How to solve $f(x) = g(y)$ in integers

B.Sury
Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in
24th May 2011
St.Petersburg, Russia

Introduction

The subject of Diophantine equations is an area of mathematics where solutions to very similar-looking problems can vary from the elementary to the deep. Problems are often easy to state, but it is usually far from clear whether a given one is trivial to solve or whether it must involve deep ideas.

In the present day, the topic is understood more widely as that of considering polynomial equations with integer or rational coefficients for which one seeks integer or rational solutions. Even the type of mathematical tools used varies drastically for equations which seem similar on the first glance.

Some Examples.

• The Congruent Number Problem.
A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.
Equivalently Can we have an *arithmetic progression* of three terms which are all squares of rational numbers and the common difference d?
That is, $x^2 - d, x^2, x^2 + d$ comprised of squares of rational numbers where x is rational?

Indeed, Let $u \leq v < w$ be the sides of a right triangle with rational sides. 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 rational legs, area $(z^2 - y^2)/2 = d$ and rational hypotenuse $2x$ because $2(y^2 + z^2) = 4x^2$.

• For example, $5, 6, 7$ are congruent numbers.
To see these, consider the following three right-angled triangles:
with sides $3/2, 20/3, 41/6$ with area 5,
with sides $3, 4, 5$ with area 6,
with sides $35/12, 24/5, 337/60$.

• $1, 2, 3$ 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 are 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.

Here is an amusing way of using the above fact that 1 is not a congruent number to show that $\sqrt{2}$ is irrational!
Indeed, consider the right-angled triangle with legs $\sqrt{2}, \sqrt{2}$ and hypotenuse 2. If $\sqrt{2}$ were rational, this triangle would exhibit 1 as a congruent number!

Though it is an ancient problem to determine which natural numbers are congruent, it is only in late 20th century that substantial results were obtained and progress has been made which is likely to lead to its complete solution.

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.

In a nutshell, here is the reason we got this elliptic curve. The real solutions of the equation $a^2 + b^2 = c^2$ defines a surface in 3-space and so do the real solutions of $\frac{1}{2}ab = d$. The intersection of these two surfaces is a curve whose equation in suitable co-ordinates is the above curve.

The set of rational solutions of an elliptic curve over $\mathbf{Q}$ 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.

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*, Stephens showed this provides a complete characterization of congruent numbers.

Another example is the question:

• *Which (are there infinitely many?) 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 $x, y > 1; m, n > 2$.

For example 31 and 8191 have this property;

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

(Observed by Goormaghtigh nearly a century ago).
However, it is still unknown whether there are only finitely many solutions in x, y, m, n. In fact, no other solutions are known.

For any *fixed bases* x, y, it was proved only as recently as in 2002 that the number of solutions for m, n is at the most 2. The basic technique used here is *Baker's method of linear forms in logarithms* from transcendental number theory.

Another problem is:

• *Can one have different finite arithmetic progressions with the same product?*

Note that

$$2.6 \cdots (4n-2) = (n+1)(n+2) \cdots (2n)$$

for all natural numbers n.

Are there other solutions to the equation

$$x(x+d_1) \cdots (x+(m-1)d_1) = y(y+d_2) \cdots (y+(n-1)d_2)$$

where d_1, d_2 are positive rational numbers and $d_1 \neq d_2$ if $m = n$?

It is only in 1999 that using ideas from *algebraic geometry*, it was proved that if m, n, d_1, d_2 are fixed, then the equation has only finitely many solutions in integers apart from some exceptions which occur when $m = 2, n = 4$.

Erdös conjectured in 1975 that for each $c \in \mathbb{Q}$, the number of (x, y, m, n) satisfying

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

with $y \geq x+m$, $\min(m,n) \geq 3$, is finite. This is unsettled as yet.

On the other hand, the question as to whether a product of k consecutive numbers (where $k \geq 3$) could be a perfect power was settled in 1975 by Erdös & Selfridge who proved that this could never be so.

They used a classical theorem due to Sylvester which asserts that any set of k consecutive numbers with the smallest one $> k$ contains a multiple of a prime $> k$.
The special case of this when the numbers are $k+1, \cdots, 2k$ is known as Bertrand's postulate. Therefore, this equation is comparatively elementary to solve.

We indicate how the proof goes basically for 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 the 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

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

a contradiction.
Finally, one easily bounds the product $a_1 a_2 \cdots a_k$ below by the product of the first k square-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.

The title of our talk mentions Diophantine equations of the form $f(x) = g(y)$.
The reason is that questions on counting often involve finding integer solutions of equations of the form $f(x) = g(y)$ for integral polynomials f, g.
For instance, suppose we are 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. When $m > n \geq 2$, the above equation turns out to have only finitely many integral solutions.

To give another natural example, for fixed but distinct natural numbers m, n, a natural question is how often $\binom{x}{m} = \binom{y}{n}$ or, more generally, whether the Diophantine equation $a\binom{x}{m} + b\binom{y}{n} = c$ for some integers a, b, c with $ab \neq 0$, has only finitely many integer solutions.
It can be proved more generally that if $a, b, c \in \mathbb{Q}$ and $ab \neq 0$, then for $m > n \geq 3$, the above equation has only finitely many integral solutions x, y.

One more result of this kind 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 $a, b, c \in \mathbb{Q}$ and $ab \neq 0$ and $m > n \geq 4$ has only finitely many solutions in integers x, y.
Note that this is false for Chebychev polynomials $T_n(x)$ defined as $T_n(\cos\theta) = \cos(n\theta)$ because $T_m(x) = T_n(y)$ when $x = T_n(z), y = T_m(z)$ for any z!

A method for $y^n = f(x)$

For equations of the form $y^n = f(x)$, Baker's methods suffice to give the following results (due to Baker and to Schinzel & Tijdeman) which we shall use:

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 $f(x) = y^n$ has infinitely many solutions in $x \in \mathbb{Z}$ and $y \in \mathbb{Q}$, and the solutions can be effectively computed.

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial having at least 2 distinct roots. Then there exists an effective constant $N(f)$ such that any solution of $f(x) = y^n$ in $x, n \in \mathbb{Z}$, $y \in \mathbb{Q}$ satisfies $n \leq N(f)$.

Erdös-Selfridge translated

After Erdös-Selfridge's result, it is a natural problem to study $x(x+1)(x+2)...(x+(m-1))+r=y^n$ for $r \in \mathbb{Q}^*$.
Note that the method of Erdös-Selfridge fails for these equations.

With Yuri Bilu and a postdoctoral visitor Kulkarni, I proved :
Theorem. For $r \in \mathbf{Q}^*$ which is not a perfect power, the equation $x(x+1)(x+2)...(x+(m-1))+r=y^n$ has only finitely many solutions (x,y,m,n) with $x,m,n \in \mathbb{Z},\ y \in \mathbf{Q},\ m,n>1$.
Moreover, all the solutions can be explicitly determined.

Later, Kulkarni and I extended this theorem (non-effectively) to the equation $x(x+1)\cdots(x+(m-1))=g(y)$, where $g(y)$ is an arbitrary irreducible polynomial.

The Theorem is deduced from three particular results which we prove.

First of all, let us note two infinite series of solutions which occur for two special values of r.
For $r = 1/4$ we have the solutions

$$x \in \mathbb{Z}, \quad y = \pm(x + 1/2), \quad m = n = 2. \tag{1}$$

For $r = 1$ we have infinitely many solutions

$$x \in \mathbb{Z}, \quad y = \pm(x^2 + 3x + 1), \quad m = 4, \quad n = 2. \tag{2}$$

In the following theorem m is fixed, and we solve the above equation in x, y, n.

Theorem 2. Let r be a non-zero rational number and $m > 1$ be an integer.

1. Assume that $(m, r) \notin \{(2, 1/4), (4, 1)\}$. Then the equation has at the most finitely many solutions (x, y, n) satisfying

$$x, n \in \mathbb{Z}, \quad y \in \mathbb{Q}, \quad n > 1, \tag{3}$$

   and all the solutions can be explicitly determined.

2. Assume that $(m, r) = (2, 1/4)$ or $(m, r) = (4, 1)$. Then, besides the above infinite classes of solutions, the equation has at most finitely many solutions (x, y, n) satisfying the conditions $x, n \in \mathbb{Z}, \quad y \in \mathbb{Q}, \quad n > 1$, and all these solutions can be explicitly determined.

The theorem implies that n is bounded in terms of m and r. It turns out that, when $r \neq \pm 1$, it is bounded in terms of r only. Indeed, we have:

Theorem 3. Let r be a rational number distinct from 0 and ± 1. Then there exists an effective constant $C(r)$ with the following property. If (x, y, m, n) is a solution, then $n \leq C(r)$.

Now, let us change the roles : n is fixed, m is variable.

Theorem 4. Let r be a non-zero rational number and $n > 1$ an integer. Assume that r is not an n-th power in $\mathbb{Q}$. Then, the equation has at the most finitely many solutions (x, y, m) satisfying

$$x, m \in \mathbb{Z}, \quad y \in \mathbb{Q}, \quad m > 1, \tag{4}$$

and all the solutions can be explicitly determined.

Proofs of Bilu-Kulkarni-Sury theorems

The first theorem is an immediate consequence of the others.

Indeed, assume that r is not a perfect power.
The second theorem implies that n is effectively bounded in terms of r.
In particular, we have finitely many possible n.
The third theorem implies that for each n there are at most finitely many possibilities of (x, y, m).
This proves the first theorem.

Remark. It is interesting to compare the equation

$$x(x+1)(x+2)...(x+(m-1))+r=y^n$$

with the classical equation of Catalan $x^m-y^n=1$ which has been solved by Mihăilescu. However, much less is known about the equation $x^m-y^n=r$ for $r\neq\pm1$. Just to the contrary, for our equation, the case $r=\pm1$ seems to be the most difficult.

