

.....

自恋性数 153 有一个奇特的性质,即对任意 3 的倍数,取其各位数字的立方和,再将这和各的各位数字再取立方和,……这样重复下去,必可在有限步内到达 153. 而一旦到达 153,因为它是一个自恋性数,就再也跳不出去了,也就是掉进了 153 这个黑洞.

例如,我们取 210 是 3 的倍数,其变换过程如下:

$$2^3 + 1^3 + 0^3 = 9,$$

$$9^3 = 729,$$

$$7^3 + 2^3 + 9^3 = 1080,$$

$$1^3 + 0^3 + 8^3 + 0^3 = 513,$$

$$5^3 + 1^3 + 3^3 = 153,$$

$$1^3 + 5^3 + 3^3 = 153.$$

探究:其他的数经过这样的步骤会掉进怎样的黑洞呢?

(二) 由自复制数造成的黑洞

另一类黑洞是一种所谓自复制数,也叫卡泼里卡常数(Kaprekar constant),因为它是印度学者卡泼里卡(D. R. Kaprekar)于 1954 年发现而命名的. 自复制数是这样一种奇特的数:由不同数字组成的一个数,按降序排好,再按升序排好,用前者减去后者,其差仍由相同数字组成. 自复制数比自恋性数还要稀少,三位仅一个,即由 4, 5, 9 所组成的数: $954 - 459 = 495$; 四位的自复制数也只有一个,由 1, 4, 6, 7 所组成: $7641 - 1467 = 6174$.

下面让我们来做个小实验:

取任意 4 个数字(不能全同)形成一个四位数,把它按降序排好,减去有这些数字按升序排好的数,得其差,再重复这一过程,你会发现什么结果?

很奇妙,我们所有人必能在有限步内到达 6174,这是因为 6174 是个自复制数,这就钻进了黑洞. 我们刚才做的这个过程就叫“卡泼里卡过程”(Kaprekar process).

探究:如果取三位数呢? 情况会怎样?

(三) 由数的因子和形成的黑洞

探究:任取自然数,把它的各个因子(包括 1,但不包括该数自身)

相加,得一数;再取该数的因子相加……如此重复下去,会出现什么情况呢?

会有以下三种情况:

1. 数的因子和恰为该数自身. 这样的数叫“完美数”. (已经在前面介绍过)

2. 某数的因子和为另一数,而这个另一数的因子和恰恰又是某数. 这样的一对数称为亲和数或友好数(amicable number).

亲和数是希腊的雅勃利丘斯(Iamblichus)在公元 320 年首先发现的. 他注意到:

$$284 \text{ 的因子和为: } 1 + 2 + 4 + 71 + 142 = 220.$$

而 220 的因子和为:

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284.$$

他觉得很有意思,向当时的大数学家毕达哥拉斯报告了他的发现. 他们想再找出一对这样的亲和数,但是没有成功. 直到 1636 年,法国的大数学家费马才找到了又一对亲和数:17 296 和 18 416;两年以后,笛卡儿发现了更大的一对亲和数:9 363 584 和 9 437 056. 一百多年以后,欧拉经过系统的研究,于 1750 年给出了 60 对亲和数. 但奇怪的是,他们都漏掉了 220 和 284 这一对之后最小的亲和数,即 1184 和 1210. 这对亲和数是 1866 年由当时年仅 16 岁的意大利数学家帕卡尼尼(Niccolo Paganini)发现的.

以后又发现了亲和数群或叫亲和数链(amicable number chain),即甲数的因子和是乙数,乙数的因子和又是丙数,……经过几个环,又回到甲数. 例如 5 个环的亲和数群:

$$12\,496 - 14\,288 - 15\,472 - 14\,536 - 14\,264 - 12\,496.$$

目前已知的最大亲和数群中有 28 个环.

3. 重复取因子和,最后都收敛为 1,即掉进 1 这个黑洞.

例如 20 这个数的演变过程如下:

$$20: 1 + 2 + 4 + 5 + 10 = 22,$$

$$22: 1 + 2 + 11 = 14,$$

$$14: 1 + 2 + 7 = 10,$$

$$10: 1 + 2 + 5 = 8,$$

$$8: 1 + 2 + 4 = 7,$$

$$7: 1.$$

由此可见,对于取因子和这一变换,只有极少极少的完美数,能始终保持“金身”不变;亲和数对亲和数链中的数由于“友谊”互相支撑,也抗拒了黑洞的吸引;其他的数都经不起变换或快或慢地要被吸引进黑洞中去.

附录

1. 费马的简介

费尔马, 1601 年生于法国南部图鲁斯附近的波蒙, 父亲是个商人, 从小费尔马就受到良好的家庭教育. 他在大学攻读法律, 毕业后当了律师. 从 30 岁起, 他才开始迷恋上数学, 直至逝世的 34 年里, 他的精神世界始终被数学牢牢地统治着. 费尔马结交了不少数学高手和哲学家, 如梅森, 罗伯瓦, 迈多治, 笛卡儿等, 他们每周一次在梅森寓所聚会, 讨论科学, 研究数学. 费尔马除了这些之外, 还经常和友人通信交流数学研究工作的信息, 但对发表著作非常淡漠. 费尔马在世时, 没有完整的著作问世. 当他去世后, 他的儿子萨缪尔·费尔马在数学家们帮助之下, 将费尔马的笔记, 批注及书信加以整理汇成《数学论集》在图鲁斯出版.



