从圆锥曲线上的有理点谈起

梁 永祺

中国科学技术大学

引言

- 数与形是数学自身发展中产生的抽象研究对象
- 数与形分别对应数论与几何
- 今天的主题：从圆锥曲线的有理点谈起——几何（圆锥曲线）、数论（有理点）

引言

- 数与形是数学自身发展中产生的抽象研究对象
- 数与形分别对应数论与几何
- 今天的主题：从圆锥曲线的有理点谈起——几何（圆锥曲线）、数论（有理点）

引言

- 数与形是数学自身发展中产生的抽象研究对象
- 数与形分别对应数论与几何
- **今天的主题**：从圆锥曲线的有理点谈起——几何（圆锥曲线）、数论（有理点）

几何

- 几何研究 图形
- Geometry 字面意思：geo大地，metry测量，几何学来源于土地测量
- 从这个具体的生活场景抽象出来的是研究图形的形状、大小

几何

- 几何研究 图形
- Geometry　字面意思：geo大地，metry测量，几何学来源于土地测量
- 从这个具体的生活场景抽象出来的是研究图形的形状、大小

几何

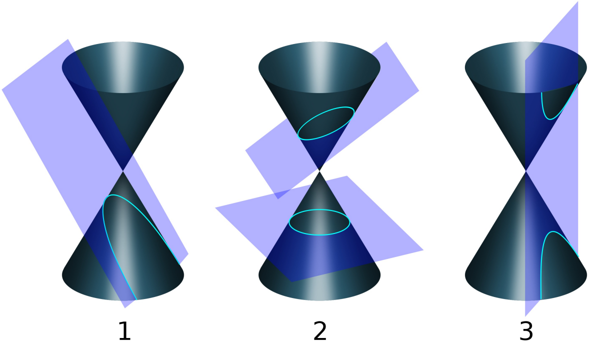
- 几何研究 图形
- Geometry　字面意思：geo大地，metry测量，几何学来源于土地测量
- 从这个具体的生活场景抽象出来的是研究图形的形状、大小

圆锥曲线

- 椭圆（包括圆）、抛物线、双曲线。如图
- 圆锥方程：$x^2 + y^2 = kz^2$
- 平面方程：$ax + by + cz = d$
- 消去一个变量，代入后得到一个二次方程，重新建立坐标系（即作可逆的变量替换）后：圆锥曲线=平面二次曲线

圆锥曲线

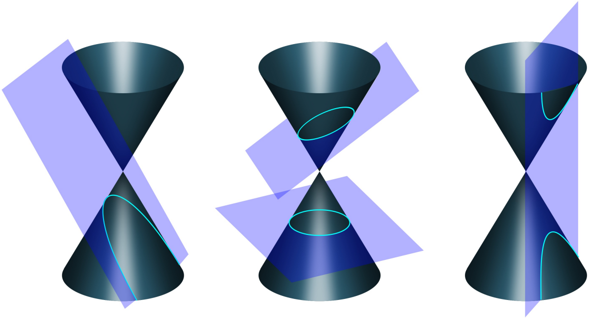
- 椭圆（包括圆）、抛物线、双曲线。如图



- 圆锥方程：$x^2 + y^2 = kz^2$
- 平面方程：$ax + by + cz = d$
- 消去一个变量，代入后得到一个二次方程，重新建立坐标系（即作可逆的变量替换）后：圆锥曲线=平面二次曲线

圆锥曲线

- 椭圆（包括圆）、抛物线、双曲线。如图

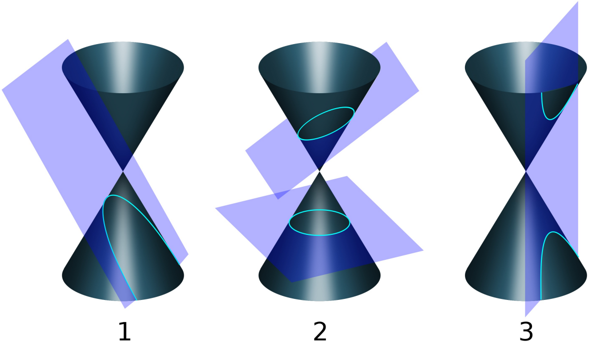


1　　2　　3

- 圆锥方程：$x^2 + y^2 = kz^2$
- 平面方程：$ax + by + cz = d$
- 消去一个变量，代入后得到一个二次方程，重新建立坐标系（即作可逆的变量替换）后：圆锥曲线=平面二次曲线

圆锥曲线

- 椭圆（包括圆）、抛物线、双曲线。如图



- 圆锥方程：$x^2 + y^2 = kz^2$
- 平面方程：$ax + by + cz = d$
- 消去一个变量，代入后得到一个二次方程，重新建立坐标系（即作可逆的变量替换）后：圆锥曲线=平面二次曲线

几何

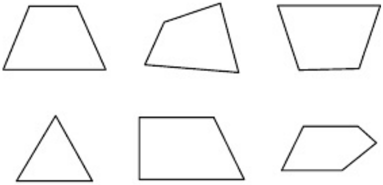
- 如何研究形状?
- 分类——几何学的中心问题
- 例子：分类多边形
- 最直观的答案：按边数分类[三角形、四边形、五边形……]
- 分类的关键：找到好的不变量 边数

几何

- 如何研究形状?
- 分类——几何学的中心问题
- 例子：分类多边形
- 最直观的答案：按边数分类[三角形、四边形、五边形……]
- 分类的关键：找到好的不变量 边数

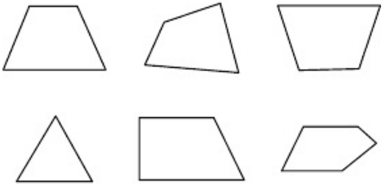
几何

- 如何研究形状?
- 分类——几何学的中心问题
- 例子：分类多边形



- 最直观的答案：按边数分类[三角形、四边形、五边形……]
- 分类的关键：找到好的不变量 边数

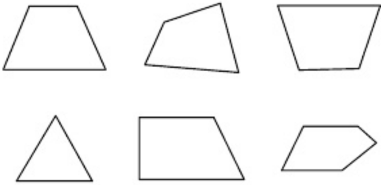
- 如何研究形状?
- 分类——几何学的中心问题
- 例子：分类多边形



- 最直观的答案：按边数分类[三角形、四边形、五边形······]
- 分类的关键：找到好的不变量 边数

几何

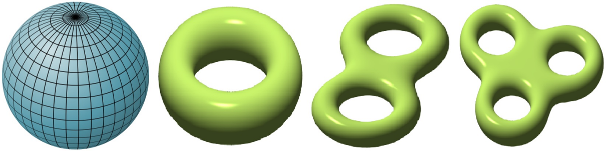
- 如何研究形状?
- 分类——几何学的中心问题
- 例子：分类多边形



- 最直观的答案：按边数分类[三角形、四边形、五边形……]
- 分类的关键：找到好的不变量 边数

封闭曲面的分类

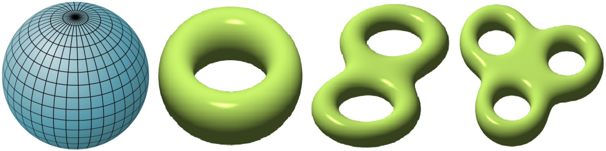
球面、救生圈面……



- 直观的不变量：洞的个数（严格数学称呼：亏格）
- “洞的个数”缺点：太描述性，比较难以用确定的数学语言（或公式）来给定义
- 几何学的一个任务：
  - 找到一个严格的方式去定义亏格（= 曲面的某个同调群的维数）
  - 证明这个量是一个不变量：随意连续形变（只要不撕破）这个曲面，亏格还是不变的

