The Mathematics Student ISSN: 0025-5742
Vol. 84, Nos. 1-2, January-June (2015), 135-155

DIOPHANTINE EQUATIONS OF THE FORM $F(X) = G(Y)$ - AN EXPOSITION

MANISHA KULKARNI AND B. SURY

(Received : 07 - 04 - 2015)

Abstract. In this article, we discuss some of the present-day methods used in dealing with Diophantine equations of the form $f(x) = g(y)$ for solutions in integers x, y, where f, g are polynomials with integer coefficients. We mention mainly results proved in the last two decades and, point out in the last section some unsolved questions arising from an observation of Ramanujan. This is a survey meant for non-experts and students. The last section has some new results for which we give complete proofs.

1. Introduction

The theory of Diophantine equations is a branch of number theory which deals with the solutions of integer polynomial equations in integers; more generally, it is customary to also consider solutions in rational numbers. A unique aspect of this subject is that it is most often very easy to state the problem but it is very difficult to guess if the problem is trivial to solve or, if it needs deep ideas from other branches of mathematics. A well-known example is Fermat's Last theorem which was solved more than 350 years after it was stated, using very deep ideas from various branches of mathematics.

Questions on counting often involve finding integer solutions of equations of the form $f(x) = g(y)$ for integral polynomials f, g. An example comes from counting lattice points in generalized octahedra. The number of integral points on the n-dimensional octahedron $|x_1| + |x_2| + \cdots + |x_n| \leq r$ is given by the expression $p_n(r) = \sum_{i=0}^{n} 2^i \binom{n}{i}\binom{r}{i}$ and the question of whether two octahedra of different dimensions m, n can contain the same number of integral points becomes equivalent to the solvability of $p_m(x) = p_n(y)$ in integers x, y. Another natural question is to determine, for fixed distinct natural numbers m, n, how often $\binom{x}{m} = \binom{y}{n}$ in integers x and y. Bilu, Rakaczki, Stoll and Tichy ([3]) have established precise finiteness

2010 Mathematics Subject Classification: 11D45, 11B68, 14H25.
Keywords and Phrases: Diophantine equations, Siegel's theorem on integral solutions, Genu -s of a plane curve, extrema of a polynomial, Decomposable polynomials, Elliptic curves, Berno -ulli polynomials, Bilu-Tichy theorem.

results for these equations. One more result of this kind proved by Stoll & Tichy is that for the sequences of classical orthogonal polynomials $p_m(x)$ like the Laguerre, Legendre and Hermite polynomials, an equation of the form $ap_m(x) + bp_n(y) = c$ with $a, b, c \in Q$ and $ab \neq 0$ and $m > n \geq 4$ has only finitely many solutions in integers x, y. Yet another classical problem is to find products of consecutive integers which are perfect powers. Erdős and Selfridge ([9]) proved in 1975 that any finite product of consecutive integers can never be a perfect power. In other words, the Diophantine equation

$$x(x+1)(x+2)\cdots(x+m-1) = y^n$$

does not have any nontrivial solution in integers when $m,\ n > 1$. In a later section, we will outline a proof of this classical result. Another example is the question as to which natural numbers have all their digits to be 1 with respect to two different bases. This is equivalent to solving

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

in natural numbers $x, y > 1$ for some $m, n > 2$. For example, it was Observed by Goormaghtigh nearly a century ago that 31 and 8191 have this property

$$(11111)_2 = (111)_5\ ,\ (111)_{90} = 2^{13} - 1.$$

However, it is still unknown whether there are only finitely many solutions in all variables x, y, m, n. In fact, no other solutions are known.

Let us begin by discussing a beautiful theorem.

2. Erdős-Selfridge theorem

As mentioned in the introduction, Erdős and Selfridge ([9]) proved in 1975 that *any finite product of consecutive integers can never be a perfect r-th power for any $r > 1$.* They used a classical theorem due to Sylvester which asserts (see also [25]):

Theorem 2.1 (Sylvester)**.** *Any set of k consecutive positive integers, with the smallest $> k$, contains a multiple of a prime $> k$.*

Note that the special case of this, when the numbers are $k+1, \cdots, 2k$, is known as Bertrand's postulate. We outline the proof of the Erdős-Selfridge theorem for the case of squares.

Suppose $(n+1)(n+2)\cdots(n+k) = y^2$ in positive integers n, y where $k \geq 2$. Write $n + i = a_i x_i^2$ with a_i square-free. Clearly each prime factor of each a_i is less than k. *The key point is to show that all these a_i's must be distinct.*

Now, if $n < k$ then Bertrand's postulate gives a prime p between $[(n+k)/2]$ and $n + k$. As $n < (n+k)/2$, the prime p is one of the terms $n + i (1 \leq i \leq k)$ and, therefore, p^2 cannot divide the product $(n+1)(n+2)\cdots(n+k)$ which is a contradiction.

If $n \geq k$ then Sylvester's theorem gives a prime number $q > k$ which divides the product $(n+1)(n+2)\cdots(n+k) = y^2$. So, q^2 divides some $n+i$ and hence $n+i \geq q^2 \geq (k+1)^2$. Therefore, $n \geq k^2+1$; that is, $n > k^2$.
But, if $a_i = a_j$ for some $i > j$, then

$$k > (n+i) - (n+j) = a_j(x_i^2 - x_j^2) > 2a_jx_j \geq 2\sqrt{a_jx_j^2} = 2\sqrt{n+j} > \sqrt{n},$$

a contradiction.

Finally, one easily bounds the product $a_1a_2\cdots a_k$ below by the product of the first k s quare-free numbers and one uses the fact that each prime divisor of each a_i is $< k$ to bound the product of the a_i's from above to get a contradiction.

3. Modus operandi-Siegel's theorem

Many results appearing in the last ten years have been made possible by a beautiful theorem of Bilu & Tichy which was built out of deep ideas of Michael Fried (see [11], [12], [13]). To motivate these results, we first need to recall the basic classical theorem due to C. L. Siegel. More generally, consider a polynomial $F \in \mathbb{Z}[X,Y]$. Recall that F is said to be absolutely irreducible if it is irreducible over the field $\overline{\mathbb{Q}}$ of algebraic numbers. Then, the celebrated 1929 theorem due to Siegel ([26]) asserts:

Theorem 3.1 (Siegel, 1929)**.** *If $F \in \mathbb{Z}[X,Y]$ is absolutely irreducible and the curve $F = 0$ has genus > 0, then the number of integral points on the curve is finite. Further, the finiteness of the number of integer points holds good except when the (projective completion of the) curve defined by $F = 0$ has genus 0 and at most 2 points at infinity.*

For the rational solutions, a finiteness theorem is the following one due to Faltings ([10]).

Theorem 3.2 (Faltings, 1983)**.** *If $F \in \mathbb{Q}[X,Y]$ is irreducible, and if the curve $F = 0$ has genus > 1, then the equation $F(x,y) = 0$ has only finitely many solutiuons $x, y \in \mathbb{Q}$.*

As this article is meant for students also, we will explain the notions involved and how one computes the relevant things. Before that, we explain how the theorem is used in proving finiteness of solutions of Diophantine equations. It should be pointed out that Siegel's theorem is, unfortunately, ineffective - in other words, no explicit bound for x, y can be determined beyond which there are no solutions.
To determine finiteness or otherwise of the integral solutions of a given equation $F(x,y) = 0$ using Siegel's theorem, one splits $F(x,y)$ into irreducible factors in $\mathbb{Q}[x,y]$, and for each factor which is irreducible over $\bar{\mathbb{Q}}$ one finds the genus and the number of points at infinity. Then, for each of those factors which have genus 0

and ≤ 2 points at infinity, one can try to determine whether the number of integral solutions is finite or not.