Let us put $f_m(x) = x(x+1)\cdots(x+m-1)$.

Proposition. Let λ be a complex number. Then the polynomial $f_m(x) - \lambda$ has at least 2 simple roots if $(m, \lambda) \notin \left\{(2, -1/4), \left(3, \frac{\pm 2}{3\sqrt{3}}\right), (4, -1)\right\}$. It has at least three simple roots if $m > 2$ and $(m, \lambda) \notin \left\{\left(3, \pm 4/3\sqrt{3}\right), (4, -1), (4, 9/16), \left(6, 16(10 \pm 7\sqrt{7})/27\right)\right\}$.

Sketch of Proof.

By the Theorem of Rolle, $f_m'(x)$ has $m-1$ distinct real roots. Hence $f_m(x) - \lambda$ may have roots of order at most 2.

It can be proved that for even m at most 2 double roots are possible, and for odd m only one double root may occur.

It follows that for $m \notin \{2, 3, 4, 6\}$ the polynomial $f(x) - \lambda$ has at least 3 simple roots.

We are left with $m \in \{2, 3, 4, 6\}$. Since the polynomial $f(x) - \lambda$ has multiple roots if and only if λ is a stationary value of the polynomial $f(x)$ (that is, $\lambda = f(\alpha)$ where α is a root of $f'(x)$), it remains to determine the stationary values of each of the polynomials f_2, f_3, f_4 f_6 and count the simple roots of corresponding translates. The details are routine.

Corollary.

Let r be a non-zero rational number. The polynomial $f_m(x) + r$ has at least 2 simple roots if $(m, r) \notin \{(2, 1/4), (4, 1)\}$. It has at least three simple roots if $m > 2$ and $(m, r) \notin \{(4, 1), (4, -9/16)\}$.

Proof of the second theorem.

Corollaries above imply that the theorem is true if $m > 2$ and $(m, r) \notin \{(4, 1), (4, -9/16)\}$.

It remains to consider the cases $m = 2$ and $(m, r) \in \{(4, 1), (4, -9/16)\}$.

Case 1 : $m = 2$, $r \neq 1/4$

In this case $f_2(x) + r$ has two simple roots, and Corollary above implies that $f_2(x) + r = y^n$ has at most finitely many solutions with $n > 2$ (and these solutions can be explicitly determined). We are left with the equation $x(x+1) + r = y^2$, which is equivalent to the equation $(x + 1/2 + y)(x + 1/2 - y) = 1/4 - r$, having finitely many solutions.

Case 2 : $m = 2$, $r = 1/4$

In this case we have the equation $(x + 1/2)^2 = y^n$. It has infinitely many solutions given as above and no other solutions. Indeed, if (x, y, n) is a solution with $n > 2$ then $x + 1/2$ is a perfect power, which is impossible because its denominator is 2.

Case 3 : $m = 4,\ r = 1$

In this case we have the equation $\left(x^2 + 3x + 1\right)^2 = y^n$. It has infinitely many solutions given as above and only finitely many other solutions, all of which can be explicitly determined.

Indeed, let (x, y, n) be a solution with $n > 2$.
If n is odd, then y is a perfect square: $y = z^2$ and $x^2 + 3x + 1 = \pm z^n$.
Since $x^2 + 3x + 1$ has two simple roots, the latter equation has only finitely many solutions with $n \geq 3$.

If $n = 2n_1$ is even then $x^2 + 3x + 1 = \pm y^{n_1}$, which has finitely many solutions with $n_1 \geq 3$.
We are left with $n = 4$, in which case $x^2 + 3x + 1 = \pm y^2$.
Equation $x^2 + 3x + 1 = y^2$ is equivalent to
$(2x + 3 + 2y)(2x + 3 - 2y) = 5$, which has finitely many solutions.
Equation $x^2 + 3x + 1 = -y^2$ is equivalent to $(2x + 3)^2 + 4y^2 = 5$, which has finitely many solutions as well.

Case4 : $m = 4$, $r = -9/16$

In this case we have the equation $(x + 3/2)^2(x^2 + 3x - 1/4) = y^n$.
Since its left-hand side has 2 simple roots, this equation has only finitely many solutions with $n > 2$.
We are left with the equation $(x + 3/2)^2(x^2 + 3x - 1/4) = y^2$, which is equivalent to the equation $16(x^2 + 3x + 1 - y)(x^2 + 3x + 1 + y) = 25$, having only finitely many solutions.

The proofs of both theorems 3 and 4 rely on the following simple proposition.
First recall that if α is a non-zero rational number and p a prime number, then $\mathrm{ord}_p(\alpha)$ is the integer t such that $p^{-t}\alpha$ is a p-adic unit.

Proposition.

Let p be a prime number and $t = \mathrm{ord}_p(r)$. Then for any solution (x, y, m, n), one has either $m < (t+1)p$ or $n|t$.

Proof.

Assume that $m \geq (t+1)p$. Then $\mathrm{ord}_p\big(x(x+1)(x+2)...(x+(m-1))\big) \geq t+1$. Hence

$$\mathrm{ord}_p\big(x(x+1)(x+2)...(x+(m-1))+r\big) = t,$$

that is, $\mathrm{ord}_p(y^n) = t$, which implies that $n|t$.

Proof of the third theorem.

Since $r \neq \pm 1$, there exists a prime number p such that $t = \mathrm{ord}_p(r) \neq 0$. Theorem above implies that for every $m > 1$ there exists an effective constant $N(m)$ such that for any solution, we have $n \leq N(m)$. Put $C'(r) = \max\{N(m) : 2 \leq m < (t+1)p\}$ if $t > 0$ and $C'(r) = 0$ if $t < 0$. Then $n \leq C'(r)$ when $m < (t+1)p$, and $n \leq |t|$ by the above Proposition when $m \geq (t+1)p$. Thus, in any case $n \leq C(r) := \max\{C'(r), t\}$.

Proof of the fourth theorem.

The proof splits into two cases.

Case 1: there is a prime p such that n does not divide $t = \mathrm{ord}_p(r)$ In this case Proposition above implies that $m \leq (t+1)p$. Also, $(n, r) \notin \{(2, 1/4), (4, 1)\}$, because in both these cases r is an n-th power. Now Theorem above implies that we may have only finitely many solutions.

Case 2: n is even and $r = -r_1^n$, where $r_1 \in \mathbb{Q}$ Write $z = (y/r_1)^{n/2}$.
Let p be prime number congruent to $3 \bmod 4$ and such that $\mathrm{ord}_p(r) = 0$.
If $m \geq p$ then

$$\mathrm{ord}_p\left(1 + z^2\right) = \mathrm{ord}_p\left(r^{-1}x(x+1)\cdots(x+m-1)\right) > 0,$$

which implies that -1 is a quadratic residue $\bmod p$, a contradiction.
Thus, $m < p$ and Theorem again implies that we may have only finitely many solutions.

However, the methods used in the above theorems do not work even for the general equation of the form $x(x+1)\cdots(x+m-1) = g(y)$ and different ideas are required. We discuss one technique which has proved very useful for these equations as well as for many others in recent times. Many results on equations of the form $f(x) = g(y)$ appearing in the last decade have been made possible by a beautiful theorem of Bilu & Tichy to be recalled below.

Siegel's theorem

To motivate the basic approach and statement of Bilu-Tichy's theorem, let us start more generally, for a polynomial $F(x, y) \in \mathbb{Z}[x, y]$.
Basic problem: Determine if $F(x, y) = 0$ has only finitely many solutions with x, y in $\mathbb{Z}$.

When $F(x, y)$ is absolutely irreducible, Siegel's celebrated 1929 theorem shows the finiteness of the number of integer solutions except when the (projective completion of the) curve defined by $F(x, y) = 0$ has genus 0 and at most 2 points at infinity.

Siegel's theorem generalizes also to S-integers in algebraic number fields but is, unfortunately, *ineffective*.

Bilu-Tichy's remarkable theorem produces a set $\mathcal{F}$ of five families of pairs of polynomials (called standard pairs) over $\mathbb{Q}$, such that any pair (f, g) of polynomials over $\mathbb{Q}$ for which the curve $f(x) = g(y)$ has genus zero and at most two points at infinity, is a pair in $\mathcal{F}$ up to a linear change of variables. Moreover, they show that each pair (f, g) for which $f(x) = g(y)$ has infinitely many solutions can be determined from standard pairs.

Curves $f(X) = g(Y)$

To determine finiteness, or otherwise, of the integral solutions of any given $F(x, y) = 0$ using Siegel's theorem, one proceeds along the following steps:

- Split $F(x, y)$ into irreducible factors in $\mathbb{Q}[x, y]$.
- For each factor which is irreducible over $\mathbb{Q}$, find the genus and the number of points at infinity.
- For each of those factors which have genus 0 and ≤ 2 points at infinity, try to determine whether the number of integral solutions is finite or not.

In several of the classical problems, $F(x, y)$ has the special form $f(x) - g(y)$. In this case, there are nice results answering the sub-problems which rise while attempting to apply Siegel's theorem.

For instance, Ehrenfeucht (1958) proved : *If (deg f , deg g) = 1, then* $f(X) - g(Y)$ *is irreducible.*

There are some cases when one can observe that $f(X) - g(Y)$ is reducible. For instance, note that if f, g, F are arbitrary polynomials with deg $F > 0$, then $f_1(X) - g_1(Y)$ is a factor of $f(X) - g(Y)$ where $f(X) = F(f_1(X))$ and $g(Y) = F(g_1(Y))$.

