A Hasse-type principle for exponential diophantine equations and its applications

L. Hajdu

University of Debrecen

Erdős Centennial
July 1 - 5, 2013
Budapest

WARNING - work in progress !!!

Results, references, etc. may not yet be in their final forms.

Plan of the talk

Part 1. A Hasse-type principle for exponential Diophantine equations

1/a Formulating the principle (conjecture)

1/b Connections to a conjecture of Skolem and related known results

1/c A new theoretical result - the principle is “almost always” valid

1/d Numerical results supporting the principle

Part 2. Application: complete solution of exponential diophantine equations in several terms and unknowns

2/a Known results from the literature

2/b The scheme of application

2/c Numerical results

The presented results are joint with **Csanád Bertók**.

Exponential Diophantine equations

Let $a_1, \ldots, a_k$, $b_{11}, \ldots, b_{1\ell}, \ldots, b_{k1}, \ldots, b_{k\ell}$ be non-zero integers, c be an integer.

Consider the exponential diophantine equation

$$a_1 b_{11}^{\alpha_{11}} \ldots b_{1\ell}^{\alpha_{1\ell}} + \cdots + a_k b_{k1}^{\alpha_{k1}} \ldots b_{k\ell}^{\alpha_{k\ell}} = c \tag{1}$$

in non-negative integers $\alpha_{11}, \ldots, \alpha_{1\ell}, \ldots, \alpha_{k1}, \ldots, \alpha_{k\ell}$.

That is, we consider equations like

$$5 \cdot 2^{\alpha} \cdot 7^{\beta} \cdot 15^{\gamma} - 10 \cdot 17^{\delta} \cdot 22^{\varepsilon} + 3 \cdot 7^{\zeta} \cdot 17^{\eta} = 101.$$

Brief history of equation (1)

The effective and ineffective theory of (1) has a long history.

In case of $k = 2$, by Baker's method it is possible to give explicit bounds for the exponents $\alpha_{11}, \ldots, \alpha_{1\ell}, \alpha_{21}, \ldots, \alpha_{2\ell}$. See results of **Győry (1979, 1992, 2002), Shorey, Tijdeman (1986), Evertse, Győry, Stewart, Tijdeman (1988), Bugeaud, Győry (1996), Győry, Yu (2006)** and many others, also concerning more general domains.

By results of **Vojta (1983)** and **Bennett (2010)**, the solutions to (1) can still be effectively determined for $k = 3, 4$, under some further restrictive assumptions.

Brief history of equation (1) - continued

In case of $k \geq 2$, by the help of the subspace theorem it is possible to give explicit bounds for the number of solutions of equation (1) having no vanishing subsums.

See results of **Evertse (1984), Evertse, Győry (1985, 1988), Evertse, Győry, Stewart, Tijdeman (1988), Evertse, Schlickewei, Schmidt (2002), Evertse, Zannier (2008)** and many others, also concerning more general domains.

A Hasse-type principle for equation (1)

We propose the following

New Conjecture. Suppose that equation (1) has no solutions. Then there exists an integer m with $m \geq 2$ such that the congruence

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} \equiv c \pmod{m} \qquad (2)$$

has no solutions in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$.

The conjecture is a generalization of a classical conjecture of **Skolem (1937)**.

The conjecture of Skolem (1937)

The original conjecture of **Skolem (1937)** is the following:

Using the previous notation, consider the exponential diophantine equation

$$a_1 b_{11}^{\alpha_1} \dots b_{1\ell}^{\alpha_\ell} + \dots + a_k b_{k1}^{\alpha_1} \dots b_{k\ell}^{\alpha_\ell} = 0. \tag{3}$$

Suppose that equation (3) is not solvable. Then the congruence

$$a_1 b_{11}^{\alpha_1} \dots b_{1\ell}^{\alpha_\ell} + \dots + a_k b_{k1}^{\alpha_1} \dots b_{k\ell}^{\alpha_\ell} \equiv 0 \pmod{m}$$

is not solvable for some integer $m \geq 2$.

In fact, the conjecture of **Skolem** has been formulated for algebraic numbers. However, the New Conjecture also can have such a variant.

Comparing the conjectures

• In the New Conjecture, we can have an arbitrary integer c on the right hand side.

• In the conjecture of Skolem the exponents of b_{ij} for $i = 1, \ldots, k$ are the same α_j ($j = 1, \ldots, \ell$).

Still, the principle behind the both congruences is the same.