高等数学发展的起点是解析几何与微积分. 费尔马为此作出实质性的贡献. 从费尔马与罗伯瓦, 帕斯卡的通信中可以看出, 他在笛卡儿《几何学》发表前至少 8 年就已相当清晰地掌握了解析几何一些基本原理. 费尔马在《平面和立体轨迹引论中》得出一些重要结论, 还在一定程度上掌握了利用移轴和转轴的方法化简方法的技法; 在解析几何的圆锥曲线的研究上已经初步系统化. 因此说费尔马和笛卡儿分享创立解析几何的荣誉是当之无愧的.

费尔马也是微积分的先驱者, 微积分的发明人牛顿曾坦率地说: “我从费尔马的切线作法中得到了这种方法的启示, 我推广了它, 把它直接并且反过来应用于抽象方程上.” 费尔马是从研究透镜的设计和光学理论出发, 致力于探求曲线的切线的. 1692 年他在《求最大值和最小值的方法》手稿中就提出了求切线的方法. 可是当时的费尔马没有清晰的极限概念, 没有得出导数即切线的结论, 因此与微积分失去了交臂之缘, 只能作为微积分的杰出的先驱者而写入史册.

费尔马还开创了近代数论的研究. 对数的性质的研究从古希腊数学家欧几里得, 丢番图等人就已经开始了, 但是他们的研究缺乏系统

化. 费尔马注意到了这个问题, 并且指出对数的性质的研究应当有独自的园地——(整)数论. 同时, 费尔马认为在数论中素数的研究非常重要, 因为数论中的大量问题都与素数有关. 在这方面的研究成果是费尔马在数学许多部门中最为突出的, 其中最为著名是“费尔马小定理”, “费尔马大定理”, 值得一提的是, 300 多年来“费尔马大定理”一直困扰着数学界, 直到 1993 年才被普林斯顿大学的数学教授安德鲁·怀尔斯完全证明. 在“完全数”的研究上, 费尔马也有着两个重要的结论, 虽然这两个结论未能解决寻找完全数的方法, 但是在解决问题的途径上前进了一大步.

1653 年, 法国骑士梅累曾向帕斯卡提出“赌点问题”, 1654 年帕斯卡向费尔马转告了这个问题, 费尔马经研究后得到和帕斯卡同样的结果. 由于费尔马, 帕斯卡及惠更斯等人的深入研究, 使 16 世纪卡丹诺等已开始探讨的赌博问题引起数学家们广泛研究, 使之进一步数学理论化, 形成古典概率论. 可以说是费尔马点燃了古典概率论的火种.

毋庸置疑, 费尔马尽管是业余数学家, 但他在微积分、解析几何、概率论、数论等数学领域中, 都做出了开创性的贡献. 他在数学史上的作用与地位是不可低估的.

2. 斐波那契的简介

斐波那契(Leonardo Fibonacci, 约 1175—约 1240), 也许是在生活在丢番图(Diophantos)之后费尔马(Pierre de Fermat)之前这 2000 年间欧洲最杰出的数论学家. 我们对他的生平知道得很少. 他出生在意大利那个后来因为伽利略做过落体实验而著名的斜塔所在的城市里, 现在那里还有他的一座雕像. 他年轻时跟随经商的父亲在北非和欧洲旅行, 大概就是由此而学习到了世界各地不同的算术体系. 在他最重要的著作《算盘书》(Liber Abaci, 写于 1202 年)中, 引进了印度-阿拉伯数字(包括 0)及其演算法则. 数论方面他在丢番图方程和同余方程方面有重要贡献.

数学中有一个以他的名字命名的著名数列:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...

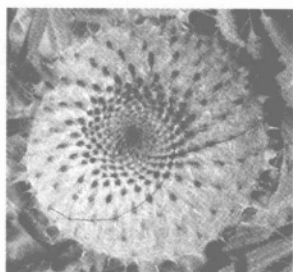
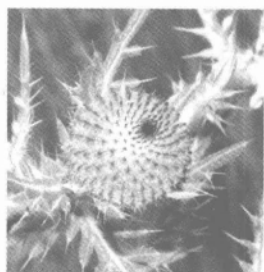
从第三项开始每一项都是数列中前两项之和. 这个数列是斐波那契在他的《算盘书》的“兔子问题”中提出的. 在问题中他假设如果一对兔子每月能生一对小兔(一雄一雌), 而每对小兔在它出生后的第三个月, 又

能开始生小兔,如果没有死亡,由一对刚出生的小兔开始,一年后一共会有多少对兔子?将问题一般化后答案就是,第 n 个月时的兔子数就是斐波那契数列的第 n 项.斐波那契数列和黄金分割数有很密切的联系.