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 $T_n(2\cos x) = 2\cos nx$:
$T_n(x) + T_n(y) = \prod_{k\ odd}(x^2 - 2xy\cos \pi k/n + y^2 - \sin^2 \pi k/n)$ for n even and
$T_n(x) + T_n(y) = (x+y)\prod_{k\ odd, k<n}(x^2 - 2xy\cos \pi k/n + y^2 - \sin^2 \pi k/n)$ for n odd.

Davenport, Fried, Lewis, Runge, Schinzel and Siegel have made fundamental contributions to the question of irreducibility of $f(X) - g(Y)$.

Fried had made a deep study of the factors of $f(X) - g(Y)$.
He proved in 1973 that given $f, g \in \mathbf{Q}[X]$, there are f_1, f_2, g_1, g_2 in $\mathbf{Q}[X]$ such that :
(i) $f(X) = f_1(f_2(X)), g(X) = g_1(g_2(X))$,
(ii) 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
(iii) the irreducible factors of $f_1(X) - g_1(Y)$ are in bijection with irreducible factors of $f(X) - g(Y)$ under the correspondence

$$F_1(X, Y) \mapsto F_1(f_2(X), g_2(Y)).$$

Here is a simple way of computing the genus of the curve $f(X) - g(Y)$ using the Riemann-Hurwitz formula.

Let $f, g \in \mathbf{C}[X]$ have degrees m, n respectively. Suppose $f(X) - g(Y)$ is irreducible. Assume that the stationary points of f and g are all simple. For a stationary point α of f, let r_α denote the number of stationary points β of g such that $g(\beta) = f(\alpha)$. Then, the genus is

$$\frac{1}{2}\sum_{\alpha \in S_f}(n - 2r_\alpha) - \frac{m}{2} + 1 - \frac{(m,n)}{2}$$

where the sum is over the set S_f of stationary points of f.

Let us see how useful this is by means of the following simple example. Consider any $\lambda \in \mathbb{C}^*$ and the equation

$$x(x+1) = \lambda y(y+1)(y+2).$$

If $f(X) = X(X+1), g(Y) = Y(Y+1)(Y+2)$, then

$$S_f = \{-1/2\}, S_g = \{-1 \pm 1/\sqrt{3}\}.$$

$$g(-1 \pm 1/\sqrt{3}) = \pm 2\sqrt{3}\lambda/9 = f(-1/2) = -1/4$$

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

$$x(x+1) = \lambda y(y+1)(y+2)$$

has only finitely many integral solutions unless $\lambda = \pm 3\sqrt{3}/8$.

Decomposition of polynomials

In order to state the theorem of Bilu & Tichy, we need to recall a definition and some properties ensuing from it.

A *decomposition* of a polynomial $F(X) \in K[X]$ over a field K, is an equality of the form $F(X) = G_1(G_2(X))$, where $G_1(X), G_2(X) \in K[X]$.
The decomposition is called *nontrivial* if deg $G_1 > 1$, deg $G_2 > 1$.
Two decompositions $F(X) = G_1(G_2(X))$ and $F(X) = H_1(H_2(X))$ are called *equivalent* over K if there exist a linear polynomial $l(X) \in K[X]$ such that $G_1(X) = H_1(l(X))$ and $H_2(X) = l(G_2(X))$.
The polynomial called *decomposable* if it has at least one nontrivial decomposition, and is *indecomposable* otherwise.

Capelli lemma and Ritt theorems

Before stating the Bilu-Tichy theorem, we recall some very early results on compositions of polynomials due to Capelli (who discovered the Frattini argument in group theory) and to Ritt.

Capelli lemma. For polynomials f, g over a field K, the polynomial $f \circ g$ is irreducible if and only if f is irreducible over K and, for each root α of f, the polynomial $g(x) - \alpha$ is irreducible over $K(\alpha)$.

Ritt's first theorem. Let $f_1 \circ f_2 \circ \cdots f_r = g_1 \circ g_2 \circ \cdots g_s$ where $f_i, g_j \in \mathbf{C}[X]$ be nontrivial decompositions into indecomposables. Then, $r = s$ and the sets of degrees $\{deg(f_1), \cdots, deg(f_r)\} = \{deg(g_1), \cdots, deg(g_s)\}$.

Ritt's second theorem. let $f_1 \circ g_1 = f_2 \circ g_2$ be two proper decompositions over $\mathbf{C}$ where $deg(f_1) = deg(g_2)$ is relatively prime to $deg(g_1) = deg(f_2)$. Then, either

$$f_1(X) = X^r P(X)^s = g_2(X) \ , \ g_1(X) = f_2(X) = X^s$$

or

$$f_1(X) = g_2(X) = D_m(X) \ , \ g_1(X) = f_2(X) = D_n(X)$$

where $D_n(X)$ is the Dickson polynomial of degree n defined by

$$D_n(X + 1/X) = X^n + 1/X^n.$$

Bilu-Tichy theorem

If f, g are polynomials in $\mathbb{Q}[X]$, then the equation $f(x) = g(y)$ is said to have infinitely many rational solutions *with a bounded denominator* if there is an integer N such that there are infinitely many rational solutions x, y with $Nx, Ny \in \mathbb{Z}$.

Theorem (Bilu & Tichy) 2000

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

Standard Pairs (f_1, g_1)

First kind :

$$(X^t, aX^r p(X)^t) \quad or \quad (aX^r p(X)^t, X^t)$$

where $0 \leq r < t$, $(r, t) = 1$ and $r + deg\ p(X) > 0$.
Second kind :

$$(X^2, (aX^2 + b)p(X)^2) \quad or \quad ((aX^2 + b)p(X)^2, X^2).$$

Third kind :

$$(D_k(X, a^t), D_t(X, a^k))$$

where $(k, t) = 1$. Here the Dickson polynomial

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

Fourth kind:

$$(a^{-t/2} D_t(X, a), -b^{-k/2} D_k(X, b))$$

where $(k, t) = 2$.
Fifth kind :

$$((aX^2 - 1)^3, 3X^4 - 4X^3) \quad or \quad (3X^4 - 4X^3, (aX^2 - 1)^3).$$

Kulkarni & S used Bilu Tichy's theorem to study the equation $f_m(x)=g(y)$ where $f_m(X)=X(X+1)\cdots(X+m-1)$. Before stating some of the results, let us note that one needs to find all possible decompositions of f_m. This is quite easy and one has :

Let $m\geq 3$ and $f_m(X)=X(X+1)...(X+(m-1))$. Then,
(i) $f_m(X)$ is indecomposable if m is odd and,
(ii) 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.

Theorem

(Kulkarni, S)
Suppose $f_m(x) = g(y)$ *has infinitely many rational solutions* $x,\ y$ *with a bounded denominator. Then we are in one of the following cases:*

1. $g(y) = f_m(g_1(y))$ *for some* $g_1(y) \in \mathbf{Q}[\mathbf{Y}]$.

2. m *is even and* $g(y) = \phi(g_1(y))$ *where* $\phi(X) = (X - (\frac{1}{2})^2)(X - (\frac{3}{2})^2) \cdots (X - (\frac{(m-1)}{2})^2)$ *and* $g_1(y) \in \mathbf{Q}[\mathbf{Y}]$ *is a polynomial whose square-free part has at most two zeroes.*

3. $m = 3$ *and* g *of any degree* $n \geq 3$ *when* $g(X) = \frac{1}{3^{3(n+1)/2}} D_n(\mu(X), 3^3)$ *and* $\mu(X)$ *is a linear polynomial over* $\mathbf{Q}$.

4. $m = 4$ *and* $g(y) = \frac{9}{16} + b\ \delta(y)^2$ *where* δ *is a linear polynomial.*

Theorem

Assume that $g(y)$ is an irreducible polynomial in $\mathbb{Q}[y]$. Then there exists a constant $C = C(g)$ such that for any $m > C$, there does not exist any $x, \quad y \in \mathbb{Z}$ satisfying $f_m(x) = g(y)$. Moreover, C can be calculated effectively.

Proof.

Let n be the degree of g. Write $g(X) = g_1(X)/\Lambda$ for some non-zero integer Λ and an irreducible, integral polynomial g_1. Assume that $f_m(x) = g(y)$ has a rational solution (x, y) with bounded denominator Δ where Δ is a positive integer. Since g_1 is irreducible, Chebotarev density theorem guarantees the existence of infinitely many primes p such that g_1 has no roots modulo p. Choose such a prime p which does not divide $\Lambda\Delta$. We claim that $m < p$. Suppose, if possible, $m \geq p$. Write $x = x_0/d, y = y_0/d_1$ with x_0, y_0, d, d_1 integers with d, d_1 dividing Δ.Then

$$\Lambda x_0(x_0 + d) \cdots (x_0 + (m-1)d) = d^m g_1(y_0/d_1).$$

Clearing the denominator on the right hand side, we get

$$d_1^n \Lambda x_0(x_0 + d) \cdots (x_0 + (m-1)d) = d^m h(y_0)$$

for an integral polynomial h. As $m \geq p$, the left hand side is a multiple of p; as $p \not| d$, we get $p|h(y_0)$. Since $h(X) = d_1^n g_1(X/d_1)$ and $p \not| d_1$, we have $p|g_1(z_0)$ for some integer z_0 (indeed, $d_1 z_0 \equiv y_0 \bmod p$ would do). This contradicts the choice of p. Thus, one may take $C = p$ as above.

