Elem. Math. 66 (2011) 19 – 25
0013-6018/11/010019-7
DOI 10.4171/EM/165

Elemente der Mathematik

Practical solution of the diophantine equation $X^{nr}+Y^n = q$

Konstantinos A. Draziotis

Konstantinos Draziotis received his Ph.D. from the Aristotle University of Thessaloniki, Greece, in 2005. After a five years visiting professorship at the Technological and Educational Institute of Kavala, Greece, he is now working as a teacher in secondary education. His research interests are diophantine geometry and cryptography.

1 Introduction

The binomial theorem is a fundamental result of elementary algebra, which describes the algebraic expansion of powers of a binomial $(a + b)^\alpha$, where α is a complex number. It asserts that if $|x| < 1$ and α is a complex number, then

$$(1 + x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k.$$

This seemingly simple theorem allows us to study the diophantine equation

$$X^{nr} + Y^n = q, \tag{1.1}$$

with positive integers n, r, q, where n is assumed to be odd and $n \geq 3$.

Das Finden ganzzahliger Lösungen polynomialer Gleichungen ist in der Regel eine schwierige Aufgabe, wie beispielsweise die Vermutung von Fermat zeigt. In dem nachfolgenden Beitrag untersucht der Autor für natürliche Zahlen $n > 2$ (ungerade) und $r > 0$ sowie ganze Zahlen $q \neq 0$ die diophantische Gleichung $X^{nr} + Y^n = q$. Er beweist, dass die ganzzahligen Lösungen (x, y) der zur Diskussion stehenden Gleichung der Abschätzung $|x| \leq |q|^{1/r}$ genügen. Da diese Abschätzung interessanterweise unabhängig von n ist, findet man, dass die Gleichung $X^{nr} + Y^n = 1$ nur die offensichtlichen trivialen ganzzahligen Lösungen besitzt. Für seinen Beweis benötigt der Autor im wesentlichen nur den binomischen Lehrsatz sowie einige elementare Eigenschaften der Eulerschen Γ-Funktion.

We shall prove the following theorem:

Theorem 1.1 *If* $(x, y) \in \mathbb{Z}^2$ *is a solution to the equation* $X^n + Y^n = q$, *then* $|x| \le |q|$.

If (x, y) is a solution to the equation (1.1), then (x^r, y) is a solution to the equation $X^n + Y^n = q$. Thus applying Theorem 1.1 to equation (1.1) we get

Corollary 1.2 *If* $(x, y) \in \mathbb{Z}^2$ *is a solution to the equation* $X^{nr} + Y^n = q$, *then* $|x| \le \sqrt[r]{|q|}$.

Our proof of Theorem 1.1 is entirely elementary, the basic tool being the binomial theorem which will finally provide us with a representation of the integer solutions of the equation $X^n + Y^n = q$ in terms of the gamma function.

Note that the bound on $|x|$ in the theorem does not depend on the exponent n. Applying this to the corollary, we see that the number of integer solutions of equation (1.1) is bounded in terms of only q and r. Observe that, if $|x| \le \sqrt[r]{|q|}$, then $|y| \le \sqrt[n]{2|q|}$. Let X, Y, x, y be unknowns and c, r fixed positive integers. We consider an exponential equation of the form[1]

$$X^x \pm Y^y = c \quad \text{with } x = ry \text{ and } y \ge 3, \text{ odd.} \tag{1.2}$$

Corollary 1.2 reduces the study of an exponential diophantine equation of the form (1.2) to studying a bounded number of (simpler) exponential diophantine equations of the form

$$a^x \pm b^y = c, \tag{1.3}$$

where (a, b) takes values from a finite list of pairs of integers. Indeed, if we fix x, y under the restriction $x = ry$ and $y \ge 3$ (odd), then Corollary 1.2 yields

$$|X| \le \sqrt[r]{|c|} \quad \text{and} \quad |Y| \le \sqrt[y]{2|c|} < 2|c|. \tag{1.4}$$

So it is enough to solve $a^x \pm b^y = c$, for the finitely many (a, b) satisfying the inequalities (1.4). Since this holds for every x, y (with the previous restriction) this reduces equation (1.2) to finitely many equations of the form (1.3). Also, in the special case where X, Y are fixed, say $(X, Y) = (a, b)$, then LeVeque, in [6], proved that the equation $a^x - b^y = 1$ has at most one solution (in x, y).[2] We conclude then that the number of solutions to equation (1.2) (with $x = ry$ and $y \ge 3$, odd) is $\le 2|c|^2$.

