

二元一次不定方程的变量替换求解方法及其计算复杂度分析

陈 功

(上海交通大学 电子信息与电气工程学院,上海 200240)

摘要:对运用变量替换法求解二元一次不定方程的过程作一般化处理,得到其通解公式和特解计算公式,并证明了所得结果与运用辗转相除法所得的经典结论相一致;进一步通过计算复杂度的估计,得出两种解法计算量相当的结论。

关键词:二元一次不定方程;变量替换;辗转相除;通解;计算复杂性;位运算

中图分类号:O122.2 **文献标识码:**A **文章编号:**1671-5322(2017)04-0068-04

关于二元一次不定方程 $ax + by = c(a, b, c$ 是整数)的求解,有如下主要结论^[1-3]:

- (1)方程 $ax + by = c(a, b, c$ 是整数)有解的充分必要条件是 $(a, b) | c$;
- (2)当 $d = (a, b) | c$, 记 $a = a_1d, b = b_1d, c = c_1d$, 则方程 $a_1x + b_1y = c_1$ 与 $ax + by = c$ 同解;
- (3)方程 $ax + by = c$ 与 $(\pm a) \times (\pm x) + (\pm b) \times (\pm y) = c, by + ax = c$ 等价。

综上,二元一次不定方程的求解问题可简化为下列情形:

$$ax + by = c \tag{1}$$

其中 a, b, c 是整数,且 $a > b > 0, (a, b) = 1$ 。本文的讨论均在此情形下展开。

对 b 除 a 实施辗转相除,有 $a = bq_1 + r_1, b = r_1q_2 + r_2, r_1 = r_2q_3 + r_3, \cdots, r_{n-2} = r_{n-1}q_n + r_n$, 由于 $(a, b) = 1$, 必存在某个正整数 n , 有 $r_n = (a, b) = 1$ 和 $r_{n+1} = 1$ 。这时,方程有通解公式

$$x = x_0 - bt, y = y_0 + at, t \in \mathbb{Z} \tag{2}$$

其中特解

$$x_0 = (-1)^{n-1}cQ_n, y_0 = (-1)^ncP_n \tag{3}$$

这里的 P_n 和 Q_n 由递推公式

$$\begin{aligned} P_0 &= 1, P_1 = q_1, P_k = q_kP_{k-1} + P_{k-2}; \\ Q_0 &= 0, Q_1 = 1, Q_k = q_kQ_{k-1} + Q_{k-2} \end{aligned} \tag{4}$$

确定。上述方法又称为扩展的 Euclid 算法^{[4]108, [5]}。

下面的定理 1 源自文献[6]第 29 页的定理 3,该定理为求解方程(1)的另一种方法,即本文所称的“变量替换法”提供了基本原理。

定理 1 设有二元一次不定方程 $ax + by = c$ (a, b, c 是整数,且 $a > b > 0, (a, b) = 1$), $a = bq + r, c = bq' + r', 0 \leq r, r' < b, q, q_1, r, r'$ 为整数。当 X, Y 取方程 $bY + rX = r'$ 的一切整数解,则方程 $ax + by = c$ 的一切整数解均可由 $x = X, y = q' - qX + Y$ 得出。

1 变量替换法

以定理 1 为原理,本节给出变量替换方法的基本步骤和一般形式。

变形方程(1),即 $ax + by = c$, 得 $y = \frac{c - ax}{b} = q'_1 - q_1x + \frac{r'_1 - r_1x}{b}$, 其中 $a = bq_1 + r_1, c = bq'_1 + r'_1$ ($0 \leq r_1, r'_1 < b$), 记 $x = Y_0, Y_1 = \frac{r'_1 - r_1x}{b} = \frac{r'_1 - r_1Y_0}{b}$, 则有 $y = q'_1 - q_1Y_0 + Y_1, bY_1 + r_1Y_0 = r'_1$ 和 $Y_0 = \frac{r'_1 - bY_1}{r_1}$; 再由 $b = r_1q_2 + r_2, r'_1 = r_1q'_2 + r'_2$ ($0 \leq r_2, r'_2 < r_1$) 得 $Y_0 = q'_2 - q_2Y_1 + \frac{r'_2 - r_2Y_1}{r_1}$, 其中 $Y_2 = \frac{r'_2 - r_2Y_1}{r_1}$ 。

