Abstract. "Professor Littlewood, when he makes use of an algebraic identity, always saves himself the trouble of proving it; he maintains that an identity, if true, can be verified in a few lines by anybody obtuse enough to feel the need of verification." (Dyson [Dj]).

Nowadays obtuse mathematicians can use computer algebra. Littlewood's dictum is obvious for finite algebraic identities like \((a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\). In this paper, identities are classified into three classes: Real-time-Littlewoodian, Zillion years-Littlewoodian, and Non-Littlewoodian. I suggest a research program whose purpose will be to classify identities, and families of identities, into these classes, and to try and enlarge the family of real-time Littlewoodian identities by devising efficient algorithms.

1. Introduction. David Blackwell once said that in order for a result to be interesting, it is not enough that it be new. For example, if one takes any two ten-digit numbers and multiplies them together, then the resulting identity is very probably a new result, but it is uninteresting. In any case, it is unnecessary nowadays to prove a result like \("123 \times 234 = 28782"\), because it clearly belongs to a class of identities for which there is a well known verification algorithm. This algorithm of multiplication of two integers written in decimal notation is known to any four-grades and has been programmed into every calculator (for integers whose product has up to ten digits). Furthermore, in most computer algebra systems, one can multiply integers with an arbitrary number of digits, where the limit depends on the available memory of the computer.

So let us make the following definition:

**Definition.** An identity is **Littlewoodian** if it clearly belongs to a class of identities for which there is a known and programmable algorithm for determining the truth of the identity.

For example any identity like \("123 \times 234 = 28782"\) is obviously Littlewoodian, as are finite algebraic identities like

\[(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\]

Of course being Littlewoodian is time-dependent, and it is not enough that there is an algorithm, we must know how to perform it. It is conceivable that one can prove that a class of identities is intrinsically non-Littlewoodian, in analogy to Matijasevic's solution of Hilbert's tenth problem.

Consider the identity

\[(100^{100^{100}} + 1) \times (100^{100^{100}} - 1) = 100^{100^{100}} - 1,\]

*Supported in part by NSF grant DMS-8800662
†Department of Mathematics, Drexel University, Philadelphia, PA 19104
where it is assumed that the integers are spelled out in decimal notation, with \((10^{100})^{100}\) digits. Although this identity is certainly Littlewoodian, it will take a zillion years, and zillion bytes of memory to perform. Such an identity I call Zillion years Littlewoodian. Of course any moderately smart human or artificially smart machine will recognize the above identity as a special case of the algebraic identity \((a + 1)(a - 1) = a^2 - 1\), which is itself Real-time Littlewoodian, but this is not allowed, because finding the right generalization is not a purely mechanical operation in general.

The notion of “Real-time–Littlewoodian” is also time dependent, because any day there may be a better algorithm. However it is conceivable that a class of identities be declared intrinsically zillion years–Littlewoodian, in analogy with the notion of intractableness in computer science.

Once a class of identities has been declared Littlewoodian, the human mathematician is far from superseded. We still need human mathematicians to conjecture nice identities, relate them to other branches of mathematics, and give proofs with insight, that explain why the identity is true. This insight will often show us how to generalize it to an identity that is non-Littlewoodian. The purpose of the computer is to save humans the dreadful task of devising proofs that Hardy called scornfully “essential verifications”, and concentrate on trying to find insightful proofs.

2. Quiz. For each of the following identities, state whether the identity is Real-time–Littlewoodian, Zillion years–Littlewoodian, or Non–Littlewoodian. Answers to this quiz are given in the next section.

1. (Euler) \[ 2^5 + 1 = 641 \times 670041. \]

2. (Landau and Parkin [L-P]) \[ 27^5 + 84^5 + 110^5 + 133^5 = 144^5. \]

3. a. (Leonardo of Pisa) \[ (a^2 + b^2) \times (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \]

b. (Euler) \[
(a^2 + b^2 + c^2 + d^2) \times (A^2 + B^2 + C^2 + D^2) =
(aA + bB + cC + dD)^2 + (aB - bA - cD + dC)^2 + (aC - bD - cA + dD)^2 +
(aD - bC - cB + dA)^2.
\]

4. \[
\sum_{i=1}^{N} n^3 = (N(N + 1))^2 / 4.
\]

5. \[ \sin(x + a) = \sin x \cos a + \cos x \sin a. \]

6. (Cassini) Let \( F_n \) be the Fibonacci numbers defined by \( F_0 = 0, F_1 = 1, \) and \( F_n = F_{n-1} + F_{n-2}, \) then \( F_{n+1}F_{n-1} - F_n^2 = (-1)^n. \)

7. Let \( b(n) \) be the number of complete binary trees with \( n \) leaves, and \( t(n) \) be the number of ordered trees with \( n \) vertices, then \( b(n) = t(n). \)