Specializing further to the case $c = 1$, we get the equation $X^x - Y^y = 1$, which is related with the well-known Catalan conjecture [3] proved 160 years after its first appearance by Mihăilescu [8]. This conjecture (now a theorem) asserts that the only two consecutive positive integers which are perfect powers are 8 and 9, i.e., the equation $X^x - Y^y = 1$ has no other non-trivial solution in positive integers, except $3^2 - 2^3 = 1$. The rich history of this problem is traced in paper [7] and also gives a brief summary of the proof of P. Mihăilescu. If y is odd and ≥ 3, then from Corollary 1.2 we get $|X| \le 1$, so $X = 0$

[1] This is really a diophantine equation in X, Y, y, since $r = x/y$ is fixed as in (1.1).

[2] Except when $a = 3$, $b = 2$, in which case one finds the two solutions $(x, y) = (1, 1), (2, 3)$.

or 1 (the case $X = -1$ is not possible since $X > 0$); thus in the first case we derive the contradiction $Y^y = -1 < 0$ and the second case gives the trivial solution $(X, Y) = (1, 0)$. If y is even, then $x = ry$ is even too. Factorizing the equation $X^x - Y^y = 1$ we get $(X, Y) = (1, 0)$. Thus,

Corollary 1.3 *If r is a fixed positive integer, then the diophantine equation $X^{yr} - Y^y = 1$ admits no non-trivial integer solution in (X, Y, y) with $y \geq 2$ and $X, Y > 0$.*

If we fix x, y at nr and n, respectively, then we get the initial equation (1.1), which can be treated by what is known as Runge's method. Results of this sort have been established for instance in [1, 4, 5, 9, 10]. This method, whenever it can be applied, provides a polynomial bound for $|x|$, with respect to the absolute values of the coefficients of the defining polynomial and the degree, which in our case is nr. Thus, these bounds are not useful if we want to study the corresponding exponential equation.

Here is a brief outline of the paper. In Section 2 we give the proof of Theorem 1.1. In Section 3 we obtain an algorithm for the computation of the integer solutions of equation (1.1). Finally, the method is illustrated by some examples.

2 Solutions of the equation $X^n + Y^n = q$

Let (x, y) be an integer solution of $X^n + Y^n = q$. Then the binomial theorem gives

$$(q - x^n)^{\frac{1}{n}} = \sum_{j \geq 0} \frac{(-1)^{j+1}}{j!} \frac{1}{n}\Big(\frac{1}{n} - 1\Big) \dots \Big(\frac{1}{n} - (j-1)\Big) q^j x^{1-nj}.$$

Note that the binomial series is convergent when $|x|^n > |q|$.

Applying repeatedly the functional equation of the gamma function $z\Gamma(z) = \Gamma(z+1)$, we see that

$$\prod_{i=0}^{j-1} \Big(\frac{1}{n} - i\Big) = \frac{(-1)^j \Gamma(j - \frac{1}{n})}{\Gamma(-\frac{1}{n})}.$$

Thus

$$\begin{aligned}(q - x^n)^{\frac{1}{n}} &= \sum_{j \geq 0} \frac{(-1)^{j+1}}{j!} \frac{(-1)^j \Gamma(j - \frac{1}{n})}{\Gamma(-\frac{1}{n})} q^j x^{1-nj} \\ &= -\frac{1}{\Gamma(-\frac{1}{n})} \sum_{j \geq 0} \frac{\Gamma(j - \frac{1}{n})}{j!} q^j x^{1-nj}.\end{aligned}$$

We set

$$a_j = \frac{\Gamma(j - \frac{1}{n})}{j!},$$

so that

$$\left(q - x^n\right)^{\frac{1}{n}} = -\frac{x}{\Gamma\left(-\frac{1}{n}\right)} \sum_{j \geq 0} a_j \left(\frac{q}{x^n}\right)^j. \tag{2.1}$$

All these equalities are valid if $|x|^n > |q|$.

Recall that a function $f(x)$ is called completely monotonic (c.m.) on an interval I, if $(-1)^n f^{(n)}(x) \geq 0$ for every non-negative integer n and every $x \in I$.

