整数的素数分解问题的公钥系统 RSA 算法, 是由 R. Rivest, A.

Shamir 和 L. Adleman 三人在 1976 年提出的¹。

首先寻找两个大素数 p 和 q ，计算 $n = pq$ 和 $\varphi(n) = (p-1)(q-1)$ ，再选择一个随机数 $0 < e < \varphi(n) - 1$ 并满足最大公因子 $\gcd(e, \varphi(n)) = 1$ ，然后用大衍求一术去计算 $de \equiv 1 \pmod{\varphi(n)}$ ，得到 d 。

公钥取为 n 和 e 两个数，记为 $PK = (n, e)$ ，可在网上公布，用户按其加密；私钥取为 n 和 d 两个数，记为 $SK = (n, d)$ ，其中 n 是公开的， d 则要严加保密，管理公司用其解密。RSA 的陷门函数是 $y \equiv x^e \pmod{n}$ 。显然，已知 x 去计算 y 十分容易，所以用户按其加密并不困难。例如，用户的明文（长度） $M < n$ ，容易算得密文（长度） $C \equiv M^e \pmod{n}$ 。管理公司用私钥解密得明文 $M \equiv C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n} \equiv M \pmod{n}$ ，其中用到欧拉定理的推论（即，若 $ed \equiv 1 \pmod{n}$ ，则 $M^{ed} \pmod{n} \equiv M \pmod{n}$ ）。而黑客想通过攻击获得明文，则面临由 y 算 x 的困难，除非他能够分解 $n = pq$ ，否则无法知道私钥，从而无法解密。

RSA 的安全性是基于大整数素数分解困难的假定，其困难性并没有证明。因此选择的模数 n 的长度必须足够长。随着计算技术的发展，RSA 已被破解到 512 二进制位，所以 n 的长度至少应该为 1024 位。近来量子计算机异军突起，据《科学》2016 年 3 月 4 日报道，人们借助量子计算机用 Shor 算法实现了对整数 15（可扩展）的素数分解。这意味着基于大整数素数分解的 RSA 加密算法或将成为摆设！故此人们必须另辟蹊径。

2 DLP 算法

1985 年，T. ElGamal 提出了基于有限域上离散对数问题（Discrete Logarithm Problem）的公钥系统 DLP 算法²。先选择一个大素数 p ，然后所有整数通过模 p 的加法及乘法运算生成有限域 F_p 。再寻找其乘法群生成元 g ，它是其幂能遍历 F_p 所有非零元素的数。例如，3 是 F_7 的生成元，因为 $3^1 \equiv 3 \pmod{7}$ ， $3^2 \equiv 2 \pmod{7}$ ， $3^3 \equiv 6 \pmod{7}$ ， $3^4 \equiv 4 \pmod{7}$ ， $3^5 \equiv 5 \pmod{7}$ ， $3^6 \equiv 1 \pmod{7}$ 。DLP 的陷门函数是 $y \equiv g^x \pmod{p}$ ，由 x 算 y 易，但其逆运算比大整数的素数分解更加困难。

现在将 (p, g) 作为公共参数在网上公布。这时每个用户都在 $2 \leq x \leq p-2$ 中随机选择一个整数作为私钥；计算 $y \equiv g^x \pmod{p}$ 作为公钥。用户 A 若要将明文 M 传送给用户 B ，先将 M 编码成 F_p 的元素 m ，再挑选一个秘密随机数 $2 \leq r \leq p-2$ ，然后计算 $c_1 \equiv g^r \pmod{p}$ 和 $c_2 \equiv m \cdot y^r \pmod{p}$ ，这里 y 是用户 B 的公钥。所得到的 (c_1, c_2) 就是用户 A 传送给用户 B 的密文。用户 B 收到密文后，做解密计算 $m \equiv c_2 \cdot (c_1^x)^{-1} \pmod{p} \equiv m \cdot y^r \cdot (g^{rx})^{-1} \pmod{p} \equiv m \cdot y^r \cdot (g^x)^{-r} \pmod{p}$

¹ R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and Public-Key cryptosystems. Communications of the ACM, 1078, 21, 120–126.