Sums of powers

Let us now consider the Bernoulli polynomials $B_n(x)$ defined by the generating series

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

Then, $B_n(x) = \sum_{i=0}^{n} \binom{n}{i} B_{n-i}x^i$ where $B_r = B_r(0)$ is the r-th Bernoulli number. In fact, B_r are rational numbers defined recursively by $B_0 = 1$ and $\sum_{i=0}^{n-1} \binom{n}{i} B_i = 0$ for all $n \geq 2$. The odd Bernoulli number $B_r = 0$ for r odd > 1 and the first few are :

$$B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_4 = -1/30.$$

The Bernoulli polynomials B_n are related to the sums of n-th powers of the first few natural numbers as follows. For any $n \geq 1$, the sum $1^n + 2^n + \cdots + k^n$ is a polynomial function $S_n(k)$ of k and $S_n(x) = \frac{B_{n+1}(x+1)-B_{n+1}}{n+1}$.

The decomposition of Bernoulli polynomials has been investigated by Y. Bilu, B. Brindza, P. Kirschenhofer, A.Pintér and R.F. Tichy - they prove :

Theorem.

Let $m \geq 2$. Then,

(i) B_m is indecomposable 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 $\mathbb{Q}$.

It is natural to ask if $S_n(x) = S_m(y)$ has solutions when $m \neq n$.
Note that the polynomials $B_n(X) = \pm B_n(1 - X)$ which give infinitely many solutions to $B_n(x) = B_n(y)$.
More generally, we have:

Theorem

(Kulkarni, S)
For $C(T) \in \mathbb{Q}[T]$ and $m \geq n > \deg C + 2$, the equation

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

has only finitely many rational solutions with a bounded denominator unless $m = n, a = \pm b$ and $C \equiv 0$.
Inparticular, for all $m, n > 2$ and any $c \in \mathbb{Q}^*$, the equation

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

has only finitely many rational solutions with a bounded denominator.

Theorem

(Kulkarni, S)
Let $f_n(x) = x(x+1)\cdots(x+n-1)$. *For* $m \geq n > deg(C) + 2$, *the equation*

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

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

(Kulkarni, S)
For $m \geq n > deg(C) + 2$, the equation

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

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 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 $m - 4$.

Theorem.

Let $g(y) \in \mathbb{Q}[y]$ 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 such that $B_m(x) = \phi((x - \frac{1}{2})^2)$.

(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 $g(x) = \frac{1}{2^{2(n+3)}} D_n(\delta(x), 2^4) - \frac{1}{480}$.

(iv) $m = 4, n \equiv 2 \bmod 4$ 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.

The proof of our finiteness result uses (apart from the Bilu-Tichy theorem, of course) special properties of the Bernoulli polynomials. For instance, it is known (due to Brillhart and Inkeri) that the Bernoulli polynomial B_m has only simple roots if $m > 3$ is odd, and has no rational roots if $m > 2$ is even. Instead of going through all details of the proof, we just give a sample of the proof.
One of the cases leads to an equation of the form

$$B_m(rx + s) = \phi_0 + \phi_1 a x^r p(x)^3$$

where $m = 3d + r$ with $r = 1$ or 2. We will rule this out as follows.

If $r = 2$, then $B_m(ux + v) = \phi_0 + \phi_1 a x^2 p(x)^3$. By taking the derivative, it follows that mB_{m-1} has at least one rational root. But we know that, if B_k has a rational root then k must be odd by Inkeri's result quoted above. In our case, this gives a contradiction since $m - 1$ is even.
Let $r = 1$. Then $B_m(x) - \phi_0 = \lambda(x)p(x)^3$ for a linear polynomial $\lambda(x)$ and a polynomial $p(x)$ of degree $(m - 1)/3$ over $\mathbb{Q}$. As every root of $p(x)$ is a multiple root of $B_m(x) - \phi_0$ with multiplicity ≥ 3, such a root is also a root of $B_{m-1}(x)$ and of $B_{m-2}(x)$.

From this discussion, it follows that p has no rational roots (since this is true for B_{m-1}), and all its roots are simple (since this is true for B_{m-2}). We show now that it is impossible for an equality

$$B_m(x) - \phi_0 = \lambda(x)p(x)^3$$

of polynomials to hold where λ is linear and $B_m(\alpha) = \phi_0$ and $B_{m-1}(\alpha) = 0$.

To show this, we note that $x = 0, \frac{1}{2}, 1$ are zeroes of $B_m(x)$. Hence, writing $\lambda(x) = c_0 + c_1 x$, we have

$$-\phi_0 = c_0 p(0)^3 = (c_0 + c_1/2)p(1/2)^3 = (c_0 + c_1)p(1)^3.$$

Note that $B_{m-1}(\alpha) = \phi_0 \neq 0$ as B_m has only simple roots.
As p is not zero at rational numbers, we have

$$\frac{c_0 + \frac{c_1}{2}}{c_0} = s^3, \ \frac{c_0 + c_1}{c_0} = t^3$$

for nonzero rational numbers s, t. Hence we have

$$t^3 + 1 = 2s^3$$

where evidently $s \neq 1 \neq t$. The above equation is equivalent to

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

in nonzero integers x, y, z which are not all equal (as $t \neq 1 \neq s$). But, it is well-known and easy to prove that the above equation has no solutions other than $xyz = 0$ or $x = y = z$.

Dropping terms

If we drop terms from $f_m(X) = X(X+1)\cdots(X+m-1)$ to get some f, what can be said about solutions of $f(x) = y^n$? How many terms can we drop?

Theorem. Let $r \in \mathbf{Q}$, let $0 \leq a_1 < a_2 < \cdots < a_k$ be integers where $k > 2$. Further, let $n > 2$ and assume that we are not in the case when $n = k = 4$. Then, there are only finitely many solutions $x \in \mathbf{Z}$, $y \in \mathbf{Q}$ to the equation

$$(x - a_1)(x - a_2)\cdots(x - a_k) + r = y^n$$

and, all the solutions satisfy

$$\max\{H(x), H(y)\} < C$$

where C is an effectively computable constant depending only on n, r and the a_i's.

A more interesting result bounding k when r is an integer which is not a perfect n^{th} power, is contained in the following result.

Theorem 2. Let n be a fixed positive integer > 2 and let r be a nonzero integer which is not a perfect n^{th} power. Let $\{t_m\}_m$ be a sequence of positive integers such that $m/t_m \to \infty$ as $m \to \infty$. There exists a constant C such that if $(x - a_1)(x - a_2) \cdots (x - a_{m-t_m}) + r = y^n$ with $0 \leq a_1 < a_2 < \cdots < a_{m-t_m}$ has a solution, then $m/(t_m + 1) < C$.

The polynomial $1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!}$

Now, we consider finiteness of the number of rational solutions with bounded denominators (and point out all the exceptions) for certain equations of the form $f(x) = g(y)$ which includes the polynomials

$$f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots + \frac{x^n}{n!}$$

for any $n \geq 3$, and the Bernoulli polynomials $B_n(x)$, where g is an arbitrary polynomial of degree $m \geq 3$ in $\mathbb{Q}[y]$. This f is the 'exponential polynomial' of the title and, it should be remarked that the name exponential polynomial is used in another sense also.

Kulkarni & S proved the following results :

Theorem.

Let $E_n(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$ with $n \geq 3$. Then, we have :

(a) E_n is indecomposable for each n,

(b) for $g \in \mathbb{Q}[y]$ of degree $m \geq 3$, the equation $E_n(x) = g(y)$ has only finitely many rational solutions with a bounded denominator except in the following two cases :

(i) $g(y) = E_n(h(y))$ for some nonzero polynomial $h(y) \in \mathbb{Q}(y)$,

(ii) $n = 3, m$ is odd, and $g(x) = \frac{1}{3} + \frac{1}{6} D_m(\mu(x), -1)$, where μ is a linear polynomial over $\mathbb{Q}$.

In each exceptional case, there are infinitely many solutions.

As a matter of fact, the proof works more generally and we have :

Theorem.

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.

Indecomposability of E_n

We start with a simple observation which gives a sufficient condition for indecomposability of a complex polynomial.
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 $P(x) - c$.
Observation 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 so 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 latter 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 concludes the proof.

In order to prove indecomposability of E_n's using the above lemma, the key result needed is the following :

Proposition.

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 $\alpha, \alpha\theta$. Using Galois theory, this can be shown to be impossible.

In the course of the proof, one needs some basic facts about Dickson polynomials. These are summarized in the following result due to Bilu :

Theorem.

(a) The Dickson polynomial $D_l(x, 0)$ has exactly one extremum 0; it is of type (l).

(b) If $a \neq 0$ and $l \geq 3$ then $D_l(x, a)$ has exactly the two extrema $\pm 2a^{\frac{l}{2}}$.

If l is odd, then both are of type $(1, 2, 2 \cdots, 2)$.

If l is even, then $2a^{\frac{l}{2}}$ is of type $(1, 1, 2, \cdots, 2)$ and $-2a^{\frac{l}{2}}$ is of type $(2, 2, \cdots, 2)$.

Quadratic factors of f(X)-g(Y)

Yuri Bilu classified the pairs of polynomials f, g over a field of characteristic 0 such that $f(X) - g(Y)$ has an irreducible factor of degree 2.
This is used in the seminal work of Bilu & Tichy on equations of the form $f(x) = g(y)$.
The point is that they are interested in determining 'exceptional factors' of $f(X) - g(Y)$.
An exceptional curve $F(X, Y)$ is one when Siegel's theorem does not give finitely many integral points on a curve - this is if the genus is 0 and there are only two points at infinity.

Determining exceptional factors of $f(X) - g(Y)$ reduces by a trick due to Fried to finding quadratic factors - this is the motivation to find quadratic factors in general characteristic.
In this section, we extend Bilu's results to arbitrary characteristic - this work is in collaboration with M.Kulkarni & P.Müller.

Our method is completely different from Bilu's and, if one skips all the arguments specific to this, one obtains a particularly short and natural proof of Bilu's result.