依此类推,得到递推关系

$$\begin{cases} Y_{k-2} = q'_k - q_k Y_{k-1} + Y_k, \\ r_{k-1} Y_k + r_k Y_{k-1} = r'_k \\ Y_k = \frac{r'_k - r_k Y_{k-1}}{r_{k-1}} \end{cases} \quad (5)$$

以及回代公式

$$Y_{k-1} = \frac{r'_k - r_k Y_k}{r_k}, \quad (6)$$

其中 $r_{k-2} = r_{k-1} q_k + r_k, r'_{k-1} = r_{k-1} q'_k + r'_k (0 \leq r_k, r'_k < r_{k-1}), r_0 = b, k = 2, 3, \dots, n_0$

如此下去,因为 $r_n = (a, b) = 1$, 得到

$$Y_{n-1} = \frac{r'_n - r_{n-1} Y_n}{r_n} = r'_n - r_{n-1} Y_n \quad (7)$$

若令 $Y_n = s$, 则 $Y_{n-1} = r'_n - r_{n-1} s (s \in \mathbb{Z})$, 将二者代入 $Y_{n-2} = q'_n - q_n Y_{n-1} + Y_n$ 并整理, 即可求出含参数 s 的 Y_{n-2} ; 依此向前回代, 最终可求出 $x = Y_0 = q'_2 - q_2 Y_1 + Y_2$ 和 $y = q'_1 - q_1 Y_0 + Y_1$ 。由定理 1 可知, 所得解必为原方程的解。

文献[6]还通过一个例题展现了变量替换法的操作程序, 本文将运用该方法以一般形式推导方程(1)的求解公式, 并证明所得结果与(2)~(4)式完全一致。

2 两个引理

首先对 $k = n, n-1, \dots, 1, 0, -1$, 约定记号 T_k :

$$T_n = 0, T_{n-1} = 1, T_k = q_{k+2} T_{k+1} + T_{k+2} \quad (8)$$

引理 1 对任意整数 $k, -1 \leq k \leq n-1$, T_{k+1} 与 T_k 之间有如下关系:

$$\text{I. } 1 + (-1)^{n-k-1} r_k T_{k+1} = (-1)^{n-k-1} r_{k+1} T_k;$$

$$\text{II. } 0 \leq T_{k+1} < T_k$$

证明: 这里对 k 由大到小进行归纳。

I. 当 $k = n-1$, 由 $T_n = 0, T_{n-1} = 1$ 和 $r_n = 1$, 即证命题;

当 $k = n-2$, 由 $T_{n-1} = 1, T_{n-2} = q_n$ 和 $r_n = 1$, 即得 $1 - r_{n-2} T_{n-1} = r_n - r_{n-2} = -r_{n-1} q_n = -r_{n-1} \times T_{n-2}$ 。

假设对不小于 k 的下标, 均有 $1 + (-1)^{n-k-1} \times r_k T_{k+1} = (-1)^{n-k-1} r_{k+1} T_k$, 则对于 $k-1$,

$$1 + (-1)^{n-k} r_{k-1} T_k =$$

$$1 + (-1)^{n-k} (r_k q_{k+1} + r_{k+1}) T_k = (-1)^{n-k} r_k q_{k+1} T_k + 1 + (-1)^{n-k} r_{k+1} (q_{k+2} T_{k+1} + T_{k+2}) = (-1)^{n-k} (r_k q_{k+1} T_k + r_{k+1} q_{k+2} T_{k+1}) + 1 +$$

$$(-1)^{n-k-2} r_{k+1} T_{k+2}$$

由归纳假设, 对 $k+1$ 有

$$1 + (-1)^{n-k-2} r_{k+1} T_{k+2} = (-1)^{n-k-2} r_{k+2} \times T_{k+1}, \text{ 所以}$$

$$\begin{aligned} 1 + (-1)^{n-k} r_{k-1} T_k &= (-1)^{n-k} (r_k q_{k+1} T_k + r_{k+1} q_{k+2} T_{k+1}) + (-1)^{n-k-2} r_{k+2} T_{k+1} = (-1)^{n-k} [r_k q_{k+1} T_k + (r_{k+1} q_{k+2} + r_{k+2}) T_{k+1}] = (-1)^{n-k} [r_k q_{k+1} T_k + r_k T_{k+1}] = (-1)^{n-k} r_k (q_{k+1} T_k + T_{k+1}) = (-1)^{n-k} r_k T_{k-1} \end{aligned}$$

