初等数论专题一

北京理工大学 吕珍涛

2024年1月29日

第一节：整除理论

数论是什么

数论: 数学的女王

- 数论，也称为高等算术，是研究整数及其它相关对象的性质的一个数学分支。

- 著名的德国数学家高斯：数学是科学的女王，数论是数学的女王。

数论研究什么

- 素数的判定
- 素数分布
- 同余
- 不定方程
- 其它相关的代数结构

研究方法

- 初等数论
- 解析数论：孪生素数猜想（张益唐）
- 代数数论：费马大定理
- 其它数学分支、物理

“He went to the deepest of the deep and he fully understood. And his paper estab-

数的整除

整除

- 自然数与整数
- 加、减、乘
- 除：整除
- 整数a, b, c, 如果$a = bc$, 则称 b整除 a，记作 $b|a$。
- 约数和倍数

最大公约数

- $a_1, ..., a_n$是n个整数。
- 公约数：能同时整除$a_1, ..., a_n$的整数。
- 最大公约数：$\gcd(a_1, ..., a_n)$，或者$(a_1, ..., a_n)$。
- 互素：$(a_1, ..., a_n) = 1$。
- 两两互素。

辗转相除法

- 带余除法：设a, b为整数，$b > 0$，则存在整数q和r，使得$a = bq + r$，其中$0 \leq r < b$。
- 辗转相除法（欧几里得算法）求最大公约数。
- a, b为整数，$b > 0$，反复作带余除法，能够得其最大公约数。同时，也能证明方程$ax + by = (a, b)$有整数解。
- 裴蜀（Bezout）等式
- a, b互素的充分必要条件是：存在整数x, y，使得

$$ax + by = 1.$$

辗转相除法

a, b互素的充分必要条件是：存在整数x, y，使得

$$ax + by = 1.$$

证明：（1）a, b互素$\Rightarrow (a, b) = 1$，由辗转相除法可以得到一组整数x, y，使得$ax + by = 1$.

（2）反之，若存在整数x, y，使得$ax + by = 1$，由$(a, b)|a$，$(a, b)|b$ 知 $(a, b)|1$. 故$(a, b) = 1$.

最大公约数的性质

- 欧几里得算法与裴蜀等式$ax + by = (a, b)$。
- a, b的任何公约数都是(a, b)的约数。
- 如果m是正整数，那么$m(a, b) = (ma, mb)$。
- $(a_1, a_2, ..., a_n) = ((a_1, a_2), ..., a_n)$。
- 如果$b|ac$，且$(b, c) = 1$，那么$b|a$。

最小公倍数

- 非零整数$a_1, \ldots, a_n$的最小公倍数记作 $\mathrm{lcm}(a_1, \ldots, a_n)$，或者$[a_1, a_2, \ldots, a_n]$。
- 设m为整数，$a|m, b|m$，则$[a, b]|m$。
- 设m为正整数，则有$m[a, b] = [ma, mb]$。
- $(a, b)[a, b] = |ab|$。
- 如果$(b_1, b_2) = 1$，并且$b_1|a$，$b_2|a$，那么$b_1 b_2|a$。

素数

素数的定义和性质

- 大于1的正整数p称为素数（质数），如果它只有1和p两个因数。
- 正整数分三类：1，素数，合数。
- p是素数，a, b是整数，$p|ab$，则$p|a$或$p|b$（欧几里得）。
- 素数有无穷多个。
  - 证明：反证法。假设只有有限个素数$p_1, ..., p_n$。考虑

$$p_1 \cdot p_2 \cdots p_n + 1 \text{ 。}$$

算术基本定理

- 正整数的唯一分解定理：每个大于1的正整数都可以分解为有限个素数的乘积。如果不计素因子的次序，那么这种分解是唯一的。
- 也叫做算术基本定理。
- “基本定理”家族：代数基本定理，微积分基本定理，...

