Algorithmic implementation of elementary version of Runge's method for cubic Diophantine equations

N. N. Osipov
nnosipov@rambler.ru

Siberian Federal University

Seminar on Computer Algebra, CMC faculty of MSU & CCAS
http://www.ccas.ru/sabramov/seminar/doku.php
26th december 2018

Plan

- Classical Diophantine equations
- Runge's method
- Elementary version of Runge's method for Diophantine equations of total degree $d \leqslant 4$
- Algorithmic implementation in particular cases
- Extra results

Classical Diophantine equations I

References

- *Mordell L.J.* Diophantine equations. Academic Press, 1969
- *Sprindzhuk V.G.* Classical diophantine equations. Springer, 1993

Classical Diophantine equation (in two variables)

$$f(x, y) = 0$$

where $f(x, y) \in \mathbb{Z}[x, y]$ is irreducible over $\mathbb{Q}$ and $(x, y) \in \mathbb{Z}^2$

Simplest examples

- Linear equation $Ax + By + C = 0$ (*Euclid*)
- Pell equation $x^2 - Ay^2 = 1$ with $0 < A \neq \square$ (*Fermat*)
- Quadratic equation $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ (*Brouncker*, *Euler*, *Lagrange*, *Legendre*, *Gauss*)

Classical Diophantine equations II

For the equation $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ let

$$\Delta = B^2 - 4AC$$

be the discriminant of the quadratic form. The **set of solutions** is

- $\Delta < 0 \quad \Rightarrow \quad$ finite
- $\Delta = 0 \quad \Rightarrow \quad$ empty or infinite
- $0 < \Delta = \square \quad \Rightarrow \quad$ finite
  After a suitable linear substitution of the variables we get

$$Axy + Bx + Cy + D = 0 \tag{1}$$

  (the simplest case of Runge's method)
- $0 < \Delta \neq \square \quad \Rightarrow \quad$ empty or infinite

Classical Diophantine equations III

Some examples

- $x^2 - 61y^2 = 1$ (*Brahmagupta*, *Fermat*)
  The smallest solution is $(x, y) = (1766319049, 226153980)$
- $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$ (*Gauss*, in his famous book «Disqusitiones Arithmeticae»)

Software

- CAS *Maple* for the case $x^2 - Ay^2 = B$
- CAS *Mathematica* `https://www.wolframalpha.com`
- `http://www.alpertron.com.ar/QUAD.HTM`
- `http://www.numbertheory.org/php/main_pell.html`

Further information

- *Jacobson M., Williams H.* Solving the Pell Equation. Springer, 2009

Classical Diophantine equations IV

Examples of the equations of degree $\geqslant 3$

- Thue equation (*A. Thue*, 1909)

$$f_n(x, y) = A \quad (A \neq 0)$$

where $f_n(x, y)$ is a form of degree $n \geqslant 3$ irreducible over $\mathbb{Q}$

- Mordell equation (*L. Mordell*, 1914)

$$y^2 = x^3 + k \quad (k \neq 0)$$

- Elliptic equation

$$y^2 = P(x)$$

where $P(x) \in \mathbb{Z}[x]$ is a cubic polynomial having no multiple roots

Classical Diophantine equations V

Effective estimates for solutions

Definition

The *height* of an arbitrary polynomial is the maximum of absolute values of its coefficients

- Thue equation:

$$\max\{|x|,|y|\} \leqslant c_1(|A|H)^{c_2}$$

where H is the height of $f_n(x,y)$, c_i are computable constants which depend on the field $K=\mathbb{Q}(\alpha)$ with $f_n(1,\alpha)=0$

- Mordell equation:

$$\max\{|x|,|y|\} \leqslant \exp\left(c_3|k|\ln\left(|k|+1\right)^6\right)$$

where c_3 is computable absolute constant

Classical Diophantine equations VI

- Elliptic equation:

$$\max\{|x|, |y|\} \leqslant \exp\left(c_4 H^{6+\varepsilon}\right)$$

where H is the height of $P(x)$ and the constant $c_4 = c_4(\varepsilon)$ can be effectively computed

The proofs are based on Baker's method (*A. Baker*, 1968). For more details see Sprindzhuk's book