关系 I 得证。

II. 当 $k = n-1$, 由 $0 = T_n < T_{n-1} = 1$ 。

假设对某个 k , 有 $0 \leq T_{k+1} < T_k$, 则 $T_{k-1} = q_{k+1} \times T_k + T_{k+1} > (q_{k+1} + 1) T_k$, 而 q_{k+1} 是非负整数, $q_{k+1} + 1 \geq 1$, 故必有 $T_{k-1} > T_k$, 关系 II 得证。

引理 2 记 $a = r_{-1}, b = r_0, c = r'_0$ 。设 $r_{k-2} = r_{k-1} q_k + r_k, r'_{k-1} = r_{k-1} q'_k + r'_k$, 其中 $0 \leq r_k, r'_k < r_{k-1}, k = 1, 2, \dots, n_0$ 。若 $r_n = 1$, 则有 $Y_k = (-1)^{n-k-1} (r'_k T_k - r_k Z_k)$, 其中 $Z_n = Y_n = s, s \in \mathbb{Z}, Z_k = q'_{k+1} T_k + Z_{k+1}, k = 0, 1, 2, \dots, n-1$ 。

证明: 与引理 1 的证明相仿, 由大到小对 k 运用归纳法。

当 $k = n-1$, 将 $r'_n = r'_{n-1} - r_{n-1} q'_n$ 和 $T_{n-1} = 1$ 代入(7)式, 并由 $(-1)^{n-(n-1)-1} = 1$ 和 $q'_n + s = q'_n T_{n-1} + Z_n = Z_{n-1}$, 即得

$$Y_{n-1} = (-1)^{n-(n-1)-1} \times (r'_{n-1} T_{n-1} - r_{n-1} \times Z_{n-1})。$$

对一般的 k , 假设有 $Y_k = (-1)^{n-k-1} (r'_k T_k - r_k Z_k)$, 则对于 $k-1$, 将该式代入回代公式(6), 整理后有

$$Y_{k-1} = r'_k \frac{1 + (-1)^{n-k} r_{k-1} T_k}{r_k} + r_{k-1} (-1)^{n-k-1} Z_k$$

由引理 1, $1 + (-1)^{n-k} r_{k-1} T_k = (-1)^{n-k} \times r_k T_{k-1}$, 而 $r'_k = r'_{k-1} - r_{k-1} q'_k$, 故

$$Y_{k-1} = (-1)^{n-k} [r'_{k-1} T_{k-1} - r_{k-1} (q'_k T_{k-1} + Z_k)] = (-1)^{n-k} (r'_{k-1} T_{k-1} - r_{k-1} Z_{k-1})$$

其中 $Z_{k-1} = q'_{k+1} T_{k-1} + Z_k$ 。引理 2 得证。

3 主要结论

定理 2 $x_0 = (-1)^{n-1} T_0 c, y_0 = (-1)^n T_{-1} c$ 是原方程(1)的一个特解。

证明: 在引理 1 中, 取 $k = -1$, 得 $1 +$

$(-1)^n a T_0 = (-1)^n b T_{-1}$, 两边同乘以 c 并移项, 得 $a(-1)^{n-1} T_0 c + b(-1)^n T_{-1} c = c$, 即 $ax_0 + by_0 = c$, 于是 $x_0 = (-1)^{n-1} T_0 c$, $y_0 = (-1)^n T_{-1} c$ 是原方程(1)的一个特解, 定理 2 得证。

定理 3 若 $r_n = (a, b) = 1$, 则 $T_0 = Q_n, T_{-1} = P_n$, 这里 P_n, Q_n 由(4)式、(5)式确定。进一步, 若令 $(-1)^{n-1} Z_0 = t, t \in \mathbb{Z}$, 则按上述变量替换法求得原方程(1)的通解为 $x = x_0 - bt, y = y_0 + at$, 其中 $x_0 = (-1)^{n-1} T_0 c, y_0 = (-1)^n T_{-1} c$ 。

证明: 由(8)式记号 T_k 的约定以及引理 1 中的关系 II 可见, 递推关系 $T_k = q_{k+2} T_{k+1} + T_{k+2} (k = n-2, n-3, \dots, 1, 0, -1), T_n = 0, T_{n-1} = 1$, 实际上就是 T_0 除 T_{-1} 的辗转相除式, q_{k+2} 是各式中的不完全商, T_{k+2} 为余数。由文献[6]第 10 页定理 1 可知, 存在关系 $Q_k T_{-1} - P_k T_0 = (-1)^{k-1} T_k$, 其中 P_k 和 Q_k 由(4)式确定, 这里 $k = n-1, n-2, \dots, 1$ 。分别取 $k = n-1$ 和 $k = n-2$, 得到关于 T_{-1} 和 T_0 的线性方程组 $Q_{n-1} T_{-1} - P_{n-1} T_0 = (-1)^n \times T_{n-1}, Q_{n-2} T_{-1} - P_{n-2} T_0 = (-1)^{n-1} T_{n-2}$ 。不难算