Lemma 2.1

(i) *Let* $a + 1 \geq b > a$, $\alpha = \max(-a, -c)$, *and*

$$g(x; a, b, c) = (x + c)^{a-b} \frac{\Gamma(x + b)}{\Gamma(x + a)} \quad (x > \alpha).$$

Then, $1/g(x; a, b, c)$ *is c.m. on the interval* (b, ∞), *if* $c \geq a$.

(ii) *We have* $\sum\limits_{j=0}^{k-1} a_j = -nb_k$, *where*

$$b_k = \frac{\Gamma\left(k - \frac{1}{n}\right)}{(k-1)!}.$$

(iii) *We have* $\lim\limits_{k \to \infty} b_k = 0$.

Proof. (i) See [2, Theorem 3 (ii)].

(ii) This follows via induction on k from the functional equation

$$\Gamma(1 + z) = z\Gamma(z) \qquad (z \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}).$$

(iii) Using the notation of part (i) of our lemma, we set $a = -1/n$, $b = 0$. Then $a + 1 \geq b > a$. Let

$$g(x) = (x + c)^{a-b} \frac{\Gamma(x + b)}{\Gamma(x + a)},$$

then $1/g(x)$ is c.m. on $(0, \infty)$ for $c \geq -1/n$. Thus,

$$\frac{1}{g(x)} = (x + c)^{\frac{1}{n}} \frac{\Gamma\left(x - \frac{1}{n}\right)}{\Gamma(x)}$$

is decreasing on $(0, \infty)$, for some fixed $c > 0$. The same holds true, if $x = k \in \mathbb{Z}_{>0}$. Thus,

$$r_k = (k + c)^{\frac{1}{n}} \frac{\Gamma\left(k - \frac{1}{n}\right)}{\Gamma(k)}$$

is a decreasing sequence. Therefore $r_k < r_2$, for $k > 2$. So

$$(k + c)^{\frac{1}{n}} \frac{\Gamma\left(k - \frac{1}{n}\right)}{\Gamma(k)} < r_2,$$

hence

$$0 \leq \frac{\Gamma\left(k - \frac{1}{n}\right)}{\Gamma(k)} = b_k < r_2(k+c)^{-\frac{1}{n}} \to 0,$$

when $k \to \infty$. The result follows. □

Remark. Instead of deducing (iii) from part (i) of the lemma, one may for instance apply Stirling's formula for the gamma function.

Proof of Theorem 1.1. We proved in Lemma 2.1 that $\sum_{j=0}^{\infty} a_j = 0$, so

$$-a_0 = -\Gamma\left(-\frac{1}{n}\right) = \sum_{j=1}^{\infty} a_j.$$

Let (x, y) be an integer solution of the equation $X^n + Y^n = q$. Relation (2.1) gives

$$\Gamma\left(\frac{-1}{n}\right) y = \Gamma\left(\frac{-1}{n}\right)(q - x^n)^{\frac{1}{n}} = -a_0 x - x \sum_{j \geq 1} a_j \left(\frac{q}{x^n}\right)^j,$$

thus

$$\left|\Gamma\left(\frac{-1}{n}\right)\right| |y + x| \leq \sum_{j \geq 1} |a_j| \frac{|q|^j}{|x|^{jn-1}} < \sum_{j \geq 1} |a_j| \frac{|q|^{jn-1}}{|x|^{jn-1}}.$$

Suppose that $|x| > |q|$. Then all the previous inequalities are valid since the series are convergent. Thus,

$$\left|\Gamma\left(\frac{-1}{n}\right)\right| |y + x| < \sum_{j \geq 1} |a_j|.$$

Since $a_j > 0$ for $j > 0$, we get

$$\sum_{j \geq 1} |a_j| = \sum_{j \geq 1} a_j = -a_0 = |a_0| = \left|\Gamma\left(\frac{-1}{n}\right)\right|.$$

So

$$\left|\Gamma\left(\frac{-1}{n}\right)\right| |y + x| < \sum_{j \geq 1} |a_j| = |a_0| = \left|\Gamma\left(\frac{-1}{n}\right)\right|.$$

It follows that $|y + x| < 1$, thus $|y + x| = 0$. So $y = -x$. On the other hand $x^n + y^n = q$, thus replacing y with $-x$, we get $x^n + (-1)^n x^n = q$. Since n is odd, we get the contradiction $q = 0$. We conclude therefore that $|x| \leq |q|$. □