Remark

An algorithm for Thue equation is implemented in CAS *Maple*, *Mathematica*, *PARI/GP*, *SIMATH*. Also an algorithm for elliptic equation is implemented in CAS *PARI/GP*, *SIMATH*, *Magma*

Classical Diophantine equations VII

Extra information on effective methods

- *Nesterenko Yu.V.* Effective methods in theory of diophantine equations (Steklov Mathematical Institute of RAS, 2011) `http://www.mathnet.ru/php/seminars.phtml`
- *Smart Nigel P.* The algorithmic resolution of diophantine equations. Cambridge University Press, 1998

Runge's method I

Carl Runge (1856–1927)
German physicist and mathematician

`https://en.wikipedia.org/wiki/Runge`

Main achievements in mathematics

- Runge-Kutta method for solving differential equations
- Runge's phenomenon in the polynomial interpolation
- Runge's approximation theorem for analytic functions
- Laplace-Runge-Lenz vector in classical mechanics

Runge's method II

Original version of Runge's method

- *Runge C.* Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen // J. reine und angew. Math. 100 (1887)

General result Consider the polynomial

$$f(x,y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j \in \mathbb{Z}[x,y]$$

Assume $\deg_x f(x,y) = m$, $\deg_y f(x,y) = n$ and denote

$$L = \{x/m + y/n = 1\}$$

$$S = \{(i,j) : a_{ij} \neq 0\}, \quad T = S \cap L$$

Runge's method III

Runge's theorem

Suppose that $f(x, y)$ is irreducible over $\mathbb{Q}$. If the equation

$$f(x, y) = 0$$

has infinitely many solutions then

(a) no point of S lies above the line L

(b) the L-leading part of $f(x, y)$ satisfies

$$\sum_{(i,j)\in T} a_{ij} x^i y^j = a p(x, y)^k$$

where $0 \neq a \in \mathbb{Z}$, $p(x, y) \in \mathbb{Z}[x, y]$ is irreducible over $\mathbb{Q}$

(c) all Puiseux expansions of $y = \Psi(x)$ at $x = \infty$ are pairwise conjugate

Runge's method IV

Definition

Let

$$f(x,y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j \in \mathbb{Z}[x,y]$$

be an irreducible polynomial over $\mathbb{Q}$. We say that $f(x,y)$ satisfies *Runge's condition* if either (a), (b) or (c) is violated

Runge's theorem: short equivalent form

If $f(x,y)$ satisfies Runge's condition then the equation

$$f(x,y) = 0$$

has only finite set of solutions

Runge's method V

Particular case Let

$$f(x, y) = f_d(x, y) + \ldots \in \mathbb{Z}[x, y]$$

be an irreducible polynomial over $\mathbb{Q}$ where $d = \deg f(x, y)$ is the total degree and $f_d(x, y)$ is the leading homogeneous part of $f(x, y)$

Runge's theorem: well-known particular case

Suppose that $f_d(x, y)$ can be factored out into a product of two non-constant relatively prime polynomials. Then the equation

$$f(x, y) = 0$$

has only finite set of solutions

Runge's method VI

Proofs of Runge's theorem for this case

- *Mordell L.J.* Diophantine equations. Academic Press, 1969.
- *Sprindzhuk V.G.* Classical diophantine equations. Springer, 1993
- *Klazar M.* Runge's theorem on diophantine equations `http://kam.mff.cuni.cz/~klazar/ostrava2.pdf`

Runge's method: an example

$$y^3 - 2x^2y - x + 1 = 0$$

$$y = \Psi_1(x) = \frac{2\sqrt{2}}{\sqrt{3}}\, x \cos\left(\frac{1}{3}\arccos\left(\frac{9\sqrt{2}}{8\sqrt{3}} \cdot \frac{x-1}{x^3}\right)\right)$$

The Laurent expansion of $y = \Psi_1(x)$ at $x = \infty$ is

$$\sqrt{2}\,x + \frac{1}{4x} - \frac{1}{4x^2} - \frac{3\sqrt{2}}{64x^3} + \frac{3\sqrt{2}}{32x^4} + \dots$$