² T. Elgamal, A Public-Key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31, 469–472.

$\equiv m \cdot (y^r y^{-r}) \pmod{p} \equiv m$, 这里 x 是用户 B 的私钥。因为破解有限域上离散对数问题比整数的素数分解难度更大, 所以 DLP 用作保密通讯的安全性更高。

3 ECC 算法

1985 年 N. Koblitz 和 V. Miller 分别独立开发了基于有限域上椭圆曲线加法点群运算公钥系统的 ECC (Elliptic Curves Cryptography) 算法^{3,4}。这里, 平面上的椭圆曲线并非圆锥曲线之一的椭圆, 前者是三次曲线 $y^2 = x^3 + ax + b$, 见图 2a; 而后者是二次曲线。

在介绍 ECC 公钥系统前, 先讨论一下椭圆曲线 $y^2 \equiv x^3 + ax + b \pmod{p}$ 上点 (x, y) 的生成方法, 其中 p 是大素数, a, b 满足 $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, 见图 2b。显然, x 可取的元素是 F_p 中的每个数, 即 $0, 1, \dots, p-1$ 。但为了确定 y 必须解二次同余式方程。步骤是: 对 x 每个可取的数, 计算 $c \equiv x^3 + ax + b \pmod{p}$, 然后解 $y^2 \equiv c \pmod{p}$ 。若它有解 y , 则称 c 是 p 的平方剩余, 这时得到点 (x, y) 。若它无解, 则称 c 是 p 的非平方剩余。因此, 并不是 x 每个可取的数都一定有点与之对应。

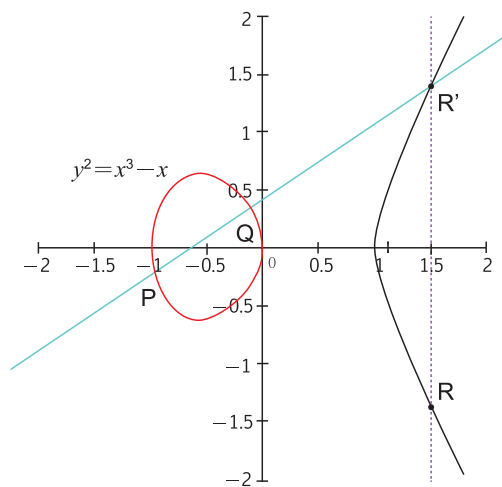


图 2 a. 椭圆曲线上的点加法

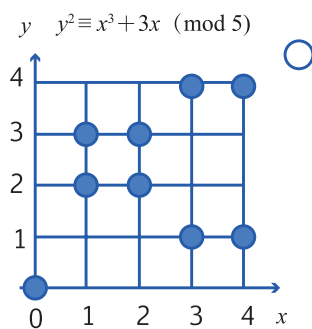


图 2 b. 有限域上椭圆曲线的点

椭圆曲线上点加法运算如下: 加法单位元 O 与任意点 P 有 $P + O = P$; 点 P 的逆元 S 满足 $P + S = O$ 。由于点加法的几何意义见图 2a, 因此 PS (O 对应无穷远点) 连线平行于 y 轴, 它们有相同的 x 坐标和绝对值相同的 y 坐标。而对一般的两点 $P = (x_1, y_1)$, 求点加运算 $P + Q = R = (x_3, y_3)$ 的公式如下: $x_3 \equiv s^2 - x_1 - x_2 \pmod{p}$, $y_3 \equiv s(x_1 - x_3) - y_1 \pmod{p}$, 其中

³ N. Koblitz, Elliptic curves cryptography. Mathematics of Computation, 1987, 48, 203-209.