4. Genus of the curves $f(X) = g(Y)$

In order to keep the discussion as elementary as possible, we do not go into general definitions of genus but merely recall how the genus is determined. As mentioned at the outset, we will stick to curves of the form $f(X) = g(Y)$. Recall that a complex zero of f' is called a stationary point of the polynomial f; we denote by S_f, the set of stationary points of f. The classical Riemann-Hurwitz formula can be applied to the function field extension $\mathbb{C}(X,Y)/\mathbb{C}(Y)$ given by $f(X) - g(Y)$ to deduce ([4]) the following explicit result.

Lemma 4.1. *Let $f, g \in \mathbb{C}[X]$ be two polynomials such that the polynomial $f(X) - g(Y) \in \mathbb{C}[X,Y]$ in two variables is irreducible. Suppose the stationary points of f and g are simple. For each stationary point $a \in S_f$, define*

$$r_a := |\{b \in S_g : f(a) = g(b)\}|.$$

Then, the genus g of the curve $f(X) = g(Y)$ is given by

$$2g = \sum_{a \in S_f} (\deg(g) - 2r_a) - \deg(f) + 2 - GCD(\deg(f), \deg(g)).$$

Let us see how useful this is by means of the following simple example.

Example 4.2. *For any $\lambda \in \mathbb{C}^*$, consider the equation*

$$x(x+1) = \lambda y(y+1)(y+2). \tag{4.1}$$

If $f(X) = X(x+1)$ and $g(Y) = Y(Y+1)(Y+2)$ then $S_f = \{-1/2\}$ and $S_g = \{2\sqrt{3}/9, -2\sqrt{3}/9\}$. Now $g(\pm 2\sqrt{3}/9) = f(-1/2)$ if, and only if, $\lambda = \pm 3\sqrt{3}/8$, and in this case $r_{-1/2} = 1$. Therefore, the genus is 0 for $\lambda = \pm 3\sqrt{3}/8$, and 1 for other λ. Hence, it follows from Siegel's theorem that the equation (4.1) has only finitely many integral solutions unless $\lambda = \pm 3\sqrt{3}/8$.

Definition 4.3 (Points at infinity)**.** *Given $F \in \mathbb{Q}[X,Y]$, one may homogenize this polynomial to a homogeneous polynomial of three variables X, Y, Z. Then, the points in the projective space corresponding to the solutions of $F(x,y,0) = 0$ are called the points at infinity of the curve $F = 0$.*

In Siegel's theorem, finiteness of integral solutions follows if either genus of the curve is positive or, if the genus is 0 but there are at least three points at infinity. Therefore, to check for finiteness of integral solutions, one computes the genus and, when it is 0 and there are at most two points at infinity, check separately for finiteness of integral solutions.

5. Congruent numbers

In this section, we discuss the classical congruent number problem which leads to an equation of the form $f(x) = g(y)$; more precisely, an equation of the form $y^2 = x(x+n)(x-n)$ where n is a positive integer. However, in this case, we will be interested in solutions in *rational* numbers. The curve $Y^2 - X(X+n)(X-n) = 0$ arising in this manner has genus 1 as we can easily check from the above lemma on genus computation. Therefore, Siegel's theorem shows finiteness of the number of integer solutions. However, Faltings's theorem quoted above for finiteness of rational solutions does not apply as the genus is 1.

A positive integer d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.

It is an ancient Greek problem to determine which positive integers are congruent numbers and which are not. Firstly, the property of being a congruent number for a positive integer d turns out to be equivalent to the existence of an arithmetic progression of three terms which are all squares of rational numbers having the common difference d. Here is an argument to show the equivalence.

Indeed, let $u \leq v < w$ be the sides of a right triangle with sides rational. Then $x = w/2$ is such that $(v-u)^2/4, w^2/4, (u+v)^2/4$ form an arithmetic progression. Conversely, if $x^2 - d = y^2, x^2, x^2 + d = z^2$ are three rational squares in arithmetic progression, then $z-y, z+y$ are the legs of a right angled triangle with legs rational, area $(z^2 - y^2)/2 = d$ and rational hypotenuse $2x$ because $2(y^2 + z^2) = 4x^2$.

For example, $5, 6$ and 7 are congruent numbers. This can be seen by considering the following three right-angled triangles:

with sides $3/2, 20/3$ and $41/6$ having area 5;

with sides $3, 4$ and 5 having area 6;

and, with sides $35/12, 24/5$ and $337/60$ having area 7.

On the other hand, $1, 2$ and 3 are not congruent numbers. The fact that $1, 2$ are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4.

Indeed, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 1$ for some rational numbers a, b, c then $x = c/2, y = |a^2 - b^2|/4$ are rational numbers satisfying $y^2 = x^4 - 1$. Similarly, if $a^2 + b^2 = c^2, \frac{1}{2}ab = 2$ for rational numbers a, b, c, then $x = a/2, y = ac/4$ are rational numbers satisfying $y^2 = x^4 + 1$.

These equations reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat, using the method of descent, not to have nontrivial solutions. The unsolvability of $y^2 = x^4 \pm 1$ in rational numbers is exactly equivalent to showing $1, 2$ are not congruent.

In fact $y^2 = x^4 - 1$ for rational x, y gives a right-angled triangle with sides $y/x, 2x/y, (x^4+1)/xy$ and area 1. Similarly, $y^2 = x^4 + 1$ for rational x, y gives a right-angled triangle with sides $2x, 2/x, 2y/x$ and area 2.

Though it is an ancient problem to determine which natural numbers are congruent, it is only in late 20th century that substantial progress has been made.

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$. Such equations define *elliptic curves*. It turns out that

d is a congruent number if, and only if, the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a solution with $y \neq 0$.

In fact, $a^2+b^2 = c^2, \frac{1}{2}ab = d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$. Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y, 2xd/y, (x^2 + d^2)/y$ and area d.

The set of rational solutions of an elliptic curve over $\mathbb{Q}$ forms a group and it is an easy fact, from the way the group law is defined, that there is a solution with $y \neq 0$ if and only if there are infinitely many rational solutions ([15]). Therefore, if d is a congruent number, there are infinitely many rational-sided right-angled triangles with area d.

A point to note is that even for an equation with integral coefficients as the one above, it is the set of rational solutions which has a nice (group) structure. Thus, from two rational solutions, one can produce another rational solution by 'composition'. So, it is inevitable that in general one needs to understand rational solutions even if we are interested only in integral solutions. For example, the equation $y^2 = x^3 + 54$ has only *two integral solutions* $(3, \pm 9)$ but the set of rational solutions is the *infinite cyclic* group generated by $(3, 9)$.

The connection with elliptic curves has been used to show that numbers which are $1, 2$ or 3 mod 8 are not congruent.

Further, assuming the truth of the weak Birch & Swinnerton-Dyer conjecture ([15]), Stephens showed this provides a complete characterization of congruent numbers.