封闭曲面的分类

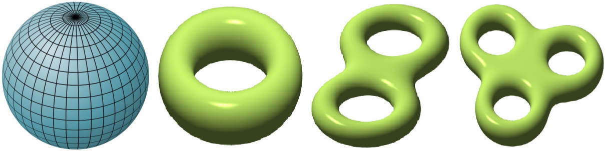
球面、救生圈面……



- 直观的不变量：洞的个数（严格数学称呼：亏格）
- “洞的个数”缺点：太描述性，比较难以用确定的数学语言（或公式）来给定义
- 几何学的一个任务：
  - 找到一个严格的方式去定义亏格（= 曲面的某个同调群的维数）
  - 证明这个量是一个不变量：随意连续形变（只要不撕破）这个曲面，亏格还是不变的

封闭曲面的分类

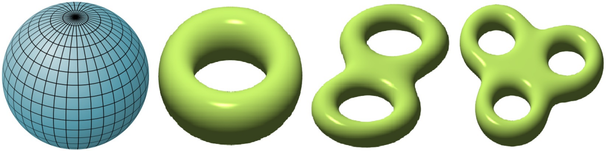
球面、救生圈面……



- 直观的不变量：洞的个数（严格数学称呼：亏格）
- “洞的个数”缺点：太描述性，比较难以用确定的数学语言（或公式）来给定义
- 几何学的一个任务：
  - 找到一个严格的方式去定义亏格（= 曲面的某个同调群的维数）
  - 证明这个量是一个不变量：随意连续形变（只要不撕破）这个曲面，亏格还是不变的

封闭曲面的分类

球面、救生圈面……



- 直观的不变量：洞的个数（严格数学称呼：亏格）
- “洞的个数”缺点：太描述性，比较难以用确定的数学语言（或公式）来给定义
- 几何学的一个任务：
  - 找到一个严格的方式去定义亏格（= 曲面的某个同调群的维数）
  - 证明这个量是一个不变量：随意连续形变（只要不撕破）这个曲面，亏格还是不变的

- 欧拉 瑞士数学家 

- 平面图中：V=顶点数，E=边数，F=面数（含最外一块）
-

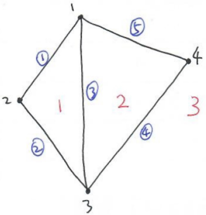
  左图：$V=4$，$E=5$，$F=3$
  右图：$V=5$，$E=7$，$F=4$
- 欧拉数 $\chi = V - E + F = 2$

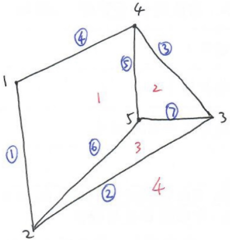
- 欧拉 瑞士数学家 

- 平面图中：V=顶点数，E=边数，F=面数（含最外一块）
- 左图：$V=4$，$E=5$，$F=3$
  右图：$V=5$，$E=7$，$F=4$
- 欧拉数 $\chi=V-E+F=2$

一个有趣的不变量：Euler欧拉数

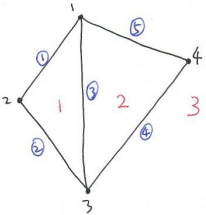
- 欧拉 瑞士数学家
- 平面图中：V=顶点数，E=边数，F=面数（含最外一块）

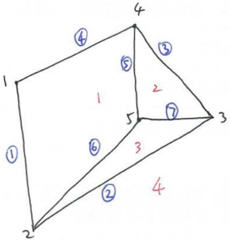




-
  左图：$V=4$，$E=5$，$F=3$
  右图：$V=5$，$E=7$，$F=4$
- 欧拉数 $\chi = V - E + F = 2$

- 欧拉 瑞士数学家
- 平面图中：V=顶点数，E=边数，F=面数（含最外一块）

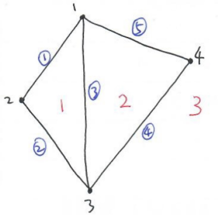


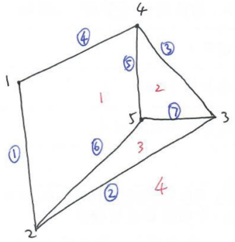


- 左图：$V = 4, \ E = 5, \ F = 3$
  右图：$V = 5, \ E = 7, \ F = 4$
- 欧拉数 $\chi = V - E + F = 2$

一个有趣的不变量：Euler欧拉数

- 欧拉 瑞士数学家
- 平面图中：V=顶点数，E=边数，F=面数（含最外一块）





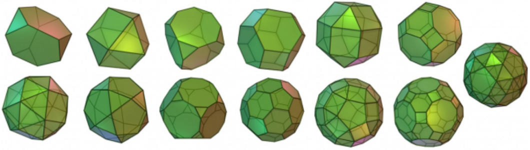
- 左图：$V=4,\ E=5,\ F=3$
  右图：$V=5,\ E=7,\ F=4$
- 欧拉数 $\chi = V - E + F = 2$

Theorem (欧拉公式)

任何简单（边互不相交）平面图的顶点、边、面个数都满足公式

$$\chi = V - E + F = 2。$$

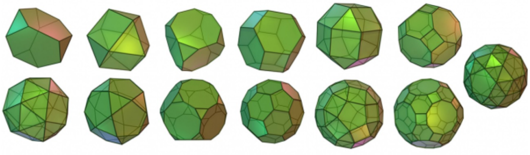
- 下图的多面体都称为球面的剖分



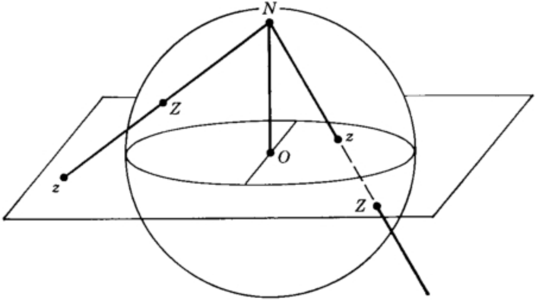
- 平面与球面（去掉北极点）的一一对应：球极投影
- 平面图 → 球面的一个剖分（图最外围的面变成包含北极的一块）

球极投影和球面的剖分

- 下图的多面体都称为球面的剖分



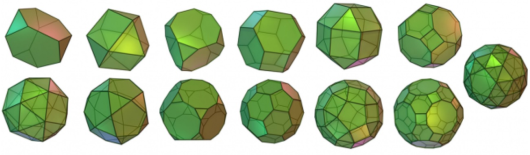
- 平面与球面（去掉北极点）的一一对应：球极投影



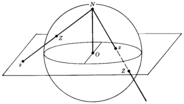
- 平面图 → 球面的一个剖分（图最外围的面变成包含北极的一块）

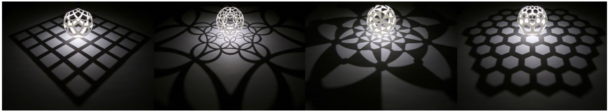
球极投影和球面的剖分

- 下图的多面体都称为球面的剖分



- 平面与球面（去掉北极点）的一一对应：球极投影

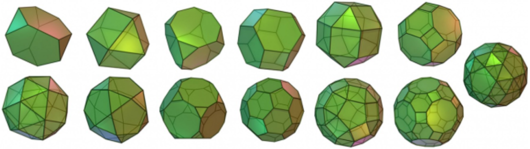




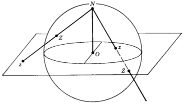
- 平面图 $\rightarrow$ 球面的一个剖分（图最外围的面变成包含北极的一块）

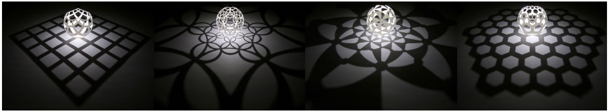
球极投影和球面的剖分

- 下图的多面体都称为球面的剖分

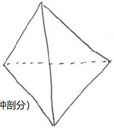


- 平面与球面（去掉北极点）的一一对应：球极投影

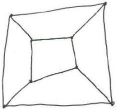


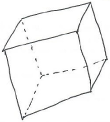


- 平面图 → 球面的一个剖分（图最外围的面变成包含北极的一块）



平面图 ⟶ 四面体（球面的一种剖分）





平面图 ⟶ 六面体（球面的一种剖分）

简单多面体的欧拉数

连续变换意义下，球面和它的剖分（即简单多面体[简单指没有洞]）是同一个几何对象

Name	Image	顶点 V	边 E	面 F	Euler characteristic: V − E + F
正四面体		4	6	4	**2**
正六面体		8	12	6	**2**