Fundamental theorems of mathematical topics [edit]

- Fundamental theorem of algebra
- Fundamental theorem of algebraic K-theory
- Fundamental theorem of arithmetic
- Fundamental theorem of Boolean algebra
- Fundamental theorem of calculus
- Fundamental theorem of curves
- Fundamental theorem of cyclic groups
- Fundamental theorem of equivalence relations
- Fundamental theorem of exterior calculus
- Fundamental theorem of finitely generated abelian groups
- Fundamental theorem of finitely generated modules over a principal ideal domain
- Fundamental theorem of finite distributive lattices
- Fundamental theorem of Galois theory
- Fundamental theorem of geometric calculus
- Fundamental theorem on homomorphisms
- Fundamental theorem of ideal theory in number fields
- Fundamental theorem of Lebesgue integral calculus
- Fundamental theorem of linear programming
- Fundamental theorem of noncommutative algebra
- Fundamental theorem of projective geometry
- Fundamental theorem of Riemannian geometry
- Fundamental theorem of tessarine algebra
- Fundamental theorem of symmetric polynomials

标准分解

- 大于1的正整数n的标准分解:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \alpha_1, ..., \alpha_k \text{是正整数。}$$

- d是n的约数，则d的可以表示为

$$d = p_1^{\beta_1} \cdots p_k^{\beta_k}, 0 \leq \beta_i \leq \alpha_i, i = 1, ..., k.$$

- n的约数的个数：

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

约数的和与完全数

- n的约数的和：

$$\begin{aligned}\sigma(n) &= (1+p_1+p_1^2\cdots+p_1^{\alpha_1})\cdots(1+p_k+\cdots+p_k^{\alpha_k}) \\ &= \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}\end{aligned}$$

- 完全数：一个正整数的除自身以外的所有因数的和等于自己。
- 比如6，28，496，8128
- n是完全数，$\sigma(n)=?$
- $\sigma(220)=?$ $\sigma(284)=?$

偶完全数的刻画

- 欧拉：偶数n是完全数当且仅当 $n = 2^{k-1}(2^k - 1)$，且 $2^k - 1$ 是素数。
- 证明：设$n = 2^{k-1}m$，其中$k \geq 2$，$2 \nmid m$。一方面，由$n = 2^{k-1}m$ 得$2n = 2^k m$。另一方面，$\sigma(n) = (2^k - 1)\sigma(m)$。由于$n$是完全数，$\sigma(n) = 2n$。所以$(2^k - 1)\sigma(m) = 2^k m$。所以，$\sigma(m) = m + \frac{m}{2^k-1}$。由于$m$ 和 $\frac{m}{2^k-1}$ 都是 m的约数，且不相等，并且根据定义$\sigma(m)$ 是m 所有约数的和，所以 m只有这两个约数，所以 $\frac{m}{2^k-1} = 1$，且 $m = 2^k - 1$为素数。

总结：最重要的性质

- 欧几里得算法
- 裴蜀等式
- 唯一分解定理
- p是素数，a, b是整数，$p|ab$，则$p|a$或$p|b$。

思考题

- 求证：有无穷多个形如$4k-1$的素数
- 提示：反证法，假设只有有限个这样的素数，排列成$4k_1-1,\ldots,4k_m-1$，考虑$4(4k_1-1)\cdots(4k_m-1)-1$。

第二节：同余

同余的定义和基本性质

同余的概念

- 设m是正整数，a, b是两个整数。如果 $m|(a-b)$，我们称 a 和 b **模** m **同余**，记作

$$a \equiv b \pmod{m}.$$

- “星期运算”：$3+5 \equiv 1 \pmod{7}$.
- 同余有反身性、对称性和传递性：

$$a \equiv a \pmod{m},$$
$$a \equiv b \pmod{m}, \text{则 } b \equiv a \pmod{m},$$
$$a \equiv b \pmod{m}, \text{且 } b \equiv c \pmod{m}, \text{则 } a \equiv c \pmod{m}.$$

模算术

- 加、减、乘法运算跟整数类似，满足

$$a \equiv b \pmod{m}，且\ c \equiv d \pmod{m}，则$$
$$a \pm c \equiv b \pm d \pmod{m},$$
$$ac \equiv bd \pmod{m}$$

- “消除”：

$$ac \equiv bc \pmod{m}，则\ a \equiv b \pmod{\frac{m}{(c,m)}}.$$

- 特别地，当$(c,m)=1$时：

$$ac \equiv bc \pmod{m}，则\ a \equiv b \pmod{m}.$$

应用：整除的判定

- $\overline{abc}$ 能被9整除 $\Leftrightarrow$ $a+b+c$能被9整除。
- $\overline{abcd}$ 能被11整除 $\Leftrightarrow$ $a+c \equiv b+d \pmod{11}$。
  证明：

$$\begin{aligned} & \overline{abcd} \\ = \; & 1000a+100b+10c+d \\ = \; & 1001a-a+99b+b+11c-c+d \\ \equiv \; & -a+b-c+d \pmod{11} \end{aligned}$$