Runge's method VII

Runge's idea

Construct the function

$$\Phi_1(x) = P_0(x) + P_1(x)\Psi_1(x) + P_2(x)\Psi_1^2(x)$$

with $P_j(x) \in \mathbb{Z}[x]$ such that the equality

$$\lim_{x\to\infty} \Phi_1(x) = 0$$

holds

Assuming

$$\deg P_j(x) \leqslant h - j \quad (j = 0, 1, 2)$$

we come to a system of $2(h+1)$ linear homogeneous equations with respect to $3h$ unknown coefficients of $P_j(x)$. If $3h > 2(h+1)$ then this system has non-trivial solutions

Runge's method VIII

Taking $h = 3$, we find

$$P_0(x) = 4x^3 + 4x^2, \quad P_1(x) = 1, \quad P_2(x) = -2x - 2$$

For such $P_j(x)$ we have

$$\Phi_1(x) = \frac{1 + 2\sqrt{2}}{2x} + O\left(\frac{1}{x^2}\right) \quad \text{at} \quad x \to \infty$$

Thus, we obtain an additional condition

$$4x^3 + 4x^2 + y - (2x + 2)y^2 = 0$$

for the solutions (x, y) with $|x| > M$. Here M is a constant such that

$$|x| > M \quad \Rightarrow \quad |\Phi_1(x)| < 1$$

Runge's method IX

Remark

The constant M can be computed. In general, Runge's condition provides effective bounds for all solutions

Case $F(x) = G(y)$ with $\gcd(\deg F, \deg G) > 1$

Tengely Sz. Effective Methods for Diophantine Equations, PhD thesis

Runge's method: implementation

Beukers F., Tengely Sz. An implementation of Runge's method for Diophantine equations `http://arxiv.org/abs/math/0512418`

From abstract: *"...In this implementation we avoid the use of Puiseux series and algebraic coefficients."*

Runge's method X

Effective estimates For the polynomial

$$f(x,y) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij}x^i y^j \in \mathbb{Z}[x,y]$$

we put $d = \max\{m,n\}$, $H = \max|a_{ij}|$. Suppose that $f(x,y)$ satisfies Runge's condition. We have the following results:

Hilliker, Straus (1983)

$$\max\{|x|,|y|\} < (8dH)^{d^{2d^3}}$$

Hilliker D.L., Straus E.G. Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's Theorem // Trans. Amer. Math. Soc. 280 (1983)

Runge's method XI

Walsh (1992)

$$\max\{|x|,|y|\} < (2d)^{18d^7} H^{12d^6}$$

Walsh P.G. A quantitative version of Runge's theorem on Diophantine equations // Acta Arithmetica LXII.2 (1992)

The Walsh's result is based on the paper:

Dwork B.M., van der Poorten A.J. The Eisenstein constant, Duke Math. J. 65 (1992)

Extra information on Runge's method (some generalizations, algebraic geometry language, and references)

Beukers F., Tengely Sz. An implementation of Runge's method for Diophantine equations `http://arxiv.org/abs/math/0512418`

Elementary version of Runge's method I

Some elementary problems

a) Show that all solutions in integers of the equation

$$y^2 = x^4 + x^3 + x^2 + x + 1$$

are given by $(x, y) = (-1, \pm 1), (0, \pm 1), (3, \pm 11)$ [T.H. Gronwall, Amer. Math. Monthly 26 (1919)]

b) Solve the equation

$$y^2 + y = x^4 + x^3 + x^2 + x$$

in integers [First All USSR Mathematical Olympiad, 1967]

Hint for b): Place the number $4x^4 + 4x^3 + 4x^2 + 4x + 1$ between two consecutive squares

Elementary version of Runge's method II

Obvious generalization The equation $y^2 = P(x)$ with

$$P(x) = x^4 + ax^3 + bx^2 + cx + d$$

which is not square in $\mathbb{Z}[x]$

- Estimate for the solutions:

  $$|x| < 26H^3$$

  where H is the height of $P(x)$
  Masser D.W. Polynomial Bounds for Diophantine Equations // Amer. Math. Monthly 93 (1986)
  Masser D.W. Auxiliary polynomials in number theory. Cambridge University Press, 2016
- Algorithm for solving:
  Poulakis D. A simple method for solving the diophantine equation $y^2 = x^4 + ax^3 + bx^2 + cx + d$ // Elem. Math. 54 (1999)

