SKOLEM'S CONJECTURE CONFIRMED FOR A FAMILY OF EXPONENTIAL EQUATIONS, III

L. HAJDU, F. LUCA, AND R. TIJDEMAN

Dedicated to János Pintz on the occasion of his 70th birthday.

Abstract. We prove Skolem's conjecture for the exponential Diophantine equation $a^n + tb^n = \pm c^n$ under some assumptions on the integers a, b, c, t. In particular, our results together with Wiles' theorem imply that for fixed coprime integers a, b, c Fermat's equation $a^n + b^n = c^n$ has no integer solution $n \geq 3$ modulo m for some modulus m depending only on a, b, c. We also provide a generalization where in the equation b^n is replaced by a product $b_1^{k_1} \cdots b_\ell^{k_\ell}$.

1. Introduction

Skolem's conjecture states that if a purely exponential Diophantine equation is not solvable, then it is not solvable modulo an appropriate modulus (see [13]). The conjecture and its variants have been proved only in certain special cases. One can mention results of Schinzel [10] concerning the one-term case, Bartolome, Bilu and Luca [1] concerning the case where the bases generate a multiplicative group of rank one, Hajdu and Tijdeman [8] concerning equations of the form $a^n - b^k = 1$, and Bérczes, Hajdu and Tijdeman [2] concerning equations of the form $a^n - tb_1^{k_1} \dots b_\ell^{k_\ell} = \pm 1$. See also Bertók and Hajdu [3, 4] for a result asserting that in some sense Skolem's conjecture is valid for "almost all" equations. For related problems and results concerning recurrence sequences, one can consult the papers [6, 9, 11, 12], and the references

Date: December 19, 2020.

2010 *Mathematics Subject Classification.* 11D61, 11D79.

Key words and phrases. Exponential Diophantine equations, Fermat's equation, Skolem's conjecture.

Research of L. H. was supported in part by grants 115479, 128088 and 130909 of the Hungarian National Foundation for Scientific Research and by the projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015, co-financed by the European Union and the European Social Fund. F. L. worked on this paper during a 7 month research visit at the Max Planck Institute for Software Systems in Saarbrücken, Germany in late 2020 and early 2021.

there and for a more detailed survey of the related literature, see [2] or [3].

In this note, we prove that under some natural assumptions, Skolem's conjecture is valid for the equations $a^n + tb^n = \pm c^n$ (see Theorem 2.1). Note that our result contains the case of Fermat's equation $a^n + b^n = c^n$ with fixed coprime integers a, b, c. We also give a more general result, where in the equation b^n is replaced by a product $b_1^{k_1} \dots b_\ell^{k_\ell}$ (see Theorem 2.2).

2. New results

Theorem 2.1. *Let a, b, c, t be non-zero integers with $\gcd(a, tb, c) = 1$ and $|b| > 1$, and let $\varepsilon \in \{-1, 1\}$. Then there exists a modulus m such that the congruence*

$$a^n + tb^n \equiv \varepsilon c^n \pmod{m}$$

has the same solutions in positive integers n as the equation

$$a^n + tb^n = \varepsilon c^n.$$

Further, such a modulus m can be effectively calculated in terms of a, b, c, t.

By the famous result of Wiles [14] on Fermat's Last Theorem, the following statement follows from Theorem 2.1.

Corollary 2.1. *Let a, b, c be integers with $\gcd(a, b, c) = 1$. Then there exists a modulus m such that the congruence*

$$a^n + b^n \equiv c^n \pmod{m}$$

has no solutions in positive integers n with $n \geq 3$. Further, such a modulus m can be effectively calculated in terms of a, b, c.

Remarks. 1. We note that the coprimality condition in Theorem 2.1 cannot be dropped. Indeed, as one can easily check, the equation

$$2^n + 2^n = 4^n$$

has only the solution $n = 1$ in positive integers. However, they have infinitely many solutions modulo m for any m. This also means that the versions of Skolem's conjecture proposed in [3] and [4] should be carefully reformulated. On the other hand, the statement holds also when $atbc = 0$, even with non-negative integer unknown n. The proofs of these statements are simple, however, involve quite a lot technicalities. So to keep the presentation clear, we exclude these cases.