3 An algorithm for the solution of the equation $X^{nr} + Y^n = q$

As before, let $(x, y) \in \mathbb{Z}^2$ with $x^{nr} + y^n = q$. The only interesting case is $xy < 0$. Let $x > 0$ and $y < 0$. We set $y = -z$, where $z > 0$. Then we get $x^{nr} - z^n = q$, thus

$$(x^r - z)P(x, z) = q, \quad \text{where} \quad P(x, z) = x^{nr-r} + x^{nr-2r}z + \ldots + x^r z^{n-2} + z^{n-1}.$$

Hence $(x^r - z)|q$. So we get $z = x^r - h$ for some divisor h of q. Substituting this into $P(x, z)$, we then compute the integer roots of the equation

$$P(x, x^r - h) = \frac{q}{h}.$$

Thus, we get

$$nx^{nr-r} + \ldots + x^r z^{n-2} + h^{n-1} = \frac{q}{h},$$

so

$$x^r | \left(h^{n-1} - \frac{q}{h}\right) = \frac{h^n - q}{h}.$$

The same holds true, if $x < 0$ and $y > 0$. So we get the following algorithm:

Input. n, r, q positive integers with $n \geq 3$, odd.

Output. The integer solutions of the equation (1.1).

1. Compute the divisors of q.
2. For each divisor h of q compute the rational number $k_h = (h^n - q)/h$.
3. Compute the set S_h of the divisors of k_h.
4. Compute the set S'_h of elements of S_h which are $\leq \sqrt[r]{|q|}$.
5. The integer solutions of (1.1) are

$$\{(x, y) \in \mathbb{Z}^2 \mid x^r \in S'_h \ \text{with} \ x^{nr} + y^n = q\},$$

where h runs through the set of divisors of q.

Below we give some examples. Here the values of q have been chosen experimentally, using Maple, in order to give non-trivial solutions to the diophantine equation (1.1).

For $(n, r, q) = (3, 2, 2\,985\,985)$, we get $(x, y) = (\pm 12, 1), (\pm 1, 144)$.

For $(n, r, q) = (3, 3, 10\,604\,499\,381)$, we get $(x, y) = (13, 2)$.

For $(n, r, q) = (3, 1, 3\,383)$, we get $(x, y) = (15, 2), (2, 15)$.

For $(n, r, q) = (5, 2, 576\,650\,390\,657)$, we get $(x, y) = (\pm 15, 2)$.

For $(n, r, q) = (5, 1, 102\,400\,032)$, we get $(x, y) = (2, 40), (40, 2)$.

For $(n, r, q) = (15, 1, 1\,453)$ and $(n, r, q) = (15, 1, 2\,141)$, there is no integer solution.

In all these examples it took a few seconds to find the results on a Pentium 2.6 GHz PC.

Acknowledgements

The author is indebted to the referee for valuable remarks.

References

[1] Ayad, M.: Sur le théorème de Runge. *Acta Arith.* 58 (1991), 203–209.

[2] Bustoz, J.; Ismail, M.E.H.: On gamma function inequalities. *Math. Comp.* 47 (1986) 176, 659–667.

[3] Catalan, E.: Note extraite d'une lettre adressée a l'éditeur. *J. Reine Angew. Math.* 27 (1844), 192.

[4] Grytczuk, A.; Schinzel, A.: On Runge's Theorem about Diophantine equations. *Colloq. Math. Soc. János Bolyai* 60 (1991), 329–356.

[5] 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) 2, 637–657.

[6] LeVeque, Wm.J.: On the equation $a^x - b^y = 1$. *Amer. J. Math.* 74 (1952), 325–331.

[7] Metsänkylä, T.: Catalan's conjecture: another old Diophantine problem solved. *Bull. Amer. Math. Soc. (N.S.)* 41 (2004) 1, 43–57.

[8] Mihăilescu, P.: Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.* 572 (2004), 167–195.

[9] Schinzel, A.: An improvement of Runge's theorem on diophantine equations. *Comment. Pontificia Acad. Sci.* 2 (1969), 1–9.

[10] Tengely, Sz.: On the Diophantine equation $F(x) = G(y)$. *Acta Arith.* 110 (2003) 2, 185–200.

Konstantinos A. Draziotis
Kromnis 33
54454 Thessaloniki, Greece
e-mail: `drazioti@gmail.com`