费马最后定理，四色猜想

数学小品

⑦

献给愚人节的费尔马最后定理，四色猜想，以及比尔·克林顿

250--258

0157.7

0157.5

Edward B. Burger and Frank Morgan

Burg., EB 刘尚平

1. 引言. 我们经常愚弄我们的学生. 我们通过陈述并证明经过润色的最后形式的定理来愚弄他们. 结果，学生们往往不知道思想、策略、陈述、证明的演变，甚至对必然导致他们所见之漂亮定理及其证明的重要错误也不了解. 尽早明白思想以及错误是很有价值的. 在某些情况下，错误导致强大而深刻的新数学事实的发现. 因此，我们相信，有时也应当庆贺数学的错误. 并且，对于这样的庆贺来说，我们不能想象有比愚人节更好的时间.

这里我们概略地论述自十九世纪以来的三个错误的证明. 我们提供关于费尔马最后定理，四色猜想，以及我们当中有一个人是比尔·克林顿这一事实的"证明". 本文是基于作者们于 1996 年 4 月 1 日所组织的专门的大学生数学座谈会而写成的.

2. 费尔马最后定理. 该问题已成为数学中一个名声最坏的未解决问题，它有着最不祥的开端. 大约在 1637 年，皮埃尔·德·费尔马 (图 1a 略) 在研究 Bachet 译为拉丁文之 Diophantus 的《算术》时，需要讨论 Pythagoras 定理. 这激发了费尔马在文章边缘空白处写出了如今著名的下列几行：

> "不可能把一个立方分成两个立方，或一个四次方分成两个四次方，或更一般地，除平方以外的任意幂分成两个具同样指数的幂. 我已发现了此点之一个真正奇妙的证明，只是这里的空白太窄小，容纳不下它."

费尔马因为给出这样一些通常既缺少根据又没有证明的命题而出了名. 在十九世纪期间，所有的费尔马命题都已解决，唯独上面这一个除外，这是他的"最后定理".

费尔马最后定理. 对任意整数$N \geq 3$,

$$x^N + y^N = z^N, \text{ 其中 } xyz \neq 0$$

没有整数解.

原题: Fermat's Last Theorem, the Four Color Conjecture, and Bill Clinton for April Fools' Day. 译自: *Amer. Math.* Monthly, 104(1997), No.3, pp. 246–255.

我们强调指出，费尔马本人确曾提供了以上结果在 $N=4$ 情况的完全证明. 他的证明包含一个巧妙的构思，如今以费尔马下降法而知名. "下降法" 要领是，假设现有问题存在一些正整数解，利用那些解来构造另一些正整数解的集，而这些解在某种意义上较假设之解更小. 无限地重复这个程序将导致矛盾. 因为仅有有穷多个比假设之解更小的正整数解.

Gabriel Lamé [9](图 1b 略) 在业已对 $N=7$ 之情况证明此结果之后，于 1847 年 3 月 1 日对巴黎科学院宣称，他已获得了费尔马最后定理的完全证明. 然而，Joseph Liouville [10] 很快指出其论证中的一个严重错误. 下面是费尔马最后定理之一个 "证明" 的概述，它包含某些与 Lamé 所犯之错误相同的错误. 你能找到这些错误吗？

在着手费尔马最后定理的 "证明" 之前，我们定义某些记号，它们在以下的论证中起较大的作用. 令 p 是奇素数，并考虑多项式 $f_p(x)=x^p-1$. 如果我们写 $\zeta_p=e^{2\pi i/p}$, 则由于 ζ_p 的幂是 f 的零点，我们容易断定：

$$f_p(x)=(x-\zeta_p^0)(x-\zeta_p^1)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1}).$$

以下论证的关键是扩充整数概念的思想和使用广义整数的算术. 我们定义 p 分圆整数环 $\mathbb{Z}[\zeta_p]$ 为

$$\mathbb{Z}[\zeta_p]=\left\{\sum_{n=0}^{p-1}a_n\zeta_p^n : a_n\in\mathbb{Z}\right\}.$$