Theorem

Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has a quadratic irreducible factor $q(X, Y)$. If the characteristic p of K is positive, then assume that at least one of the polynomials f, g cannot be written as a polynomial in X^p. Then there are $f_1, g_1, \Phi \in K[X]$ with $f = \Phi \circ f_1$, $g = \Phi \circ g_1$ such that $q(X, Y)$ divides $f_1(X) - g_1(Y)$, and one of the following holds:

(a) $\max(\deg f_1, \deg g_1) = 2$ and $q(X, Y) = f_1(X) - g_1(Y)$.

(b) There are $\alpha, \beta, \gamma, \delta \in K$ with $g_1(X) = f_1(\alpha X + \beta)$, and $f_1(X) = h(\gamma X + \delta)$, where $h(X)$ is one of the following polynomials.

  (i) p does not divide n, and $h(X) = D_n(X, a)$ for some $a \in K$. If $a \neq 0$, then $\zeta + 1/\zeta \in K$ where ζ is a primitive n-th root of unity.

  (ii) $p \geq 3$, and $h(X) = X^p - aX$ for some $a \in K$.

  (iii) $p \geq 3$, and $h(X) = (X^p + aX + b)^2$ for some $a, b \in K$.

  (iv) $p \geq 3$, and $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.

  (v) $p = 2$, and $h(X) = X^4 + (1 + a)X^2 + aX$ for some $a \in K$.

(c) n is even, p does not divide n, and there are $\alpha, \beta, \gamma, a \in K$ such that $f_1(X) = D_n(X + \beta, a)$, $g_1(X) = -D_n((\alpha X + \gamma)(\xi + 1/\xi), a)$. Here ξ denotes a primitive $2n$-th root of unity. Furthermore, if $a \neq 0$, then $\xi^2 + 1/\xi^2 \in K$.

(d) $p \geq 3$, and there are quadratic polynomials $u(X), v(X) \in K[X]$, such that $f_1(X) = h(u(X))$ and $g_1(X) = h(v(X))$ with $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.

The theorems exclude the case that f and g are both polynomials in X^p. The following handles this case, a repeated application reduces to the situation of the Theorems above.

Theorem

Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has an irreducible factor $q(X, Y)$ of degree at most 2. Suppose that $f(X) = f_0(X^p)$ and $g(X) = g_0(X^p)$, where $p > 0$ is the characteristic of K. Then one of the following holds:

(a) *$q(X, Y)$ divides $f_0(X) - g_0(Y)$, or*

(b) *$p = 2$, $f(X) = f_0(X^2)$, $g(X) = f_0(aX^2 + b)$ for some $a, b \in K$, and $q(X, Y) = X^2 - aY^2 - b$.*

Remark

Under suitable conditions on the parameters and the field K, all cases listed in Theorem 3 give examples such that $f_1(X) - g_1(Y)$ indeed has an irreducible quadratic factor. The cases of the Dickson polynomials are classically known and look as follows where n is even and ξ is a primitive $2n$-th root of unity:

$$D_n(X,a)+D_n(Y,a) = \prod_{1\le k\le n-1 \text{ odd}} (X^2-(\xi^k+1/\xi^k)XY+Y^2+(\xi^k-1/\xi^k)^2a).$$

We illustrate with two examples:
(b)(v). Here $p = 2$ and $h(X) = X^4 + (1 + a)X^2 + aX$. We have $h(X) - h(Y) = (X + Y)(X + Y + 1)(X^2 + X + Y^2 + Y + a)$. If $Z^2 + Z = a$ has no solution in K, then the quadratic factor is irreducible.
(b)(iv). Here $p \geq 3$ and $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$, and $a \neq 0$ of course. If α is a root of $Z^{p-1} - a$, then so is $-\alpha$. Let T be a set such $T \cup (-T)$ is a disjoint union of the roots of $Z^{p-1} - a$.

We compute

$$h(X^2) - h(Y^2) = (X^2 - Y^2) \prod_{t \in T \cup (-T)} [((X - Y) - t)((X + Y) - t)]$$

$$= (X^2 - Y^2) \prod_{t \in T} [((X - Y) - t)((X + Y) - t)$$

$$((X + Y) + t)((X - Y) + t)]$$

$$= (X^2 - Y^2) \prod_{t \in T} ((X^2 - Y^2)^2 - 2t^2(X^2 + Y^2) + t^4).$$

and therefore

$$h(X) - h(Y) = (X - Y) \prod_{t \in T} ((X - Y)^2 - 2t^2(X + Y) + t^4).$$

The discriminant with respect to X of the quadratic factor belonging to t is $16t^2 Y$, so all the quadratic factors are absolutely irreducible.

Davenport problem, Schur conjecture

We discuss a classical conjecture which involves the same analysis which is used in Bilu-Tichy's work.

For an integral polynomial $f(X)$, and each prime number p, let us consider the set $Val_p(f)$ of values of $f(\mathbf{Z})$ modulo p.
If f and g are linearly related in $\mathbf{Q}$, obviously $Val_p(f) = Val_p(g)$ for all but finitely many primes p.
Davenport problem asks whether the converse is true.
Note the special case $f(X) = aX^n, g(X) = X^n$ of this is already interesting - if a is an n-th power modulo p for all but finitely many primes p, then is a an n-th power?
The answer is known to be 'yes' if n is not a multiple of 8 and 'no' in the exceptional cases.

A conjecture of a similar flavour is Schur's conjecture which was solved affirmatively by M.Fried.
Schur's conjecture requires us to find all integral polynomials $f(X)$ such that $Val_p(f)$ is the full set for infinitely many primes p. These are exactly the ones linearly related to Dickson polynomials.

Group-theoretic approach

The method of approach to both Schur's conjecture and the Davenport problem is group-theoretic which we briefly describe.

First, we point out that Davenport conjecture has been solved by Fried for f, g when f is indecomposable. Later, P.Müller solved the case when the decomposition length of f is 2. In fact, a version is proved for algebraic number fields where there are finitely many exceptions which are explicitly pointed out. The rest is completely open.

Let $f, g \in K[X]$ where K is an algebraic number field. Take a Galois extension E of the function field $K(t)$ which contains roots x of $f(X) - t \in K(t)[X]$ and y of $g(X) - t \in K(t)[X]$.
Note that we have located elements $x, y \in E$ such that $f(x) = g(y)$.
Call $G = Gal(E/K(t))$ and U, V to be the stabilizers in G of x, y respectively. Then, Fried proved using the Chebotarev density theorem that:

Theorem (Fried). Let $f, g \in O_K[X]$ be non-constant polynomials. Then, $Val_P(f) = Val_P(g)$ for almost all prime ideals P if, and only if,

$$\bigcup_{g \in G} gUg^{-1} = \bigcup_{g \in G} gVg^{-1}$$

The last condition is very interesting for any finite group G and subgroups U, V because even if one of $U \subset V$, it is sometimes true that $U = V$ and sometimes not!

Proofs of M-K-S Theorems

Theorem

Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has a quadratic irreducible factor $q(X, Y)$. If the characteristic p of K is positive, then assume that at least one of the polynomials f, g cannot be written as a polynomial in X^p. Then there are $f_1, g_1, \Phi \in K[X]$ with $f = \Phi \circ f_1$, $g = \Phi \circ g_1$ such that $q(X, Y)$ divides $f_1(X) - g_1(Y)$, and one of the following holds:

(a) $\max(\deg f_1, \deg g_1) = 2$ and $q(X, Y) = f_1(X) - g_1(Y)$.

(b) There are $\alpha, \beta, \gamma, \delta \in K$ with $g_1(X) = f_1(\alpha X + \beta)$, and $f_1(X) = h(\gamma X + \delta)$, where $h(X)$ is one of the following polynomials.

  (i) p does not divide n, and $h(X) = D_n(X, a)$ for some $a \in K$. If $a \neq 0$, then $\zeta + 1/\zeta \in K$ where ζ is a primitive n-th root of unity.

  (ii) $p \geq 3$, and $h(X) = X^p - aX$ for some $a \in K$.

  (iii) $p \geq 3$, and $h(X) = (X^p + aX + b)^2$ for some $a, b \in K$.

  (iv) $p \geq 3$, and $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.

  (v) $p = 2$, and $h(X) = X^4 + (1 + a)X^2 + aX$ for some $a \in K$.

(c) n is even, p does not divide n, and there are $\alpha, \beta, \gamma, a \in K$ such that $f_1(X) = D_n(X + \beta, a)$, $g_1(X) = -D_n((\alpha X + \gamma)(\xi + 1/\xi), a)$. Here ξ denotes a primitive $2n$-th root of unity. Furthermore, if $a \neq 0$, then $\xi^2 + 1/\xi^2 \in K$.

(d) $p \geq 3$, and there are quadratic polynomials $u(X), v(X) \in K[X]$, such that $f_1(X) = h(u(X))$ and $g_1(X) = h(v(X))$ with $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.

Definition

For elements a, b of a group G, let a^b denote the conjugate $b^{-1}ab$.

Lemma

Let G be a finite dihedral group, generated by the involutions a and b. Then a and a suitable conjugate of b generate a Sylow 2-subgroup of G.

Proof. Set $c = ab$. For $i \in \mathbb{N}$, the order of $< a, b^{c^i} >$ is twice the order of ab^{c^i}. We compute $ab^{c^i} = a(c^{-1})^i bc^i = a(ba)^i b(ab)^i = (ab)^{2i+1} = c^{2i+1}$. Let $2i+1$ be the largest odd divisor of $|G|$. The claim follows.

Definition

For a, b, c, d in a field K with $ad - bc \neq 0$ let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ denote the image of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ in $PGL_2(K)$.