6. Irreducibility, indecomposability and Fried's work

It was Michael Fried who realized the peculiarities of factorizing a polynomial of the form $f(X) - g(Y)$. He used geometric methods - particularly, the theory of monodromy groups - to deduce several striking results. Historically, one of the earliest irreducibility results was proved by Ehrenfeucht ([8]) in 1958; it asserts :

Theorem 6.1 (Ehrenfeucht)**.** *If* $\deg f, \deg g$ *are relatively prime, then* $f(X)-g(Y)$ *is irreducible.*

The proof is not difficult and can be worked out by defining a weighted degree of

polynomials in $\mathbb{C}[X, Y]$ with weight $\deg(f)$ for X and $\deg(g)$ for Y and comparing the top degree terms in an expression of the form

$$f(X) - g(Y) = F(X, Y)G(X, Y).$$

We mention in passing that Davenport, Fried, Leveque, Lewis, Runge, and Schinzel made fundamental contributions to the question of irreducibility of $f(X) - g(Y)$; see [16], [7], [23], [24], [27], [28].

There are some cases when one can observe that $f(X) - g(Y)$ is reducible. For instance, over $\mathbf{C}$, $T_n(X) + T_n(Y)$ is a product of quadratic factors (and a linear factor if n is odd) where $T_n(X)$ is the Chebychev polynomial $T_n(X + X^{-1}) = X^n + X^{-n}$. Another simple observation is that if f_1, g_1, F are polynomials with $\deg F > 0$, then $f_1(X) - g_1(Y)$ is a factor of $F(f_1(X)) - F(g_1(Y))$. Thus, the possibility of decomposing two given polynomials f, g in the form $f = F \circ f_1, g = F \circ g_1$ for a single, nonconstant polynomial F becomes interesting and is of relevance. A remarkable result due to Fried & MacRae (1969) ([14]) is that the converse also holds.

Proposition 6.2. *$f(X) - g(Y)$ has a factor of the form $f_1(X) - g_1(Y)$ if (and only if), there is $F(T) \in \mathbf{C}[T]$ such that*

$$f(T) = F(f_1(T)) \ , \ g(T) = F(g_1(T)).$$

Fried had made a deep study of the factors of $f(X) - g(Y)$ and proved in 1973 the following theorem([11]).

Theorem 6.3. *Given $f, g \in \mathbb{Z}[X]$, there exist f_1, f_2, g_1, g_2 in $\mathbf{Z}[X]$ such that*

1. *$f(X) = f_1(f_2(X)), g(X) = g_1(g_2(X))$,*
2. *Splitting fields of $f_1(X) - t$ and of $g_1(X) - t$ over $\mathbb{Q}(t)$ (where t is a new indeterminate) are the same, and*
3. *the irreducible factors of $f(X) - g(Y)$ are in bijection with those of $f_1(X) - g_1(Y)$.*

6.1. **Arithmetic monodromy groups.** The above results follow by considerations of monodromy groups. Firstly, we call $f = f_1 \circ f_2$ a proper decomposition of the polynomial f if f_1, f_2 are both nonconstant polynomials. If a proper decomposition exists, one says f is *decomposable*; otherwise, it is said to be *indecomposable*. As this notion is insensitive to linear changes of the variable, there is an evident notion of equivalent decompositions.

Now, if $f \in \mathbb{Z}[X]$ is a nonconstant monic polynomial, then consider a splitting field K of the polynomial $f(X) - t$ over $\mathbb{Q}(t)$; the Galois group $G := \mathrm{Gal}\,(K/\mathbb{Q}(t))$ viewed as a group of permutations of the roots of $f(X) - t$ in K, is known as the *arithmetic monodromy group of f*. If $K = \mathbb{Q}(t)(\alpha)$, then $f(\alpha) = t$. Consider

the stabilizer subgroup H of α in G. The theorem of Luröth helps us derive the following reformulation of decomposability of f.

Proposition 6.4 ([17], Lemma 2.7)**.** *Let f, K, α, G, H be as above. Let $f = f_1(f_2(\cdots(f_r))\cdots)$ be a decomposition of f into indecomposable polynomials f_i over $\mathbb{Q}$. Let H_i denote the stabilizer in G of $f_i(f_{i+1}(\cdots(f_r(\alpha)))\cdots)$ for $1 \leq i \leq r$. Then,*

$$G \supset H_1 \supset H_2 \cdots \supset H_r \supset H$$

is a maximal strictly decreasing chain of intermediate subgroups between G and H. Conversely, any such strictly decreasing maximal chain of subgroups corresponds to a decomposition of f into indecomposables.

Implicit in the above proposition are two classical theorems of Ritt ([22]) from 1922. The first theorem says that any two proper decompositions have the same length and the second one finds all solutions of $f_1 \circ f_2 = g_1 \circ g_2$ when f_1, g_1 have coprime degrees and g_1, g_2 have coprime degrees.
As we mentioned earlier, applying Siegel's theorem involves checking irreducibility of $f(X) - g(Y)$; so, a related question is to determine when a decomposable polynomial $f_1 \circ f_2$ is irreducible. This is addressed by the following elementary classical lemma.

Lemma 6.5 (Capelli)**.** *Let $f_1, f_2 \in K[X]$, where K is an arbitrary field. Let α be a root of f_1 in a fixed algebraic closure $\bar{K}$ of K. Then, $f_1 \circ f_2$ is irreducible over K if, and only if, f_1 is irreducible over K and $f_2 - \alpha$ is irreducible over $K(\alpha)$.*

Proof. Let $f_2(\beta) = \alpha$ where $\beta \in \bar{K}$. Then $f_1(f_2(\beta)) = 0$ which means that

$$[K(\beta) : K] \leq \deg(f_1 \circ f_2) = \deg(f_1)\deg(f_2).$$

But, $[K(\beta) : K(\alpha)] \leq \deg(f_2 - \alpha) = \deg(f_2)$. As $[K(\alpha) : K] \leq \deg(f_1)$, it follows that

$$[K(\beta) : K] = [K(\beta) : K(\alpha)][K(\alpha) : K] \leq \deg(f_1)\deg(f_2)$$

with equality holding in the last inequality if, and only if, $[K(\beta) : K(\alpha)] = \deg(f_2)$, and $[K(\alpha) : K] = \deg(f_1)$. In other words, $f_1 \circ f_2$ is irreducible if, and only if, f_1 is irreducible over K and $f_2 - \alpha$ is irreducible over $K(\alpha)$. □

In various special cases, the following elementary observation can be used to prove indecomposability of a polynomial. First, we recall a definition.

For a polynomial $P(x) \in \mathbb{C}[x]$, a complex number c is said to be an *extremum*, if $P(x) - c$ has multiple roots. The *type of c* (with respect to P) is defined to be the tuple $(\mu_1, \cdots, \mu_s)$ of the multiplicities of the distinct roots of $P(x) - c$.