⁴ V. Miller, Uses of elliptic curves in cryptography. Proc. Lecture Notes in Computer Science 218, Springer, 1986, 417-426.

$$s \equiv \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} (\bmod p), & P \neq Q \\ \frac{3x_1 + a}{2y_1} (\bmod p), & P = Q \end{cases}$$

类似于 DLP 算法, 公钥系统 ECC 选择一条椭圆曲线 $y^2 \equiv x^3 + ax + b (\bmod p)$ 和它一个点 G 作为基点, 使得 $nG = O$, 其中 $n \neq p$ 是足够大的素数, 并在网上公开。然后每个用户都在 $2 \leq x \leq n-2$ 中随机选择一个整数作为私钥; 计算点 $X = xG$ 作为公钥。假设用户 A 的公钥是 P_A , 私钥是 r ; 用户 B 的公钥是 P_B , 私钥是 s 。若用户 A 想将明文 P_m 传送给用户 B , 他选择一个随机整数 k , 产生密文点对 $(kG, P_m + kP_B)$ 发给用户 B 。用户 B 收到后, 解密密文 $P_m + kP_B - skG = P_m + ksG - skG = P_m$ 。因为除了用户 A 知道 k , 用户 B 知道 s , 别人是无法破解的。ECC 算法涉及计算点 $Y = xG$ 的问题。如果将点加法群看成“点乘法群”, 则函数为 $Y = G^x$ 。因为它类似 $y \equiv g^x (\bmod p)$, 所以也称为椭圆曲线上离散对数难题。

ECC 算法与 RSA 算法在安全性相同情况下的密钥长度有很大节省。例如, 若 RSA 需要 1024、2048 二进制位的话, 则 ECC 分别只需 160、210 位! 但是, 研究表明⁵, 在对付量子计算攻击方面 ECC 算法比 RSA 算法更脆弱: 量子攻击 1024 位的 RSA 程序需要 2000 qubits (量子比特) 的运算, 而攻击具有等效保密程度的 160 位 ECC 程序只需不到 1000 qubits 的运算。

同余的情缘

上个世纪伴随电子技术的发展和各类高科技产品的涌现, 一场信息革命的号角催生了许多新兴学科, 特别是引人注目的网络新科学, 其中同余与网络联姻焕发了新的生机, 这段未了情或许会带来意外惊喜!

1 自然数网络

随着计算机和互联网技术的不断发展和进步, 一门新兴的交叉学科——网络科学在千禧年前夕应运而生。研究人员利用互联网获取了许多现实复杂系统的数据, 提出了与传统随机图论不同的复杂网络模型, 通过实证统计和模型分析发现了大多数复杂网络具有小世界和无标度特性^{6,7}。小世界特性由网络平

⁵ J. Proos and C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves, Journal of Quantum Information & Computation, 2003, 3(4), 317-344.

⁶ D. J. Watts and S. H. Strogatz, Collective dynamics of small-world networks. Nature, 1998, 393: 440-442.

⁷ A. L. Barabasi and R. Albert, Emergence of scaling in random networks. Science, 1999, 286: 509-512.

均路径和群集系数刻画；无标度特性由网络度分布描述。主要的结果是：网络（节点之间的）平均路径 $\bar{l} \sim \ln n$ ，网络（节点）度分布 $P(k) \sim k^{-\gamma}$ ，其中 n 为网络节点数， $1 < \gamma$ 为网络自身决定的常数，而网络群集系数大只是定性说法。

网络是描述复杂系统的一个理想框架，它将单元抽象为节点，相互作用或关系通过连线表示。因此，网络可用来描述几乎所有的复杂系统。自然数系统是数学中最重要的系统，也是数论的研究对象，其中两个数最基本的关系是整除。所以在网络科学诞生后，很快就有人研究自然数整除网络并获得了一系列有趣的结果。例如，周涛等人证明了合数无向整除网络具有超小世界特性⁸；史定华等人证明了自然数有向整除网络具有 $\gamma = 2$ 的无标度特性，发现其度分布与随机复制模型完全吻合⁹；文¹⁰则研究了自然数二分加权整除网络，等等。