2. Observe that Corollary 2.1 implies the validity of Fermat's conjecture. However, this should not be interpreted as an elementary proof

of Fermat's Last Theorem, as the proof of Corollary 2.1 via Theorem 2.1 relies on Wiles' theorem [14].

3. We note that there is a close connection between Theorem 2.1 and ternary linear recurrence sequences which we now describe. Let a, b, c, t be non-zero integers with $\gcd(a, tb, c) = 1$ and $|b| > 1$, and let $\varepsilon \in \{-1, 1\}$. Consider the sequence $\mathbf{u} := \{u_n\}_{n \geq 0}$ given by

$$u_n := a^n + tb^n - \varepsilon c^n \qquad \text{for all} \quad n \geq 0. \tag{1}$$

This is a ternary recurrent sequence of integers, that is, it satisfies a linear recurrence of order 3 with constant coefficients which we do not write down explicitly. Put

$$\mathcal{Z}_{\mathbf{u}} := \{n \geq 0 : u_n = 0\}.$$

The set $\mathcal{Z}_{\mathbf{u}}$ is called the zero set of the recurrence $\mathbf{u}$ and it is an object which has been frequently studied in the theory of linear recurrences. It follows from a famous theorem of Skolem–Mahler–Lech that $\mathcal{Z}_{\mathbf{u}}$ is finite. In our case the members of $\mathcal{Z}_{\mathbf{u}}$ are effectively computable using the theory of linear forms in p-adic logarithms. Indeed, let p be a prime factor of b. Write $\nu_p(m)$ for the exponent of p in the factorization of m. Suppose that $\mathcal{Z}_{\mathbf{u}}$ contains an element $n_0 > 0$. If $p \mid ac$, then p divides both a and c, which is false. Thus, p does not divide ac and then

$$n_0 \leq \nu_p(tb^{n_0}) = \nu_p(a^{n_0} \pm c^{n_0}) \ll \log n_0.$$

The last inequality holds by linear forms in p-adic logarithms [15]. So, either there is a prime factor p of b which divides ac in which case $\mathcal{Z}_{\mathbf{u}} \subseteq \{0\}$, or p does not divide ac in which case the members of $\mathcal{Z}_{\mathbf{u}}$ are effectively computable.

4. In our proof we shall often use the following strategy. If we get some information about the solutions modulo m_1 and also modulo m_2, then we can combine them using the modulus $m = m_1 m_2$. In particular, in this way we can handle the solutions with n bounded separately.

Our method permits the following generalization.

Theorem 2.2. *Let $a, c, t, b_1, \ldots, b_\ell$ be non-zero integers with $|b_i| > 1$ $(i = 1, \ldots, \ell)$ and $\gcd(a, c, tb_1 \cdots b_\ell) = 1$. Further, let $\varepsilon \in \{-1, 1\}$. Then for any monotone non-decreasing real function $f(x)$ there exists a modulus m which can be effectively calculated in terms of $a, c, t, b_1, \ldots, b_\ell$ and f, such that the congruence*

$$a^n + tb_1^{k_1} \cdots b_\ell^{k_\ell} \equiv \varepsilon c^n \pmod{m} \tag{2}$$

has the same solutions in positive integers $n, k_1, \ldots, k_\ell$ satisfying

$$n \leq f(\max(k_1, \ldots, k_\ell)) \tag{3}$$

as the equation

$$a^n + tb_1^{k_1} \cdots b_\ell^{k_\ell} = \varepsilon c^n. \tag{4}$$

Remarks. 5. Similarly to Theorem 2.1, the statement holds also when $actb_1 \cdots b_\ell = 0$, even with non-negative integer unknowns $n, k_1, \dots, k_\ell$. The proof of this claim is easy, but would need several technical considerations. So for the sake of clarity, we do not include this case into the theorem.

