**从勾股方程到椭圆曲线**

作者 雨露琴趣

1. 勾股方程与单位圆

勾股定理是平面几何中最著名的结论之一。 它断言直角三角形两直角边长的平方之和恰好等于斜边长的平方。中国古代将两直角边分别称作勾和股，斜边称作弦。“勾股”一词正是由此而来. 这一结论也常被称为毕达哥拉斯定理或商高定理，以纪念早期的发现者。 我们将直角三角形的勾、股、弦三边长度分别记为X,Y,Z. 勾股定理则可写为如下方程形式:



若要求 (X, Y, Z) 皆整数, 则称上述方程为勾股方程.

一个有趣的问题是：什么样的整数组 (X, Y, Z) 满足勾股方程? 显然并非所有的整数都能出现在上述方程的解中。 《周髀算经》曾提及“折矩以为勾广三， 股修四，经隅五”, 相当于给出一组特殊解 (3, 4, 5). 一般的解则可通过数论方法得到:

 (1)

这里a, b可以取任何整数.

尽管勾股方程求解从表面上看是纯粹的数论问题（即取决于整数本身性质的问题）， 但实际上我们可以用几何的方法重新得到它。我们在勾股方程两边除以 并且记x=X/Z, y=Y/Z, 则有



上述方程在平面上描绘的图形恰好是单位圆. 当 (X, Y, Z) 是整数时, (x,y) 是一对有理数, 它在平面上对应的点称作有理点. 因此求解勾股方程等价于寻找单位圆上所有的有理点!

进一步的操作很简单:

1. 以单位圆上点Q(-1,0)为固定点, 作斜率为t的射线L\_t.
2. L\_t与单位圆相交一点P\_t. 容易计算, P\_t点坐标为

 (2)

反之, 单位圆上每个点都有某条这样的射线通过它.

1. 若P\_t(x,y) 是有理点, 并且P\_t 不是固定点Q, 那么由关系式



立知t也必须是有理数. 反过来, 如果已知t是有理数, 则显然对应的P\_t是有理点.

1. 如果我们将Q点看成对应的交点P\_t, 那么上面的讨论显示, 当t跑遍所有有理数或者无穷远点时, P\_t恰好不重复地跑遍单位圆上的所有有理点.
2. 设t=b/a, 这里a,b是任何整数 (若a取零, 则令) . 代入 (2) 后，即得

,

这样由x=X/Z, y=Y/Z 就得到原来的勾股方程整数解 (1).

2.二次不定方程与圆锥曲线

上面介绍的几何方法极富启发性. 它将数论（即研究整数本身的特性）与几何巧妙联系起来。 两者表面上看似乎没有特别的关联，因为一个是研究整数，而另一个则是研究几何图形. 由此又产生了一个有趣问题： 对于数论中其他的不定方程， 是否也能用几何方法去处理呢? 事实上,这一问题正是推动数论与代数几何理论发展的动力之一.

让我们尝试在一些特殊情况下回答这一问题吧。 如前所见, 勾股方程求解最终变成了寻找单位圆上的有理点. 在平面几何中, 单位圆是比直线稍稍复杂的几何图形；而比单位圆更高级一点的图形则是总众所周知的圆锥曲线--它包括椭圆、抛物线和双曲线. 古典几何学对圆锥曲线的研究成果丰硕。 如果你承认数论和几何存在着这样一种对应关系, 那么自然有理由相信，圆锥曲线在数论中也必定对应着丰富的性质. 事实正是如此！

比如初等数论中著名的佩尔方程



这里d是事先给定的正整数. 显然上述方程定义了平面上的双曲线. 古典数论要求找出佩尔方程全部的整数解 (x, y). 当然我们可以退而求其次, 先求出有理数解 (x, y). 这样，问题就转化为寻找上述双曲线上的全部有理点. 利用类似单位圆有理点的求解方法, 我们可以轻而易举地解决这一问题.