- $F = 12(黑) + 20(白) = 32$，$E = 90$，$V = 60$，仍有$V - E + F = 2$
- 球的各种剖分的不变量可以认为是球面的不变量

简单多面体的欧拉数

连续变换意义下，球面和它的剖分（即简单多面体[简单指没有洞]）是同一个几何对象

Name	Image	顶点 V	边 E	面 F	Euler characteristic: $V-E+F$
正四面体		4	6	4	**2**
正六面体		8	12	6	**2**

- $F=12(\text{黑})+20(\text{白})=32$，$E=90$，$V=60$，仍有$V-E+F=2$
- 球的各种剖分的不变量可以认为是球面的不变量

简单多面体的欧拉数

连续变换意义下，球面和它的剖分（即简单多面体[简单指没有洞]）是同一个几何对象

Name	Image	顶点 V	边 E	面 F	Euler characteristic: $V-E+F$
正四面体		4	6	4	**2**
正六面体		8	12	6	**2**

- $F=12$(黑)$+20$(白)$=32$，$E=90$，$V=60$，仍有$V-E+F=2$
- 球的各种剖分的不变量可以认为是球面的不变量

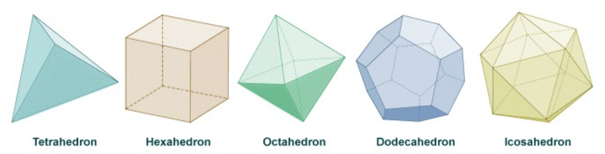
Theorem

简单多面体的欧拉数$\chi=V-E+F$总是2。

习题：正多面体

Exercise (欧拉公式$V-E+F=2$的应用)

正多面体只有这五种：

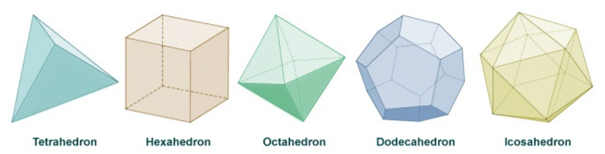


- 提示：除了$V-E+F=2$之外，V,E,F还有其他的关系
- 面都必须是正m边形且内角$<120°$（$\Rightarrow m=3,4,5$）
- 再找出V,E,F的又一个关系，就能够解方程求出V,E,F的值

习题：正多面体

Exercise (欧拉公式$V-E+F=2$的应用)

正多面体只有这五种：

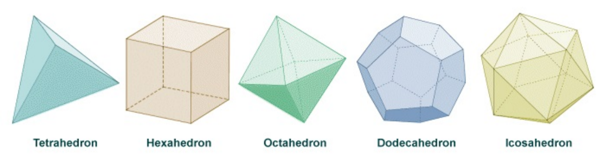


- 提示：除了$V-E+F=2$之外，V,E,F还有其他的关系
- 面都必须是正m边形且内角$<120^\circ$（$\Rightarrow m=3,4,5$）
- 再找出V,E,F的又一个关系，就能够解方程求出V,E,F的值

习题：正多面体

Exercise (欧拉公式$V-E+F=2$的应用)

正多面体只有这五种：

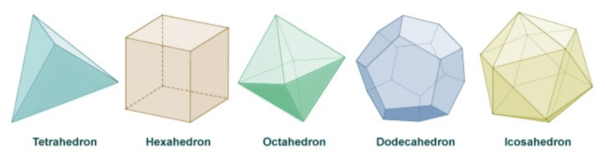


- 提示：除了$V-E+F=2$之外，V,E,F还有其他的关系
- 面都必须是正m边形且内角$<120^\circ$（$\Rightarrow m=3,4,5$）
- 再找出V,E,F的又一个关系，就能解方程求出V,E,F的值

习题：正多面体

Exercise (欧拉公式$V-E+F=2$的应用)

正多面体只有这五种：

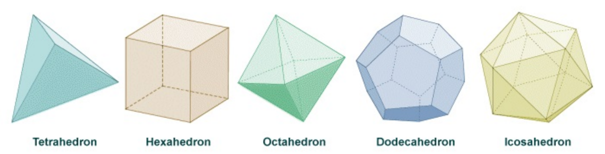


- 提示：除了$V-E+F=2$之外，V,E,F还有其他的关系
- 面都必须是正m边形且内角$<120°$（$\Rightarrow m=3,4,5$）
- 思考：能否找出面数F和边数E的一个关系？
- 再找出V,E,F的又一个关系，就能够解方程求出V,E,F的值

习题：正多面体

Exercise (欧拉公式$V-E+F=2$的应用)

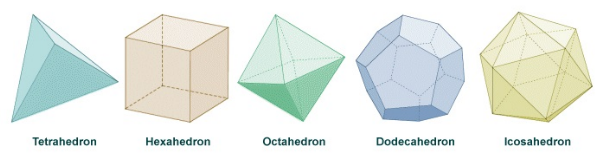
正多面体只有这五种：



- 提示：除了$V-E+F=2$之外，V,E,F还有其他的关系
- 面都必须是正m边形且内角$<120^\circ$（$\Rightarrow m=3,4,5$）
- 每个面有m条边、每条边被2个面共享 $\Rightarrow \frac{F\times m}{2}=E$
- 再找出V,E,F的又一个关系，就能够解方程求出V,E,F的值

Exercise (欧拉公式$V-E+F=2$的应用)

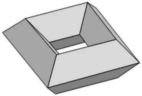
正多面体只有这五种：



- 提示：除了$V-E+F=2$之外，V, E, F还有其他的关系
- 面都必须是正m边形且内角$< 120°$（$\Rightarrow m=3,4,5$）
- 每个面有m条边、每条边被2个面共享 $\Rightarrow \frac{F\times m}{2}=E$
- 再找出V, E, F的又一个关系，就能够解方程求出V, E, F的值

不简单的多面体、一般曲面

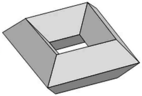
多面体剖分后：



- $V = 16, E = 32, F = 16, \ \chi = V - E + F = 0 \neq 2$
  右边对应的图不是一个简单平面图：无法把这些边压到平面上使得边都不相交
- 规律：$\chi = 2 - 2g$ （欧拉数和亏格本质上是同一个不变量）

不简单的多面体、一般曲面

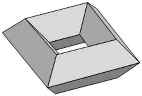
多面体剖分后：



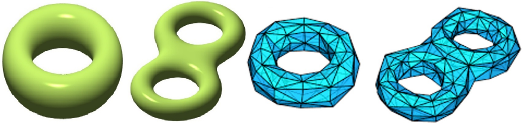
- $V = 16, E = 32, F = 16,\ \chi = V - E + F = 0 \neq 2$
  右边对应的图不是一个简单平面图：无法把这些边压到平面上使得边都不相交
- 规律：$\chi = 2 - 2g$（欧拉数和亏格本质上是同一个不变量）

不简单的多面体、一般曲面

多面体剖分后:

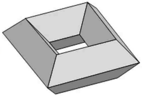


- $V = 16, E = 32, F = 16,\ \chi = V - E + F = 0 \neq 2$
  右边对应的图不是一个简单平面图：无法把这些边压到平面上使得边都不相交

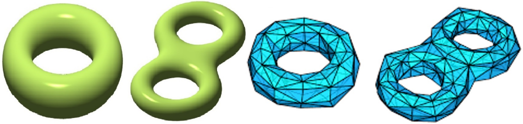


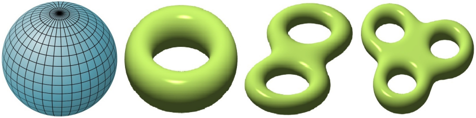
- 规律：$\chi = 2 - 2g$（欧拉数和亏格本质上是同一个不变量）

多面体剖分后：



- $V = 16, E = 32, F = 16,\ \chi = V - E + F = 0 \neq 2$
  右边对应的图不是一个简单平面图：无法把这些边压到平面上使得边都不相交