Elementary version of Runge's method III

Typical example Using this algorithm, we can find all solutions of the equation

$$y^2 = x(x+1)(x+2)(x+3)(x+m)(x+m+1)(x+m+2)(x+m+3)$$

for any m, $1 \leqslant m \leqslant 10^6$

Tengely Sz. On a problem of Erdös and Graham // Period Math Hung 72 (2016)

Elementary version of Runge's method IV

Equations of small total degree Let

$$f(x, y) = f_d(x, y) + \ldots \in \mathbb{Z}[x, y]$$

be an irreducible polynomial over $\mathbb{Q}$ and $d = \deg f(x, y) \leqslant 4$. We suppose that the leading homogeneous part $f_d(x, y)$ factors into a product of two non-constant coprime polynomials. For this case, an elementary version of Runge's method was proposed in:

- *Осипов Н.Н.* Элементарная версия метода Рунге для кубических уравнений // Математика в школе. 2012. № 1.
- *Осипов Н.Н.* Метод Рунге для уравнений 4-й степени: элементарный подход // Математическое просвещение. Сер. 3. Вып. 19. М.: МЦНМО, 2015. `https://www.mccme.ru/free-books/matpros/pdf/mp-19.pdf`

Elementary version of Runge's method V

Case $d = 3$ (key idea) Write down the equation as

$$(a_1x + b_1y)(a_2x^2 + b_2xy + c_2y^2) + \ldots = 0$$

After a suitable linear substitution we can put $a_1 = 1$, $b_1 = 0$ (hence $c_2 \neq 0$). Rewrite it as

$$x(a_2x^2 + b_2xy + c_2y^2) + xL_{\leqslant 1}(x, y) + Ay^2 + By + C = 0$$

We can assume $A = 0$ (otherwise $c_2x + A \to x$). Then the number

$$m = \frac{By + C}{x}$$

must be integer. Moreover, since

$$\frac{By + C}{x} \to \alpha \quad \text{as} \quad x \to \infty$$

then the number m lies between $[\alpha]$ and $[\alpha] + 1$ for $|x| > M$ (the limit α and the constant M can be computed explicitly)

Elementary version of Runge's method VI

Case $d = 4$, first type

$$f(x, y) = (a_1x + b_1y)(a_2x^3 + b_2x^2y + c_2xy^2 + d_2y^3) + \dots \quad (2)$$

We can do as in the case $d = 3$ but with one extra step. Suppose that the equation is rewritten in the form

$$x(a_2x^3 + b_2x^2y + c_2xy^2 + d_2y^3) + \\ + xQ_{\leqslant 2}(x, y) + Ay^3 + By^2 + Cy + D = 0$$

WLOG assume $A = 0$. Finally we get that a number of the form

$$m = \frac{B^2(By^2 + Cy + D) - C_1xy - D_1x}{x^2}$$

must be integer and bounded when $x \to \infty$

Elementary version of Runge's method VII

Case $d = 4$, second type

$$f(x, y) = (a_1x^2 + b_1xy + c_1y^2)(a_2x^2 + b_2xy + c_2y^2) + \dots \quad (3)$$

An equation of this type one can rewrite in the form

$$F_1(x, y)F_2(x, y) = F_3(x, y)$$

where $\deg F_j(x, y) = 2$. Furthermore, we can use the fact that one of the numbers

$$m_1 = \frac{F_3(x, y)}{F_1(x, y)}, \quad m_2 = \frac{F_3(x, y)}{F_2(x, y)}$$

must be bounded at $x \to \infty$

Problem

For both cases (2), (3) we would like to estimate explicitly the growth of their roots $y = \Psi_i(x)$ at $x \to \infty$

Elementary version of Runge's method VIII

Case $d = 4$, third type

$$f(x, y) = p(x, y)^2 + \dots \tag{4}$$

where $p(x, y) = Ax^2 + Bxy + Cy^2$ is a quadratic form with

$$0 < \Delta = B^2 - 4AC \neq \square$$

In general, Runge's method does not work for the equation (4)

Remark

For this case the conditions (a) and (b) (see Runge's theorem) are fulfilled

We may hope that in some cases the condition (c) will be violated

Elementary version of Runge's method IX

Comparative examples The following two equations

$$(y^2 - 2x^2)^2 - 2y^2 - x - y = 0$$
$$(y^2 - 2x^2)^2 - 3y^2 - x - y = 0$$

are different with respect to Runge's method. Why?