Lemma

Let K be an algebraically closed field of characteristic p, and $\rho \in PGL_2(K)$ be an element of finite order n. Then one of the following holds:

(a) *p does not divide n, and ρ is conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$, where ζ is a primitive n-th root of unity.*

(b) *$n = p$, and ρ is conjugate to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.*

Proof. Let $\hat{\rho} \in GL_2(K)$ be a preimage of ρ. Without loss of generality we may assume that 1 is an eigenvalue of $\hat{\rho}$. The claim follows from the Jordan normal form of $\hat{\rho}$.

Lemma

Let K be an algebraically closed field of characteristic p, and $G \leq PGL_2(K)$ be a dihedral group of order $2n \geq 4$, which is generated by the involution τ and the element ρ of order n. Then one of the following holds:

(a) *p does not divide n. There is $\sigma \in PGL(K)$ such that $\tau^\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$, where ζ is a primitive n-th root of unity.*

(b) *$n = p \geq 3$. There is $\sigma \in PGL(K)$ such that $\tau^\sigma = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.*

(c) *$n = p = 2$. There is $\sigma \in PGL(K)$ such that $\tau^\sigma = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ for some $1 \neq b \in K$.*

Proof.

By Lemma 6 we may assume that ρ has the form given there. From $\rho^\tau = \rho^{-1}$ we obtain the shape of τ:

First assume that p does not divide n, so $\rho = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$. Let $\hat{\tau} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ be a preimage of τ. From $\rho^\tau = \rho^{-1}$ we obtain $\rho\tau = \tau\rho^{-1}$, hence

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

for some $\lambda \in K$. This gives $(\lambda\zeta - 1)a = 0$, $(\lambda - 1)b = 0$, $(\lambda - 1)c = 0$, and $(\lambda - \zeta)d = 0$. First assume $b = c = 0$. Then ρ and τ commute, so G is abelian, hence $n = 2 \neq p$ and therefore $\zeta = -1$. It follows $\tau = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \rho$, a contradiction.

Thus $b \neq 0$, so $\lambda = 1$. This yields $a = d = 0$, as $\zeta \neq 1$. We obtain $\tau = \begin{bmatrix} 0 & 1 \\ c & 0 \end{bmatrix}$. Choose $\beta \in K$ with $\beta^2 = c$, and set $\delta = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$. The claim follows from $\rho^\delta = \rho$ and $\tau^\delta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Now assume the second case of Lemma 6, that is $p = n$ and $\rho = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Again setting $\hat{\tau} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we obtain

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

for some $\lambda \in K$.

This gives $a+c=\lambda a$, $b+d=\lambda(-a+b)$, $c=\lambda c$, and $d=\lambda(-c+d)$. If $c\neq 0$, then $\lambda=1$, so $c=0$ by the first equation, a contradiction. Thus $c=0$, so $a\neq 0$. We may assume $a=1$, so $d=-1$. This gives the result for $p=n=2$. If $p\neq 2$, then set $\sigma=\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}$ with $\beta=-b/2$.

From $\rho^{\sigma}=\rho$ and $\tau^{\sigma}=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ we obtain the claim.

(b) If L is a polynomial, then R has no poles, so is a polynomial as well. Suppose now that L is not a polynomial. Then there is $\alpha \in K$ with $L(\alpha) = \infty$. Let $\bar{K}$ be an algebraic closure of K. Choose $\beta \in \bar{K}$ with $g(\beta) = \alpha$. If we can find $\gamma \in \bar{K}$ with $R(\gamma) = \beta$, then we get the contradiction $f(\gamma) = \infty$. The value set of R on $\bar{K}$ is $\bar{K}$ minus the element $R(\infty) \in K$. Thus we are done except for the case that the equation $g(X) = \alpha$ has only the single solution $\beta = R(\infty) \in K$. In this case, however, $g(X) = \alpha + \delta(X - \beta)^n$ with $\delta \in K$. From $L^{-1}(f(R^{-1}(X))) = g(X)$ we analogously either get that L and R are polynomials, or $f(X) = \alpha' + \delta'(X - \beta')^n$ with $\alpha', \delta', \beta' \in K$. The claim follows.

Lemma

Let K be a field of characteristic p, and $n \in \mathbb{N}$ even and not divisible by p (so in particular $p \neq 2$). Let ξ be a primitive $2n$-th root of unity and $a \in K$. Then

$$D_n(X,a)+D_n(Y,a) = \prod_{1\leq k\leq n-1 \text{ odd}} (X^2-(\xi^k+1/\xi^k)XY+Y^2+(\xi^k-1/\xi^k)^2 a).$$

Proof.

This is essentially a proposition proved by Bilu in the paper we are generalizing. The factorizations of $D_m(X,a) - D_m(Y,a)$ are known from Turnwald's proof of Schur's conjecture. The claim then follows from that and $D_{2n}(X,a) - D_{2n}(Y,b) = D_n(X,a)^2 - D_n(Y,b)^2 = (D_n(X,a) + D_n(Y,b))(D_n(X,a) - D_n(Y,b))$. □

The following proposition classifies polynomials f over K with a certain Galois theoretic property. To facilitate the notation in the statement and its proof, we introduce a notation: If E is a field extension of K, and $f, h \in K[X]$ are polynomials, then we write $f \sim_E h$ if and only if there are linear polynomials $L, R \in E[X]$ with $f(X) = L(h(R(X)))$. Clearly, $\sim_E$ is an equivalence relation on $K[X]$. In determining the possibilities of f in Proposition 0.1, we first determine certain polynomials $h \in \bar{K}[X]$ with $f \sim_{\bar{K}} h$, and from that we conclude the possibilities for f. The following Lemma illustrates this latter step.

Lemma

Let $\bar{K}$ be an algebraic closure of the field K of characteristic p. Suppose that $f \sim_{\bar{K}} X^p - 2X^{(p+1)/2} + X$ for $f \in K[X]$. Then $f \sim_K X^p - 2aX^{(p+1)/2} + a^2X$ for some $a \in K$.

Proof There are $\alpha, \beta, \gamma, \delta \in \bar{K}$ with $f(X) = \alpha h(\gamma X + \delta) + \beta \in K[X]$, where $h(X) = X^p - 2X^{(p+1)/2} + X$.
The coefficients of X^p and $X^{(p+1)/2}$ of $f(X)$ are $\alpha\gamma^p \in K$ and $-2\alpha\gamma^{(p+1)/2} \in K$, so $\gamma^{(p-1)/2} \in K$ and $\alpha\gamma \in K$.

Suppose that $p > 3$. Then the coefficient of $X^{(p-1)/2}$ is (up to a factor from K) $\alpha\gamma^{(p-1)/2}\delta \in K$, so $\alpha\delta \in K$ and therefore $\delta/\gamma \in K$. Thus, upon replacing X by $X - \delta/\gamma$, we may assume $\delta = 0$. Then $\beta \in K$, so $\beta = 0$ without loss of generality. Now dividing by $\alpha\gamma^p$ and setting $a = 1/\gamma^{(p-1)/2}$ yields the claim.
In the case $p = 3$ we get from above $\gamma \in K$ and then $\alpha \in K$. Thus we may assume $\alpha = \gamma = 1$. Looking at the coefficient of X, which is $-4\delta + 1$, shows $\delta \in K$, so $\delta = \beta = 0$ without loss of generality. Thus $f(X) = X^3 - 2X^2 + X$.

Proposition

Let K be a field of characteristic p, and $f(X) \in K[X]$ be a polynomial of degree $n \geq 3$ which is not a polynomial in X^p. Let x be a transcendental, and set $t = f(x)$. Suppose that the normal closure of $K(x)/K(t)$ has the form $K(x, y)$ where $F(x, y) = 0$ with $F \in K[X, Y]$ irreducible of total degree 2. Furthermore, suppose that the Galois group of $K(x, y)/K(t)$ is dihedral of order $2n$. Then one of the following holds:

(a) p does not divide n, and $f \sim_K D_n(X, a)$ for some $a \in K$. If $a \neq 0$, then $\zeta + 1/\zeta \in K$ where ζ is a primitive n-th root of unity.

(b) $n = p \geq 3$, and $f \sim_K X^p - aX$ for some $a \in K$.

(c) $n = 2p \geq 6$, and $f \sim_K (X^p + aX + b)^2$ for some $a, b \in K$.

(d) $n = p$, and $f \sim_K X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.

(e) $n = 4$, $p = 2$, and $f \sim_K X^4 + (1 + a)X^2 + aX$ for some $a \in K$.

In the cases (b), (d), (e), and (a) for odd n, the following holds: If $K(w)$ is an intermediate field of $K(x,y)/K(t)$ with $[K(x,y):K(w)]=2$, then $K(w)$ is conjugate to $K(x)$.
In case (a) suppose that $f(X)=D_n(X,a)$ and $K(w)$ is not conjugate to $K(x)$. Furthermore, suppose that $t=g(w)$ for a polynomial $g(X)\in K[X]$. Then $g(X)=-D_n(b(\xi+1/\xi)X+c,a)$ for $b,c\in K$ and ξ a primitive $2n$-th root of unity.

Proof of the Theorems

Suppose that $f(X)$ is not a polynomial in X^p, so not all exponents of f are divisible by p. Let $q(X, Y)$ be an irreducible divisor of $f(X) - g(Y)$ of degree at most 2. Set $t = f(x)$, where x is a transcendental over K. Clearly both variables X and Y appear in $q(X, Y)$. In an algebraic closure of $K(t)$ choose y with $q(x, y) = 0$. Note that $g(y) = t$. The field $K(x) \cap K(y)$ lies between $K(x)$ and $K(t)$, so by Lüroth's Theorem, $K(x) \cap K(y) = K(u)$ for some u. Writing $t = \Phi(u)$ and $u = f_1(x)$ for rational functions $\Phi, f_1 \in K(X)$, we have $f = \Phi \circ f_1$. By Lemma 10(a), we may replace u by u' with $K(u) = K(u')$, such that t is a polynomial in u, and u is a polynomial in x. Thus without loss of generality we may assume that Φ and f_1 are polynomials. From that it follows that u is also a polynomial in y, so $g(X) = \Phi(g_1(X))$ for a polynomial g_1 with $g_1(y) = u$. As q is irreducible and $f_1(x) - g_1(y) = u - u = 0$, we get that $q(X, Y)$ divides $f_1(X) - g_1(Y)$. Thus, in order to prove the theorems, we may assume that $f = f_1$ and $g = g_1$, so $K(x) \cap K(y) = K(t)$.