6. In view of $\gcd(a, c, tb_1 \cdots b_\ell) = 1$, it is well-known that all solutions $n, k_1, \dots, k_\ell$ of the S-unit equation (4) satisfy

$$\max(n, k_1, \dots, k_\ell) < C, \tag{5}$$

where C is an effectively computable constant depending only on the parameters $a, c, b_1, \dots, b_\ell, t$. (See Section 4 of [7] for related results and history.) Thus taking $f(x) = C$ in Theorem 2.2, we see that the solution set of (4) and the set of solutions of (2) (with the appropriate modulus) satisfying (3), coincide. So in principle, one can solve (4) in the following way. Calculate C such that (5) is satisfied (by Baker's method; see e.g. Section 5.1 of [7] for details). Then find all solutions to (2) with $n < C$, where m is the modulus corresponding to $f(x) = C$. However, we do not think that this method would be more efficient than the reduction method based upon the LLL algorithm (see e.g. Sections 5.2 and 5.3 of [7] for details).

7. From the proof it will be clear that there exists a modulus m_0 such that for all solutions $n, k_1, \dots, k_\ell$ of (2) with $m = m_0$ we have

$$\max(k_1, \dots, k_\ell) < k_0.$$

Here m_0 and k_0 depend only on $a, c, b_1, \dots, b_\ell, t$. Hence, in Theorem 2.2 we can take any f having the property $f(x) = f(k_0)$ for $x \geq k_0$.

We conclude this section with an open problem.

Problem 2.1. *Does there exist a modulus m such that the solution sets of congruence* (2) *and of equation* (4) *coincide? In other words, can one remove condition* (3) *and retain the conclusion of Theorem 2.2?*

3. An auxiliary result

In the proof of our results we use the following lemma which nowadays is a simple consequence of a deep theorem of Bilu, Hanrot and Voutier [5]. However, the version below follows already from a classical result of Zsigmondy [16].

Lemma 3.1. *Let a, c be coprime non-zero integers with $|ac| > 1$. Then apart from at most four values of $n \geq 2$ the number $c^n - a^n$ has a primitive prime divisor, which is a prime factor p such that $p \nmid c^r - a^r$ for any $1 \leq r < n$. The same holds for $c^n + a^n$.*

Proof. The statement concerning $c^n - a^n$ immediately follows from Theorem C, Theorem 1.3 and Theorem 1.4 in [5]. The statement for $c^n + a^n$ is a direct consequence of this assertion as well upon noting that

$$c^n + a^n = \frac{c^{2n} - a^{2n}}{c^n - a^n} \qquad \text{holds for all} \qquad n \geq 1.$$

□

4. Proofs of the main results

We start with the proof of Theorem 2.2. Clearly, Theorem 2.1 can then be obtained as a simple consequence.

Proof of Theorem 2.2. First we treat some special cases and then we turn to the general situation.

The proof in some special cases.

Case A) $|a| = |c| = 1$.

Let p_i be a prime divisor of b_i $(1 \leq i \leq \ell)$, put $P = p_1 \cdots p_\ell$, and let q be an odd prime which does not divide $tb_1 \cdots b_\ell$. Then

$$m = P^2 q(|tb_1 \cdots b_\ell| + 3)$$

is an appropriate choice. Indeed, by considering (2) modulo q, we see that $\varepsilon c^n - a^n \neq 0$. Then considering it modulo P^2, we obtain $k_i \leq 1$ $(1 \leq i \leq \ell)$. Finally, considering it modulo $|tb_1 \cdots b_\ell| + 3$ we get that $n, k_1, \ldots, k_\ell$ is a solution of the congruence if and only if it is a solution to (4).

Case B) The numbers $a, c, tb_1 \cdots b_\ell$ are not pairwise coprime.

If a and c are not coprime, then let p be a common prime factor of a and c. In view of $\gcd(a, c, tb_1 \cdots b_\ell) = 1$, we have $p \nmid tb_1 \cdots b_\ell$. Thus the congruence

$$a^n + tb_1^{k_1} \cdots b_\ell^{k_\ell} \equiv \varepsilon c^n \pmod{p}$$

gives $n = 0$ which is excluded.