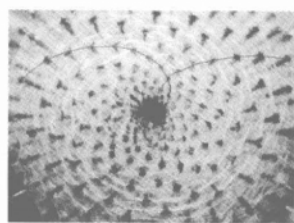
斐波那契并没有把这个问题和这个数列看得特别重要,在《算盘书》中兔子问题只不过是书里许多问题中并不特别的其中一个罢了.但是在此后的岁月中,这个数列似乎和题中的高产兔子一样,引发了为数众多的数学论文和介绍文章(本文似乎也在步此后尘).不过在这里我不想介绍浩如烟海的有关斐波那契数列的数学文章,只想欣赏大自然的造化.

3. 斐波那契螺旋的简介

在现实的自然世界中,《算盘书》里那样的神奇兔子自然是找不到的,但是这并不妨碍大自然使用斐波那契数列.



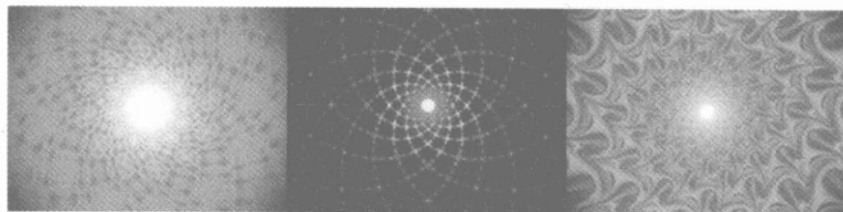
这是起绒草椭圆球状的花头,你可以看见那上面有许多螺旋.很容易想象,如果从上面俯视下去的话,这些螺旋从中心向外盘旋,有些是顺时针方向的,还有些是逆时针方向的.为了仔细观察这些螺旋,我们挑选另一种具有类似特点的植物——蓟,它们的头部几乎呈球状.在下面这个图里,标出了两条不同方向的螺旋.我们可以数一下,顺时针旋转的(和左边那条旋转方向相同)螺旋一共有13条,而逆时针旋转的则有



21 条. 而下面这幅图中的顺逆方向螺旋数目则恰好相反. 以这样的形式排列种子, 花瓣或叶子的植物还有很多(最容易让人想到的是向日葵), 下面的图片是一些看起来明显的例子, 事实上许多常见的植物, 我们食用的蔬菜如青菜, 包心菜, 芹菜等的叶子排列也具有这个特性, 只是不容易观察清楚. 尽管这些顺逆螺旋的数目并不固定, 但它们也并不随机, 它们是斐波那契序列中的相邻数字. 这样的螺旋被称为斐波那契螺旋. 这些植物懂得斐波那契数列吗? 应该并非如此, 它们只是按照自然的规律才进化成这样. 这似乎是植物排列种子的“优化方式”, 它能使所有种子具有差不多的大小却又疏密得当, 不至于在圆心处挤了太多的种子而在圆周处却又稀稀拉拉. 叶子的生长方式也是如此, 对于许多植物来说, 每片叶子从中轴附近生长出来, 为了在生长的过程中一直都能最佳地利用空间(要考虑到叶子是一片一片逐渐地生长出来, 而不是一下子同时出现的), 每片叶子和前一片叶子之间的角度应该是 222.5° , 这个角度称为“黄金角度”, 因为它和整个圆周 360° 之比是黄金分割数 $1.618\ 033\ 989\dots$ 的倒数, 而这种生长方式就决定了斐波那契螺旋的产生. 向日葵的种子排列形成的斐波那契螺旋有时能达到 89, 甚至 144 条.



由于是自然规律而并非抽象的数学或哲学原理决定了植物各种器官的排列图样; 另外还有具体环境的影响, 比如地形, 气候或病害, 你并不总能找到完美的斐波那契螺旋. 即使是生长得很健康的植物, 也难免有这样那样的缺陷. 仔细观察上面的图片, 你会发现螺旋的中心经常是一片混乱. 所以最后还是让我们来欣赏一下由计算机绘制出来的完美的斐波那契螺旋.



参考书目：

《好玩的数学》——吴鹤龄编著

《数学与联想》——戴维·韦尔斯著

圆心在一个圆上运动

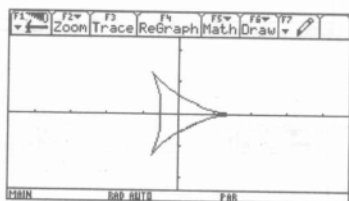
2007 届(3)班 尤逸之 毛亦欧

1. 曲线方程推导(只考虑圆进行无滑动滚动)

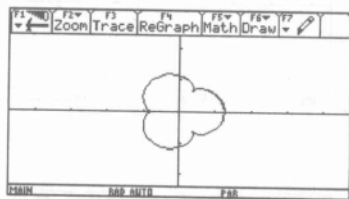
设圆 C 的圆心沿着一个半径为 R 的圆 B 运动,圆 B 的圆心位于原点,圆 C 的圆心起始点位于 $(R, 0)$,取定圆上一点 $A(R+r, 0)$,求圆 C 滚动时 A 点的运动轨迹.