对 $\alpha,\beta\in\mathbb{Z}[\zeta_p]$, 我们说 α整除β, 并表示为 $\alpha|\beta$, 如果存在一个元 $\gamma\in\mathbb{Z}[\zeta_p]$, 使得 $\beta=\alpha\gamma$. 这时，我们说 α 是 β 的一个 因子. 元 $\omega\in\mathbb{Z}[\zeta_p]$ 称为 单位, 如果 $\omega|1$. 例如，对任意 $t\in\mathbb{Z}$, ζ_p^t 是单位. 非零元 $\pi\in\mathbb{Z}[\zeta_p]$ 为 素数, 如果 π 不是单位，并且只要 $\pi=\omega_1\omega_2, \omega_1,\omega_2\in\mathbb{Z}[\zeta_p]$, 则 ω_1 或者 ω_2 有一个是单位.

费尔马最后定理的 "证明". 将指数 N 分解为素因子，不难看出，对 $N=4$ 以及对 N 为任意奇素数来证明费尔马最后定理就足够了. 如我在前面讲过的，费尔马本人曾证明了 $N=4$ 的情况，因此我们仅需要考虑 $N=p$, 而 p 是奇素数的情况. 在 1770 年，Euler 对 $p=3$ 证明了此结论，因此可以假设 p 是大于 3 的素数.

我们用反证法来证明此定理，这就是说，假设

$$x^p+y^p=z^p,\quad xyz\neq 0 \tag{1}$$

有一整数解，通过约去所有公因子，我们可以假设 x,y 与 z 都是两两互素的. 现在考虑两种可能的情况.

情况 1. 素数 p 不整除 xyz.

情况 2. 素数 p 整除 xyz.

为了分析这些情况，我们进行下面的基本观察：

$$z^p = x^p + y^p = (-y)^p\left(-\left(\frac{x}{y}\right)^p - 1\right)$$
$$= (-y)^p f_p\left(-\frac{x}{y}\right) = (-y)^p \prod_{n=0}^{p-1}\left(-\frac{x}{y} - \zeta_p^n\right).$$

因此，

$$\prod_{n=0}^{p-1}(x + \zeta_p^n y) = z^p. \tag{2}$$

也许并不奇怪，分圆整数 $\mathbb{Z}[\zeta_p]$ 的算术类似于普通整数 $\mathbb{Z}$ 的算术. 例如，两个元 $\alpha, \beta \in \mathbb{Z}[\zeta_p]$ 称为 互素 是指它们没有异于单位的公因子. 基于此，对于 **情况 1**，在 (2) 中出现的因子都是两两互素. 可是对于 **情况 2**，在乘积 (2) 中出现的所有元都以素数 $\zeta_p - 1$ 为公因子，并且只要从每个元中约去这个因子，余下的分圆整数都是两两互素的.

假设 (1) 的上述解属于 **情况 1**. 在此情况下，由于 (2) 中乘积的因子是两两互素的，该乘积中的每个元必定是一个分圆整数的完满 p 次幂乘以某一单位. 特别，必定存在一个非零分圆整数 ω 和一个单位 ϵ，使得

$$x + \zeta_p y = \epsilon\omega^p.$$

经过某些推理和计算，可以证出 $x \equiv y \mod p$.

因此，由我们的初始方程 $x^p + y^p + (-z)^p = 0$，已经看出 $x \equiv y \mod p$. 由于对称性，重复我们的论证，可导出 $x \equiv -z \mod p$，以及 $y \equiv -z \mod p$. 这些同余式连同费尔马小定理 (即对于任意整数 n，$n^p \equiv n \mod p$)，推出

$$0 = x^p + y^p + (-z)^p \equiv x + y + (-z) \equiv 3x \mod p.$$

所以，p 整除 $3x$. 由于 p 是大于 3 的素数，p 必须整除 x，但这与 **情况 1** 的假定相矛盾. 因此 **情况 1** 是不可能的.