  所以，$\overline{abcd} \equiv 0 \pmod{11} \Leftrightarrow -a+b-c+d \equiv 0 \pmod{11}$
  $\Leftrightarrow a+c \equiv b+d \pmod{11}$。
- 练习：完全平方数模3余0或1，模4余0或1，模5余0，1，或4，模8余0，1，或4。完全立方数模9余0或± 1。

同余类与同余系

- 模m的同余类：把整数按照模m的同余分为m类，M_k表示所有模m余k的整数的集合，$k = 0, 1, ..., m-1$。
- 模3的同余类：$\bar{0}, \bar{1}, \bar{2}$。
- 完全剩余系：从模m的每个同余类取一个代表，这样的m个数称为模m的一个**完全剩余系**(完系)。
- 模m的最小非负完系：$0, 1, ..., m-1$。

缩同余类与欧拉函数

- 模m的缩同余类：只取与m互素的同余类。
- $\varphi(m)=$ 模m的缩同余类的个数 $=0$到$m-1$中与m互素的整数的个数，称为**欧拉函数**。
- 如果m是素数，那么$\varphi(m)=m-1$。
- 模m的缩系：从模m的缩同余类中各取一个代表，构成一个模m的缩系 $r_1,\ldots,r_{\varphi(m)}$.
- 缩系的性质：如果$r_1,\ldots,r_{\varphi(m)}$是模$m$的缩系，且$(a,m)=1$，那么$ar_1,\ldots,ar_{\varphi(m)}$也是模$m$的缩系。

几个著名的定理

几个著名的定理

- 欧拉定理：设$(a,m)=1$，则$a^{\varphi(m)}\equiv 1 \pmod{m}$.
- 费马小定理：设p是素数，且$p \nmid a$，则$a^{p-1}\equiv 1 \pmod{p}$.
- 威尔逊定理：设p是素数，则有$(p-1)!\equiv -1 \pmod{p}$.

欧拉定理的证明

我们取模m的一个缩系$r_1, \ldots, r_{\varphi(m)}$。由于$(a, m) = 1$，那么$ar_1, \ldots, ar_{\varphi(m)}$也是模$m$的缩系。也就是说，他们各自都代表了模$m$的缩同余类（比如$ar_1$ 可能代表的是同余类 r_2，但他们分别遍历模m的缩同余类）。所以

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv ar_1 ar_2 \cdots ar_{\varphi(m)} \pmod{m}.$$

消掉$r_1, \ldots, r_{\varphi(m)}$, 得

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

练习

练习

- 设p是素数，证明有无穷多个正整数n，使得$p|2^n - n$。
- 证明对于任意给定的正整数m，总存在无穷多个正整数n，使得 $2^n + 3^n - 1, 2^n + 3^n - 2, ..., 2^n + 3^n - m$ 都是合数。

解析： 首先$p=2$的情况是显然的。下面只考虑$p>2$的情况。要证明存在无穷多个这样的正整数n，我们可以先做这样一件事情，也就是证明下面的引理：

引理A：如果已知存在一个正整数n，使得$p|2^n-n$，那么可以构造出无穷多个新的正整数n'，使得$p|2^{n'}-n'$。如果引理A成立，那么我们只需要证明找到一个正整数n就可以了。

引理A的证明：现在已知有一个n使得$2^n \equiv n \pmod{p}$，由费马小定理，$2^{p-1} \equiv 1 \pmod{p}$，所以可以尝试在改变$n$的同时，使得同余等式$2^n \equiv n \pmod{p}$的左右两边保持不变。这可以通过在左边指数上增加$(p-1)$的倍数，右边在$n$的基础上加$p$的倍数来实现。要保持$2^{n'} \equiv n' \pmod{p}$的形式，我们取$n'=n+kp(p-1)$，这样有 $2^{n+kp(p-1)} \equiv 2^n \equiv n \equiv n+kp(p-1)$。这样我们就证明了：若$p|2^n-n$，则对于$n'=n+kp(p-1)$，$k$任意正整数，有$p|2^{n'}-n'$。