当然, 如果要求x,y都是整数, 这个问题会稍稍困难点. 初等数论利用连分数的方法可以巧妙求出一组特殊的整数解(x\_0,y\_0). 有趣的是, 全部整数解都可以通过它求出来:

. (3)

有兴趣的读者不妨验证一些例子试试。

对应抛物线情形, 我们则有著名的二次剩余方程



这里p,q是事先取定的正整数. 读者也可以类似地求出所有有理解. 当然我们更关心它的整数解 (x,y). 求解这类不定方程的整数解可以说是初等数论的中心课题. 天才数学家高斯在其经典名著《算术研究》中给出了一系列漂亮的研究成果。 其中包括对数论发展极为重要的二次互反律—高斯称之为“数论之酵母”，以强调它的重要性.

二次互反律要回答如下问题: 如果p,q是两个不同的奇素数（所谓素数, 即指除了1及其本身外不被其它数所整除的正整数）, 那么以下两个方程

 

什么时候同时有解或无解？ 什么时候一个有解另一个无解？互反律证明了：

1. 当p和q其中有一个被4除余数为1时, 则两方程同时有解或无解.
2. 当p和q被4除余数皆为3时, 则两方程一个有解另一个无解.

高斯及其他一些数学家也进一步研究了更一般的二次不定方程（传统上称为二次型），建立了一套优美的理论. 在所有的结果背后。 人们总是可以看到数论与几何之间若隐若现的微妙联系. 当然, 那时的数学家还没有将这种深刻关系以完全明确的方式诠释出来. 让这种关系明朗化并使之成为数学研究重要思想的原动力之一，则是著名的”费马最后的定理”(FLT). 费马曾猜测(n>2)



没有非平凡整数解(即X,Y,Z均不为零). 它等价于说曲线



上除了 (1,0), (0,1) 等显而易见的点外没有其他有理点.

3.费马方程与椭圆曲线

证明费马方程



无非平凡解是极其困难的问题. 尽管费马在这一猜测的注记中声称自己找到了巧妙的证明, 但事实上，以费马所处时代的数学发展水平来看, 那是不可能的.

费马本人曾用无穷递降方法证明了n=4的情况. 这样一来, 人们只需要考虑n是奇素数的情形即可。 欧拉以较为繁琐的方法, 证明了n=3情形；高斯则巧妙地利用代数数论的性质（当时还没有系统形成这门理论）漂亮地解决该情形. 此后有许多优秀的数学家对此作过深刻研究, 并在此过程中发展出了许多重要的数学理论与工具（如代数数论，戴德金理想论等）. 最终由外尔斯于1995年前后彻底解决.

我们这里并不打算具体介绍费马方程的研究历史. 有兴趣的读者可以找相关的科普读物来了解这些内容. 现在，我们试图将它和平面上一类特殊的曲线联系起来—正如前几节所做的那样.

首先考虑n=3情形的费马方程. 我们设



于是费马方程转变成新方程

.

原始的费马方程有平凡的解(1,0,1),(0,1,0), 因此新方程相应地有平凡解 (12,36), (12,-36). 这样, 问题就转化为证明新方程定义的曲线上没有非平凡的有理点.

再看看n=4 的费马方程. 设



于是费马方程转变成新方程



与原始方程相比, 这样的简化方程形式上更简单, 而且方程次数也降低了.

这两个例子中, 我们都得到一类新的方程, 它可以写为



这里A,B都是给定的常数. 通常我们把它对应的平面几何图形称作椭圆曲线. 这里“椭圆”二字并非指该曲线是椭圆的. 实际上, 这一名词来自于椭圆的周长积分公式--在一定的变换后会出现如下项

，

故而得名。

椭圆曲线是比圆锥曲线更为复杂的一类几何对象。 它具有极其丰富的性质。这些性质包含了数学中的各个方面 (几何、数论、代数、分析等等). 它是联系数学各分支的一座桥梁，是不折不扣的“会生金蛋的鸡”。 事实上, 证明费马猜想的第一步正是先将它归结到某条特殊的椭圆曲线上, 然后人们可以利用深刻的研究工具去讨论这条椭圆曲线的性质.