First suppose that the polynomial $q(x, Y)$, considered in the variable Y, is inseparable over $K(x)$. Then the characteristic of K is 2, and (up to a factor) $q(X, Y) = aX^2 + bX + c + Y^2$, hence $y^2 = ax^2 + bx + c$. So $K(y^2) \subseteq K(x) \cap K(y) = K(t)$, therefore $[K(y) : K(t)] \leq 2$. But $[K(x) : K(t)] = [K(x, y) : K(y)][K(y) : K(t)]/[K(x, y) : K(x)] \leq 2$. We obtain $\deg f, \deg g \leq 2$, a situation which gives case (a) in the theorems.

Thus we assume that $K(x,y)/K(x)$ is separable. By the assumption that $f(X)$ is not a polynomial in X^p (this property is inherited by the new f), we also obtain that $K(x)/K(t)$ is separable. Thus $K(x,y)/K(t)$ is separable. From $K(x) \cap K(y) = K(t)$ we obtain that the fields $K(x)$, $K(y)$, and $K(x,y)$ are pairwise distinct. So $K(x,y)$ is a quadratic extension of $K(x)$ and $K(y)$. Thus $K(x,y)/K(t)$ is a Galois extension, whose Galois group G is generated by involutions τ_x and τ_y, where τ_x and τ_y fix x and y, respectively. In particular, G is a dihedral group. For $\deg f = \deg g = 2$ we obtain case (a) of the Theorems. Thus assume $n = \deg f = \deg g \geq 3$ from now on.

The possibilities for f are given in Proposition 0.1. In the cases (b), (d), (e), and (a) for odd n, we obtain that $K(x)$ and $K(y)$ are conjugate, yielding the case (a) of Theorem **??** and case (b) of Theorem 3.

Let us assume case (c) of Proposition 0.1. Here G is a dihedral group of order $4p$. If τ_x and τ_y are conjugate, then we obtain case (a) of Theorem **??** and case (b)(iii) of Theorem 3. Thus suppose that τ_x and τ_y are not conjugate. By Lemma 4 there is a conjugate τ_y' of τ_y such that τ_x and τ_y' generate a group of order 4. Thus $K(x)$ and $K(y')$ have degree 2 over $K(x) \cap K(y')$. So there are $f_0, g_0, h \in K[X]$ with f_0 and g_0 of degree 2 and $f = h \circ f_0$, $g = h \circ g_0$, giving case (a) of Theorem **??**. Without loss of generality assume that $f(X) = (X^p + aX + b)^2$, and $f_0(X) = X^2$. From $f(-X) = h((-X)^2) = h(X^2) = f(X)$ we obtain $b = 0$, so $f(X) = h(X^2)$ with $h(X) = X^p + 2aX^{\frac{p+1}{2}} + a^2X$. This yields case (d) of Theorem 3.

Finally, assume the situation of Proposition 0.1, case (a) for even n. If $K(x)$ and $K(y)$ are conjugate, then we obtain the case (a) of Theorem **??** and case (b)(i) of Theorem 3. If however $K(x)$ and $K(y)$ are not conjugate, then Proposition 0.1 yields case (c) of Theorem 3. In order to obtain case (b) of Theorem **??** one applies Lemma 4 in order to show that τ_x and a conjugate of τ_y generate a dihedral 2-group and argues as in the previous paragraph.

Let z be a transcendental over the field K. The group of K-automorphisms of $K(z)$ is isomorphic to $PGL_2(K)$, where $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ sends z to $\frac{az+b}{cz+d}$. Note that $K(z) = K(z')$ for $z \in K(z)$ if and only if $z' = \frac{az+b}{cz+d}$ with $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(K)$.

Let $r(z) \in K(z)$ be a rational function. Then the *degree* $\deg r$ of r is the maximum of the degrees of the numerator and denominator of $r(z)$ as a reduced fraction. Note that $\deg r$ is also the degree of the field extension $K(z)/K(r(z))$.

For $a \in K$ recall the nth Dickson polynomial $D_n(X, a)$ (of degree n) defined implicitly by $D_n(z + a/z, a) = z^n + (a/z)^n$.
Note that $D_n(X, 0) = X^n$.
Furthermore, from $b^n D_n(z + a/z, a) = b^n(z^n + (a/z)^n) = (bz)^n + (\frac{b^2 a}{bz})^n = D_n(bz + \frac{b^2 a}{bz}, b^2 a) = D_n(b(z + a/z), b^2 a)$ one obtains $b^n D_n(X, a) = D_n(bx, b^2 a)$, a relation we will use.

Lemma

(a) *Let* $f(X) = g(h(X))$ *with* $f \in K[X]$ *and* $g, h \in K(X)$. *Then* $f = g \circ h = (g \circ \lambda^{-1}) \circ (\lambda \circ h)$ *for a rational function* $\lambda \in K(X)$ *of degree* 1, *such that* $g \circ \lambda^{-1}$ *and* $\lambda \circ h$ *are polynomials.*

(b) *Let* $f, g \in K[X]$ *be two polynomials such that* $f(X) = L(g(R(X)))$ *for rational functions* $L, R \in K(X)$ *of degree* 1. *Then there are linear polynomials* $\ell, r \in K[X]$ *with* $f(X) = \ell(g(r(X)))$.

Proof.

(a) This is well known. For the convenience of the reader, we supply a short proof. Let $\lambda \in K(X)$ be of degree 1 such that $\lambda(h(\infty)) = \infty$. Setting $\bar{g} = g \circ \lambda^{-1}$ and $\bar{h} = \lambda \circ h$ we have $f = \bar{g} \circ \bar{h}$ with $\bar{h}(\infty) = \infty$. Suppose that $\bar{g}$ is not a polynomial. Then there is $\alpha \in \bar{K}$ ($\bar{K}$ denotes an algebraic closure of K) with $\bar{g}(\alpha) = \infty$. Let $\beta \in \bar{K} \cup \{\infty\}$ with $\bar{h}(\beta) = \alpha$). From $\bar{h}(\infty) = \infty$ we obtain $\beta \neq \infty$. Now $f(\beta) = \bar{g}(\bar{h}(\beta)) = \bar{g}(\alpha) = \infty$ yields a contradiction, so $\bar{g}$ is a polynomial. From that it follows that $\bar{h}$ is a polynomial as well.

Proof

Let $\hat{K}$ be the algebraic closure of K in $K(x,y)$. Then $K(x) \subseteq \hat{K}(x) \subseteq K(x,y)$, so either $\hat{K} = K$ or $K(x,y) = \hat{K}(x)$.
We start looking at the latter case. Here $\hat{K}(x)/\hat{K}(t)$ is a Galois extension with group C which is a subgroup of $G = \mathrm{Gal}(\hat{K}(x)/K(t))$ of order n.
Note that C is either cyclic or dihedral. Let $\sigma \in C$, so $x^\sigma = \frac{ax+b}{cx+d}$ with $a, b, c, d \in \hat{K}$. From $f(\frac{ax+b}{cx+d}) = f(x^\sigma) = f(x)^\sigma = t^\sigma = t = f(x)$ we obtain that $\frac{ax+b}{cx+d}$ is a polynomial, so $x^\sigma = ax + b$.

Suppose that p does not divide n. Then we may assume that the coefficient of X^{n-1} of f vanishes. From $f(ax+b) = f(x)$ we obtain $b = 0$. Thus C is isomorphic to a subgroup of $\hat{K}^{\times}$, in particular C is cyclic and generated by σ with $x^{\sigma} = \zeta x$ with ζ a primitive nth root of unity. From $f(x) = f(\zeta x)$ we see that, up to a constant factor, $f(X) = X^n$. This is case (a) with $a = 0$.
From now on it is more convenient to work over an algebraic closure $\bar{K}$ of K.
Now $\bar{K}(t) \cap K(x,y) = \hat{K}(t)$ as noticed in Turnwald's notes on monodromy of polynomials, we obtain that $\mathrm{Gal}(\bar{K}(x)/\bar{K}(t)) = C$.

Now suppose that p divides $n = |C|$, but $p \geq 3$. First assume that C is cyclic. From Lemma 6 we get $p = n$. Let ρ be a generator of C. Lemma 6 shows the following: There is $x' \in \bar{K}(x)$ with $\bar{K}(x) = \bar{K}(x')$, such that $x'^{\rho} = x' + 1$. So $t' = x'^{p} - x'$ is fixed under C. We obtain $t' \in \bar{K}(t)$, because $\bar{K}(t)$ is the fixed field of C. From $p = [\bar{K}(x') : \bar{K}(t')]$ we obtain $\bar{K}(t') = \bar{K}(t)$. So there are rational functions $L, R \in \bar{K}(X)$ of degree 1 with $x' = R(x)$ and $t = L(t')$. Then
$f(x) = t = L(t') = L(x'^{p} - x') = L(r(x)^{p} - R(x))$, so
$f = L \circ (X^{p} - X) \circ R$. By Lemma 10 we may assume that L and R are polynomials over $\bar{K}$. Then $f(X) = \alpha(X^{p} - aX) + \beta$ with $\alpha, \beta, a \in K$. From that we get case (b).