Next assume that $\gcd(tb_1 \cdots b_\ell, ac) \neq 1$. We do not actually prove the statement in this case, we only show that without loss of generality we may assume that this situation does not occur. Suppose first that there is a prime divisor p of t such that $p \mid ac$. By what we have already proved, we may assume that p divides one of a, c, but not both. Thus the congruence

$$a^n + tb_1^{k_1} \cdots b_\ell^{k_\ell} \equiv \varepsilon c^n \pmod{p}$$

in view of $n > 0$ gives a contradiction. Hence we may assume that $\gcd(t, ac) = 1$. Now rearranging indices if necessary, we may assume that for some j with $0 \le j < \ell$ we have $\gcd(b_i, ac) = 1$ $(1 \le i \le j)$ and $p_i \mid \gcd(b_i, ac)$ with some prime p_i $(j < i \le \ell)$. As before, we may assume that every p_i $(j < i \le \ell)$ divides one of a, c, but not both. Then the congruence

$$tb_1^{k_1} \cdots b_\ell^{k_\ell} \equiv \varepsilon c^n - a^n \pmod{p_{j+1} \cdots p_\ell}$$

gives that either $n = 0$ or $k_{j+1} = \cdots = k_\ell = 0$. Since these cases are excluded, we are done.

The proof of the statement in the general case.

By our assumptions and what we have proved so far, we may assume that $|ac| > 1$, $|b_i| > 1$ for $i = 1, \ldots, \ell$, $t \neq 0$ and that a, c, $tb_1 \cdots b_\ell$ are pairwise coprime. Further, we are interested in positive integer solutions $n, k_1, \ldots, k_\ell$ of (2) and (4).

We prove the statement by induction on ℓ. For simplicity, for $\ell = 1$ we rewrite equation (4) as

$$a^n + tb^k = \varepsilon c^n.$$

With this notation, the statement concerns only the solutions n, k with $n \le f(k)$. Throughout the proof of the case $\ell = 1$, p is a prime factor of b. Hence, by Case B, $p \nmid ac$.

Consider first the case $\varepsilon = 1$. Let $z(p)$ be the order of appearance of p in $\{a^n - c^n\}_{n \ge 0}$. This coincides with the order o_p of the residue class a/c modulo p, where $1/c$ modulo p stands for the inverse of c modulo p. It is also the smallest positive integer r such that $a^r - c^r \equiv 0 \pmod{p}$. Write $a^{z(p)} - c^{z(p)} = p^{\lambda_p} q$ for some integers $\lambda_p \ge 1$ and q coprime to p. Let $K = \omega(tb) + 6$, where $\omega(u)$ denotes the number of distinct prime factors of u.

Take the numbers $a^{z(p)p^r} - c^{z(p)p^r}$ for $r = 0, \ldots, K - 1$. By Lemma 3.1, each of these numbers with at most 5 exceptions have a primitive prime divisor, namely a prime q_r with $q_r \mid a^{z(p)p^r} - c^{z(p)p^r}$, which does not divide $a^s - c^s$ for any $s < z(p)p^r$. Set $q_r = 1$ if r is an exception, and put $Q := q_1 \cdots q_{K-1}$.

We show that if n, k is a solution to the congruence

$$a^n + tb^k \equiv c^n \pmod{p^{\lambda_p + K} Q}. \tag{6}$$

then $k < \lambda_p + K$. For this, assume to the contrary that we have a solution n_0, k_0 to (6) with $k_0 \geq \lambda_p + K$. For such a solution we have $p^{\lambda_p+K} \mid a^{n_0} - c^{n_0}$. By the properties of the order of appearance, we have that $z(p)p^{K-1} \mid n_0$. The numbers $a^{z(p)p^r} - c^{z(p)p^r}$ divide $a^{n_0} - c^{n_0}$ for $r = 0, \ldots, K-1$. Hence $a^{n_0} - c^{n_0}$ is a multiple of $Q := q_0 \cdots q_{K-1}$. Then by (6) it follows that $Q \mid tb^{k_0}$. However, since $\omega(Q) \geq K - 5 > \omega(tb^{k_0})$ this is not possible. Hence our claim $k < \lambda_p + K$ follows.