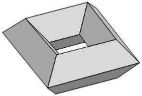




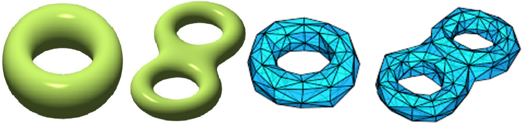
洞数(亏格g)	0	1	2	3
欧拉数	2	0	-2	-4

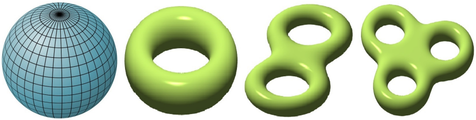
- 规律：$\chi = 2 - 2g$（欧拉数和亏格本质上是同一个不变量）

多面体剖分后:



- $V=16, E=32, F=16,\ \chi=V-E+F=0\neq 2$
  右边对应的图不是一个简单平面图：无法把这些边压到平面上使得边都不相交





洞数(亏格g)	0	1	2	3
欧拉数	2	0	-2	-4

- 规律：$\chi=2-2g$（欧拉数和亏格本质上是同一个不变量）

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）
- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M K dA = \chi(M) = 2 - 2\times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M K dA = \chi(M) = 2 - 2 \times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M KdA = \chi(M) = 2 - 2 \times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M K dA = \chi(M) = 2 - 2 \times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M KdA = \chi(M) = 2 - 2\times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

- 欧拉数 优点：严格定义、容易计算（通过剖分）、体现几何性质
  非平凡处：需要证明确实是个不变量（不依赖于不同剖分）

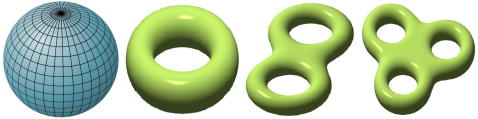
Theorem (Gauss-Bonnet公式)

对于任何光滑封闭曲面M有

$$\frac{1}{2\pi}\int_M K dA = \chi(M) = 2 - 2 \times \text{洞数}。$$

- $\chi(M)$为欧拉特征
- K为曲率：表示曲面在某点处的弯曲程度
- 求积分：把弯曲程度累加起来
- 左边：几何量
- 右边：组合计算得到的关于形状的不变量

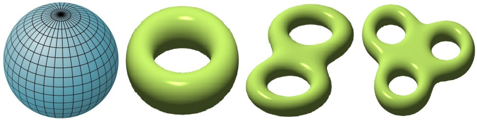
曲率



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负

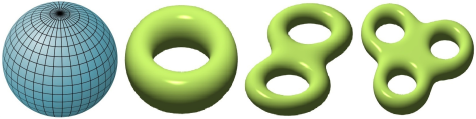
曲率



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负

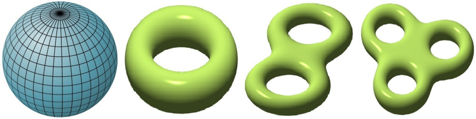
曲率



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

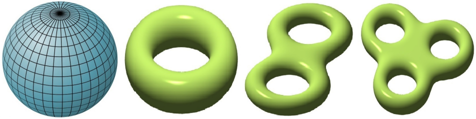
- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负

曲率



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

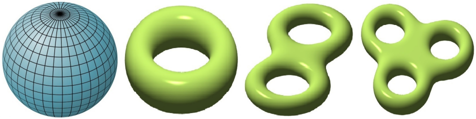
- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负

曲率



欧拉数	2	0	-2	-4
曲率平均值	正	0	负	负

- 零曲率：平的
- 正曲率的直观：无法按平到地上，中间总是鼓起来
- 负曲率的直观：无法按平到地上，边上总是翘起来
- 甜甜圈：曲率平均为零，有正有负
- 习题：判断以下曲面的曲率正负

手拿比萨饼的正确方法

- 这样拿，上面的料会掉！

- 正确拿法：
- 曲率(=0)两个方向曲率的乘积

手拿比萨饼的正确方法

- 这样拿，上面的料会掉！

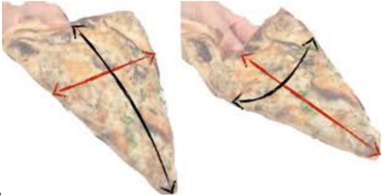
- 正确拿法:

- 曲率(=0)两个方向曲率的乘积

手拿比萨饼的正确方法

- 这样拿，上面的料会掉！

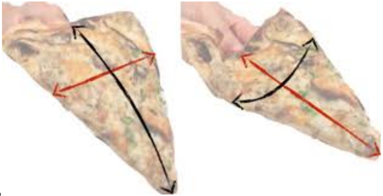
- 正确拿法：



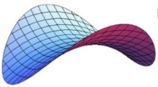
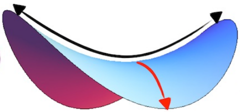
- 曲率(=0)两个方向曲率的乘积

-

- 正确拿法:



- 曲率(=0)两个方向曲率的乘积


回到主题：二次曲线分类

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2 + bxy + cy^2 + dx + ey + f = 0$ 配平方：
- $a(x + \frac{b}{2a}y)^2 - \frac{b^2-4ac}{4a}y^2 + dx + ey + f = 0$(小心$a = 0$)
- 换元（可逆的）$X^2 + \varepsilon Y^2 + DX + EY + F = 0(\varepsilon = \pm 1, 0)$
- $X \rightsquigarrow X + g, Y \rightsquigarrow Y + h$:(小心$\varepsilon = 0$)
  $X^2 \pm Y^2 + F' = 0$或$X^2 + Y + F' = 0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm 1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2 + bxy + cy^2 + dx + ey + f = 0$ 配平方：
- $a(x + \frac{b}{2a}y)^2 - \frac{b^2-4ac}{4a}y^2 + dx + ey + f = 0$(小心$a = 0$)
- 换元（可逆的）$X^2 + \varepsilon Y^2 + DX + EY + F = 0(\varepsilon = \pm 1, 0)$
- $X \rightsquigarrow X + g, Y \rightsquigarrow Y + h$:(小心$\varepsilon = 0$)
  $X^2 \pm Y^2 + F' = 0$或$X^2 + Y + F' = 0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

回到主题：二次曲线分类

- $ax^2+bxy+cy^2+dx+ey+f=0$ 配平方：
- $a(x+\frac{b}{2a}y)^2-\frac{b^2-4ac}{4a}y^2+dx+ey+f=0$(小心$a=0$)
- 换元（可逆的）$X^2+\varepsilon Y^2+DX+EY+F=0(\varepsilon=\pm 1,0)$
- $X\rightsquigarrow X+g, Y\rightsquigarrow Y+h$:(小心$\varepsilon=0$)
  $X^2\pm Y^2+F'=0$或$X^2+Y+F'=0$分类完成（椭圆、双曲线、抛物线）
- 缺点：
  - 配平方不唯一
  - 需要注意讨论的地方比较繁杂
  - 难以解释为什么通过不同的配平方得到的是同一类曲线

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵：$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵：$M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$（关于对角线翻转）
- 对称矩阵：若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

矩阵可逆⇔判别式$\Delta \neq 0$

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵：$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵：$M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$（关于对角线翻转）
- 对称矩阵：若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

矩阵可逆⇔判别式$\Delta \neq 0$

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵：$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵：$M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$（关于对角线翻转）
- 对称矩阵：若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

$$ax^2 + bxy + cy^2 = (x \quad y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

矩阵可逆⇔判别式$\Delta \neq 0$

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵：$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵：$M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$（关于对角线翻转）
- 对称矩阵：若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

$$ax^2 + bxy + cy^2 = (x \quad y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