因为 (1) 的假设之解必须满足 **情况 2**. 在此情况下，我们知道乘积 (2) 中的每个元都有素公因子 $\zeta_p - 1$，而且分圆整数 $(x+y)(\zeta_p-1)^{-1}$，$(x+\zeta_p y)(\zeta_p-1)^{-1}$，$(x+\zeta_p^2 y)(\zeta_p-1)^{-1}$，$\cdots$，$(x+\zeta_p^{p-1}y)(\zeta_p-1)^{-1}$ 都是两两互素的. 通过类似于对 **情况 1** 的分析，我们必须有

$$(x + \zeta_p^n y)(\zeta_p - 1)^{-1} = \epsilon_n \omega_n^p, \tag{3}$$

这里 ϵ_n 是单位而 ω_n 是分圆整数，$n = 0, 1, 2, \cdots, p-1$，而 $\omega_0, \omega_1, \omega_2, \cdots, \omega_{p-1}$[1] 两两互素. 利用 $\mathbb{Z}[\zeta_p]$ 中的基本代数和算术，我们可推出以下元与变数 x, y 无关的等式：

$$\omega_1^p + (\tau_1\omega_{p-1})^p = \tau_2(\zeta_p - 1)^{tp}\gamma^p, \tag{4}$$

[1] 原文是 $\omega_0, \omega_2, \cdots, \omega_{p-1}$.—— 译注.

这里 τ_1 与 τ_2 都是 $\mathbf{Z}[\zeta_p]$ 的单位，$\gamma \in \mathbf{Z}[\zeta_p]$，并且 $\omega_1, \omega_{p-1}, \gamma, \zeta_p - 1$ 皆两两互素，而 $t \in \mathbf{Z}, t$ 大于 1. 因此我们找到了两两互素的分圆整数 Z, Y, Z，并且它们都与 $\zeta_p - 1$ 互素，使得

$$X^p + Y^p = \nu(\zeta_p - 1)^{tp} Z^p, \tag{5}$$

这里 ν 是单位，$t \in \mathbf{Z}, t \geq 1$.

现在使用费尔马下降法. 首先注意到可以像前面那样地将 (5) 式左边分解因子，并导出

$$\prod_{n=0}^{p-1} (X + \zeta_p^n Y) = \nu(\zeta_p - 1)^{tp} Z^p.$$

此时，每个因子 $X + \zeta_p^n Y$ 又可被 $\zeta_p - 1$ 整除. 和以前一样，现在我们证明，存在两两互素的分圆整数 X_1, Y_1, Z_1，它们都与 $\zeta_p - 1$ 互素，并且存在单位 ν_1，使得

$$X_1^p + Y_1^p = \nu_1(\zeta_p - 1)^{t_1 p} Z_1^p,$$

这里 t_1 是整数，满足 $1 \leq t_1 < t$. 因此，对于一个很类似于 (5) 的方程，我们有一个解. 关键的差别在于，现在 $\zeta_p - 1$ 的指数中有整数 t_1，而不是整数 t，这里 $1 \leq t_1 < t$. 我们可以重复这个程序，来生成两两互素的分圆整数 X_2, Y_2, Z_2，它们都与 $\zeta_p - 1$ 互素，并生成单位 ν_2 及整数 $t_2, 1 \leq t_2 < t_1$，使得

$$X_2^p + Y_2^p = \nu_2(\zeta_p - 1)^{t_2 p} Z_2^p.$$

重复这个过程，可生成递降整数的无穷序列，它们都在 1 与 t 之间：$1 \leq \cdots < t_n < \cdots < t_2 < t_1 < t$. 这个谬论表明 **情况 2** 是不可能的. 因此，对于 $x^p + y^p = z^p$ 必定不存在非零整数解，这就完成了费尔马最后定理的 "证明". 我们在哪里出了错？

毛病. 原来，我们的句子 "也许并不奇怪，分圆整数 $\mathbf{Z}[\zeta_p]$ 的算术类似于普通整数 $\mathbf{Z}$ 的算术" 在一个很重要的方面是不准确的：分圆整数一般没有唯一的素因子分解. 如果你考虑到，对允许我们断定乘积中的每个元都是一个完满 p 次幂来说，这是关键的一步；回忆我们的叙述，"由于 (2) 中乘积的因子是两两互素的，该乘积中的每个元必定是一个分圆整数的完满 p 次幂乘以某一单位." 事实上，Lamé 自己写道 [9, p.314]:

> 现在，如果想作乘积 $k^p m m' m'' \cdots m^{(p-1)}$ 等于复数 C 的 p 次幂，则诸数 $m, m', m'' \cdots, m^{(p-1)}$(它们没有公因子，甚至它们中的任意两个也没有公因子) 必须各自等于 p 次幂.