椭圆曲线有一种让人着迷的优美性质，它对于求解某些不定方程非常有用. 这个性质是说, 你可以定义椭圆曲线上点与点之间的加法运算（和通常加法完全不同）： 假设P, Q是椭圆曲线C上两点, 用一条直线把它们连接起来. 该直线PQ会与C相交于第三个点R. 然后通过R做一条垂直于x轴的竖线, 该竖线将和C相交于第四个点, 记作P+Q. 这样定义的加法“+”有很好的性质, 它和通常加法一样具有交换律、结合律, 并且可以定义减法运算等.

有趣的是, 如果P， Q是椭圆曲线上的有理点, 那么P+Q也是有理点.特别地, nP=P+…+P (n 个P相加)也是有理点. 因此, 一旦我们找到一个特殊的有理点, 就可以用加法找到许许多多其他的有理点. 当然有时运气不好, 也可能出现循环情况, 即nP=mP（这样的点称作挠点）. 从挠点P出发, 通过取倍数就只能得到有限个有理点.

如果我们把椭圆曲线稍稍扰动一下, 可以把它退化成一条圆锥曲线加上一条直线. 那样的话, 我们也可以在圆锥曲线上引入加法运算, 从而利用已知的有理点构造出新的有理点. 事实上， 佩尔方程的通解公式(3) 正是利用这样的加法运算得到.

寻找椭圆曲线上所有的有理点是个重要的问题。 Mordell 的一个定理断言, 我们可以在椭圆曲线上选定有限个有理点，使得所有有理点一定是由这些选定的有理点通过一系列加法运算得到。 如果我们从这些选定的有理点中去掉挠点, 那么剩下的非挠点至少有多少个呢？ 人们猜测这样的非挠点个数和某类很特殊的函数的性质有关, 这就引出了著名的BSD猜想，它被列入七大数学猜想之一，与著名的黎曼猜想、霍奇猜想等等齐名。

4.同余数与椭圆曲线

椭圆曲线和另一类古老的不定方程也密切相关. 假设一个直角三角形的三条边长a,b,c都是有理数, 并且三角形的面积是整数n, 我们称满足此条件的n为同余数. 问: 哪些整数n是同余数?

并非所有整数都是同余数, 比如n=1就不是. 我们可以验证n=5是同余数, 因为可以选取直角三角形三边长为(20/3,3/2,41/6).

由勾股定理, 我们有方程组

.

如果设



那么我们就得到方程



容易验证, n 是同余数当且仅当上述方程定义的椭圆曲线除了(0,0), (n,0), (-n,0) 外还有其他有理点.

5.高次不定方程与代数曲线

从圆锥曲线到椭圆曲线, 我们分别考察了它们和数论之间的联系. 一个自然的想法当然是希望把这些讨论推广到更一般的方程上去. 比如我们考虑一个二元多项式f(x,y). 方程f=0定义了平面上的一个几何图形, 我们将它笼统地称为(平面)代数曲线.

高次不定方程的求解当然也可以归结成寻找代数曲线f=0上的所有有理点. 尽管这仅仅是观点上的转化, 并没有实质性的降低问题的难度, 但是它提供了一种重要的思想：将数论问题纳入到几何框架中, 用几何观点来研究数论.

圆锥曲线和椭圆曲线本身都集非常丰富的几何性质与数论性质等等于一身. 那么一般的代数曲线是否也如此呢? Mordell提供了一个让人颇为失望的猜测（后为Faltings所证明）. 这个猜想大致是说, 如果一条代数曲线不是直线、圆锥曲线或椭圆曲线, 那么它上面最多只有有限个有理点。曾有人这样比喻: 椭圆曲线上的有理点多如繁星；然而一般的代数曲线上的有理点却屈指可数. 两者间的反差如此之大, 确实不可思议. 实际研究也表明, 在所有代数曲线中, 只有椭圆曲线具有异常丰富且深刻的性质(涉及各个分支)， 而其他曲线都无法与之比拟. 这多少是一件令人感到神秘的事情.

2011年1月19日凌晨