矩阵可逆⇔判别式$\Delta \neq 0$

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵：$M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵：$M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$（关于对角线翻转）
- 对称矩阵：若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

矩阵可逆$\Leftrightarrow$判别式$\Delta \neq 0$

- 矩阵语言
- 矩阵 = 数表，配上奇怪的乘法（一般$MN \neq NM$），例：

$$MN = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} m_1 n_1 + m_2 n_3 & m_1 n_2 + m_2 n_4 \\ m_3 n_1 + m_4 n_3 & m_3 n_2 + m_4 n_4 \end{pmatrix}$$

- 可逆矩阵： $M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$若满足$m_1 m_4 - m_2 m_3 \neq 0$
- 转置矩阵： $M^t = \begin{pmatrix} m_1 & m_3 \\ m_2 & m_4 \end{pmatrix}$ （关于对角线翻转）
- 对称矩阵： 若$M^t = M$，即$m_2 = m_3$（关于对角线对称）
- 刚才方程的二次部分对应唯一的2×2对称矩阵

  $$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

  矩阵可逆⇔判别式$\Delta \neq 0$

Theorem (Sylvester)

任何2×2实系数对称矩阵Q，总存在可逆矩阵P使得$PP^t=I_2$，且（差± 1意义下）：

$$P^tQP=I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}1&0\\0&0\end{pmatrix},\ 或\begin{pmatrix}0&0\\0&0\end{pmatrix}。$$

——分别对应了椭圆、双曲线、抛物线（含退化情形：两相交直线、两平行直线……）

- 意义：对角线上$+1,-1,0$的个数成为了原始方程的二次部分$ax^2+bxy+cz^2$的（坐标变换下的）不变量，分类了对应的几何对象二次曲线

Theorem (Sylvester)

任何2×2实系数对称矩阵Q，总存在可逆矩阵P使得$PP^t=I_2$，且（差± 1意义下）：

$$P^tQP = I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\ 或\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}。$$

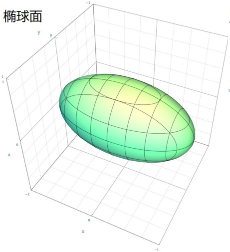
——分别对应了椭圆、双曲线、抛物线（含退化情形：两相交直线、两平行直线……）

- 意义：对角线上$+1,-1,0$的个数成为了原始方程的二次部分$ax^2+bxy+cz^2$的（坐标变换下的）不变量，分类了对应的几何对象二次曲线

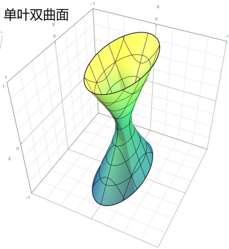
三维空间中二次曲面的分类

- 二次曲面（和之前的封闭曲面分类不一样，这些曲面大部分不封闭，这是另一个意义下的分类）
  $ax^2 + by^2 + cz^2 + dxy + exz + fyz + gx + hy + iz + j = 0$
  对应3×3对称矩阵，还有类似线性代数定理，得到几何分类
-

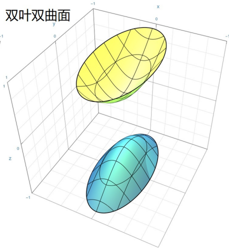
- 二次曲面（和之前的封闭曲面分类不一样，这些曲面大部分不封闭，这是另一个意义下的分类）
  $ax^2 + by^2 + cz^2 + dxy + exz + fyz + gx + hy + iz + j = 0$
  对应3×3对称矩阵，还有类似线性代数定理，得到几何分类



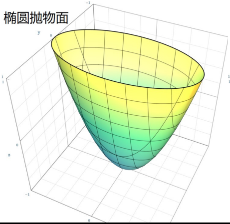
椭球面



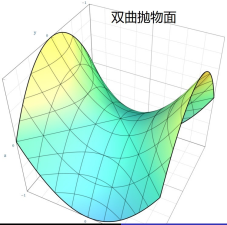
单叶双曲面



双叶双曲面

- 

椭圆抛物面



双曲抛物面

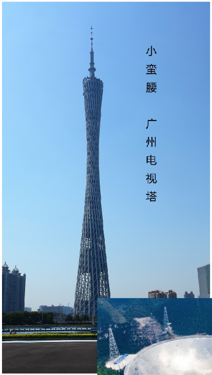
以及退化情形：

二次锥面

二次柱面

两相交平面……

二次曲面分类



FAST望远镜

- 数论（Number Theory 或 算术Arithmetic）研究 数
- 1，2，3⋯⋯ 以及数的推广
- 中心问题：在$\mathbb{Z}$或$\mathbb{Q}$中求解方程

Theorem (Andrew Wiles，费马大定理Fermat's last theorem)

当$n \geq 3$时，方程$x^n + y^n = z^n$的无非平凡整数解（平凡即$xyz = 0$）。

- 除以z：即$X^n + Y^n = 1$无非平凡有理数解（曲线上的有理点）

数论

- 数论（Number Theory 或 算术Arithmetic）研究 数
- 1，2，3⋯⋯ 以及数的推广
- 中心问题：在$\mathbb{Z}$或$\mathbb{Q}$中求解方程

Theorem (Andrew Wiles，费马大定理Fermat's last theorem)

当$n \geq 3$时，方程$x^n + y^n = z^n$的无非平凡整数解（平凡即$xyz = 0$）。

- 除以z：即$X^n + Y^n = 1$无非平凡有理数解（曲线上的有理点）

数论

- 数论（Number Theory 或 算术Arithmetic）研究 数
- 1，2，3⋯⋯ 以及数的推广
- 中心问题：在$\mathbb{Z}$或$\mathbb{Q}$中求解方程

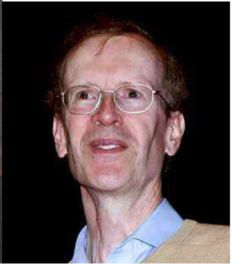
Theorem (Andrew Wiles，费马大定理Fermat's last theorem)

当$n \geq 3$时，方程$x^n + y^n = z^n$的无非平凡整数解（平凡即$xyz = 0$）。

- 除以z：即$X^n + Y^n = 1$无非平凡有理数解（曲线上的有理点）

数论

- 数论（Number Theory 或 算术Arithmetic）研究 数
- 1，2，3$\cdots\cdots$ 以及数的推广
- 中心问题：在$\mathbb{Z}$或$\mathbb{Q}$中求解方程



Theorem (Andrew Wiles，费马大定理Fermat's last theorem)

当$n \geq 3$时，方程$x^n + y^n = z^n$的无非平凡整数解（平凡即$xyz = 0$）。

- 除以z：即$X^n + Y^n = 1$无非平凡有理数解（曲线上的有理点）

- 数论（Number Theory 或 算术Arithmetic）研究 数
- 1，2，3⋯⋯ 以及数的推广
- 中心问题：在$\mathbb{Z}$或$\mathbb{Q}$中求解方程

Theorem (Andrew Wiles，费马大定理Fermat's last theorem)

当$n \geq 3$时，方程$x^n + y^n = z^n$的无非平凡整数解（平凡即$xyz = 0$）。

- 除以z：即$X^n + Y^n = 1$无非平凡有理数解（曲线上的有理点）

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）
- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）


- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）


- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）

- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）


- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

解多项式方程

- 一元2（或3，或4）次方程——有求根公式
- 一元5（或更高）次方程——一般情况：没有通过四则运算和开方的求根公式（Abel、Galois）

- m元一次方程——线性方程组：线性代数，Gauss消元法
- 其他不定方程：难，十分难！
- 已基本解决：多元2次齐次方程在$\mathbb{Q}$中求解（局部整体原则）
- 大部分未解决

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

（平面）曲线上的有理点

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- “曲线”的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

- 二元n次多项式
- 方程定义了一条平面曲线X(2变元1个方程)
- 解(又称为有理点)的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个(2维)曲面
- 例:X(由方程$xy = -1$定义)的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面(去掉一个点)在实空间中看是2维的
- 上述曲线也可以谈亏格:
  若$n = 2$亏格为0;若$n = 3$亏格为1;若$n \geq 4$亏格≥ 2

Question (几何决定算术?)

