PRACTICAL SOLUTION OF THE DIOPHANTINE EQUATION $X^{nr}+Y^n=q$

KONSTANTINOS A. DRAZIOTIS

1. Introduction

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 allow us to study the diophantine equation

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

where $n\geq 3$ (odd), and r,q are positive integers.

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 $|x|\leq|q|$.*

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 $|x|\leq\sqrt[r]{|q|}$.*

The proof of Theorem 1.1 is elementary and our basic tool is the use of Binomial Theorem which finally provide us with a representation of the integer solutions of equation $X^n+Y^n=q$ by means of Gamma function. The intriguing about this Theorem is that the bound for $|x|$ is independent of the exponent n. Applying this to the Corollary, we get that the number of integer solutions of (1.1) depends only on q and r. Remark that if $|x|\leq\sqrt[r]{|q|}$, then $|y|\leq\sqrt[n]{2|q|}$. Let X,Y,x,y, are unknowns and c,r are fixed positive integers. We consider an exponential equation of the form[1]

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

Corollary 1.2 allows to reduce the study of an exponential diophantine equation of form (1.2), to the study of some (simpler) exponential diophantine equations of the form:

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

2000 *Mathematics Subject Classification.* 11D41.

Key words and phrases. Gamma function, Binomial theorem.

[1] In fact this is a diophantine equation in X,Y,y since x,y are related with $x/y=r$ and r is fixed.

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

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

So it is enough to solve $a^x \pm b^y = c$, where a, b, belong to the finite list of integers given by the inequalities (1.4). Since this holds for every x, y (with the previous restriction) we deduce that we can reduce equation (1.2) to finite equations of the form (1.3). Also, in the special case where X, Y, are fixed, say at a, b, respectively, then LeVeque, in [6], proved that the equation $a^x \pm b^y = 1$ has at most one solution (in x, y), except when $a = 3, b = 2$ (then there are only two solutions, given by $(x, y) = (1, 1), (2, 3)$). We conclude therefore that the number of solutions to equation (1.2) (with $x = ry$ and $y \geq 3$ odd) is $\leq 2|c|^2$.

In the special case where $c = 1$ we get the equation $X^x - Y^y = 1$, which is related with the well-known Catalan conjecture [3], and proved 160 years after its first appearance, in the landmark paper of Mihăilescu [8]. This conjecture (now Theorem) asserts that two consecutive positive integers except 8 and 9 can not be perfect powers. In other words the equation $X^x - Y^y = 1$ has no other non trivial integer 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 $|X| \leq 1$, so $X = 0$ or 1, (the case $X = -1$ is not accepted 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 there is not any non trivial integer solution in (X, Y, y) with $y \geq 2, X, Y > 0$ of the diophantine equation $X^{yr} - Y^y = 1$.*

If we fix x, y at nr and n, respectively, then we get the initial equation (1.1), which can be treated by the so called Runge's method. Results of this sort have been proven by a number of people, for instance [1, 4, 5, 9, 10]. This method(whenever 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(in our case the degree is nr). Thus, these bounds are not useful if we want to study the corresponding exponential equation.

We give 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 (1.1). Then, Binomial Theorem gives

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

Note that, the binomial series is convergent when $|x|^n > |q|$. We shall need two auxiliary lemmas.

Lemma 2.1. *Let α and m be two positive integers. Then*

$$\prod_{i=0}^{m}(\alpha - i) = \frac{(-1)^{m+1}\Gamma(m-\alpha+1)}{\Gamma(-\alpha)}. \tag{2.1}$$

Proof. We apply the basic functional equation $\Gamma(z+1) = z\Gamma(z)$, which holds for $z \in \mathbb{C} - \mathbb{Z}_{\leq 0}$, to the relation,

$$\frac{\Gamma(\alpha+1)}{\Gamma(\alpha-m)} = (-1)^{m+1}\frac{\Gamma(m-\alpha+1)}{\Gamma(-\alpha)}.$$

□

We set $\alpha = 1/n$. Then we get

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

Thus

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

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

Also, we set

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

thus

$$\big(q-x^n\big)^{1/n} = -\frac{x}{\Gamma(-\frac{1}{n})}\sum_{j\geq 0}a_j\Big(\frac{q}{x^n}\Big)^j. \tag{2.2}$$

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

We recall the definition of completely monotonic (c.m.) function on an interval I.

Definition. $f(x)$ is called c.m. on I, if $(-1)^n f^{(n)}(x) \geq 0$ for every non negative integer n and every $x \in I$.

Lemma 2.2. (i) *Let $a+1 \geq b > a$, $\alpha = \max(-a,-c)$ and*

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

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

(ii) $\displaystyle\sum_{j=0}^{k-1}a_j = -nb_k$, *where*

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

(iii) $\displaystyle\lim_{k\to\infty} b_k = 0.$

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

(ii). Applying induction with respect to k and using the formula

$$\Gamma(1+z) = z\Gamma(z),\ (z \in \mathbb{C} - \mathbb{Z}_{\leq 0})$$

we get the desired result.

(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 completely monotonic on $(0,\infty)$, for $c \geq -1/n$. Thus

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

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

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

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

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

hence

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

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 2.2, that $\sum_{j=0}^{\infty} a_j = 0$, so

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

Let (x,y) be an integer solution of the equation $X^n + Y^n = q$. Relation (2.2) gives:

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

thus

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

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

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

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

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

So

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

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 $0=q$. We conclude therefore that $|x|\leq|q|$. □

3. An Algorithm for the Solution of the equation $X^{nr}+Y^n=q$

As previous $(x,y)\in\mathbb{Z}^2$ 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

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

Hence $x^r-z|q$. So we get $z=x^r-h$ for some divisor h of q. We substitute the value of z to $P(x,z)$ and then we compute the integer roots of the equation

$$P(x,x^r-h)=q/h.$$

Thus, we get

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

so

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

The same holds 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 points of C are

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

where h runs on the set of divisors of q.

Below we give some examples (the values of q are chosen, after some search in Maple, in order to give non trivial solutions to the diophantine equation (1.1)).

For $(n,r,q)=(3,2,2985985)$, we get $(x,y)=(\pm 12,1),(\pm 1,144)$.
For $(n,r,q)=(3,3,10604499381)$, we get $(x,y)=(13,2)$.
For $(n,r,q)=(3,1,3383)$, we get $(x,y)=(15,2),(2,15)$
For $(n,r,q)=(5,2,576650390657)$, we get $(x,y)=(\pm 15,2)$.
For $(n,r,q)=(5,1,102400032)$, we get $(x,y)=(2,40),(40,2)$.
For $(n,r,q)=(15,1,1453)$ and $(n,r,q)=(15,1,2141)$, we do not take any integer solution.

To all previous examples it took some seconds to find the results on a Pentium 2.6 GHz PC.

Acknowledgments. The author is indebted to the Referee for his 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), no. 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, in Colloq. Math. Soc. Janos Bolyai **60**, North-Holland, 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), no. 2, 637–657.

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

[7] Metsänkylä, Tauno; Catalan's conjecture: another old Diophantine problem solved. Bull. Amer. Math. Soc. (N.S.) **41** (2004), no. 1, 43-57.

[8] Mihăilescu, Preda; 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), no. 2, 185–200.

E-mail address: `drazioti@gmail.com`