Answer: They have different types of Puiseux's expansion of algebraic function $y = \Psi(x)$ at $x = \infty$

Useful observation The first equation can be rewritten as

$$(y^2 - 2x^2 - 2x)(y^2 - 2x^2 + 2x) - 2(y^2 - 2x^2) - x - y = 0$$

The second equation cannot be converted to a similar form

Elementary version of Runge's method X

Key idea Let

$$z = y^2 - 2x^2 - 2x, \quad w = y^2 - 2x^2 + 2x$$

be new variables. The corresponding equation $F(z, w) = 0$ is quite similar to the equation (1). Namely, we have

$$F(z, w) =$$
$$= (16z^2 - 40z + 23)w^2 + (-24z^2 + 34z - 8)w + 7z^2 - 8z$$

The curve defined by new equation looks like the usual rectangular hyperbola. Finally, all solutions are:

$$(x, y) \in \{(0, 0), (0, -1), (4, -5)\}$$

Algorithmic implementation I

Case $d = 3$ Consider the family of cubic equations

$$x(Ax^2 + Bxy + Cy^2) + a_1x^2 + a_2xy + 0 \cdot y^2 + a_4x + a_5y + a_6 = 0$$

where $C \neq 0$ and $a_5 \neq 0$

- *Osipov N.N., Gulnova B.V.* An algorithmic implementation of Runge's method for cubic diophantine equations // J. Sib. Fed. Univ. Math. Phys. 11 (2018) `http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=jsfu&paperid=662`

Algorithmic implementation II

Case $d = 4$ Suppose that the polynomial (4) can be rewritten as

$$f(x, y) = (p(x, y) + a_1 x + b_1 y)(p(x, y) + a_2 x + b_2 y) - \\ - dp(x, y) - a_3 x - b_3 y - c$$

where $(a_1, b_1) \neq (a_2, b_2)$. Then Runge's method also works:

- *Osipov N.N., Medvedeva M.I.* An elementary algorithm for solving a diophantine equation of degree fourth with Runge's condition // J. Sib. Fed. Univ. Math. Phys. (accepted, 2019)

Extra results I

Something else:

- **Estimates for solutions**
- **Bounds and/or statistics for the number of solutions**
- **Improvement of solving algorithms in special cases**

For details, see Osipov's papers cited above

Extra results II

Family of Diophantine equations with big solution from *Masser D.W.* Polynomial Bounds for Diophantine Equations // Amer. Math. Monthly. 93 (1986)

Consider the equation

$$y^4 + 8Hy^3 - 12y^2 + 4 = z^2 \tag{5}$$

which has the big solution (y, z) with $y = 4H^3 - 2H$

- The standard algorithm need $\approx 64H^3$ squaring of the integers with the maximal value $O(H^{12})$
- The optimized (for this case) elementary version of Runge's method for cubic equations need $\approx 96H^2$ squaring of the integers with the maximal value $O(H^6)$

Extra results III

Let

$$g(y) = y^4 + 8Hy^3 - 12y^2 + 4, \quad h(y) = y^2 + 4Hy - 8H^2 - 6$$

and $x = z - h(y)$. Then the equation (5) can be performed in

$$F(x, y) = 0 \tag{6}$$

with the polynomial

$$\begin{gathered} F(x,y) = (h(y) + x)^2 - g(y) = \\ = 2xy^2 + x^2 + 8Hxy + (-16H^2 - 12)x + \\ + (-64H^3 - 48H)y + 64H^4 + 96H^2 + 32 \end{gathered}$$

The equation (6) can be solved faster than the equation (5)

The End

Thanks for your attention!