Known results

Schinzel (1975): For $k = 1$ the conjectures are true (even in a stronger form).

Bartolome, Bilu, Luca (2013): In case of $\ell = 1$, i.e. for equations of the form

$$a_1 b_1^{\alpha} + \cdots + a_k b_k^{\alpha} = 0$$

the conjecture of Skolem is true, provided that the multiplicative group generated by $b_1, \ldots, b_k$ is of rank one. (The result is valid over number fields, too.)

Beside these, there are many interesting results about the conjecture of Skolem over function fields due to **Sun (201?)**, and concerning the case $k = 2$, due to **Schinzel (1975, 1980, 2003)** and **Broughan, Luca (2010)** and others.

New results

The next theorem shows that the New Conjecture is "almost always" valid.

Theorem 1. (Bertók, H, 201?). Let $b_{11}, \ldots, b_{1\ell}, \ldots, b_{k1}, \ldots, b_{k\ell}$ be fixed, and let H be the set of right hand sides c for which the New Conjecture is violated, that is

$$H = \{c \ : \ c \text{ is an integer for which (1) is not solvable,}$$

$$\text{but (2) is solvable for all } m\}.$$

Then H has density zero inside the set

$$H_0 = \{c \ : \ c \text{ is an integer for which (1) is not solvable}\}.$$

New results - continued

In fact Theorem 1 is a consequence of the following result.

Let $\lambda(m)$ be the Carmichael function of the positive integer m, that is the least positive integer for which

$$b^{\lambda(m)} \equiv 1 \pmod{m}$$

for all $b \in \mathbb{Z}$ with $\gcd(b, m) = 1$.

Theorem 2. (Bertók, H, 201?). There exist positive constants C_1, C_2 such that for any integer r and for every large integer i there is an integer m with $r \mid m$, and

$$\log m \in [\log i + \log r, (\log i)^{C_1} + \log r],$$

$$\lambda(m) < r(\log m/r)^{C_2 \log\log\log m/r}.$$

Remarks about Theorem 2.

• The statement is a variation of a theorem of **Erdős, Pomerance, Schmutz (1991)** and **Tijdeman, H (2011)**.

• The important difference is the extra requirement that the appropriate moduli should be divisible by a fixed number r. This relation will play an important role in the applications later on.

• The proof is "constructive" in the sense that a sequence of appropriate moduli m are given. They are products of primes p having only "small" prime factors. This appears already in the original version due to **Erdős, Pomerance, Schmutz (1991)**.

Numerical results supporting the New Conjecture

Dimitrov, Hoewe (2011): proved the insolvability of equations of the form $2^{\alpha_1}3^{\beta_1} \pm \cdots \pm 2^{\alpha_t}3^{\beta_t} = c_t$ for $t \leq 6$, for particular values of c_t.

Theorem 3. (Bertók, H, 201?). Let p_1, p_2, p_3 be distinct primes less than 100 and $0 \leq c \leq 1000$. Then the New Conjecture is valid for the equations

$$p_1^{\alpha_1} - p_2^{\alpha_2} = c$$

and

$$p_1^{\alpha_1} + p_2^{\alpha_2} - p_3^{\alpha_3} = c.$$

Theorem 4. (Bertók, H, 201?). Let $p_1 < \cdots < p_t$ be primes less than 30 with $4 \leq t \leq 8$ nd $0 \leq c \leq 1000$. Then the New Conjecture is valid for the equation

$$p_1^{\alpha_1} + \cdots + p_{t-1}^{\alpha_{t-1}} - p_t^{\alpha_t} = c.$$

Numerical results supporting the New Conjecture - continued

Theorem 5. (Bertók, H, 201?). The New Conjecture is valid for the equation

$$2^{\alpha_1} + 3^{\alpha_2} + 5^{\alpha_3} + 7^{\alpha_4} + 11^{\alpha_5} + 13^{\alpha_6} + 17^{\alpha_7} + 19^{\alpha_8} - 23^{\alpha_9} = 55191.$$

Remark. The equation in Theorem 5 has no solutions, but has solutions if 55191 is replaced by any c with $0 \leq c < 55191$.

Remarks about the proofs of Theorems 3-5

- The modulus

$$m = 2^4 \cdot 3^2 \cdot \prod_{\substack{p-1=2^u3^v5^w \\ 3<p<20000}} p$$

is appropriate in all cases. (In many cases it could be much smaller.) Recall the proof of Theorem 2.