是否可以由亏格这个几何不变量决定(二元n次)方程是否有解?有多少解?

（平面）曲线上的有理点

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy=-1$定义）的复数解和$\mathbb{C}\setminus\{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n=2$亏格为0；若$n=3$亏格为1；若$n\geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

（平面）曲线上的有理点

- 二元n次多项式
- 方程定义了一条平面曲线X（2变元1个方程）
- 解（又称为有理点）的集合记为$X(\mathbb{Q})$、$X(\mathbb{R})$、$X(\mathbb{C}) \neq \varnothing$
- "曲线"的复有理点集$X(\mathbb{C})$其实构成一个（2维）曲面
- 例：X（由方程$xy = -1$定义）的复数解和$\mathbb{C} \setminus \{0\}$一一对应
- 复平面（去掉一个点）在实空间中看是2维的
- 上述曲线也可以谈亏格：
  若$n = 2$亏格为0；若$n = 3$亏格为1；若$n \geq 4$亏格≥ 2

Question (几何决定算术？)

是否可以由亏格这个几何不变量决定（二元n次）方程是否有解？有多少解？

回到这次报告的标题

- 最简单情形：$n=2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$"几乎"一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?
- 粗略地说："几乎"指应该算上无穷远处的解
  射影平面 $=$ 平面$\cup\{$无穷远处的点$\}$
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

回到这次报告的标题

- 最简单情形：$n=2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$“几乎”一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?
- 粗略地说：“几乎”指应该算上无穷远处的解
  射影平面 $=$ 平面$\cup\{$无穷远处的点$\}$
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

回到这次报告的标题

- 最简单情形：$n=2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$"几乎"一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?
- 粗略地说："几乎"指应该算上无穷远处的解
  射影平面 = 平面$\cup$\{无穷远处的点\}
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

回到这次报告的标题

- 最简单情形：$n = 2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$“几乎”一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?

Theorem

系数在$\mathbb{Q}$中的二元二次方程在$\mathbb{Q}$中一旦有解（$X(\mathbb{Q}) \neq \varnothing$），则解集合$X(\mathbb{Q})$和$\mathbb{Q}$“几乎”是一一对应的。于是有无穷个解。

- 粗略地说：“几乎”指应该算上无穷远处的解
  射影平面 = 平面$\cup${无穷远处的点}
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

回到这次报告的标题

- 最简单情形：$n=2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$“几乎”一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?

Theorem

系数在$\mathbb{Q}$中的二元二次方程在$\mathbb{Q}$中一旦有解（$X(\mathbb{Q})\neq\varnothing$），则解集合$X(\mathbb{Q})$和$\mathbb{Q}$“几乎”是一一对应的。于是有无穷个解。

- 粗略地说：“几乎”指应该算上无穷远处的解
  射影平面 = 平面$\cup${无穷远处的点}
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

回到这次报告的标题

- 最简单情形：$n = 2$ 二次曲线（圆锥曲线，亏格为0）
- 亏格0对应球面，$X(\mathbb{C})$和$\mathbb{C}$“几乎”一一对应（球极投影）
- 问题：是否可以求出$X(\mathbb{Q})$?

Theorem

系数在$\mathbb{Q}$中的二元二次方程在$\mathbb{Q}$中一旦有解（$X(\mathbb{Q}) \neq \varnothing$），则解集合$X(\mathbb{Q})$和$\mathbb{Q}$“几乎”是一一对应的。于是有无穷个解。

- 粗略地说：“几乎”指应该算上无穷远处的解
  射影平面 = 平面$\cup$\{无穷远处的点\}
- 看起来并不显然：（$\mathbb{Q}$系数的）圆锥曲线上横纵坐标都是有理数的点有无数个

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
  （可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$（可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
  （可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
  （可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
  （可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
（可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\varnothing$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

例子：勾股数

- 几何与算术的区别：
- 几何：$x^2+y^2=-1$在$\mathbb{C}$上等同于$XY=-1$
  （可逆坐标变换：$X=x+\sqrt{-1}y, Y=x-\sqrt{-1}y$）
- 算术：$x^2+y^2=-1$在$\mathbb{Q}$上无解但$XY=-1$在$\mathbb{Q}$上有无数解
- 上面定理$X(\mathbb{Q})\neq\emptyset$条件不可去掉（几何无法决定$\mathbb{Q}$上是否有解）
- 圆方程$x^2+y^2=1$的有理数解（去分母后）正好是勾股数：$(\frac{3}{5},\frac{4}{5})\rightsquigarrow(3,4,5)$、$(\frac{5}{13},\frac{12}{13})\rightsquigarrow(5,12,13)$、$(\frac{96354}{237730},\frac{217328}{237730})\rightsquigarrow(96354,217328,237730)\cdots\cdots$
- 上述定理结论：圆上的有理点$X(\mathbb{Q})$和$\mathbb{Q}$之间有一个一一对应，如果把这个对应具体公式写出来就能求出所有勾股数
- 根据之后的证明，可以计算出以下公式

$$\frac{m}{n}\mapsto\left(\frac{m^2-n^2}{m^2+n^2},\frac{2mn}{m^2+n^2}\right)$$

Bézout定理（几何）

- n次多项式共有n个复根（计重数），推广成：
- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）
- 必须算上无穷远处的交点（例：平行线交于无穷远处）
- 计算个数时要算重数：例如二重点算两个（例：抛物线的切线）
- 特殊情况：$m = 1$
  直线方程消元代入二元n次多项式后得到一元n次多项式，共n个复根

Bézout定理（几何）

- n次多项式共有n个复根（计重数），推广成：

Theorem (Bézout)

次数分别为 m 和 n 的两条平面曲线必相交于 mn 个复点（计重数且需包括无穷远处的交点）。

- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）

Bézout定理（几何）

- n次多项式共有n个复根（计重数），推广成：

Theorem (Bézout)

次数分别为 m 和 n 的两条平面曲线必相交于 mn 个复点（计重数且需包括无穷远处的交点）。

- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）
- 必须算上无穷远处的交点（例：平行线交于无穷远处）
- 计算个数时要算重数：例如二重点算两个（例：抛物线的切线）
- 特殊情况：$m = 1$
  直线方程消元代入二元n次多项式后得到一元n次多项式，共n个复根

Bézout定理（几何）

- n次多项式共有n个复根（计重数），推广成：

Theorem (Bézout)

次数分别为 m 和 n 的两条平面曲线必相交于 mn 个复点（计重数且需包括无穷远处的交点）。

- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）
- 必须算上无穷远处的交点（例：平行线交于无穷远处）
- 计算个数时要算重数：例如二重点算两个（例：抛物线的切线）
- 特殊情况：$m = 1$
  直线方程消元代入二元n次多项式后得到一元n次多项式，共n个复根

Bézout定理（几何）

- n次多项式共有n个复根（计重数），推广成：

Theorem (Bézout)

次数分别为 m 和 n 的两条平面曲线必相交于 mn 个复点（计重数且需包括无穷远处的交点）。

- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）
- 必须算上无穷远处的交点（例：平行线交于无穷远处）
- 计算个数时要算重数：例如二重点算两个（例：抛物线的切线）
- 特殊情况：$m=1$
  直线方程消元代入二元n次多项式后得到一元n次多项式，共n个复根

- n次多项式共有n个复根（计重数），推广成：

Theorem (Bézout)