得系数行列式 $\begin{vmatrix} Q_{n-1} & -P_{n-1} \\ Q_{n-2} & -P_{n-2} \end{vmatrix} = (-1)^{n-1} \neq 0$, 且

$$\begin{vmatrix} (-1)^n T_{n-1} & -P_{n-1} \\ (-1)^{n-1} T_{n-2} & -P_{n-2} \end{vmatrix} = (-1)^{n-1} P_n,$$

$$\begin{vmatrix} Q_{n-1} & (-1)^n T_{n-1} \\ Q_{n-2} & (-1)^{n-1} T_{n-2} \end{vmatrix} = (-1)^{n-1} Q_n, \text{故方程组}$$

有解 $T_0 = Q_n, T_{-1} = P_n$ 。

进一步, 在引理 2 的递推式 $Y_k = (-1)^{n-k-1} \times (r'_k T_k - r_k Z_k), k = 0, 1, 2, \dots, n-1$ 中, 取 $k = 0$, 因为 $r_0 = b, r'_0 = c$, 且在定理 1 中有 $x_0 = (-1)^{n-1} \times T_0 c, y_0 = (-1)^n T_{-1} c$, 所以 $x = Y_0 = (-1)^{n-1} (cT_0 - bZ_0) = x_0 - b(-1)^{n-1} Z_0$ 。再由递推关系 $Z_k = q'_{k+1} T_k + Z_{k+1}$, 有 $Z_0 = q'_1 T_0 + q'_2 T_1 + \dots + q'_n T_{n-1} + Z_n$, 由于其中 $Z_n = Y_n = s$ 可取一切整数, 故 $(-1)^{n-1} Z_0$ 也取一切整数, 当令 $(-1)^{n-1} Z_0 = t \in \mathbb{Z}$, 则有 $x = x_0 - bt$ 。

又因为 $x = Y_0 = (-1)^{n-1} (cT_0 - bZ_0), a = r_{-1}$, 运用引理 1 以及 $(-1)^{n-1} Z_0 = t$ 得 $y = \frac{c-ax}{b} = c \frac{1 + (-1)^n r_{-1} T_0}{b} + a(-1)^{n-1} Z_0 = (-1)^n T_{-1} c + at = y_0 + at$, 定理 3 得证。

4 关于计算的复杂性

设正整数 $a > b$, b 的十进制位数为 k , 整数 $k >$

0, 这时 $b \leq 10^k$ 。Lame'定理^{[4]105}指出, 用辗转相除算法计算两个正整数的最大公因子时, 所需除法的次数不超过两个整数中较小数的十进制位数的 5 倍。也就是说, 按辗转相除求 $(a, b) = r_n$ 共需除法 $n+1$ 次, 那么 $n+1 \leq 5 \log_{10} b \leq 5k$, 自然也有 $n+1 \leq 5 \log_{10} a$ 。

因为衡量计算复杂度的单位是基于二进制定义的位运算, 因此作为 Lame'定理的改进, 将上面的 $\log_{10} a$ 换成以 2 为底的对数, 则 $n+1 \leq 5 \lg 2 \log_2 a$ 。显然 $5 \lg 2 > 0$, 因此 $n+1 = O(\log_2 a)$, 即求 (a, b) 需作除法 $O(\log_2 a)$ 次。另一方面, 每次除法又需要 $O((\log_2 a)^2)$ 次的位运算^{[4]64-66}, 故辗转相除共需位运算 $O((\log_2 a)^3)$ 次。再加上递推式(4)中 2 组不超过 n 次的乘法计算, 每次乘法所需位运算次数也不超过 $O((\log_2 a)^2)$ ^{[4]64}, 于是运用辗转相除法求解不定方程(1), 整体的位运算总次数依然是 $O((\log_2 a)^3)$ 。