当圆 C 运动了时间 t 后,可知圆 C 圆心相对于原点转动了 $\frac{r\omega t}{R}$ 角度,所以此时 A 点的坐标变为了

$$\begin{cases} x = R\cos\left(\frac{r\omega t}{R}\right) + r\cos\omega t, \\ y = R\sin\left(\frac{r\omega t}{R}\right) - r\sin\omega t. \end{cases} \quad (\text{圆顺时针转})$$



或者 $\begin{cases} x = R\cos\left(\frac{r\omega t}{R}\right) + r\cos\omega t, \\ y = R\sin\left(\frac{r\omega t}{R}\right) + r\sin\omega t. \end{cases} \quad (\text{圆逆时针转})$



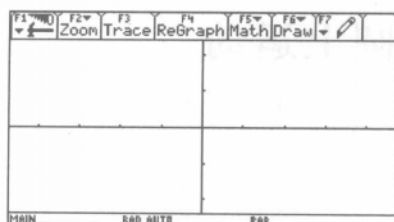
设 $\frac{r}{R} = k$, 则轨迹方程为 $\begin{cases} x = \frac{r}{k}\cos k\theta + r\cos\theta, \\ y = \frac{r}{k}\sin k\theta - r\sin\theta. \end{cases} \quad (\text{圆顺时针转})$

$\begin{cases} x = \frac{r}{k}\cos k\theta + r\cos\theta, \\ y = \frac{r}{k}\sin k\theta + r\sin\theta. \end{cases} \quad (\text{圆逆时针转})$

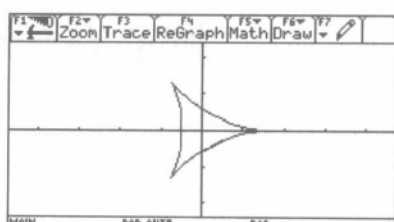
2. 变量 k 的改变与曲线形状的关系

(1) 圆顺时针转动时

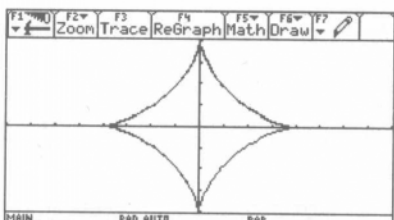
利用 TI 绘图的功能,对于 k 取不同值的图形分别如下:(取 $r = 1$)



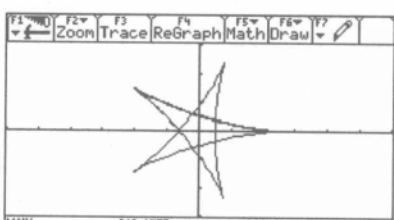
$k = 1$ (一条直线 $y = 0$, x 从 $-2r$ 到 $2r$)