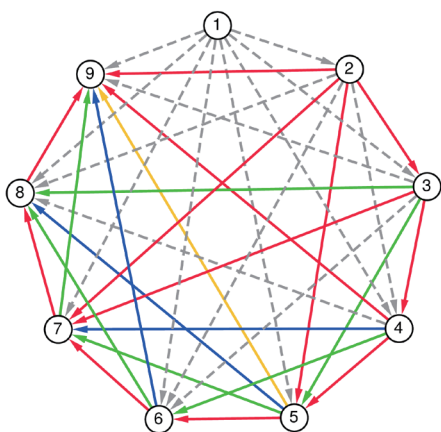


图 3 a. 自然数同余网络
虚线表示整除网络，红色余数为 1，等等

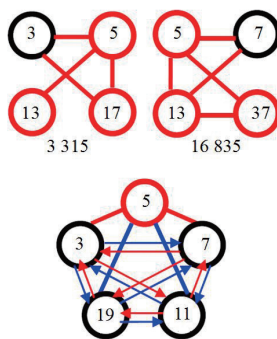


图 3 b. (非)平方剩余网络
红色连线为非平方剩余网络

自然数系统中，除了最基本的整除关系，还有许多关系。例如两个数的同余关系就是整除关系的自然推广，于是我们研究了自然数同余网络，见图 3a。它可将求解一组一次同余式问题转化为多层网络来研究¹¹。同余关系的进一步推广是平方剩余和非平方剩余，而冯克勤等人早就用非平方剩余网络研究过非同余数问题¹²，见图 3b。

⁸ T. Zhou, B. H. Wang and P. Hui, et al. Topological properties of integer networks. *Physica A*, 2006, 367, 613-618.

⁹ D. H. Shi, H. J. Zhou, Natural number network and prime number theorem. *Complex Systems and Complexity Science*, 2010 7, 52-54.

¹⁰ G. García-Pérez, M. Á. Serrano and M. Boguñá, The complex architecture of primes and natural numbers. *Physical Review E*, 2014, 90, 022806.

¹¹ X. Y. Yan, W. X. WANG, G. R. CHEN, D. H. SHI. Multiplex congruence network of natural numbers. *Scientific Reports*, 2016, 4: 23714.

¹² K. Q. Feng. *Non-Congruent Numbers and Elliptic Curves with Rank Zero*. Hefei: University of Science & Technology, China Press, 2008.

2 网络动力学

复杂系统的研究重点是其动力学行为。有了网络这样一个理想框架，自然就会研究网络上的动力学。主要思想是对每个节点加上一个动力学方程，研究网络拓扑和节点动力学的相互影响。汪小帆和陈关荣首先研究了复杂网络的同步问题¹³，其后带出了多智能体的一致性研究。若网络自身不能实现同步，他们又引入牵引控制使得网络能够被牵引到目标状态¹⁴。于是，对给定的网络拓扑，需要牵引多少节点才能达到目标就成为关键的研究问题。

考虑网络线性控制模型

$$\dot{x}(t) = Ax(t) + Bu(t)$$

其中 $x(t)$ 是 N 维状态向量， A 是耦合矩阵，描述网络拓扑及其连接的耦合强度， $u(t)$ 是 $M \leq N$ 维外部输入控制向量， B 是 $N \times M$ 维控制输入矩阵。采用经典的状态可控概念，即网络从任意初始状态能在有限时间内被控制到任意目标状态，文¹⁵利用图匹配方法，得到结构可控的驱动节点数公式

$$N_D^S = \max\{1, n - |M^*|\}$$

其中 $|M^*|$ 为匹配节点数（因而 $n - |M^*|$ 表示未匹配节点数）。再用空穴（cavity）方法推导出无标度网络驱动节点比公式（其中 $\langle k \rangle$ 为网络节点的平均度）

$$n_D^S \approx \exp\left\{-\frac{1}{2}[1 - 1/(\gamma - 1)]\langle k \rangle\right\}.$$

据此，可以认为当 $\gamma = 2$ 时，几乎所有节点都需要被控制，而且对蓄意攻击高度数节点的策略具有十分脆弱的抵抗能力。文¹⁶利用矩阵特征值理论还得到一般有向加权网络精确可控的驱动节点数公式

$$N_D^E = \max\{\mu(\lambda_i)\}$$

其中 $\mu(\lambda_i)$ 表示耦合矩阵 A 特征值 λ_i 的几何重数。最近，王琳等人¹⁷对一般的高维节点复杂网络给出了牵制可控性的充分必要条件。

自然数有向整除网络是 $\gamma = 2$ 的无标度网络。我们通过计算发现，它确实需要驱动一半节点才能达到控制目标。然而，当我们研究自然数有向同余网络

¹³ X. F. Wang, G. R. Chen, Synchronization in scale-free dynamical networks: Robustness and fragility. IEEE Transactions on Circuits and Systems, 2002, 49: 54-62.