Next assume that C is dihedral of order n. As $p \geq 3$, we get that p divides $n/2$. We apply Lemma 7 now. This yields $n = 2p$, and there is x' with $\bar{K}(x') = \bar{K}(x)$ such that $\bar{K}(t)$ is the fixed field of the automorphisms $x' \mapsto -x'$ and $x' \mapsto x' + 1$. Obviously $t' = (x'^p - x')^2$ is fixed under these automorphisms, and as $[\bar{K}(x') : \bar{K}(t')] = 2p$, we obtain $\bar{K}(t) = \bar{K}(t')$. The claim follows similarly as above.

Now assume that $p = 2$ divides n. Applying Lemmata 6 and 7, we get that C is the Klein 4 group. We see that $t' = x'(x'+1)(x'+b)(x'+b+1)$ is fixed under the automorphisms sending x' to $x'+1$ and to $x'+b$. So $t' = h(x')$ with $h(X) = X^4 + (1+b+b^2)X^2 + (b+b^2)X$. Next we show that $b^2 + b \in K$. A suitable substitution $\gamma f(\alpha X + \beta) + \delta$ should give $f(X) \in K[X]$. We obtain $\gamma f(\alpha X + \beta) + \delta = \gamma(f(\alpha X) + f(\beta)) + \delta \in K[X]$. Looking at the coefficients of X^2 and X yields $\alpha \in K$, so $\alpha = 1$ without loss of generality. Looking at X^4 gives $\gamma \in K$, so $\gamma = 1$ without loss. Finally the coefficient of X yields the claim. Thus $f(X) = X^4 + (1+b+b^2)X^2 + (b+b^2)X \in K[X]$ and $\hat{K} = K(b)$, which gives case (e). In this case assume that w is as in the proposition. Let τ_x and τ_w be the involutions of the dihedral group G of order 8 which fix x and w, respectively. From $K(x,y) = K(x,b) = K(w,b)$ we obtain that $\tau_x, \tau_w \notin C$. This shows that τ_x and τ_w are conjugate in G, so $K(w)$ is conjugate to $K(x)$.

It remains to study the case $K = \hat{K}$, so $\hat{K}(x, y)/\hat{K}(t)$ is Galois with group G. By the Diophantine trick we obtain a rational parametrization of the quadric $F(X, Y) = 0$ over $\bar{K}$ (actually, a suitable quadratic extension over which $F(X, Y) = 0$ has a rational point suffices). In terms of fields that means $\bar{K}(z) = \bar{K}(x, y)$ for some element z.

We apply Lemma 7. Up to replacing x and t by x' and t' as above, we get the following possibilities:
(a) p does not divide n, x is fixed under the automorphism sending z to $1/z$, and t is fixed under this automorphism and the one sending z to z/ζ. So we may choose $t = z^n + 1/z^n$, $x = z + 1/z$. But then $t = D_n(x, 1)$. There are linear polynomials $L, R \in \bar{K}[X]$ with $L \circ D_n(X, 1) \circ R = f \in K[X]$, so we get case (a) of the proposition by Turnwald's work on Schur's conjecture. For the remaining claims concerning this case, we may assume that $f(X) = D_n(X, a)$. Again set $t = f(x)$, and now choose z with $z + a/z = x$. Then $t = D_n(x, a) = D_n(z + a/z, a) = z^n + (a/z)^n$. The normal closure $K(x, y) = K(x, w)$ of $K(x)/K(t)$ is contained in $K(\zeta, z)$. The elements $x' = \zeta x + \frac{a}{\zeta x}$ and $x'' = \frac{x}{\zeta} + \frac{\zeta a}{x}$ are conjugates of x, so $x, x', x'' \in K(x, y)$. From $x' + x'' = (\zeta + 1/\zeta)(x + a/x)$ we obtain $\zeta + 1/\zeta \in K(x, y)$. However, we are in the case that K is algebraically closed in $K(x, y)$, so $\zeta + 1/\zeta \in K$.

Suppose that $K(w)$ is not conjugate to $K(x)$. As extending the coefficients does not change Galois groups, this is equivalent to $\bar{K}(x)$ not being conjugate to $\bar{K}(w)$ in $\bar{K}(x,y) = \bar{K}(z)$. Note that x is fixed under the involution $z \mapsto a/z$. The other involutions in $\mathrm{Gal}(\bar{K}(z)/\bar{K}(t))$ have the form $z \mapsto a\beta/z$, where β is an nth root of unity, or $z \mapsto -z$. The latter involution cannot fix w, because the fixed field would be $\bar{K}(z^2)$, however, $z^n + (a/z)^n$ cannot be written as a polynomial in z^2. Thus suppose that $z \mapsto a\beta/z$ fixes w. If $\beta^{n/2} = 1$, then an easy calculation shows that $\begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & \beta a \\ 1 & 0 \end{bmatrix}$ are conjugate in $\mathrm{Gal}(\bar{K}(z)/\bar{K}(t))$, contrary to $\bar{K}(x)$ and $\bar{K}(w)$ not being conjugate. Thus $\beta^{n/2} \neq 1$, hence $\beta^{n/2} = -1$, because $\beta^n = 1$. The element $w' = z + (\beta a)/z$ is fixed under the involution $z \mapsto a\beta/z$, so $\bar{K}(w') = \bar{K}(w)$.

Furthermore,

$$t = z^n + (a/z)^n = z^n + (\beta a/z)^n = D_n(z + (\beta a)/z, \beta a) = D_n(w', \beta a),$$

so $g(X) = D_n(uX + v, \beta a)$ for some $u, v \in \bar{K}$. The condition that $g(X)$ has coefficients in K shows that $\frac{v}{u} \in K$, by Turnwald's work on Schur's conjecture. Thus, upon replacing X by $X - \frac{v}{u}$, we may assume $v = 0$. The transformation formula gives
$g(X) = D_n(uX, \beta a) = \beta^{n/2} D_n(\frac{u}{\sqrt{\beta}} X, a) = -D_n(\frac{1}{\delta} X, a)$ with $\delta \in \bar{K}$. As each conjugate of w has degree 2 over $K(x)$ we obtain that $f(X) - g(Y)$ splits over K in irreducible factors of degree 2. One of the factors of $f(X) - g(Y) = D_n(X, a) + D_n(\frac{1}{\delta} Y, a)$ is
$X^2 - \frac{1}{\delta}(\xi + 1/\xi)XY + \frac{1}{\delta^2} Y^2 - (\xi - 1/\xi)^2 a$. All coefficients of this factor have to be in K, so there is $b_1 \in K$ with $\frac{1}{\delta}(\xi + \frac{1}{\xi}) = b_1$. We obtain
$g(X) = -D_n(\frac{b_1}{\xi + 1/\xi} X, a) = -D_n(b(\xi + 1/\xi)X, a)$, where
$b = \frac{b_1}{(\xi + 1/\xi)^2} \in K$. The claim follows.

(b) $n = p \geq 3$. From a computation above we obtain $t = (z^p - z)^2$. We may assume that x is fixed under the automorphism sending z to $-z$, so for instance $x = z^2$. Let $h \in \bar{K}(X)$ with $h(x) = t$. That means $h(z^2) = (z^p - z)^2 = z^{2p} - 2z^{p+1} + z^2$, hence $h(X) = X^p - 2X^{\frac{p+1}{2}} + X$. Lemma 9 yields the claim.
(c) The case $n = p = 2$ does not arise, because we assumed $n \geq 3$.

The conjugacy of $K(w)$ and $K(x)$ has been shown in the derivation of case (e) above. In the cases (a) (n odd), (b) and (d) it holds as well, because G is dihedral of order $2n$ with n odd, so all involutions in G are conjugate.

Proof of 2nd theorem:

We have $f(X) = u(X)^p$ and $g(X) = v(X)^p$, where the coefficients of u and v are contained in a purely inseparable extension L of K. (This includes the case $K = L$.) In particular, $[L : K]$ is a power of p, so $q(X, Y)$ remains irreducible over L if $p > 2$.
Suppose first that $p > 2$, or that $q(X, Y)$ is irreducible over L if $p = 2$.
As each irreducible factor of
$f(X) - g(Y) = u(X)^p - v(X)^p = (u(X) - v(Y))^p$ arises at least p times, we obtain that $q(X, Y)^p = q(X^p, Y^p)$ divides
$f(X) - g(Y) = f_0(X^p) - g_0(Y^p)$, and the claim follows in this case.

It remains to look at the case that $p = 2$ and $q(X, Y) = q_1(X, Y)q_2(X, Y)$ is a nontrivial factorization over L. If q_1 and q_2 do not differ by a factor, then as above $q_1(X, Y)^2$ and $q_2(X, Y)^2$ divide $u(X)^2 - v(Y)^2$, so $q(X, Y)^2$ divides $u(X)^2 - v(Y)^2$, and we conclude as above.
Thus $q(X, Y) = \delta(\alpha X + Y + \beta)^2$ for some $\alpha, \beta \in L$, $\delta \in K$. Then $q(X, Y) = \delta(aX^2 + Y^2 + b)$ with $a, b \in K$ divides $f_0(X^2) - g_0(Y^2)$, so $aX + Y + b$ divides $f_0(X) - g_0(Y)$, hence $g_0(X) = f_0(aX + b)$, and the claim follows.

Remark

The method of the discussion is easily extended to the study of degree 2 factors of polynomials of the form $a(X)b(Y) - c(X)d(Y)$, where a, b, c, d are polynomials. For if $q(X, Y)$ is a quadratic factor, x is a transcendental, and y chosen with $q(x, y) = 0$, then $a(x)/c(x) = d(y)/b(y)$, so setting $t = a(x)/c(x) = d(y)/b(y)$ and studying the field extension $K(x, y)/K(t)$ requires only minor extensions of the arguments given in the discussion.