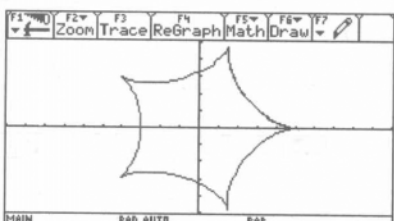
$$k = \frac{1}{2}$$



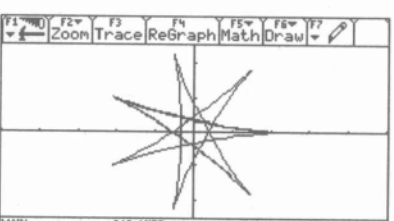
$$k = \frac{1}{3}$$



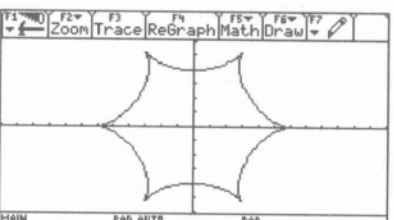
$$k = \frac{2}{3}$$



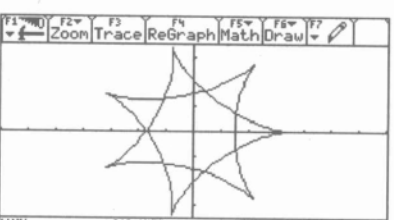
$$k = \frac{1}{4}$$



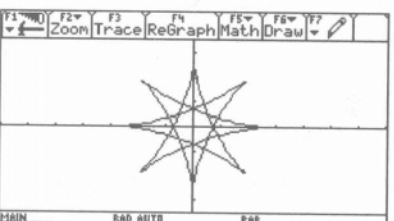
$$k = \frac{3}{4}$$



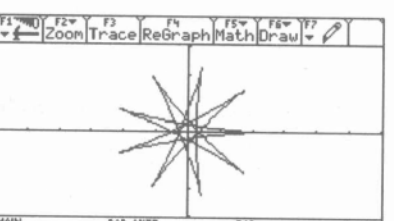
$$k = \frac{1}{5}$$



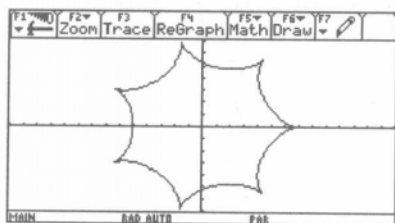
$$k = \frac{2}{5}$$



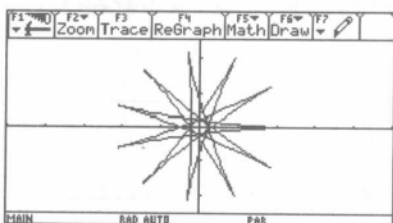
$$k = \frac{3}{5}$$



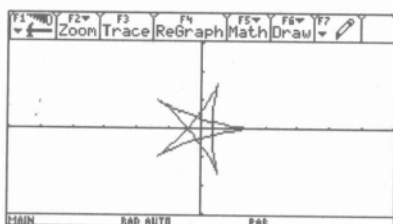
$$k = \frac{4}{5}$$



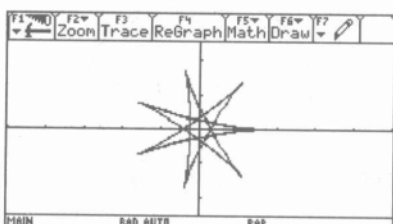
$$k = \frac{1}{6}$$



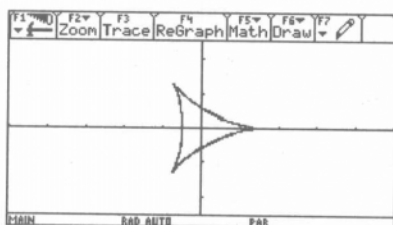
$$k = \frac{5}{6}$$



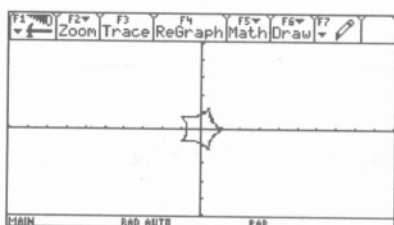
$$k = \frac{3}{2}$$



$$k = \frac{4}{3}$$



$$k = 2$$

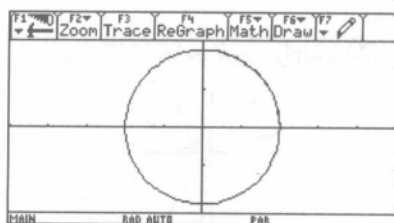


$$k = 4$$

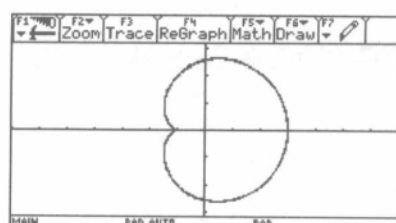
- ① $k = \frac{1}{n} (n \in \mathbf{Z})$ 时, 图形有 $n+1$ 个顶点;
- ② $k = \frac{q}{n} ((n, q) = 1, n, q \in \mathbf{Z})$, 图形是 q 层交织线;
- ③ $k = \frac{q}{n} ((n, q) = 1, n, q \in \mathbf{Z})$, 图形有 $n+q$ 个顶点, $n+q$ 个交点;
- ④ $k = q$ 与 $k = \frac{1}{q}$ 的图形一样.

(2) 圆逆时针转动时

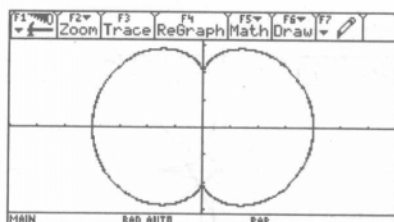
利用 TI 绘图的功能, 对于 k 取不同值的图形分别如下: (取 $r=1$)