¹⁴ X. F. Wang, G. R. Chen, Pinning control of scale-free dynamical networks. Physica A, 2002, 310: 521-531.

¹⁵ Y. Y. Liu, J. J. Slotine, A. L. Barabasi, Controllability of complex networks. Nature, 2011, 473: 167-173.

¹⁶ Z. Z. Yuan, C. Zhao, Z. R. Di, W. X. Wang, Y. C. Lai, Exact controllability of complex networks. Nature Communications, 2013, 4: 2447.

¹⁷ L. Wang, G. R. Chen, X. F. Wang, W. K. S. Tang, Controllability of networked MIMO systems. Automatica, 2016, 69: 405-409.

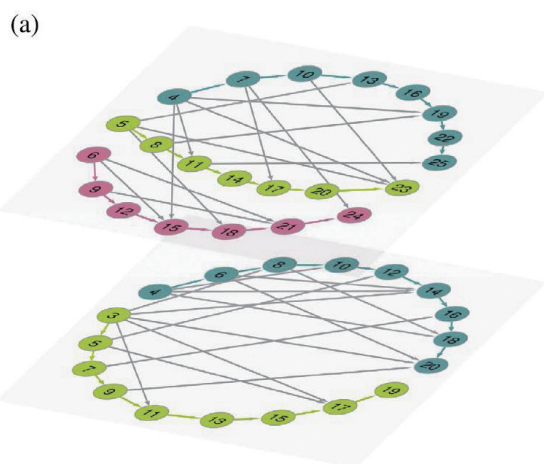


图 4 a. 余数 3 的同余有向网络只需控制 3 个节点，因有三个链条连接所有节点

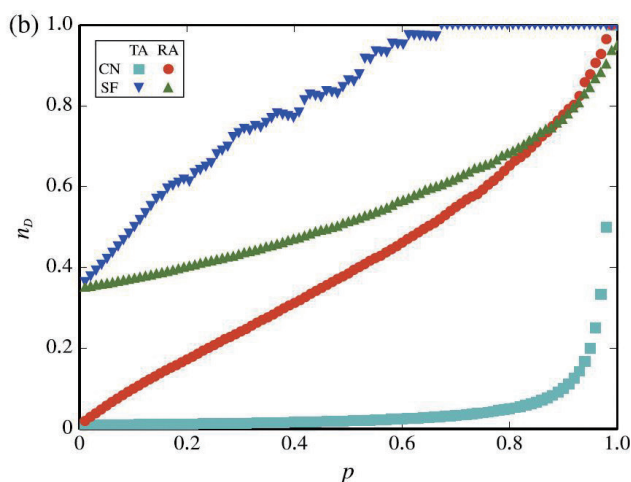


图 4 b. 蓄意和随机攻击，上面是普通无标度网络，下面是同余网络， p 是攻击节点比例

时，意外的奇迹发生了。自然数有向同余网络也是 $\gamma = 2$ 的无标度网络，但它只需要驱动有限个（等于余数）节点就能达到控制目标。不仅如此，而且面对蓄意攻击高度数节点的策略表现稳健而不脆弱，如图 4 所示（取自文 [11]）。

由于可取不同余数，容易构造多层网络去求解一组一次同余式。例如，前面介绍的“物不知数”问题可以通过构造两层网络图 5a 去求解。上层是余数为 3 的同余网络，下层是余数为 2 的同余网络。节点 3（对应模 3）的邻居有：5，8，11，14，17，20，23；节点 5（对应模 5）的邻居有：8，13，18，23；节点 7（对应模 7）的邻居有：9，16，23；而节点 3、节点 5、节点 7 他们最小的共同邻居是 23，它正好是这组一次同余式的解！我们称之为共同邻居算法，即前面数糖果的教学法。