Lemma 6.6. *Let f be any complex polynomial and suppose $f = g \circ h$ for complex polynomials g, h of degrees ≥ 2. Then, if $\alpha \in \mathbb{C}$ is such that $g'(\alpha) = 0$, then the polynomial $h(x) - \alpha$ divides both $f(x) - g(\alpha)$ and $f'(x)$. In particular, if $f(x) \in \mathbb{C}[x]$ satisfies the condition that any extremum $\lambda \in \mathbb{C}$ has the type $(1, 1, \cdots, 1, 2)$, then f is indecomposable over $\mathbb{C}$.*

Proof. The former statement implies the later one. For, it implies that if $f(x) = G_1(G_2(x))$ is a decomposition of $f(x)$ with $\deg G_1, G_2 > 1$, then there exists $\lambda \in \mathbb{C}$ such that $\deg \gcd (f(x) - \lambda, f'(x)) \geq \deg G_2$. But, then the type of λ (with respect to f) cannot be $(1, 1, \cdots, 1, 2)$. So, we prove the former statement. Evidently, for any $\alpha \in \mathbb{C}$, the polynomial $h(x) - \alpha$ divides $f(x) - g(\alpha)$. Moreover, if α is such that $g'(\alpha) = 0$, then consider any root θ of $h(x) - \alpha$. Suppose its multiplicity is a. Then, since the multiplicity of θ in $h'(x)$ is $a - 1$ and since $g'(h(\theta)) = g'(\alpha) = 0$, it follows that $(x - \theta)^a$ divides $f'(x) = g'(h(x))h'(x)$. This completes the proof. □

We remark that the proof shows the following refined version of above lemma holds for polynomials over $\mathbb{Q}$. If $f(x) \in \mathbb{Q}[x]$ is such that each extremum $\lambda \in \bar{\mathbb{Q}}$ of degree $\leq \frac{\deg f}{2} - 1$ has type $(1, 1, \cdots, 1, 2)$, then f is indecomposable over $\mathbb{Q}$. The above observation can be used to verify, for instance, that the polynomials $1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$ are indecomposable (see section 9).

7. Baker and Schinzel-Tijdeman theorems

In general, using Siegel's theorem yields ineffective results. However, for special cases, one might hope for effective results. In 1969, Alan Baker ([1]) considers the equation $f(x) = y^n$ when $n \in \mathbb{Z}$ is fixed. He proves the following theorem,

Theorem 7.1. *(Baker.) Assume that $f(x) \in \mathbb{Q}[x]$ has at least 3 simple roots and $n > 1$, or $f(x)$ has at least 2 simple roots and $n > 2$. Then, the equation $f(x) = y^n$ has only finitely many solutions in $x \in \mathbb{Z}$ and $y \in \mathbb{Q}$; further, the solutions can be effectively computed.*

In 1976, Schinzel & Tijdeman ([27]) proved the following beautiful effective result where n also varies.

Theorem 7.2. *Schinzel-Tijdeman Let $f \in \mathbb{Q}[X]$ have at least two simple roots. Then, there exists an effectively computable constant $N(f)$ such that for any solution of $f(x) = y^n$ in integers x, n and $y \in \mathbb{Q}$, we have $n \leq N(f)$.*

We note that in the above theorems we are sometimes looking more generally allowing some variables to take rational values rather than just integer values.

8. The Bilu-Tichy theorem

As Siegel's theorem is ineffective, it is particularly difficult to use when polynomials depending on parameters are involved in the Diophantine equation. Building on

Fried's work, in 2000, Bilu and Tichy proved a remarkable theorem in which they obtained an explicit finiteness criterion for the equation $f(x) = g(y)$. Before going to the statement of the theorem first let us recall some concepts.

Two decompositions $F(x) = G_1(G_2(x))$ and $F(x) = H_1(H_2(x))$ are called *equivalent* if there exist a linear polynomial $l(x) \in \mathbf{C}[x]$ such that $G_1(x) = H_1(l(x))$ and $H_2(x) = l(G_2(x))$.

The *Dickson polynomial* $D_n(x, a)$ is defined as

$$D_n(x,a) = \sum_{i=0}^{[\frac{n}{2}]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

It has degree n.

In what follows a and b are nonzero elements of some field, m and n are positive integers, and $p(x)$ is a nonzero polynomial (which may be constant).

Definition 8.1. *By a standard pair over a field k, we mean that $a, b \in k$, and $p(x) \in k[x]$. A standard pair*

1. *of the first kind is $(x^u, ax^v p(x)^u)$ or $(ax^v p(x)^u, x^u)$, where $0 \leq v < u$, $(v, u) = 1$ and $v + degp(x) > 0$.*
2. *of the second kind is $(x^2, (ax^2 + b)p(x)^2)$ or $(ax^2 + b)p(x)^2, x^2)$.*
3. *of the third kind is $(D_k(x, a^l), D_l(x, a^k))$ where $(k, l) = 1$. Here D_l is the l-th Dickson polynomial.*
4. *of the fourth kind is $(a^{-l/2} D_l(x, a), b^{-k/2} D_k(x, a))$ where $(k, l) = 2$.*
5. *of the fifth kind is $((ax^2 - 1)^3, 3x^4 - 4x^3)$ or $(3x^4 - 4x^3, (ax^2 - 1)^3)$.*

Bilu & Tichy produced five families of pairs of polynomials such that a general pair (f, g) of polynomials satisfying the two properties: (i) $f(x) - g(y)$ is absolutely irreducible and (ii) $f(X) - g(Y) = 0$ is a curve of genus zero, is a standard pair up to linear changes of the variable. The theorem allows us to consider solutions in rational numbers with bounded denominator. If $F(X, Y) = 0$ is a polynomial in $\mathbb{Q}[X, Y]$, then the equation $F(x, y) = 0$ is said to have infinitely rational solutions with bounded denominators if there exists a constant $C(F)$ such that there are infinitely many rational numbers $x,\ y$ such that $F(x, y) = 0$ and $x, y \in \frac{1}{C(F)}\mathbb{Z}$. Moreover, the Bilu-Tichy theorem showed that each pair (f, g) for which $f(x) = g(y)$ has infinitely many solutions with bounded denominator can be determined from standard pairs. The precise statement of their theorem is as follows.

Theorem 8.2 (Bilu-Tichy)**.** *For non-constant polynomials $f(x)$ and $g(x) \in \mathbf{Q}[x]$, the following are equivalent*

(a) The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.

(b) We have $f = \phi(f_1(\lambda))$ and $g = \phi(g_1(\mu))$ where $\lambda(x), \mu(x) \in \mathbf{Q}[X]$ are linear polynomials, $\phi(x) \in \mathbf{Q}[X]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbf{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.

9. Some applications of the Bilu-Tichy theorem

The theorem is particularly useful when dealing with equations of the form $f(x) = g(y)$ where f and/or g run through families of polynomials depending on certain parameters. We mention some results proved using this theorem and the theorems of Baker and of Schinzel-Tijdeman.

Theorem 9.1 ([5])**.** *Let r be a nonzero rational number which is not a perfect power in $\mathbb{Q}$. Then, the equation $x(x+1)(x+2)\cdots(x+m-1)+r = y^n$ has at most finitely many solutions $(x,\ y,\ m,\ ,n)$ satisfying $(x,\ m,\ n) \in \mathbb{Z}$ and $y \in \mathbb{Q}$, $m,\ n \geq 2$. Moreover, all the solutions can be calculated effectively.*

We may use the Bilu-Tichy theorem to study the finiteness question of solutions of the equation $f_m(x) = g(y)$ for the polynomials $f_m = X(X+1)(X+2)...(X+(m-1))$ where, $m > 2$ and g is a polynomial of degree $n \geq 2$ over $\mathbb{Q}$. We obtain the following precise result.

Theorem 9.2 ([18])**.** *The following holds true.*

(i) Fix $m \geq 3$ such that $m \neq 4$ and let g be an irreducible polynomial in $\mathbb{Q}[X]$. Then, there are only finitely many solutions of the equation $x(x+1)\cdots(x+m-1) = g(y)$ in rational numbers x, y with any bounded denominator.

(ii) If $m = 4$ and g is irreducible in $Q[y]$ then the equation $x(x+1)\cdots(x+m-1) = g(y)$ has infinitely many solutions precisely when $g = \frac{9}{16} + bX^2(X+c) \in \mathbb{Q}[X]$ where $b \in \mathbb{Q}^*, c \in \mathbb{Q}$. Besides these, the above equation has only finitely many solutions.