因此 Liouville 写道 [10, p. 319]:

> 尽管如此，某些初始的调查使我相信，对这些新的复数，应该先试着建立某种与对通常整数的基本命题类似的定理，亦即，只存在一种分解为素因子之积的方式.

$\mathbb{Z}[\zeta_p]$ 不满足因子分解唯一性的最小素数是 $p = 23$. 特别，直接的计算可以证实

$$(1+\zeta_{23}^2+\zeta_{23}^4+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^{10}+\zeta_{23}^{11})(1+\zeta_{23}+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{11})$$
$$=2\zeta_{23}^5(1+\zeta_{23}+\zeta_{23}^2+\zeta_{23}^4+\zeta_{23}^5+3\zeta_{23}^6+\zeta_{23}^7+\zeta_{23}^8+\zeta_{23}^{10}+\zeta_{23}^{11}+\zeta_{23}^{12}).$$

结果，2 是 $\mathbb{Z}[\zeta_p]$ 中的素数，它不能整除以上恒等式左端之两个因子中的任何一个.

在等式 (4) 的推导中，还有另一个稍许技术性一些的问题：我们需要知道，给定任意单位 τ_0，存在一个单位 τ_1，使得 $\tau_0 = \tau_1^p$. 这不仅不是显然的，而且有时是不可能的.

Ernst Kummer 曾发现，在某些情况下，前面的问题不会出现. 特别，如果素数 p 不整除 $\mathbb{Z}[\zeta_p]$ 的类数 (用 h 表示)，他称 p 为 正则素数. 类数 h 是正整数，它灵敏地度量该环距离有唯一因子分解性质有多远 ($h = 1$ 当且仅当有唯一的素因子分解). 因此，我们概述的 "证明" 实际上是费尔马最后定理对于正则素数的一个 正确的 证明；这个结果属于 Kummer [8](进一步的细节和完全的证明看 [3],[11]). 注意，如果 $\mathbb{Z}[\zeta_p]$ 满足唯一因子分解性质，则 $h = 1$，并且很清楚，p 不整除 h. 因此对于素指数 p，如果 $\mathbb{Z}[\zeta_p]$ 有唯一因子分解性质，则费尔马最后定理成立.

Kummer 对于费尔马最后定理方面的贡献是惊人地多种多样. 在 1847 年 5 月，Kummer[7] 写信给 Liouville，他说：

> 你很正确地指出，这个证明中缺乏关于此等复数的这一命题，即一个复合的复数可以唯一地分解成素因子 —— 这是一个在其它方面也有缺陷的证明 —— 我能对你担保，它对形如
>
> $$a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$$
>
> 的复数一般不成立. 但是，通过引进一种我称之为理想复数的新复数，有可能补救它.

Kummer 的研究导致了今天称之为 理想 之概念的诞生. 最后在 1994 年，Andrew Wiles[12] (图 1c) 利用抽象代数和椭圆曲线理论中强有力的工具，对所有素数给出一个完全和正确的证明，成就了伟大的业绩.

(图 1 略)

3. 四色猜想. 在 1852 年，Francis G'uthrie 问，每张由连通区域组成的平面地图 (如图 2) 能否用至多 4 种颜色着色，使得相邻之区域有不同的颜色？该问题最终于 1976 年由伊利诺斯大学的 Kenneth Appel 和 Wolfgang Haken [1] 用计算机证出来了，他们共用了一千多个小进的计算机时间，检验了一万多种情况 (图 3a).

不过第一个 "证明" 出现于 1879 年，是由伦敦的律师和业余数学家 Alfred Kempe [6] 发表的 (图 3b,3c). 该结果维持了 11 年，直到 Percy Heawood [5] 于 1890 年找出了错误. Heawood 承认其文章之目的是 "破坏而不是建设，因为它指出在如今公认的证明中有缺陷".