现在我们来构造一个n。注意到$2^{p-1} \equiv 1 \pmod{p}$，而且指数调整为$t(p-1)$，都满足$2^{t(p-1)} \equiv 1 \pmod{p}$。令

$$t(p-1) \equiv 1 \pmod{p}, \tag{B}$$

解这个同余方程(B)，我们可以发现$t = p-1$时，$n = (p-1)^2$满足 $p|2^n - n$。再由引理A，我们可以得到$n = (p-1)^2 + kp(p-1)$, $k = 1, 2, 3, \ldots$ 是无穷多个满足条件的正整数n。当然，从同余方程(B)我们也可以直接得到 $t \equiv -1$，也就是可以取$t = kp - 1, n = (kp-1)(p-1), k = 1, 2, 3, \ldots$ 来得到无穷多个满足条件的正整数n。我用的参考书没有解释解题思路，直接取的是特例$n = (p-1)^{2k}$，对应的是我们的同余方程(B) 取$t = (p-1)^{k-1}$。

题目：证明对于任意给定的正整数m，总存在无穷多个正整数n，使得$2^n+3^n-1, 2^n+3^n-2, ..., 2^n+3^n-m$都是合数。

解析：思路，题目要求找到无穷多个正整数n，我们也可以考虑分两步，

1. 找到一个正整数n满足条件，
2. 证明如果已知存在一个正整数n满足条件，那么可以找到无穷多个正整数n满足条件。

然后就像上一道题一样，我们可以分别尝试解决1，2，而不必按顺序解决1，2。

现在考虑问题2：如果已知存在一个正整数n，使得$2^n+3^n-1, 2^n+3^n-2, ..., 2^n+3^n-m$都是合数，那么我们来尝试构造一个更大的正整数$n'$。

考虑2^n+3^n-k，它是合数，那么存在$p_k|2^n+3^n-k$。由费马小定理，如果p_k不等于2也不等于3，那么 $2^{s(p_k-1)}\equiv 1 \pmod{p_k}$，$3^{s(p_k-1)}\equiv 1 \pmod{p_k}$，所以$p_k|2^{n+s(p_k-1)}+3^{n+s(p_k-1)}-k$。如果$p_k$等于2或3，容易验证$p_k|2^{n+s(p_k-1)}+3^{n+s(p_k-1)}-k$依然成立。进一步，我们取$n'=n+s(p_1-1)(p_2-1)...(p_m-1)$，那么$p_k|2^{n'}+3^{n'}-k$ 对所有的$k=1,2,...,m$都成立。

这样，我们实际上证明了，(A) 如果已知存在一个正整数n使得$p_k|2^n+3^n-k$ 对所有的$k=1,2,...,m$ 都成立，那么可以找到无穷多个正整数n满足这个条件。
这样，其实我们得到的结论不仅仅证明了2，还为整道题目打开了思路。我们只要取n_0使得 $2^{n_0}+3^{n_0}-m$ 大于1，那么每一个$2^{n_0}+3^{n_0}-k$ 都有至少一个素因子 p_k，应用结论(A)，当 $s=1,2,3,...$ 时，我们得到无穷多个 $n'=n_0+s(p_1-1)(p_2-1)...(p_m-1)$，使得 $p_k|2^{n'}+3^{n'}-k$ 对所有的$k=1,2,...,m$ 都成立，而且 $n'>n_0$ 保证了 p_k 不是 $2^{n'}+3^{n'}-k$ 唯一的素因子，从而保证了 $2^{n'}+3^{n'}-k$ 为合数。

总结与思考

总结与思考

- 欧几里得算法
- 裴蜀等式
- 唯一分解定理
- p是素数，a, b是整数，$p|ab$，则$p|a$或$p|b$。
- 同余，模算术
- 同余类、同余系、欧拉函数
- 欧拉定理与费马小定理
- 问题与建议： zhentaolyu@bit.edu.cn
- 谢谢大家！

初等数论专题二

北京理工大学 吕珍涛

2024年1月29日

1. 第三节：同余方程
   - 一次同余方程
   - 中国剩余定理
   - 拉格朗日定理
2. 第四节：不定方程
   - 基本方法
   - 类型举例
   - 方法举例