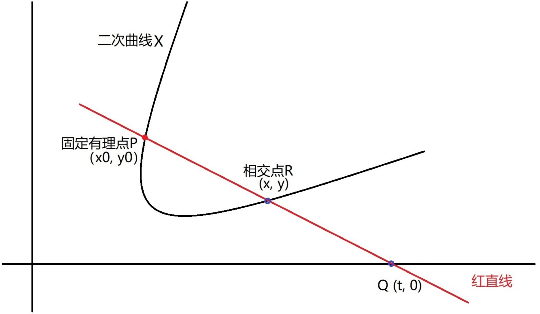
次数分别为 m 和 n 的两条平面曲线必相交于 mn 个复点（计重数且需包括无穷远处的交点）。

- 必须算复点，否则可能无实交点（例：圆与直线可以不相交）
- 必须算上无穷远处的交点（例：平行线交于无穷远处）
- 计算个数时要算重数：例如二重点算两个（例：抛物线的切线）
- 特殊情况：$m = 1$
  直线方程消元代入二元n次多项式后得到一元n次多项式，共n个复根

圆锥曲线上的有理点

- 将利用Bézout定理证明圆锥曲线上的有理点的结论：$\mathbb{Q}$与$X(\mathbb{Q})$一一对应
- 证明:
  - 取定点$P(x_0, y_0) \in X(\mathbb{Q}) \neq \varnothing$，取横轴上任一点$Q$与$P$连线和$X$交于另一点$R(x, y)$（Bézout定理）
  - 定义映射$Q \mapsto R$几乎是一一对应
  - 坐标都是有理数（韦达定理）

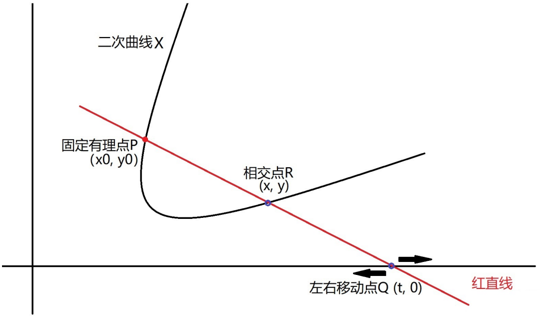
- 将利用Bézout定理证明圆锥曲线上的有理点的结论：$\mathbb{Q}$与$X(\mathbb{Q})$一一对应
- 证明：
  - 取定点$P(x_0, y_0) \in X(\mathbb{Q}) \neq \varnothing$，取横轴上任一点$Q$与$P$连线和$X$交于另一点$R(x, y)$（Bézout定理）



  - 定义映射$Q \mapsto R$几乎是一一对应
  - 坐标都是有理数（韦达定理）

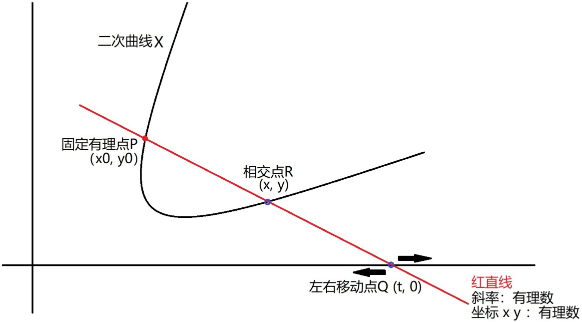
圆锥曲线上的有理点

- 将利用Bézout定理证明圆锥曲线上的有理点的结论：$\mathbb{Q}$与$X(\mathbb{Q})$一一对应
- 证明：
  - 取定点$P(x_0, y_0) \in X(\mathbb{Q}) \neq \varnothing$，取横轴上任一点$Q$与$P$连线和$X$交于另一点$R(x, y)$（Bézout定理）



  - 定义映射$Q \mapsto R$几乎是一一对应
  - 坐标都是有理数（韦达定理）

- 将利用Bézout定理证明圆锥曲线上的有理点的结论：$\mathbb{Q}$与$X(\mathbb{Q})$一一对应
- 证明：
  - 取定点$P(x_0, y_0) \in X(\mathbb{Q}) \neq \varnothing$，取横轴上任一点$Q$与$P$连线和$X$交于另一点$R(x, y)$（Bézout定理）



  - 定义映射$Q \mapsto R$几乎是一一对应
  - 坐标都是有理数（韦达定理）

- 其次简单的情形：三次平面曲线（二元3次方程）相应的曲面$X(\mathbb{C})$亏格为1（救生圈）
- 如果$X(\mathbb{Q}) \neq \varnothing$光滑三次曲线方程总能化简成以下标准形式（变量替换）
  $y^2 = x^3 + ax^2 + bx + c$（或者更简单的$y^2 = x^3 + ax + b$）
  称作**椭圆曲线**[名字起源：与椭圆周长的计算有关]

Theorem (Mordell–Weil)

椭圆曲线的有理点的集合$X(\mathbb{Q})$是一个有限生成交换群。

- 其次简单的情形：三次平面曲线（二元3次方程）相应的曲面$X(\mathbb{C})$亏格为1（救生圈）
- 如果$X(\mathbb{Q}) \neq \varnothing$光滑三次曲线方程总能化简成以下标准形式（变量替换）
  $y^2 = x^3 + ax^2 + bx + c$（或者更简单的$y^2 = x^3 + ax + b$）
  称作**椭圆曲线**[名字起源：与椭圆周长的计算有关]

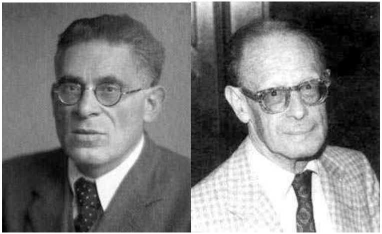
Theorem (Mordell–Weil)

椭圆曲线的有理点的集合$X(\mathbb{Q})$是一个有限生成交换群。

- 其次简单的情形：三次平面曲线（二元3次方程）相应的曲面$X(\mathbb{C})$亏格为1（救生圈）
- 如果$X(\mathbb{Q}) \neq \varnothing$光滑三次曲线方程总能化简成以下标准形式（变量替换）
  $y^2 = x^3 + ax^2 + bx + c$（或者更简单的$y^2 = x^3 + ax + b$）
  称作**椭圆曲线**[名字起源：与椭圆周长的计算有关]

Theorem (Mordell–Weil)

椭圆曲线的有理点的集合$X(\mathbb{Q})$是一个有限生成交换群。



群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算$+$的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）；
  - 交换律：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算$+$的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）;
  - 交换律：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）；
  - 交换律：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0=0+a=a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c=0=c+a$（常记为$c=-a$）；
  - 交换律：对任何$a, b \in G$有$a+b=b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0=0+a=a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c=0=c+a$（常记为$c=-a$）；
  - 交换律：对任何$a, b \in G$有$a+b=b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - 结合律：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - 零元：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - 负元：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）;
  - 交换律：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - **结合律**：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - **零元**：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - **负元**：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）;
  - **交换律**：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

群

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - **结合律**：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - **零元**：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - **负元**：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）;
  - **交换律**：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

- 什么是群?
- 整数集$\mathbb{Z}$的推广
- 群：带有一个运算+的集合G，满足：
  - **结合律**：对任何$a, b, c \in G$有$(a+b)+c = a+(b+c)$;
  - **零元**：存在一个元素$0 \in G$使得$a+0 = 0+a = a$;
  - **负元**：对任何$a \in G$存在$c \in G$使得$a+c = 0 = c+a$（常记为$c = -a$）;
  - **交换律**：对任何$a, b \in G$有$a+b = b+a$（称为交换群）
- 例：整数集$\mathbb{Z}$，模m同余类的集合$\mathbb{Z}/m\mathbb{Z}$，很多其他极其复杂的对象都有群结构
- （结构定理）有限生成交换群都等同于

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

其中后面共r（可以为0）个$\mathbb{Z}$

椭圆曲线上的加法

椭圆曲线X： $y^2 = x^3 + ax^2 + bx + c$

- 如何定义$X(\mathbb{Q})$中的加法使得它称为一个交换群?
- 如下图：过A和B作直线与三次曲线X交于第三个点C'（Bézout定理），取对称点C，如果A, B的坐标都是有理数那么C'也是，从而定义$A + B = C$
- 刚才的Mordell–Weil定理：这样定义的这个群等同于$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$，根据$r$是否为0，可能是有限的可能是无穷的