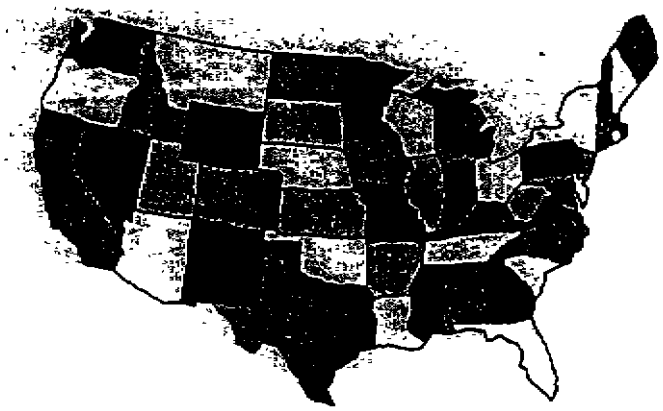

图2. 四色猜想说，由连通区域组成的平面地图可以用四种颜色着色，使得相邻之区域有不同的颜色.

(图 3 略)

图3 注： (a) W.Haken(和 K. Appel) 利用一千多小时的计算机时间，于 1976 年最终证明了四色猜想 (相片由美国数学会提供);(b) Alfred Kempe 于 1879 年发表了四色猜想的第一个 "证明"; (c) 1879 年四色猜想之 Kempe 证明的整页插图 [6].

四色猜想之 Kempe 的证明. 我们对区域数目进行归纳. 注意，如果对那些仅三个相交于一点的区域，此猜想成立的话，则此猜想也一般地成立，这是因为，举例来说，如果四个区域交于一点，可以扰动它们如图 4, 使其仅三个交于一点，然后着色，然后复原. (彼此斜对的区域可以着同样的颜色.) 所以，如果愿意的话，可以假设，区域仅三个交于一点.

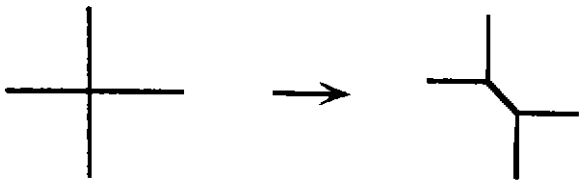

图4. 四个交于一点的区域可以扰动成三个交于一点.

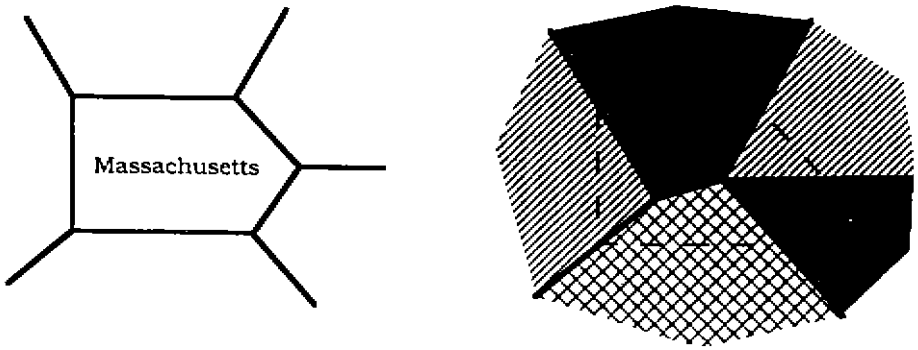

图5. 收缩掉第 n 个区域，并按归纳法给其余区域着色.

对一个区域，此猜想显然成立. 假设此猜想对 $n-1$ 个区域成立，要对 n 个区域来

证明它. 不难证明, (例如, 用欧拉示性数的概念), 某区域, 姑且说是 "马萨诸塞", 至多与五个区域相邻. 收缩掉马萨诸塞, 如图 5, 按照归纳法给其余区域着色. 现在复原马萨诸塞, 并找到一种办法, 按下述诸情况给它着色.

情况 1. 与马萨诸塞相邻的区域不到四个. 此时, 只要用某一未使用过的颜色来给马萨诸塞着色就行.