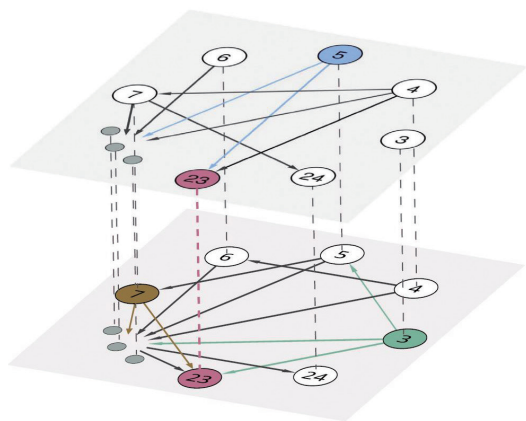


图 5 a. 两层自然数同余网络

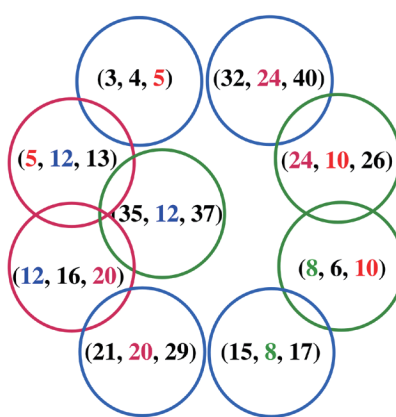


图 5 b. 勾股弦数超网络

3 数论与网络

数论中有个确定一个自然数是否为同余数的千年难题。这里应注意：不要

把一个同余数和两个数同余混淆，尽管它们有密切的内在联系。

费马不定方程 $x^2 + y^2 = z^2$ 显然有整数解。我国古代《周髀算经》中的商高定理就有“勾三股四弦五”之说，即 $(3, 4, 5)$ 是一组整数解，国外也称为“毕达哥拉斯三元组”。边为 $(3, 4, 5)$ 的直角三角形有面积 6。推而广之，若一个自然数是某个有理数边组成的直角三角形的面积，则称为同余数。所谓同余数问题是说：寻求比较简单的判别法则来决定一个自然数 n 是否为一个同余数。

利用计算机计算不定方程 $x^2 + y^2 = z^2$ 的整数解并不困难。方程 $x^2 + y^2 = z^2$ 有整数解：

$$x = u^2 - v^2; \quad y = 2uv; \quad z = u^2 + v^2, \quad u > v > 0.$$

取 $u = 2, 3, \dots, 6; v = 1, 2$ ，可算出： $(3, 4, 5); (8, 6, 10); (15, 8, 17); (24, 10, 26); (35, 12, 37); (5, 12, 13); (12, 16, 20); (21, 20, 29); (32, 24, 40)$ ，再算面积可得同余数。现在我们把上述解中出现的自然数看成节点，每组解看成一条“超边”（因现在一条边有三个节点），则可以画出勾股弦数超网络图形（见图 5b）。

超网络是网络科学发展的新方向，椭圆曲线是证明费马大定理的钥匙，BSD（贝赫和斯维纳通-戴尔）猜想是 7 个“千禧年大奖难题”之一，它们之间会有什么故事吗？

为了研究同余数，数学家们构造了一条特殊的椭圆曲线。从代数上讲， n 为一个同余数的条件是下面方程组及其等价形式有非零有理数解：

$$\begin{cases} x^2 + y^2 = z^2 \\ xy/2 = n \end{cases} \Leftrightarrow (x \pm y)^2 = z^2 \pm 4n \Leftrightarrow \left(\frac{x^2 - y^2}{4} \right)^2 = \left(\frac{z}{2} \right)^4 - n^2 \Leftrightarrow u^2 v^2 = u^6 - n^2 u^2$$