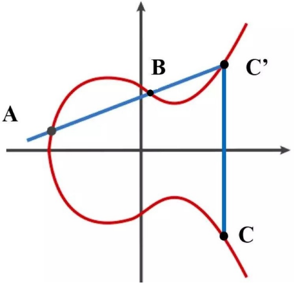
椭圆曲线上的加法

椭圆曲线X：$y^2 = x^3 + ax^2 + bx + c$

- 如何定义$X(\mathbb{Q})$中的加法使得它称为一个交换群?
- 如下图：过A和B作直线与三次曲线X交于第三个点C'（Bézout定理），取对称点C，如果A, B的坐标都是有理数那么C'也是，从而定义$A + B = C$
- 刚才的Mordell–Weil定理：这样定义的这个群等同于$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$，根据$r$是否为0，可能是有限的可能是无穷的

椭圆曲线X：$y^2 = x^3 + ax^2 + bx + c$

- 如何定义$X(\mathbb{Q})$中的加法使得它称为一个交换群?
- 如下图：过A和B作直线与三次曲线X交于第三个点C'（Bézout定理），取对称点C，如果A, B的坐标都是有理数那么C'也是，从而定义$A + B = C$

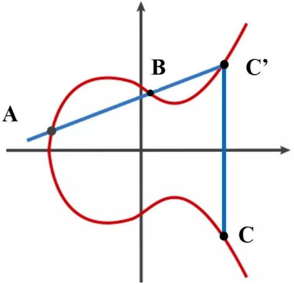


- 刚才的Mordell–Weil定理：这样定义的这个群等同于$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$，根据$r$是否为0，可能是有限的可能是无穷的

椭圆曲线上的加法

椭圆曲线X：$y^2 = x^3 + ax^2 + bx + c$

- 如何定义$X(\mathbb{Q})$中的加法使得它称为一个交换群?
- 如下图：过A和B作直线与三次曲线X交于第三个点C'（Bézout定理），取对称点C，如果A, B的坐标都是有理数那么C'也是，从而定义$A + B = C$



- 刚才的Mordell–Weil定理：这样定义的这个群等同于 $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$，根据$r$是否为0，可能是有限的可能是无穷的

一个"初等"例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量："二元三次方程"，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个"初等"例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量："二元三次方程"，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$

  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量："二元三次方程"，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c},y=\frac{364(a-b)}{6a+6b-c};a=\frac{56-x+y}{56-14x},b=\frac{56-x-y}{56-14x},c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

一个“初等”例子

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

99.99%的人解不出这道题！

求方程$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$的有理数解、整数解、正整数解

- $a^3+b^3+c^3-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)-5abc=0$
- a,b,c同时乘常数后仍是解，虽有三个变量，本质上只有两个变量：“二元三次方程”，是椭圆曲线
- 变量替换成标准形式：$y^2=x^3+109x^2+224x$
  $x=\frac{-28(a+b+2c)}{6a+6b-c}, y=\frac{364(a-b)}{6a+6b-c}; a=\frac{56-x+y}{56-14x}, b=\frac{56-x-y}{56-14x}, c=\frac{-56-12x}{56-14x}$
- （非平凡）对于这条椭圆曲线，$X(\mathbb{Q})$正好等同于$\mathbb{Z}$，$1\in\mathbb{Z}$对应于点$P=(-100,260)$，相应$(a,b,c)=(4,-1,11)$
- 运用椭圆曲线上的加法计算$nP=P+P+\cdots+P$就可以得到所有有理数解
- $2P=(\frac{8836}{25},\frac{-950716}{125})$相应的$(a,b,c)=(9499,-8784,5165)$（$a,b,c$仍不是正整数解，解的复杂度极其迅速地增加）
- 第一次出现正整数解对应于$9P$，长达80位数！
- 开始的问题用计算机暴力计算都无法找到80位那个最小解，不可缺的是人类的智慧：椭圆曲线的算术理论
- 椭圆曲线的理论还在费马大定理的最后证明中起到重要作用

- n次平面曲线（二元n次方程）$n \geq 4$相应的曲面$X(\mathbb{C})$亏格≥ 2

Theorem（Faltings）

亏格≥ 2的曲线的有理点集$X(\mathbb{Q})$是有限集。

- 这项工作让Faltings获得了1986年的 菲尔兹奖（数学界的最高奖之一）

- n次平面曲线（二元n次方程）$n \geq 4$相应的曲面$X(\mathbb{C})$亏格≥ 2

Theorem (Faltings)

亏格≥ 2的曲线的有理点集$X(\mathbb{Q})$是有限集。

- 这项工作让Faltings获得了1986年的 菲尔兹奖（数学界的最高奖之一）

高次曲线上的有理点

- n次平面曲线（二元n次方程）$n \geq 4$相应的曲面$X(\mathbb{C})$亏格≥ 2

Theorem (Faltings)

亏格≥ 2的曲线的有理点集$X(\mathbb{Q})$是有限集。

- 这项工作让Faltings获得了1986年的 菲尔兹奖（数学界的最高奖之一）

几何决定算术?

代数	几何			算术
方程	曲线分类名	$X(\mathbb{C})$曲面亏格	曲率	有理点个数
二元2次方程	圆锥曲线	0	正	无穷个
二元3次方程	椭圆曲线	1	平均0	无穷/有限
二元高次方程	一般型曲线	≥ 2	负	有限个

- 几何决定算术?

  有意思的地方在于:

  横跨了几何与数论这两大数学研究领域

几何决定算术?

代数	几何			算术
方程	曲线分类名	$X(\mathbb{C})$曲面亏格	曲率	有理点个数
二元2次方程	圆锥曲线	0	正	无穷个
二元3次方程	椭圆曲线	1	平均0	无穷/有限
二元高次方程	一般型曲线	≥ 2	负	有限个

- 几何决定算术?

  有意思的地方在于:
  横跨了几何与数论这两大数学研究领域

几何决定算术?

代数	几何			算术
方程	曲线分类名	$X(\mathbb{C})$曲面亏格	曲率	有理点个数
二元2次方程	圆锥曲线	0	正	无穷个
二元3次方程	椭圆曲线	1	平均0	无穷/有限
二元高次方程	一般型曲线	≥ 2	负	有限个

- 几何决定算术?

  有意思的地方在于:
  横跨了几何与数论这两大数学研究领域

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：
- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：

- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：
- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：

- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：

- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用? 分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：

数学，为了人类心智的荣耀！

- 谢谢聆听！

最后聊聊：数学有什么用?

- 解方程有什么用？分类几何体有什么用?
- 建议：不要问纯数学（基础数学）有什么用！
- 类比：破100米短跑的世界纪录有什么用?
- 如果非要有一个答案，两百多年前数学家Carl Jacobi已经回答过了：

数学，为了人类心智的荣耀！

- 谢谢聆听！

现代数学、大学数学概貌

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

- 近现代纯数学（基础数学、非应用数学）研究什么?
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

现代数学、大学数学概貌

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

现代数学、大学数学概貌

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

现代数学、大学数学概貌

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

现代数学、大学数学概貌

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）

- 近现代纯数学（基础数学、非应用数学）研究什么？
  - 按研究方法分
    - 分析（大学课程：数学分析或微积分、实变函数、复变函数、泛函分析）
    - 代数（大学课程：线性代数、抽象代数、交换代数、同调代数）
  - 按研究对象分
    - 几何（研究形）、数论（研究数）、数学物理（研究自然界的对象）、概率和统计（研究数量庞大时的整体规律）等
    - 几何：拓扑学、微分几何（用求导来研究几何）、代数几何（用代数来研究几何）
    - 数论：解析数论（用分析方法研究数论）、代数数论（用代数方法研究数论）
    - 数学物理：微分方程
- 今天的主题已经涉及了两大重要领域：数论（数）、几何（形）