第三节：同余方程

一次同余方程

一次同余方程

- 考虑方程$ax + b \equiv c \pmod{m}$.
- $ax \equiv c - b \pmod{m}$.
- 如果$(a, m) = 1$，那么总是存在z，使得$az \equiv 1 \pmod{m}$。我们称z为a的逆，记作a^{-1}或$\frac{1}{a}$。
- $ax \equiv c - b \pmod{m}$且$(a, m) = 1.$，则$x \equiv a^{-1}(c - b) \pmod{m}$。

练习

- 求 $\frac{1}{4} \pmod 7$。
- 求 $\frac{1}{4} \pmod{17}$。

中国剩余定理

同余方程组

中国剩余定理可以用来解如下一次同余方程组：

$$\begin{cases} k_1x + b_1 \equiv a_1 \pmod{m_1} \\ k_2x + b_2 \equiv a_2 \pmod{m_2} \\ \vdots \\ k_3x + b_3 \equiv a_n \pmod{m_n} \end{cases}$$

中国剩余定理

中国剩余定理，也称孙子定理：
当$m_1, m_2, \ldots, m_n$两两互素时，同余方程组

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

有解，并且解在模$m_1 m_2 \cdots m_n$的意义下是唯一的。

事实上，中国剩余定理能够给出上述方程组解的具体形式：
令$M = m_1 m_2 \cdots m_n$，$M_i = M/m_i$，再令M_i^{-1}为M_i模m_i的逆（即满足$M_i M_i^{-1} \equiv 1 \pmod{m_i}$），则上述方程组模$M$有唯一解 $x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_n M_n M_n^{-1} \pmod{M}$。

例题：孙子点兵

- 《孙子算经》中有一个“物不知数”的问题：“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？”
- 解这道题相当于求解方程组

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

现在 $m_1 = 3, m_2 = 5, m_3 = 7$。计算知
$M = 105, M_1 = 35, M_2 = 21, M_3 = 15,$
$M_1^{-1} \equiv 2 \pmod 3, M_2^{-1} \equiv 1 \pmod 5, M_3^{-1} \equiv 1 \pmod 7$。所以 $x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \equiv 233 \equiv 23 \pmod{105}$。

拉格朗日定理

拉格朗日定理

- 设$f(x)$为整系数多项式。拉格朗日定理：对任意素数p，若$f(x)$模p后的系数不全为零，则$f(x) \equiv 0 \pmod{p}$至多有n个（模p意义下的）不同的解，这里n是$f(x)$模p之后的次数。
- 推论：若$f(x)$为n次整系数多项式，且$f(x) \equiv 0 \pmod{p}$有至少$n+1$个（模p意义下的）不同的解，则$f(x)$的每项系数都是p的倍数。

威尔逊定理的证明

- 当素数$p \geq 3$时，由费马小定理知$x = 1, 2, \ldots, p-1$都是同余方程 $x^{p-1} \equiv 1 \pmod{p}$ 的解。进而它们都是 $x^{p-1} - 1 - (x-1)(x-2)\ldots(x-p+1) \equiv 0 \pmod{p}$ 的解。但是这是一个至多 $p-2$ 次的多项式，所以由拉格朗日定理推出该多项式模 p 恒为零。特别地，将 $x = 0$ 代入，便证得威尔逊定理：$(p-1)! \equiv -1 \pmod{p}$。

第四节：不定方程

基本方法

不定方程

- 不定方程就是未知数个数大于1的方程。

- 系数为整数的不定方程，又称为丢番图方程（Diophantine equation）。这里我们讨论的不定方程都是整系数的，也就是丢番图方程。
- 我们关心的问题：不定方程是否有整数解，是否有正整数解。

整数解与正整数解

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4$$

整数解：$a=11,b=9,c=-5$.

正整数解：

$$\begin{aligned}a=&\,437361267792869725786125260237139015281653755816161361862143799337842346772036,\\ b=&\,368751317941299998271978115652254748254929799689719709962831374716372246340555 79,\\ c=&\,154476802108746166441951315019919837485664325669565431700026634898253202035277999.\end{aligned}$$

a,b,c分别有79,80,81位.