- The checking of the impossibility of the congruences modulo m must be implemented carefully. For example, it is much more efficient to check the congruences modulo the primes (prime powers) separately and combining the information, than checking directly the congruence modulo m.

Application: complete solution of exponential diophantine equations in several terms and unknowns

• **Alex, Brenner, Foster (1980's and early 1990's)** solved several equations of the form $p_1^{\alpha_1} \pm \cdots \pm p_t^{\alpha_t} = c$, where $t \leq 4$, the p_i are "small" primes and c is also "small". They used special moduli working for the special values of the primes p_i.

• **Tijdeman, Wang (1988), Skinner (1993), Scott (1993), Luca (2003), Scott, Styer (2004, 2006)** and others: solution and effective results for equations $p^x - p^y = q^u - q^v$ with p, q primes. They used Baker's method.

• **Bennett (2010)**: all solutions to $2^{\alpha_1}3^{\beta_1} + 2^{\alpha_2} + 3^{\beta_2} - 2^{\alpha_3} - 3^{\beta_3} = 0$, using a particular modulus.

Application scheme of the New Conjecture

For simplicity assume that equation (1) has only finitely many solutions.

I. Find all solutions to equation (1) by an exhaustive search.

II. Choose one of the unknowns, α_{ij} say, and based upon the suspected list of solutions find an integer α_0 with $\alpha_{ij} < \alpha_0$.

III. Instead of equation (1) consider the equation obtained from (1) by replacing the coefficient a_i by $a_i b_{ij}^{\alpha_0}$.

IV. Find an m such that the new equation has no solution already modulo m.

Application of the New Conjecture - an example

A deep search for the equation

$$2^{\alpha} + 3^{\beta} + 5^{\gamma} + 7^{\delta} - 11^{\varepsilon} = 2$$

convinces us that there are 9 solutions, all with $\alpha \leq 8$. So apply the New Conjecture for the equation

$$2^{9} \cdot 2^{\alpha'} + 3^{\beta} + 5^{\gamma} + 7^{\delta} - 11^{\varepsilon} = 2.$$

Assume that we have been careless, and our search was not deep enough, we have checked only the cases up to $\alpha \leq 7$, and we go for the equation

$$2^{8} \cdot 2^{\alpha'} + 3^{\beta} + 5^{\gamma} + 7^{\delta} - 11^{\varepsilon} = 2.$$

Application of the New Conjecture - an example - continued

Then using an appropriate modulus M (similar to the previously mentioned one), we get

$$\alpha' + 8 \equiv 8 \pmod{2799360000},\ \beta \equiv 6 \pmod{466560000},$$

$$\gamma \equiv 1 \pmod{2799360000},\ \delta \equiv 3 \pmod{2799360000},$$

$$\varepsilon \equiv 3 \pmod{5598720000}.$$

Then we might be suspicious, and check that in fact

$$2^8 + 3^6 + 5^1 + 7^3 - 11^3 = 2.$$

Application of the New Conjecture - some remarks

• Observe that though the strategy contains heuristic points, once we succeed to find an appropriate modulus m in the last step, it is justified that the original equation (1) has no solutions with $\alpha_{ij} \geq \alpha_0$.

• After getting rid of an unknown, the procedure can be repeated. Finally, if everything works out well, we get all solutions.

• In principle, this strategy works if there exists (a not at all preliminary computable!) constant A, such that for all solutions of (1) we have $\min_{1 \leq i \leq k, 1 \leq j \leq \ell} \alpha_{ij} < A$. (Since then we can eliminate one of the unknowns.) This is the case, for example, if (1) has no solutions with vanishing subsum.

Numerical results

Theorem 6. (Bertók, H, 201?). For all $0 \leq c \leq 36$, the equation

$$2^{\alpha} + 3^{\beta} + 5^{\gamma} + 7^{\delta} - 11^{\varepsilon} = c$$

is solvable, and altogether it has precisely 281 solutions. For $c = 37$ the above equation has no solutions.

Theorem 7. (Bertók, H, 201?). The equation

$$2^{\alpha_1} + \cdots + 2^{\alpha_8} = 3^{\beta}$$

has precisely 77 solutions with $\alpha_1 \leq \cdots \leq \alpha_8$.

Remark. A modulus similar to the previously mentioned one works well also here. In fact equations like in Theorem 7 are much simpler, since there only two different bases involved, so one can find appropriate moduli rather easily.

Thank you very much

for your attention!