情况 2. 马萨诸塞恰好与四个区域相邻. 可以假设它们是四个不同颜色: 绿, 红, 蓝与黄, 如图 6; 否则就可以用还没有用上的颜色给马萨诸塞着色. 如果从上到下没有红 – 黄链, 则从上开始, 交换所有连接的红和黄色, 然后给马萨诸塞着红色. 如果从上到下有红 – 黄链, 则从左到右不可能有蓝 – 绿链. 此时从左开始, 交换所有所连接的蓝和绿色. 然后给马萨诸塞着蓝色.

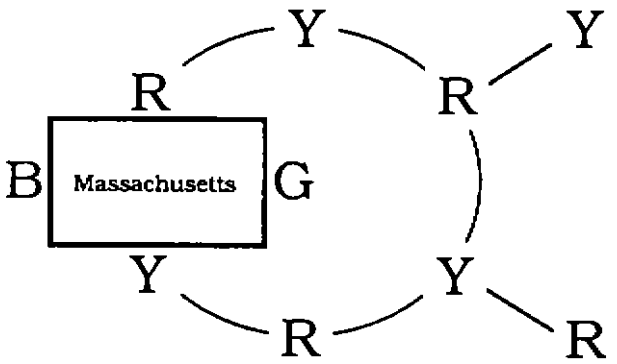

图6. 如果有红 – 黄链, 从左开始交换所有连接的蓝和绿色, 然后给马萨诸塞着蓝色.

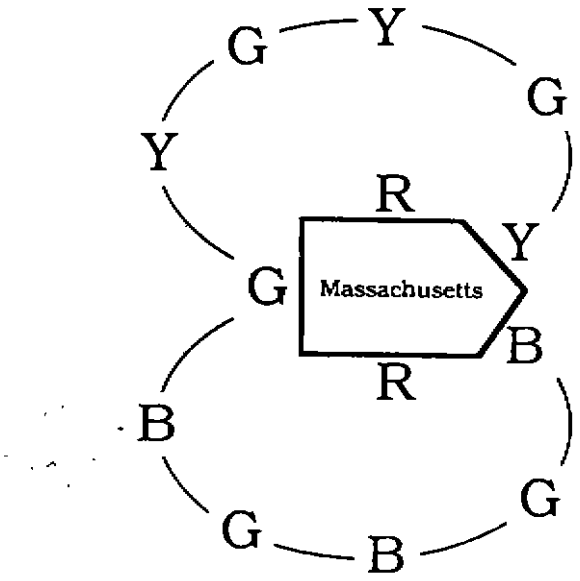

图 7. 如果从左到右既有绿 – 黄链, 又有绿 – 蓝链, 则从上开始, 交换所有连接的红和蓝色, 并从下开始, 交换所有连接的红和黄色, 然后给马萨诸塞着红色.

情况 3. 马萨诸塞恰好与五个区域相邻. 可以再假设与其相邻的区域用上了所有四种颜色，如图 7. 如果从左到右没有绿 - 黄链，则从右开始，交换所有连接的黄和绿色，然后给马萨诸塞着黄色. 如果从左到右没有绿 - 蓝链，则从右开始，交换所有连接的蓝和绿色，然后给马萨诸塞着蓝色. 如果从左到右既有绿 - 黄链又有绿 - 蓝链，则从上开始，交换所有连接的红和蓝色，并从下开始，交换所有连接的红和黄色. 然后给马萨诸塞着红色.

这就完成了 Kempe 的 "证明". 在继续读下去之前，你能找出毛病吗？

毛病. 问题在于，**情况** 3 中的两条链可以交叉，如图 8. 所以两条链包围的区域可能重叠. 于是，从上开始交换红和蓝色，与从下开始交换红和黄色，有可能抵触. 你可能认为，仍然能够补救这个证明. 但这可不是那么容易的. 关于四色猜想有一个很好的报告，请看 [13].