Thus putting $n_1 := f(\lambda_p + K)$, our statement follows e.g. modulo

$$m = p^{\lambda_p+K} Q(|a|^{n_1} + |tb^{\lambda_p+K}| + |c|^{n_1} + 1). \tag{7}$$

Indeed, assume that n, k is a solution to congruence (2) with this m, satisfying $n \leq f(k)$. Then first using the congruence modulo $p^{\lambda_p+K}Q$ only, we get that $k < \lambda_p + K$. Hence by the monotone increasing property of f we get $n \leq f(k) \leq n_1$. Then the congruence modulo $(|a|^{n_1} + |tb^{\lambda_p+K}| + |c|^{n_1} + 1)$ gives that n, k is also a solution to equation (4), implying our claim.

Let now $\varepsilon = -1$. Then

$$a^n + c^n + tb^k \equiv 0 \pmod{p}$$

yields that

$$a^n + c^n \equiv 0 \pmod{p}. \tag{8}$$

Assume that p is odd. Then a/c has even order o_p modulo p. Putting now $z(p) = o_p/2$, we have that

$$a^{z(p)} + c^{z(p)} \equiv 0 \pmod{p},$$

and $z(p)$ is the smallest positive integer s such that

$$a^s + c^s \equiv 0 \pmod{p}.$$

We take K similarly as in the case when $\varepsilon = 1$, namely $K = \omega(tb) + 6$. Consider the congruence

$$a^n + c^n + tb^k \equiv 0 \pmod{p^{\lambda_p+K}},$$

where we put $\lambda_p := \nu_p(a^{z(p)} + c^{z(p)})$. As in the case $\varepsilon = 1$, for $k \geq \lambda_p + K$ we have $z(p)p^{K-1} \mid n$ and $n/(z(p)p^{K-1})$ is odd. The rest of the argument is similar to the case $\varepsilon = 1$. Namely, we work with $a^{z(p)p^\ell} + c^{z(p)p^\ell}$ where $\ell = 0, 1, \ldots, K-1$ which are all divisors of $a^n + c^n$ since p and $n/(z(p)p^{K-1})$ are both odd.

Assume now that b is a power of 2. Then a and c are odd. We put $r := \nu_2(a + c)$. The solutions of the congruence

$$a^n + c^n + tb^k \equiv 0 \pmod{2^{r+1}}$$

satisfy $k \le r$. Indeed, if $k \ge r+1$ would hold, then we would get that 2^{r+1} divides $a^n + c^n$. This is is not possible if n is even since then $\nu_2(a^n + c^n) = 1 < r+1$ and it is not possible if n is odd since then $\nu_2(a^n + c^n) = \nu_2(a+c) = r < r+1$.

Now the proof finishes as in the case $\varepsilon = 1$ by taking m given by formula (7) with $p = 2$, and $\lambda_p + K$, Q and n_1 replaced by $r+1$, 1 and $f(r)$, respectively. Hence, the theorem follows also in this case, and the proof is complete for $\ell = 1$.

Let now $\ell > 1$, and assume that the statement is valid for $\ell - 1$. Without loss of generality we may assume that $k_1 \ge k_2 \ge \cdots \ge k_\ell$. Indeed, there are at most $\ell!$ types of solutions $n, k_1 \ldots, k_\ell$ of (4) according to the ordering $k_{i_1} \ge \cdots \ge k_{i_\ell}$, corresponding to permutations $\pi = (i_1, \ldots, i_\ell)$ of the indices $(1, \ldots, \ell)$. So finding moduli m_π for all permutations π, the modulus $m = \prod_\pi m_\pi$ is clearly appropriate. Let p_i be a prime divisor of b_i $(i = 1, \ldots, \ell)$ and set $p = p_\ell$.

Now by a similar argument as for $\ell = 1$ (replacing tb^k by $tb_1^{k_1} \cdots b_\ell^{k_\ell}$), we get that there exists a modulus m_0 such that for all solutions $n, k_1, \ldots, k_\ell$ of

$$a^n + tb_1^{k_1} \cdots b_\ell^{k_\ell} \equiv \varepsilon c^n \pmod{m_0}$$

we have $k_\ell \le C_0$ with some integer C_0. Here m_0 and C_0 depend only on $a, c, b_1, \ldots, b_\ell, t$.