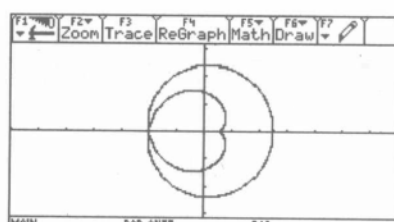
$$k = 1$$



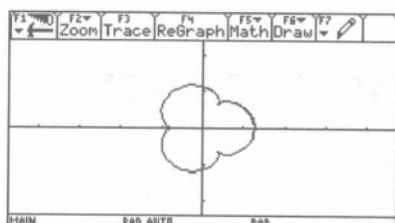
$$k = \frac{1}{2}$$



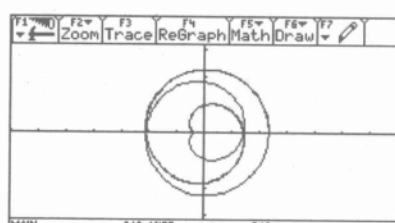
$$k = \frac{1}{3}$$



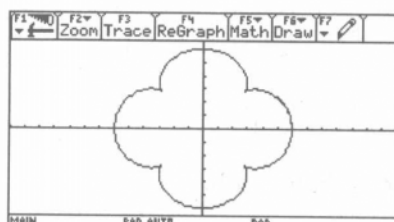
$$k = \frac{2}{3}$$



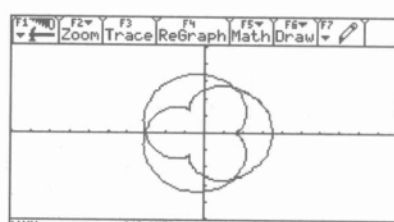
$$k = \frac{1}{4}$$



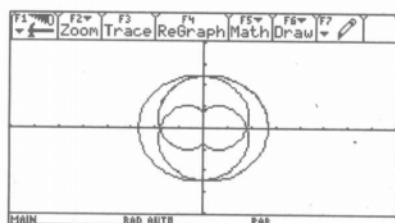
$$k = \frac{3}{4}$$



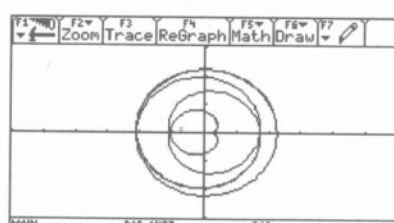
$$k = \frac{1}{5}$$



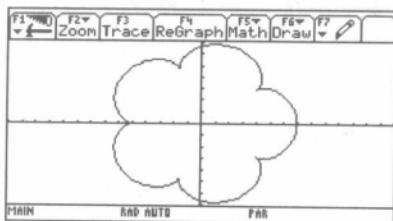
$$k = \frac{2}{5}$$



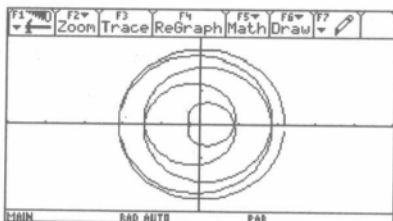
$$k = \frac{3}{5}$$



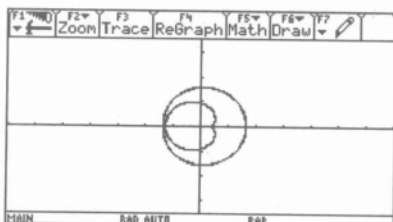
$$k = \frac{4}{5}$$



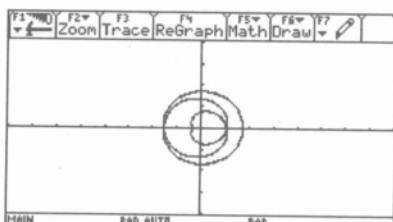
$$k = \frac{1}{6}$$



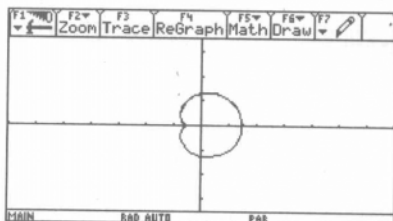
$$k = \frac{5}{6}$$



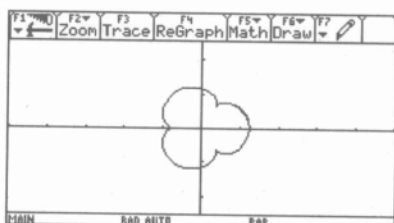
$$k = \frac{3}{2}$$



$$k = \frac{4}{3}$$



$$k = 2$$



$$k = 4$$

① $k = \frac{1}{n} (n \in \mathbf{Z})$ 时, 图形为花瓣形, 且有 $n-1$ 个瓣;

② $k = \frac{q}{n} ((n, q) = 1, n, q \in \mathbf{Z})$, 图形是 q 层交织线;

③ $k = \frac{q}{n} (n, q) = 1, n, q \in \mathbf{Z}$, q 固定时无论 n 取几, 图形最内部的形状相同;

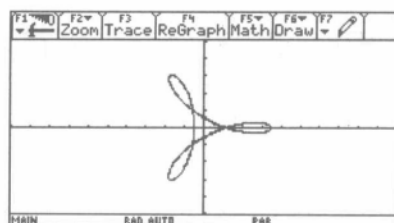
④ $k = q$ 与 $k = \frac{1}{q}$ 的图形一样.