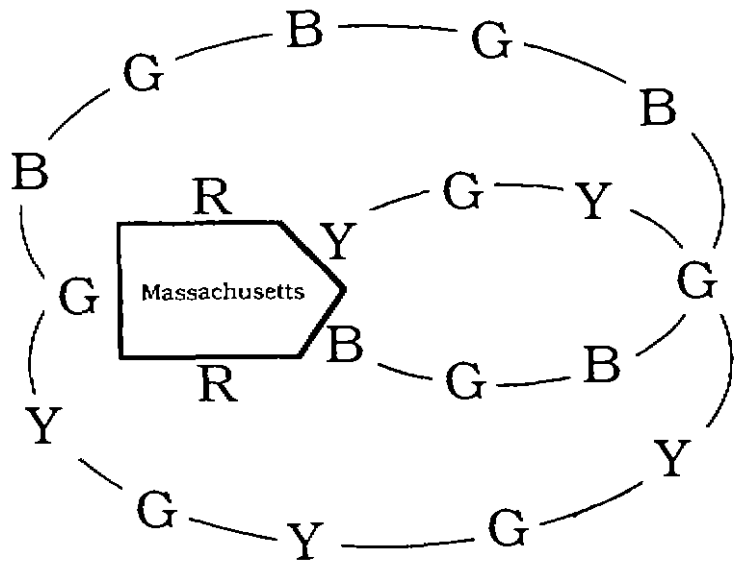

图8. 图 7 中不合理的假设是链与链不交叉，可是，如这里的插图所示，它们可以交叉.

附带地说一下，从技术上来说，四色猜想不适用于美国大陆，即使你划进水域，使得像密歇根这样的州成为连通的，因为肯塔基州有不连通的一小块被田纳西州和密苏里州包围着. 如果你不相信我们，只要试着从路易斯维尔驾车，沿所有的向西南的道路，去很小的新马德里湾地区，但不许离开肯塔基州，一切就会明白了.

4. 我是比尔 · 克林顿. 现在来说明，通过证明 "我是比尔 · 克林顿"，怎样就能 "证明" 任何事情. 考虑语句：

本语句是假的或者我是比尔 · 克林顿.

如果该语句是假的，则其第一个子句成立，从而该语句是真的，这是一个矛盾. 因

而此语句必须是真的. 由于第一个子句是假的，第二个子句必须是真的. 因此，我是比尔·克林顿. (图 9)

实际上，十九世纪的数学允许人们做这样的论证. 数学曾被重建，以禁止这样的自参考语句，它莫基于一个更加专门的 Zermelo-Frankel 集论，这种集论不允许集合是其自身的一个元，参看 [4, §3.4] 或 [2].

(图 9 略)

图9 注： "我是比尔·克林顿" 的作者 Edward Burger 和 Frank Morgan, 以及宣称 "我是比尔·克林顿" 而未经确认的第三者.

参 考 文 献

[1] K. Appel and W. Haken, Every planar map is four colorable, *Bull. Amer. Math. Soc.* **82** (1976), 711–712.

[2] J. Barwise and J. Etchemendy, *The Liar*, Oxford University Press, New York, 1987.

[3] H. M. Edwards, *Fermat's Last Theorem A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[4] W.S.Hatcher, *Foundations of Mathematics*, W.B. Saunders Co., Philaelphia, 1968.

[5] P.J.Heawood, Map-colour theorems, *Quart. J. Math. Oxford*, **24** (1980), 322–338.

[6] A.B.Kempe, On the geographical problem of the four colours, *Amer. J.Math.* **2** (1879), 193–200.

[7] E.E.Kummer, Extrait d'une lettre de M. Kummer á M. Liouville, *Jour. de Math.* **12** (1847), 136.

[8] E.E.Kummer, Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Poten-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $(\lambda-3)/2$ Bernoulli'schen Zahlen als Factoren nicht vorkommen, *Jour. für Math. (Crelle)* **40** (1850), 130–138.

[9] G.Lamé, Démonstration générale du théoréme de Fermat, sur l'impossibilité, en numbres, de l'équation $x^n + y^n = z^n$, *C.R. Acad. Sci. Paris* **24** (1947), 310–315.

[10] J.Liouville, Observations, *C.R. Acad. Sci. Paris* **24** (1947), 315–316.

[11] P.Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Heidelberg, Berlin, 1979.

[12] A.Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 433–551.

[13] R.J. Wilson and J.J. Watkins, *Graphs: an Introductory Approach*, John Wiley & Sons, Inc., New York, 1990.

(刘尚平 译　戚 征 校)