令 $x = u^2 = (z/2)^2$, $y = uv = (x^2 - y^2)z/8$ ，则得椭圆曲线 $E_n: y^2 = x^3 - n^2 x$ 。可以证明若 n 为同余数则存在非零有理数点，而全体有理数点定义加法形成阿贝尔群。文¹⁸建立了一个重要定理：存在整数 $n_1, n_2, \dots, n_r$ ，使得椭圆曲线上每个有理数点可表示为 $P_0 + n_1 P_1 + L + n_r P_r$, $r \geq 0$ ，其中 P_0 属于有限阶点生成的子群；而 r 称为椭圆曲线的秩。由此可证明 n 为同余数的充分必要条件是 $r > 0$ 。也可考虑椭圆曲线 $y^2 \equiv x^3 - n^2 x \pmod{p}$ 在有限域 F_p 上的加法点群，其中 p 是除 n 的素因子外的任意素数。这个加法点群是有限阿贝尔群，阶为 N_p 。

这些阿贝尔群能为研究同余数提供什么有用的信息呢？文¹⁹考虑了如下的狄利克雷函数：

¹⁸ L. J. Mordell, On the rational solutions of the indeterminate equation of the third and fourth degrees. Proceedings of the Cambridge Philosophy Society, 1922, 21: 179-192.

¹⁹ B. J. Birch, H. P. F. Swinnerton-Dyer. Notes on elliptic curves I and II. Journal für die reine und Angewandte Mathematik 1963, 212: 7-25; 1965, 218: 79-108.

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

其中 $a_p = 1 + p - N_p$, E 表示一般椭圆曲线, 并且提出了著名的 BSD 猜想: $L(E, s)$ 能解析开拓到整个复平面, 并且满足函数方程 $L(E, s) = f(s)L(E, 2-s)$; 函数值 $L(E, 1) = 0$ 的阶等于椭圆曲线的秩。在 BSD 猜想成立下, 可以证明自然数 $n \equiv 5, 6, 7 \pmod{8}$ 都是同余数, 这是很了不起的结果。

现在同余数问题终于与同余关系建立起了联系。因此自然会问: 同余网络能够帮助这个千年数论难题取得某些进展吗? 其实数学家早就想到了, 但不是使用同余网络, 而是使用非平方剩余网络。

如何判断一个自然数是非同余数呢? 文 [12] 引入了非平方剩余网络: 若 q 不是 p 的平方剩余, 则 $p \rightarrow q$ 建立连线, 由此得到了一系列重要结果。例如, 对无平方因子的自然数 $n = p_1 \cdots p_k \equiv 3 \pmod{8}$, 其中 $p_1 \equiv 3 \pmod{4}$, $p_i \equiv 1 \pmod{4}$, 可由 $p_1, \dots, p_k$ 为节点, 两个素数非平方剩余则建立连线, 来组成一个非平方剩余网络, 见前面图 3 b。若网络奇性 (验证网络拉普拉斯矩阵在二元域上的秩 $r = \text{rank}_{F_2} L(G) = k-1$), 则 $n = 3315$ 为非同余数; 而网络非奇性, 则 $n = 16835$ 是同余数。更奇妙的是, 利用中国剩余定理、高斯二次互反律、狄利克雷定理, 可以证明: 任何一个无向网络都能够对应 (同构) 于某个素数 (非) 平方剩余子网络。

结束语

千年以前的宋代是我国极其辉煌的朝代, 诞生了四大发明中的三个: 公元 1049 年毕昇发明活字印刷; 公元 1119 年朱或首次记录航海罗盘; 公元 1132 年陈规率先使用火枪。如果加上秦九韶公元 1247 年提出的大衍求一术, 宋代在文化、贸易、军事、科技均有世界一流的建树。在新的千年, 涉及数论、密码学、网络科学、量子计算等以椭圆曲线为媒的一段与同余的恋情, 会擦出什么更为灿烂的火花, 我们拭目以待。希望中华民族的子孙温故知新, 对中国剩余定理余情未了, 在现代数学和科学技术中有更大作为!



作者简介:

史定华 (左图), 上海大学数学系荣休教授, 高等教育出版社《网络科学与工程丛书》副主编。

陈关荣, 香港城市大学电子工程系讲座教授, 欧洲科学院院士和发展中国家科学院院士。