由第 2 节关于运用变量替换法求解不定方程(1)的过程可见, 该方法涉及 b 除 a 和 b 除 c 同步进行的 2 次辗转相除算法, 除法次数较辗转相除提高了 1 倍, 但位运算次数仍然是 $O((\log_2 a)^3)$, 并没有在数量级上有所提高。同时基于定理 3 中 $T_0 = Q_n, T_{-1} = P_n$ 的结论, 计算递推式(8)和(4)的计算量完全相同。因此, 运用变量替换法求解方程(1), 从计算的复杂度看, 与经典的辗转相除法同样具有高效的优点。

此外, 在运用变量替换法时还经常会有这样一种情形, 即 $r_n = 1$ 尚未出现, 已有某个 $m < n$, 使得 $r'_{m+1} = 0$ 。这时由(5)式得 $r_m Y_{m+1} = -r_{m+1} Y_m$, 并令 $Y_{m+1} = -r_{m+1} u, u \in \mathbb{Z}$, 则有 $Y_m = r_m u$, 然后逐一用(6)式回代, 最终可解出 x 和 y 。这时运用变量替换法求解方程(1)的计算量更小、优势更显著。

5 结语

上述讨论运用变量替换法给出求解二元一次不定方程的通解公式及其特解计算式, 同时论证了所得结果与由辗转相除法所得的经典公式相一致。因为用变量替换法求得的特解由(8)式中的 T_0 确定, 而(8)式与(4)式结构相似、方向相反, 所以变量替换法又可视为“反向辗转相除法”。二者比较, 结果相同且计算量无差异, 但变量替换法侧重于重复简单的操作方法, 对尚不具备辗转相除理论基础知识的初学者更通俗易懂。

参考文献:

[1] SILVERMAN J H. 数论概论[M]. 孙智伟,吴克俭,卢青林,等,译. 北京:机械工业出版社,2016:24-29.

[2] 陈景润. 数论经典著作系列:初等数论(I) [M]. 哈尔滨:哈尔滨工业大学出版社,2012:44-48.

[3] 单墀. 初等数论的知识与问题[M]. 哈尔滨:哈尔滨工业大学出版社,2011:63-66.

[4] ROSEN K H. Elementary Number Theory and Its Applications[M]. 6th ed. London:Pearson Education, Inc. , 2010.

[5] STEIN W. Elementary Number Theory: Primes, Congruences, and Secrets[M/OL] (2017-01-27) [2017-02-16]. <http://wstein.org/ent/ent.pdf>.

[6] 闵嗣鹤,严士健. 初等数论[M]. 3 版. 北京:高等教育出版社,2003.

Solution of Variable Substitution for Linear Indeterminate Equation in Two Unknowns and Analysis of Its Computation Complexity

CHEN Gong

(School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: This paper deals with the process of solving the linear indeterminate equation in two unknowns with variable substitution method, and obtains the general solution formula and the special solution formula. It is proved that the results are consistent with the classical conclusions obtained by using the method of successive division. The computational complexity is further estimated, and the conclusion is drawn that the two methods have the same calculation amount.

Keywords: linear indeterminate equation in two unknowns; variable substitution; division algorithm; general solution; computational complexity; bit operation

(责任编辑:张英健)

(上接第 62 页)

Synthesis and Crystal Structure Characterization of 1,5-Diaryl-3-Pyrazolidinone Derivatives

JIA Hongsheng¹, SUN Yongfeng²

(1. Medicine College of Science & Technology, Suzhou Chien-shiung Institute of Technology, Taicang Jiangsu 215411, China; 2. Novartis (China) Biomedical Research Co., Ltd., Pudong Shanghai 201203, China)

Abstract: To replace the methyl cinnamate and p - methoxy phenylhydrazine as raw material, 1,5-diaryl-3-pyrazolidinone derivatives were synthesized. A single crystal of 5-(3,4-dimethoxyphenyl) -1-p-methylphenyl-3-pyrazolidinone compound was obtained by a solvent evaporation method. Its elemental analysis, nuclear magnetic characterization and X-ray single crystal diffraction analysis were carried out. The crystal structure analysis results show that the crystal is triclinic P-1 space group, which belongs to five-element half-chair structure. The unit cell parameters are: $a = 9.429(19) \text{ \AA}$, $b = 10.107(2) \text{ \AA}$, $c = 10.848(2) \text{ \AA}$, $\alpha = 96.50(3)^\circ$, $\beta = 111.60(3)^\circ$, $\gamma = 114.43(3)^\circ$.

Keywords: 5-(3,4-dimethoxyphenyl) -1-p-methylphenyl-3-pyrazolidinone; synthesis; crystal structure

(责任编辑:孙新华)