Interestingly, it turns out that we may bound m by using a simple consequence of the Chebotarev density theorem. The simple consequence we need asserts that an irreducible polynomial over $\mathbb{Q}$ has no roots modulo infinitely many primes. For the sake of completeness, we recall the following general statement.

Chebotarev's density theorem. *Let L/K be a Galois extension of algebraic number fields. Let C be a conjugacy class in the Galois group G. Then, the set of prime ideals P of O_K which are unramified in L and whose Frobenius automorphism Fr_P is in the conjugacy class C, has density $|C|/|G|$.*

We prove the following theorem.

Theorem 9.3. *Assume that $g \in \mathbb{Q}[X]$ is irreducible and that Δ is a positive integer. Then, there exists a constant $C = C(\Delta, g)$ such that for any $m \geq C$, the*

equation $x(x+1)\cdots(x+m-1) = g(y)$ does not have any rational solutions with bounded denominator Δ. Moreover, C can be calculated effectively.

The information about possible decompositions of the polynomial is given by the following computation due to Bilu et al ([2]).

Proposition 9.4. *Let $m \geq 3$ and $f_m(X) = X(X+1)...(X+(m-1))$. Then*
(1). $f_m(X)$ is indecomposable if m is odd, and
(2). if $m = 2k$, then any nontrivial decomposition of $f_m(X)$ is equivalent to $f_m(X) = R_k((X - \frac{m-1}{2})^2)$, where

$$R_k = (X - \frac{1}{4})(X - \frac{9}{4})\cdots(X - \frac{(2k-1)^2}{4}).$$

In particular, the polynomial R_k is indecomposable.

Let us now consider the family of Bernoulli polynomials $B_m(x)$ defined by the generating series

$$\frac{te^{tx}}{e^t - 1} = \sum_{m=0}^{\infty} B_m(x)\frac{t^m}{m!}.$$

Then $B_m(x) = \sum_{i=0}^{m} \binom{m}{i} B_{m-i}x^i$, where $B_r = B_r(0)$ is called the r-th Bernoulli number. They are rational numbers and can be computed from the recursive relation $\sum_{i=0}^{n-1} \binom{n}{i} B_i = 0$. The sum of the n^{th} powers of the first k natural numbers can be expressed as

$$1^n + 2^n + \cdots + x^n = S_n(x) = \frac{B_{n+1}(x+1) - B_{n+1}}{n+1}.$$

Bernoulli polynomials have following very interesting properties ([6]).
(i) $B_n(x) = x^n - \frac{n}{2}x^{n-1} + \frac{n(n-1)}{12}x^{n-2} + \cdots$
(ii) $B'_{n+1}(x) = (n+1)B_n(x)$.
(iii) $B_n(x) = (-1)^n B_n(1-x)$.
(iv) $f(x+1) - f(x) = nx^n \ \ f(x) = B_n(x)$+Constant.
The decomposability of Bernoulli polynomials was investigated in a paper by Bilu, Brindza, Kirschenhofer, Pinter, Schinzel & Tichy with an appendix by Schinzel ([2]). They proved the following proposition.

Proposition 9.5 ((BBKPT))**.** *Let $m \geq 2$. Then*
(i) B_m is indecomposable over $\mathbb{Q}$ if m is odd, and
(ii) if $m = 2k$, then any nontrivial decomposition of B_m is equivalent to $B_m(x) = \phi((x - \frac{1}{2})^2)$ for a unique polynomial ϕ over $\mathbb{Q}$.

For a general $g \in \mathbb{Q}[X]$ we obtain ([19]) the following theorem.

Theorem 9.6. *Let $g \in \mathbb{Q}[X]$ have degree $n \geq 3$ and let $m \geq 3$. The equation $B_m(x) = g(y)$ has only finitely many rational solutions x, y with any bounded denominator apart from the following exceptions.*

(i) $g(y) = B_m(h(y))$ *where* h *is a polynomial over* $\mathbb{Q}$*;*
(ii) m *is even and* $g(y) = \phi(h(y))$*, where* h *is a polynomial over* $\mathbb{Q}$*, whose square-free part has at most two zeroes, such that* h *takes infinitely many square values in* $\mathbb{Z}$ *and* ϕ *is the unique polynomial satisfying* $B_m(x) = \phi((x - \frac{1}{2})^2)$*;*
(iii) $m = 3, n \geq 3$ *odd and* $g(x) = \frac{1}{8(3^{3(n+1)/2})} D_n(\delta(x), 3^3)$*;*
(iv) $m = 4, n \geq 3$ *odd and* $g(x) = \frac{1}{2^{2(n+3)}} D_n(\delta(x), 2^4) - \frac{1}{480}$*;*
(v) $m = 4, n \equiv 2 \bmod 4$ *and* $g(x) = \frac{-\beta^{-n/2}}{64} D_n(\delta(x), \beta) - \frac{1}{480}$.
Here δ *is a linear polynomial over* $\mathbb{Q}$ *and* $\beta \in \mathbb{Q}^*$*. Furthermore, in each of the exceptional cases, there are infinitely many solutions with a bounded denominator.*

Although the above theorem treats a general equation of the form $B_n(x) = g(y)$, it is often possible to obtain more precise results for special g for a more general equation. For instance, consider a polynomial C over $\mathbb{Q}$, and the Diophantine equations of the form

$$aB_m(x) = bB_n(y) + C(y)$$

with $m \geq n >$deg $C + 2$, or of the forms

$$ax(x+1)\cdots(x+m-1) = bB_n(y) + C(y)$$

and

$$ax(x+1)\cdots(x+m-1) + C(x) = bB_n(y)$$

for solutions in integers x, y when a, b are non-zero rational numbers. In these cases, we have the following more precise theorems ([19], [20]).

Theorem 9.7. *For nonzero rational numbers* a, b *and a polynomial* $C \in \mathbb{Q}[X]$*, if* $m \geq n >$ *deg* $C + 2$ *then the equation*

$$aB_m(x) = bB_n(y) + C(y)$$

has only finitely many rational solutions with bounded denominators except when $m = n, a = \pm b$ *and* $C(y) \equiv 0$*. In these exceptional cases, there are infinitely many rational solutions with bounded denominators if, and only if,* $a = b$ *or* $a = -b$ *and* $m = n$ *is odd.*
In particular, if c *is a nonzero constant, then the equation*

$$aB_m(x) = bB_n(y) + c$$

has only finitely many solutions for all $m, n > 2$*.*

Theorem 9.8. *Let* a, b *be nonzero rational numbers. For* $m \geq n > deg(C) + 2$*, the equation*

$$aB_m(x) = by(y+1)\cdots(y+n-1) + C(y)$$

has only finitely many rational solutions with bounded denominator except in the following situations.

(i) $m = n, m+1$ *is a perfect square,* $a = b(\sqrt{m+1})^m$,
(ii) $m = 2n, \frac{n+1}{3}$ *is a perfect square,* $a = b(\frac{n}{2}\sqrt{\frac{n+1}{3}})^n$.

In each case, there is a uniquely determined polynomial C *for which the equation has infinitely many rational solutions with a bounded denominator. Further,* C *is identically zero when* $m = n = 3$ *and has degree* $n-4$ *when* $n > 3$.

Theorem 9.9. *Let* a, b *be nonzero rational numbers. For* $m \geq n > deg(C) + 2$, *the equation*

$$ax(x+1)\cdots(x+m-1) = bB_n(y) + C(y)$$

has only finitely many rational solutions with bounded denominator excepting the following situations when it has infinitely many.