3. 变幅曲线

类比于圆心在直线上运动时的变幅曲线, 设当 A 位于圆 C 内或外时, 设 A 到圆 C 圆心距离为 D , 可以推导出曲线方程为:

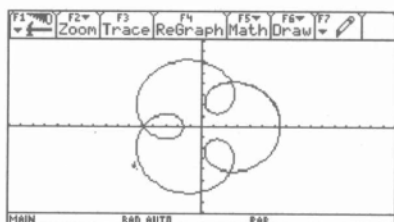
$$\begin{cases} x = R\cos\left(\frac{r}{R}\theta\right) + D\cos\theta, \\ y = R\sin\left(\frac{r}{R}\theta\right) - D\sin\theta. \end{cases}$$

这就是变幅内摆线；

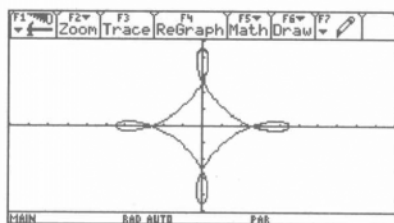


$$\begin{cases} x = R\cos\left(\frac{r}{R}\theta\right) + D\cos\theta, \\ y = R\sin\left(\frac{r}{R}\theta\right) + D\sin\theta. \end{cases}$$

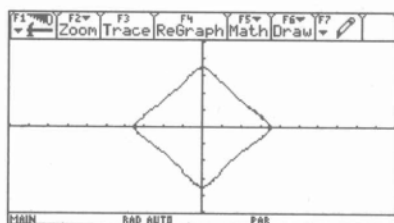
这就是变幅外摆线.



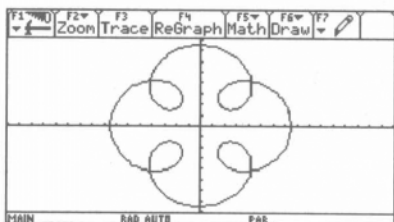
下面是 D 的不同取值得不同图形



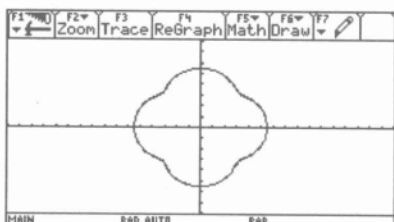
$$D = 1.5, R = 3, r = 1$$



$$D = 0.5, R = 3, r = 1$$



$$D = 2.5, R = 5, r = 1$$



$$D = 0.5, R = 5, r = 1$$

浅谈中国剩余定理

2008 届(10)班 刘仲麟 颜庭峰

一、剩余定理的介绍

在一千多年前的《孙子算经》中,有这样一道算术题:“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?”按照今天的话来说:一个数除以 3 余 2,除以 5 余 3,除以 7 余 2,求这个数.这样的问题,也就是初等数论中解同余式.它的有解条件和解的方法被称为“中国剩余定理”,这是由中国人首先提出的.

这是一个不定方程问题,答案有无数组.有人将这种奇妙的算法编成了一首歌谣:三人同行七十稀,五树梅花二十一枝,七子团圆正半月,除百零五便得知.《孙子算经》最先详细介绍了这种巧妙的算法.书中说:凡是每 3 个一数最后剩 1 个,就取 70;每 5 个一数最后剩 1 个的,就取 21;每 7 个一数最后剩 1 个,就取 15.把它们加起来,如果得数比 105 大,就减去 105,最后求出的数就是所有答案中最小的一个.在物不知数问题里,每 3 个一数最后剩 2,应该取 2 个 70;每 5 个一数最后剩 3,应该取 3 个 21;每 7 个一数最后剩 2,应该取 2 个 15.由于 $2 \times 70 + 3 \times 21 + 2 \times 15 = 233$,比 105 大,应该减去 105,得 128,仍比 105 大,再减去 105,得 23.

这种奇妙的算法有许多有趣的名称,如“鬼谷算”,“韩信大点兵”,“隔墙算”,“秦王暗点兵”等等,并被编成了许多有趣的数学故事.它于 12 世纪末就流传到了欧洲国家.到 13 世纪下半叶,我国数学家秦九韶把这种算法进一步完善,创造出一种更普遍,更强有力的巧妙算法,这就是驰名世界的“大衍求一术”.它是我国古代数学里最有独创性的成就之一,传到外国被称为“中国剩余定理”.

二、解法及证明

“孙子问题”在现代数论中是一个一次同余问题.显然,这相当于求不定方程组 $N = 3x + 2$, $N = 5y + 3$, $N = 7z + 2$ 的正整数解 N ,或用现代数论符号表示,等价于解下列的一次同余组: $N \equiv 2 \pmod{3}$, $N \equiv 3 \pmod{5}$, $N \equiv 2 \pmod{7}$.《孙子算经》给出的是符合条件的最小正整数.对于一般余数的情形,《孙子算经》术文指出,只要把上述算法中的余数 2、