基本方法(I)

- 求$x+5y=10$的整数解。

  $x=10-5y$

  $(x,y)=(10-5t,t)$，t为整数。
- 求$3x+5y=1$的整数解。

  $y=\frac{1-3x}{5}$，所以 $1-3x\equiv 0 \pmod 5$。

  所以 $x\equiv 2 \pmod 5$，因此 $(x,y)=(2+5t,-1-3t)$。

基本方法(II)

求不定方程 $x^2+xy-3x-6=0$ 的整数解。

因式分解知该方程等价于 $x(x+y-3)=5$。

为求其整数解，只需分别求解

$$\begin{cases} x=1 \\ x+y-3=5 \end{cases}, \begin{cases} x=-1 \\ x+y-3=-5 \end{cases},$$

$$\begin{cases} x=5 \\ x+y-3=1 \end{cases}, \begin{cases} x=-5 \\ x+y-3=-1 \end{cases}。$$

类型举例

一次不定方程

形如 $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ 的方程称为 n 元一次不定方程，这里的系数$a_1, \ldots, a_n$，常数项 c，以及未知元 $x_1, \ldots, x_n$ 都是整数。

不定方程 $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ 有解的充要条件是 $(a_1, \ldots, a_n)|c$。当n等于2时，这就是的裴蜀定理。

如果不定方程 $ax + by = c$ 有一组解是 (x_0, y_0)，那么它的所有的解都有如下形式：$x = x_0 + \frac{b}{(a,b)}t, y = y_0 - \frac{a}{(a,b)}t$，其中 t为整数。

勾股方程

勾股方程的形式是 $x^2+y^2=z^2$。勾股方程的正整数解称为勾股数组。满足 $(x,y,z)=1$的勾股数组都可以表示为 $x=a^2-b^2, y=2ab, z=a^2+b^2$ 的形式，而当 $(x,y,z)>1$时，方程两边同时除以 $d=(x,y,z)$ 即可转化为上述情形。

勾股方程最自然的推广是 $x^n+y^n=z^n$。当 $n>2$ 时，该方程没有非平凡的整数解。这就是著名的费马大定理。费马大定理虽然名为定理，但是费马并没有给出证明。历代数学家寻找费马大定理的过程极大地促进了数论和代数学的发展。

沛尔方程

设 d不是完全平方数，形如 $x^2 - dy^2 = \pm 1$ 的方程称为沛尔（Pell）方程。其中 $x^2 - dy^2 = 1$ 总是有无穷多组解，$x^2 - dy^2 = -1$或者无解，或者有无穷多组解。沛尔方程的解与 $\sqrt{d}$的连分数表达式有密切关系。

方法举例

同余方法

如果一个方程$f(x,y)=0$有整数解(x_0,y_0)，那么，任取正整数 m，对应的同余方程 $f(x,y)\equiv 0 \pmod m$也必然有解 $(x_0,y_0) \pmod m$。所以对方程两边取模m的同余可以给出方程解满足的必要条件。另一方面，如果选取适当的m，证明 $f(x,y)\equiv 0 \pmod m$无解，即可证明不定方程 $f(x,y)=0$没有整数解。

不等式方法

恰当运用不等式估计，可以缩小解的搜寻范围，甚至将题目简化成对有限种可能性的枚举验证。除了对所有实数都成立的一般性的不等式之外，整数中有一些特有的不等式关系，比如：

- $a|b$，则$|a| \leq |b|$。
- 整数$a > b$，则$a \geq b+1$。或者说，当a为整数时，$a < x < a+1$没有整数解。
- 给定常数N，小于N的正整数只有有限多个。

无穷递降法

证明：方程$x^2 = 2y^2$没有正整数解。

反证法。假设该方程有正整数解，并且最小的一个解是$x = p,\ y = q$。我们要证明必然存在更小的解，从而导出矛盾。现在我们有$p^2 = 2q^2$。显然$2|p$，因此可以设$p = 2u$。于是，$(2u)^2 = 2q^2 \Rightarrow q^2 = 2u^2$。所以$x = q, y = u$也是原方程的一个解。但是易见$q < p, u < q$，这与$x = p,\ y = q$是最小的解矛盾。从而假设不成立，原方程无解。

本题证明中用到的反证法有一个特别的名称，叫做**无穷递降法**：假设有正整数解，取最小的正整数解，在其基础上构造出更小的解。费马用该方法证明了$x^4 + y^4 = z^4$没有正整数解。另外，本题实际上证明了不存在有理数$\frac{p}{q}$满足$\left(\frac{p}{q}\right)^2 = 2$，或者说，$\sqrt{2}$不是有理数。