$m = n$, $m+1$ *is a perfect square,* $b = a(\sqrt{m+1})^m$.

In these exceptional situations, the polynomial C *is also uniquely determined to be*

$$C(x) = af_m((\pm\sqrt{m+1})x + \frac{1-m\mp\sqrt{m+1}}{2}) - bB_m(x)$$

and has degree $m-4$.

The next theorem addresses the equations of the form $E_n(x) = g(y)$ where $E_n = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$. Recall lemma 6.5 on the indecomposability of polynomials f whose extrema have the type $(1, 1, \cdots, 1, 2)$. We need to show that E_n has this property for each n. Here is how that is verified.

Proposition 9.10 ([21])**.** *Each extremum of the polynomial*

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$$

has the type $(1, 1, \cdots, 1, 2)$. *In particular,* $E_n(x)$ *is indecomposable for all* n. *Moreover,* E_n *has only simple roots for any* n.

Proof. Note that $E'_{n+1} = E_n$ for any $n \geq 0$. Therefore, it is clear that, for each $n \geq 0$, the roots of E_n are simple, for $E_{n+1}(\alpha) = 0$ implies

$$E'_{n+1}(\alpha) = E_n(\alpha) = E_{n+1}(\alpha) - \alpha^{n+1}/(n+1)! = -\alpha^{n+1}/(n+1)! \neq 0.$$

Now, let λ be a complex number such that $E_{n+1}(x) - \lambda$ has a multiple root α. Then $E_n(\alpha) = 0$ and $\lambda = E_{n+1}(\alpha) = \alpha^{n+1}/(n+1)!$. If β is another multiple root of $E_{n+1}(x) - \lambda$, then $\alpha^{n+1} = \beta^{n+1}$. This implies that there exists $\theta \neq 1$ with $\theta^{n+1} = 1$ such that E_n has two roots $\alpha, \alpha\theta$. We show that this is impossible.

Note that n must be > 1. Let ζ be a primitive $(n+1)$-th root of unity. Then $\theta = \zeta^i$ for some $0 < i \leq n$. It is a well-known result of Schur that E_n is irreducible over $\mathbf{Q}$ and that the Galois group of its splitting field K is A_n or S_n according as to whether 4 divides n or not.

Now, write $K = \mathbf{Q}(\alpha, \alpha\theta, \alpha_3, \cdots, \alpha_n)$ for the splitting field of E_n.

First, let $n \not\equiv 0 \bmod 4$. We shall use the fact that the Galois group contains the n-cycle $\sigma = (\alpha, \alpha\zeta^i, \alpha_3, \cdots, \alpha_n)$.
Since $\sigma(\zeta^i)$ must be a power of ζ, it follows that each α_j with $3 \leq j \leq n$ must be $\alpha\zeta^k$ for some k. Thus, the set $\{\alpha, \alpha\zeta^i, \alpha_3, \cdots, \alpha_n\}$ of all the roots of E_n is the set of all $\alpha\zeta^r$ $(0 \leq r \leq n)$ with one $\alpha\zeta^m$ missing for some $1 \leq m \leq n$.
Now, the sum of the roots of E_n gives

$$-n = \sum_{r \neq m} \alpha\zeta^r = -\alpha\zeta^m.$$

Therefore, $\alpha = n\zeta^{-m}$. The product of all roots of E_n gives

$$(-1)^n n! = \alpha^n \zeta^{n(n+1)/2-m} = n^n \zeta^{n(n+1)/2-m-mn} = n^n \zeta^{n(n+1)/2}.$$

Hence $1 = |\zeta^{n(n+1)/2}| = n!/n^n$, which is impossible for $n > 1$.
Finally, let $4|n$. Then, the Galois group, which is A_n, contains each $(n-1)$-cycle of the form $(\alpha, \alpha\zeta^i, \alpha_{i_1}, \cdots, \alpha_{i_{n-3}})$ where $\alpha_{i_1}, \cdots, \alpha_{i_{n-3}}$ are any $n-3$ among $\alpha_3, \cdots, \alpha_n$. Therefore, each α_j with $3 \leq j \leq n$ is of the form $\alpha\zeta^k$ for some k and, the argument above goes through as it is. This proves the proposition. □

In view of this proposition, we have the following finiteness results for equations of the form $E_n(x) = g(y)$ as an application of the Bilu-Tichy theorem. As noted above, it works slightly more generally for f which have each extremum to be of the type $(1, 1, \cdots, 1, 2)$.

Theorem 9.11 ([21])**.** *Let f, g be polynomials of degrees n, m respectively, with rational coefficients. Suppose each extremum (with respect to f) has type $(1, 1, \cdots, 1, 2)$. Then, for $n, m \geq 3$, the equation $f(x) = g(y)$ has only finitely many rational solutions (x, y) with a bounded denominator except in the following two cases.*
(i) $g(x) = f(h(x))$ for some nonzero polynomial $h(x) \in \mathbb{Q}(x)$,
(ii) $n = 3, m \geq 3$ and $f(x) = c_0 + c_1 D_3(\lambda(x), c^m)$, $g(x) = c_0 + c_1 D_m(\mu(x), c^3)$ for linear polynomials λ and μ over $\mathbb{Q}$ and $c_i \in \mathbb{Q}$ with $c_1, c \neq 0$.
In each exceptional case, there are infinitely many solutions.

10. An observation of Ramanujan

In this last section, we begin with the following wonderful observation due to Ramanujan.

$$2 + (1/2)^2, 2.3 + (1/2)^2, 2.3.5 + (1/2)^2, 2.3.5.7 + (1/2)^2, 2.3.5.7.11.13.17 + (1/2)^2$$

are, respectively, the perfect squares

$$(3/2)^2, (5/2)^2, (11/2)^2, (29/2)^2, (1429/2)^2$$

of rational numbers. The natural question arises as to whether there are other solutions to the equation $p_1 p_2 \cdots p_k + r^2 = y^2$ where r, y are non-zero rational

numbers and p_i's are primes. Diophantine equations seeking prime number solutions are notoriously difficult to solve compared to solutions in arbitrary integers. Wadim Zudilin asked whether for a given non-zero rational number r, the equation

$$1.3.5\cdots(2m-1)+r=y^2$$

has only finitely many solutions in m and y. Here, we show that a stronger finiteness result holds for any arithmetic progression under some conditions on r. Indeed, it can be deduced from an earlier work ([5]) with some modifications; at the time of writing that paper, this question was not asked; otherwise, we could have added the assertions made here. More precisely, we prove the following theorem.

Theorem 10.1. *Let c, d be positive integers and r be a rational number which is not a perfect power such that $v_p(r) = 0$ for each prime p dividing d. The number of 4-tuples (x, y, m, n) with $m > 2$ $(m \neq 4)$, $n > 1$, $x \in \mathbb{Z}$, $y \in \mathbb{Q}$ such that*

$$cx(cx+d)(cx+2d)\cdots(cx+(m-1)d)+r=y^n$$

is finite.

Here, $v_p(r)$ denote the integer power of p dividing the rational number r.