3、2 分别换成新的余数就行了. 以 R_1 、 R_2 、 R_3 表示这些余数, 那么《孙子算经》相当于给出公式 $N = 70 \times R_1 + 21 \times R_2 + 15 \times R_3 - P \times 105$ (p 是整数). 孙子算法的关键, 在于 70、21 和 15 这三个数的确定. 《孙子算经》没有说明这三个数的来历. $N = 70 \times 3 + 21 \times 3 + 15 \times 2 - 2 \times 105$, 这里 105 是模数 3、5、7 的最小公倍数. 容易看出, 实际上, 它们具有如下特性: 也就是说, 这三个数可以从最小公倍数 $M = 3 \times 5 \times 7 = 105$ 中各约去模数 3, 5, 7 后, 再分别乘以整数 2, 1, 1 而得到. 假令 $k_1 = 2$, $k_2 = 1$, $k_3 = 1$, 那么整数 k_i ($i = 1, 2, 3$) 的选取使所得到的三数 70, 21, 15 被相应模数相除的时候余数都是 1. 由此出发, 立即可以推出, 在余数是 R_1 、 R_2 、 R_3 的情况下,

$$R_1 \times k_1 \times \frac{M}{3} = R_1 \times 2 \times \frac{3 \times 5 \times 7}{3} \equiv R_1 \pmod{3};$$

$$R_2 \times k_2 \times \frac{M}{5} = R_2 \times 1 \times \frac{3 \times 5 \times 7}{5} \equiv R_2 \pmod{5};$$

$$R_3 \times k_3 \times \frac{M}{7} = R_3 \times 1 \times \frac{3 \times 5 \times 7}{7} \equiv R_3 \pmod{7}.$$

综合以上三式又可得到:

$$\begin{aligned} R_1 \times 2 \times \frac{3 \times 5 \times 7}{3} + R_2 \times 1 \times \frac{3 \times 5 \times 7}{5} \\ + R_3 \times 1 \times \frac{3 \times 5 \times 7}{7} &\equiv R_1 \pmod{3}, \\ &\equiv R_2 \pmod{5}, \\ &\equiv R_3 \pmod{7}. \end{aligned}$$

因为 $M = 3 \times 5 \times 7$ 可被它的任一因子整除, 于是又有:

$$\begin{aligned} (R_1 \times 2 \times \frac{3 \times 5 \times 7}{3} + R_2 \times 1 \times \frac{3 \times 5 \times 7}{5} \\ + R_3 \times 1 \times \frac{3 \times 5 \times 7}{7}) - pM &\equiv R_1 \pmod{3}, \\ &\equiv R_2 \pmod{5}, \\ &\equiv R_3 \pmod{7}, \text{ (这里 } p \text{ 是整数).} \end{aligned}$$

这就证明了《孙子算经》的公式. 应用上述推理, 可以完全类似地把孙子算法推广到一般情形: 设有一数 N , 分别被两两互素的几个数 a_1 , a_2 , $\dots$, a_n 相除得余数 R_1 , R_2 , $\dots$, R_n ,

$$k_i \frac{M}{a_i} \equiv 1 \pmod{a_i}, (i = 1, 2, \cdots n).$$

即

$N \equiv R_i \pmod{a_i} (i = 1, 2, \cdots n)$, 只需求出一组数 K_i , 使满足那么适合已给一次同余组的最小正数解是

$$N = \left(R_1 k_1 \frac{M}{a_1} + R_2 k_2 \frac{M}{a_2} + R_3 k_3 \frac{M}{a_3} + \cdots + R_n k_n \frac{M}{a_n} \right) - pM$$

(p 是整数, $M = a_1 \times a_2 \times \cdots \times a_n$), 这就是现代数论中著名的剩余定理. 如上所说, 它的基本形式已经包含在《孙子算经》“物不知数”题的解法之中. 不过《孙子算经》没有明确地表述这个一般的定理.

三、剩余定理的应用

在雷达领域中, 中国剩余定理被用在脉冲多普勒雷达上, 解目标的距离模糊和速度模糊, 在线天线阵接收雷达中解测角的模糊; 在信号处理的理论中, 基于中国剩余定理的数论变化是一种重要的快速变换方法, 只是目前还缺乏对其物理意义的描述而使其应用受到一定的限制; 在 IC 设计中, 应用中国剩余定理可以获得高效的 II R 滤波器设计的方法. 中国剩余定理还奠定了目前世界上最流行的公钥加密技术(即 RSA)的基础.

四、中国剩余定理的意义

这个算法, 给出了这类问题的非常简捷的一般解法. 这个算法, 具有非凡的数学思想, 并对数论, 代数产生了重要影响. 中国称此算法为“孙子定理”, 国际上称此为“中国剩余定理”. 这是中国数学对世界数学最重要的贡献之一. 中国剩余定理除本身的重要性之外, 它还提示人们, 要解决较复杂的问题, 最好把它分解为几个易解的子问题; 把问题各不相同的条件化成标准的条件, 然后用标准的, 统一的方法去处理. 这是两种重要的数学思想.

在西方, 直到 18 世纪, 瑞士的欧拉与法国的拉格朗日才对同余式问题进行系统的研究. 19 世纪的第一年, 德国的高斯在《算术探究》一书中, 才提出解决这类问题的方法——剩余定理, 并给出了严格证明, 被后人称为“高斯定理”. 1852 年英国基督教士伟烈亚力在《字林西报》上发表了《中国科学的记述》, 介绍《孙子算经》中的“物不知数”题, 并第