By the induction hypothesis, there exist integers $m_j \ge 2$ $(1 \le j \le C_0)$ such that writing $t_j = tb_\ell^j$, the statement is valid for the equation

$$a^n + t_j b_1^{k_1} \cdots b_{\ell-1}^{k_\ell - 1} = \varepsilon c^n$$

with modulus m_j. Then the induction step is completed by letting

$$m := m_0 m_1 \cdots m_{C_0}.$$

□

Proof of Theorem 2.1. Taking $\ell = 1$ and $f(x) = x$ in Theorem 2.2, the statement immediately follows. □

Proof of Corollary 2.1. Assume first that $abc \ne 0$. If $|b| > 1$, the statement immediately follows from Theorem 2.1 combined with the famous theorem of Wiles [14] on Fermat's equation. If $|b| = 1$ and $|a| > 1$, then switching b and a the statement follows similarly. If $|a| = |b| = 1$ and $|c| > 1$, then interchanging the roles of b and c and letting $t = \varepsilon = -1$ in Theorem 2.1, we are done in the same way. If we have $|a| = |b| = |c| = 1$, the statement follows with $m = 4$.

Let now $abc = 0$. If two out of a, b, c are zero, then by $\gcd(a, b, c) = 1$ we see that the third number is ± 1. Then the statement follows with

$m = 2$. So we may suppose that precisely one of a, b, c is zero. If the other two numbers are ±1, then we are done with $m = 3$. Thus there is a prime p which divides one of the non-zero numbers out of a, b, c, but does not divide the other non-zero number. Then we are done with $m = p$. □

Acknowledgements

The authors are grateful to the referee for the helpful remarks.

References

[1] B. Bartolome, Yu. Bilu and F. Luca, *On the exponential local-global principle*, Acta Arith. **159** (2013), 101–111.

[2] A. Bérczes, L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations, II*, Acta Arith. (published online: 8 October 2020).

[3] Cs. Bertók and L. Hajdu, *A Hasse-type principle for exponential Diophantine equations and its applications*, Math. Comput. **85** (2016), 849–860.

[4] Cs. Bertók and L. Hajdu, *A Hasse-type principle for exponential Diophantine equations over number fields and its applications*, Monatsh. Math. **187** (2018), 425–436.

[5] Yu. Bilu, G. Hanrot, P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. reine angew. Math. 539 (2001), 75-122.

[6] K. A. Broughan and F. Luca, *On the Fürstenberg closure of a class of binary recurrences*, J. Number Theory **130** (2010), 696–706.

[7] J.-H. Evertse, K. Győry, *Unit equations in Diophantine number theory*, Cambridge University Press, 2015.

[8] L. Hajdu and R. Tijdeman, *Skolem's conjecture confirmed for a family of exponential equations*, Acta Arith. **192** (2020), 105–110.

[9] A. Ostafe and I. Shparlinski, *On the Skolem problem and some related questions for parametric families of linear recurrence sequences*, arXiv:2005.06713 [math.NT] 14 May 2020.

[10] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. **27** (1975), 397–420.

[11] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274; Addendum and corrigendum, ibid. **36** (1980), 101–104.

[12] A. Schinzel, *On the congruence* $u_n \equiv c \pmod{p}$ *where* u_n *is a recurring sequence of the second order*, Acta Acad. Paedagog. Agriensis Sect. Math. **30** (2003), 147–165.

[13] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avhdl. Norske Vid. Akad. Oslo I, 1937, no. 12, 16 pp.

[14] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

[15] K. Yu, *Linear forms in logarithms in the p-adic case*, New Advances in Transcendence Theory, ed. by A. Baker, Cambridge University Press, 1988, pp. 411-434.

[16] K. Zsigmondy, *Zur Theorie der Potenzreste*, J. Monatsh. Math. **3** (1892), 265–284.

L. Hajdu
Institute of Mathematics
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
Email address: hajdul@science.unideb.hu

F. Luca
School of Mathematics
University of the Witwatersrand
Private Bag X3, WITS 2050
Johannesburg, South Africa
Research Group in Algebraic Structures and Applications
King Abdulaziz University, Jeddah, Saudi Arabia
Email address: Florian.Luca@wits.ac.za

R. Tijdeman
Mathematical Institute
Leiden University
Postbus 9512, 2300 RA Leiden, The Netherlands
Email address: tijdeman@math.leidenuniv.nl