10.1. **A lemma on stationary points.** For positive integers c, d and $m > 2$, consider the polynomial

$$f_m = cX(cX+d)(cX+2d)\cdots(cX+(m-1)d).$$

For a rational number r, we look at the polynomial $f_m + r$ and, for $n > 1$, consider the equation

$$f_m(x)+r=y^n$$

for solutions in integers x and rational numbers y.
Now

$$f_m(x) = cX(cX+d)(cX+2d)\cdots(cX+(m-1)d)$$

clearly satisfies

$$f_m(x) = d^m g_m(\frac{cx}{d}),$$

where

$$g_m(x) = x(x+1)(x+2)\cdots(x+m-1).$$

Therefore, the derivative satisfies

$$f_m'(x) = cd^{m-1}g_m'(\frac{cx}{d}).$$

The following lemma on stationary points of the polynomial g_m is elementary.

Lemma 10.2. *For any complex number a, the set*

$$S(g_m, a) := \{\alpha : g_m'(\alpha) = 0, g_m(\alpha) = a\}$$

has cardinality at most 2 (respectively, at most 1) if m is even (respectively, if m is odd).

Remark. As $f_m(x) = d^m g_m(\frac{cx}{d})$ and $f_m'(x) = cd^{m-1}g_m'(cx/d)$, we have

$$\frac{dS(g_m, a)}{c} = S(f_m, d^m a) \ \forall \ a \in \mathbf{C}.$$

Therefore, cardinality of $S(f_m, b)$ is at the most 2 when m is even and at the most 1 when m is odd.
From this, following can be deduced immediately.

Corollary 10.3. *For each $r \in \mathbb{Q}$, the polynomial $f_m(x) + r$ has at least three simple roots when $m \geq 5$ is odd or if $m > 6$ is even.*

For the smaller cases $m = 3, 4, 6$, we have

Lemma 10.4. *(i) If $m = 3$, then for any $r \in \mathbb{Q}$, the polynomial $f_3(x) + r$ has simple roots. (ii) If $m = 4$, then for any rational number $r \neq d^4, \frac{-9d^4}{16}$, the polynomial $f_4(x) + r$ has distinct roots.*

The polynomial $f_4(x) + d^4$ has two double roots $\frac{d(-3\pm\sqrt{5})}{2c}$.

The polynomial $f_4(x) - 9d^4/16$ has one double root $\frac{3d}{2c}$ and two simple roots $(-3 + \sqrt{10})d/2c, (-3 - \sqrt{10})d/2c$.

(iii) If $m = 6$, the polynomial $f_6(x) + r$ has simple roots if $r \neq (\frac{15d^3}{8})^2$.

The polynomial $f_6(x) + 15^2d^6/8^2$ has one double root $-5d/2c$ and four simple roots $\frac{-5d}{2c} \pm \frac{d}{c}\sqrt{\frac{35\pm8\sqrt{7}}{2\sqrt{3}}}$.

The Schinzel-Tijdeman theorem recalled above implies for the polynomial $f_m(x) = cX(cX + d)(cX + 2d) \cdots (cX + (m - 1)d)$ the following result.

Proposition 10.5. *(i) Let $m > 2$ ($m \neq 4$), $r \in \mathbb{Q}$, and let c, d be positive integers. Then, the equation*

$$f_m(x) + r = y^n$$

has only finitely many solutions in (x, y, n) for $n > 1$, integers x, and rational numbers y.

(ii) If $m = 4$, then for $r \neq d^4, = 9d^4/16$, the equation $f_4(x) + r = y^n$ has only finitely many solutions in x, y, n for $n > 1$.

The equation $f_4(x) - \frac{9d^4}{16} = y^n$ has only finitely many solutions in x, y, n with $n > 2$.

10.2. **Bounding n for given r.** For given $m > 2$ (with $m \neq 4$), $r \in \mathbb{Q}$, we have already seen that there are only finitely many n, x, y such that

$$cx(cx+d)(cx+2d)\cdots(cx+(m-1)d)+r = y^n.$$

Now, we show that n can be bounded in terms of r alone.

Proposition 10.6. *Let $m > 2$ (with $m \neq 4$), let c, d be positive integers and let $r \in \mathbb{Q}$ with $r \neq 0, 1, -1$ and $v_p(r) = 0$ for each prime $p|d$. Then, there exists a constant $C(r)$ depending only on r such that for any integers x and rational number y satisfying*

$$cx(cx+d)(cx+2d)\cdots(cx+(m-1)d)+r = y^n,$$

we have $n \leq C(r)$.

Proof. As $r \neq \pm 1$, there exists a prime p such that $v_p(r) = t \neq 0$. Note by hypothesis that $(p, d) = 1$. If $m \geq p$, one of the integers

$$cx, cx+d, \cdots, cx+(m-1)d$$

is a multiple of p since $(p, d) = 1$. In fact, if $m \geq (t+1)p$ then p^{t+1} divides $f_m(x)$. Thus, $v_p(f_m(x)) \geq t+1$ which means (since $v_p(r) = t$) that

$$v_p(f_m(x)+r) = t = v_p(y^n) = nv_p(y).$$

Hence, for $m \geq (t+1)p$, we have $n \leq |t|$.

Now, the proposition 10.5 shows that there is some constant $C(m)$ depending on m so that for any solution (x, y) of the equation, $n \leq C(m)$. Now, take $C_0(r) = max(C(m) : m < (t+1)p)$ if $t > 0$ and take $C_0(r) = 0$ if $t < 0$. Then, for any solution of

$$cx(cx+d)(cx+2d)\cdots(cx+(m-1)d)+r = y^n$$

we have $n \leq C(r)$ where $C(r) = max(C_0(r), |t|)$. This completes the proof. □

10.3. **Bounding m absolutely.** In this section, we show that m itself is bounded for a solution to exist.

Proposition 10.7. *Let r be any rational number such that $v_p(r) = 0$ for all primes $p|d$ and such that r is not an n-th power. Then, there are only finitely many x, y, m (for $m > 2$, $m \neq 4$) with $f_m(x) + r = y^n$.*

Proof. As r is not an n-th power and $v_p(r) = 0$ for each prime $p|d$, either n is even and $r = -s^n$ or there is a prime p divisor of n such that $v_p(r)$ is not a multiple of n. In the latter case, note that $(p, d) = 1$ by hypothesis. In the former case when n is even and $r = -s^n$, choose a prime number $p \equiv 3 \bmod 4$ such that $v_p(r) = 0$. Then, choosing $m \geq p$, the equality

$$f_m(x) - s^n = y^n$$

shows that $-1 \equiv (y^{n/2})^2 \bmod p$. This is a contradiction. Hence $m < p$ and proposition 10.5 shows finiteness of solutions x, y.

In the latter case, there is a prime p such that $v_p(r) \neq 0$ and is not a multiple of n. Choose $m \geq (v_p(r)+1)p$ if $v_p(r) > 0$ and let m be arbitrary if $v_p(r) < 0$. Then

$$v_p(cx(cx+d)(cx+2d)\cdots(cx+(m-1)d)) \geq v_p(r)+1.$$

Here, we have used the fact that $(p,d) = 1$. This gives

$$v_p(f_m(x)+r) = v_p(r) = nv_p(y)$$

which is a multiple of n, a contradiction to the choice of p.

Hence, $m \leq v_p(r)$ and, once again, proposition 10.5 implies that there are only finitely many solutions in x, y. This completes the proof. □

Combining the propositions 10.6 and 10.7, we have the following main theorem.

Theorem 10.8. *Let r be any rational number such that $v_p(r) = 0$ for all primes $p|d$ and such that r is not a perfect power. Then, there exist only finitely many tuples (m,n,x,y) for $m > 2(m \neq 4), n > 1, x \in \mathbb{Z}, y \in \mathbb{Q}$ such that*

$$cx(cx+d)(cx+2d)\cdots+(cx+(m-1)d)+r = y^n$$

Further, for $m = 4$ and $r \neq d^4, -9d^4/16$, the number of solutions in x, y, n is finite.

Proof. For r as above, the number of $n > 1$'s admitting a solution is bounded by a constant $C(r)$ by proposition 10.6. For each of these finitely many n, proposition 10.7 shows that there are only finitely many (x, y, m) for $m > 2$ (with $m \neq 4$). The last assertion was already noted above. □

We observe here that finiteness of the number of solutions of the equation $f(x)+r = y^n$ for a given rational number r and an integral polynomial f implies finiteness of the number of solutions of a related equation with integer coefficients. We observe:

Proposition 10.9. *Let $f \in \mathbf{Q}[X]$ be a polynomial which takes integer values at all integer points. Let a/b be a non-zero rational number and $n > 1$ be a positive integer. Then, for each solution $x \in \mathbf{Z}, y \in \mathbf{Q}$ of the equation $f(x) + \frac{a}{b} = y^n$ satisfies by$^n = u^n$ for some $u \in \mathbf{Z}$ and $x, u \in \mathbf{Z}$ satisfy the equation $bf(x)+a = u^n$.*

Proof. Start with $x \in \mathbf{Z}, y = \frac{u}{v} \in \mathbf{Q}$ such that

$$f(x) + \frac{a}{b} = y^n = \frac{u^n}{v^n}.$$

While writing the rational numbers a/b and u/v, we may assume that $b, v > 0$. Then

$$bf(x) + a = \frac{bu^n}{v^n}.$$

As v^n divides bu^n, and $(v^n, u^n) = 1$, we have that v^n divides b. Write $c = \frac{b}{v^n}$; then $bf(x) + a = cu^n$. Note that $c > 0$. If $c \neq 1$, look at any prime p dividing c; then $p|b$. So, the equality $bf(x) + a = cu^n$ implies that p divides a, which is a contradiction. Therefore, $b = v^n$ and we have $bf(x) + a = u^n$. □

Remarks. (i) It is not clear if there are only finitely many solutions in integers x, y and $n > 1$ for the equation $bf(x) + a = u^n$ if it is known that there are only finitely many integers x, rationals y and $n > 1$.

(ii) The question as to whether Ramanujan's observations above are the only solutions is a difficult open question. It is hard to tackle equations of the form $f(x) + r = y^n$ when r is a perfect power of a rational number.

Acknowledgements. We would like to thank Shanta Laishram for discussions. We are indebted to Wadim Zudilin who raised the question mentioned in the last section. In fact, during his visit to India, he photographed the observations of Ramanujan recalled in the beginning of this note and sent it to us. Thanks are also due to Yuri Bilu for some correspondence.

References

[1] Baker, A., Bounds for solutions of superelliptic equations, Proc Cambridge Philos. Soc. 65 (1969), 439-444.

[2] Bilu, Y., Brindza, B., Kirschenhofer, P., Pinter, A. and Tichy, R.F. with an appendix by Schinzel, A., Diophantine Equations and Bernoulli Polynomials, Compositio Mathematica 131 (2002), 173-188.

[3] Bilu, Yu. F., Stoll, Th. and Tichy, R. F., Octahedrons with equally many lattice points, Period. Math.Hungar. 40 (2000), 229-238.

[4] Beukers, F., Shorey, T. N. and Tijdeman, R., *Irreducibility of Polynomials and arithmetic progressions with equal product of terms, Number theory in Progress*, (Proc. Internat. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997), de Gruyter 1999, 11-26.

[5] Bilu, Y., Kulkarni, M. and Sury. B., On the Diophantine equation $x(x+1)\cdots(x+m-1)+r = y^n$, Acta Arithmetica, Vol.113 (2004), 303-308.

[6] Brilhart, J., On the Euler and Bernoulli polynomials, J. Reine. Angew. Math 2349 (1969), 45-64.

[7] Davenport, H., Lewsi, D. J. and Schinzel, A., Equations of the form $f(x) = g(y)$, Quart J. Math. Oxford 12 (1961), 304-312.

[8] Ehrenfeucht, A., Kryterium absolutnej nieprzywiedlnosci wielomianow, Prace Mat.2 (1958), 167-169.

[9] Erdős, P. and Selfridge, J. L., The Product of Consecutive integers is never a power, Illinois J. Math. 19 (1975), 292-301.

[10] Faltings. G., Endlichkeitssatze fur abelsche varietaaten uber zahlkorpern, Invent. Math. 73 (1983), 349-366.

[11] Fried, M., The field of definition of function fields and a problem in the reducibility of polynomials in two variables, Illinois J. of Math. 17 (1973), 128-146.

[12] Fried, M., On a Theorem of Ritt and related Diophantine problems, J. Reine Angew. Math. 264 (1974), 40-55.

[13] Fried, M., Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem, Proc. Sympos. Pure Math. 37, Amer. Math. Soc., (1980), 571-601.

[14] Fried, M. and MacRae, R. E., On Curves with separated variables, Math. Ann. 180 (1969), 220-226.

[15] Koblitz, N., *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, Springer-Verlag 1993.

[16] Leveque, W. J., On the equation $Y^m = f(x)$, Acta Arith. 9 (1964), 209-219.

[17] Müller, P., Kronecker conjugacy of polynomials, Trans. Amer. Math. Soc. Vol. 350 (1998), 1823-1850.

[18] Kulkarni, M. and Sury, B., On the Diophantine equation $x(x+1)\cdots(x+m-1) = g(y)$, Indagationes Math. 14 (2003), 35-44.

[19] Kulkarni, M. and Sury, B., Diophantine Equations with Bernoulli Polynomials, Acta Arithmetica 116, no. 1, (2005), 25-34.

[20] Kulkarni, M. and Sury, B., A Class of Diophantine Equations involving Bernoulli Polynomials, Indigationes Mathematicae 16, no. 1, (2005), 51-65.

[21] Kulkarni, M. and Sury, B., $1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} = g(y)$, Proc. of the Intl. Conf. on Diophantine Equations, Tata Institute of Fundamental Research, (2008), 121-134.

[22] Ritt, J. F., Prime and composite polynomials, Trans. Ame. Math. Soc. 23 (1922), 51-66.

[23] Runge, C., Über ganzzahlige lösungen von gleichengn zwischen zwei veränderlichen, J. Angew. Math 100 (1887), 425-435.

[24] Schinzel, A., Selected Topics on Polynomials, The Univ. of Michigan Press, Ann Arbor, 1982.

[25] Shorey, T. N. and Tijdeman, T., Some methods of Erdos applied to finite arithmetic progression, The Mathematics of Paul Erdos, Algorithms Combin 13 (1997), 251-267.

[26] Siegel, C. L., Uber einige Anwendungen Diophantischer Approximationen, Abh. Preuss. Akad. Wiss. Phys-Math. Kl, 1929, Nr.1.

[27] Schinzel, A. and Tijdeman, R., On the equation $y^m = P(x)$, Acta Arith. 31 (1976), 199-204.

[28] Tverberg, H. A., A study in irreducibility of polynomials, Ph D Thesis, Dept of Math., Univ. of Begen, 1968.

Manisha Kulkarni
International Institute of Information Technology
26 C, Electronics City, Hosur Road, Bangalore-560100, India
E-mail: *manisha.shreesh@gmail.com*

B. Sury
Statistics & Mathematics Unit, Indian Statistical Institute
8th Mile Mysore Road, Bangalore-560 059, India
E-mail: *sury@ms.isibang.ac.in*