8. Consider the lattice \[ L(n, 2) := \{(a^1, \ldots, a^n); 2 \geq a^1 \geq \cdots \geq a^n \geq 0\}. \]

The following chains \((0 \leq 2i \leq n)\) constitute a symmetric chain decomposition of \( L(n, 2) \): \[ C_i^{(n)} := 2^i \rightarrow 2^i 1 \rightarrow \cdots \rightarrow 2^i 1^{n-2i} \rightarrow 2^i 1^{n-2i} \rightarrow \cdots \rightarrow 2^n. \]

9. a. For all square matrices \( A, B, \) of size \( n \leq 9, \) \( \det(AB) = \det(A) \det(B). \)

b. For all square matrices \( A, B, \) of size \( n = 9000, \) \( \det(AB) = \det(A) \det(B). \)

c. For all square matrices of arbitrary size \( n, \) \( \det(AB) = \det(A) \det(B). \)

10. (Amitsur-Levitski)

For an arbitrary \( n, \) let \( A_1, \ldots, A_{2n} \) be \( 2n \) square \( n \times n \) matrices, then:
\[ \sum_{n=1}^{2n} \text{sgn}(\pi)A_{\pi(1)} \cdots A_{\pi(2n)} = 0. \]

11. (Dyson)

a. The constant term of \[ [(1 - x/y)(1 - y/x)(1 - x/z)(1 - z/x)(1 - y/z)(1 - z/y)]^3 \]
is \( (3a)!/a^{10}. \)

b. The constant term of
\[ \prod_{1 \leq i \leq 2000} (1 - \frac{x_i}{x_j}) \]
is \( (1000a)!/a^{1000}. \)
c) (Dyson's conjecture, see [An]) the constant term of
\[
\prod_{1 \leq i \neq j \leq n} (1 - \frac{x_i}{x_j})^a
\]
is \((na)/a^a\).

12 (Omar Khayyam)

a)
\[(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3\].

b)
\[(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}/(i!(n-k)!)]\]

c)
\[(x_1 + \cdots + x_m)^n = \sum_{k_1 + \cdots + k_m = n} \binom{n}{k_1} \cdots \binom{n}{k_m} / (k_1! \cdots k_m!)\].

13

a)
\[\sum_{n=1}^{N} \frac{1}{n^3} - \frac{5}{2} \sum_{n=1}^{N} \frac{(-1)^{n-1}}{n^3(2^n)} = \sum_{k=1}^{N} \frac{(-1)^k}{2k^3 \binom{N+k}{k} \binom{N}{k}}\].

b)
\[
\sum_{n=1}^{\infty} \frac{1}{n^3} = \frac{5}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^3(2^n)}\].

14 (Rogers–Ramanujan)

a)
\[\sum_{n=0}^{\infty} \frac{q^n}{(1-q) \cdots (1-q^n)} = \prod_{i=0}^{\infty} \frac{1}{(1-q^{5i+1})(1-q^{5i+4})}\].

b) ([Br])
\[\sum_{r=0}^{n} \frac{q^r}{(q)_{n-r}} = \sum_{r=-n}^{n} \frac{(-1)^{r}q^{(5r^2-r)/2}}{(q)_{n-r}(q)_{n+r}}\].

3. Answers to the Quiz.

Real-time–Littlewoodian: 1-8, 9a, 11a, 12a, 12b, 13a, 14b.

Zillion years–Littlewoodian: 9b, 11b.

Non–Littlewoodian: 9c, 10, 11c, 12c, 13b, 14a.

4. Discussion.

1 and 2:
These are examples of interesting numerical identities. 1) gives a refutation of Fermat's conjecture that \(2^{2^n} + 1\) is always prime, and 2) refutes Euler's conjecture that it is impossible to express a fifth power as a sum of four perfect fifth powers. A formal proof of these identities will involve writing all the integers as a combination of powers of 10, invoking the associative and distributive laws, and then using the 100 "lemmas" that comprise the multiplication table and the 100 lemmas that constitute the addition table. Since arithmetic with specific integers is so much part of our culture, it would not occur to anyone to give a proof of a statement like 2), and the proof is considered routine by general consensus.

3:
Way back in 1202, when Liber Abaci first appeared, identity 3a) was a deep theorem, and there were very few people who understood its proof. Nowadays this is a routine exercise with the same epistemological stature as \(9 \times 11 = 99\). But although routine, it is an important identity in number theory, as it implies the non-trivial fact that the product of two integers that are expressible as a sum of two squares is itself a sum of two squares. Similar remarks apply to identity 3b), which implies that if one can show that every prime is expressible as a sum of four squares, then every integer can be so expressed.

Although the proofs of 3a) and 3b) are completely routine, they are nevertheless elegant identities, and one may want to understand why they are true, as opposed to whether they are true. One such explanation is that for two complex numbers \(z_1 = a + ib\), and \(z_2 = c + id\), \(|z_1z_2| = |z_1||z_2|\). The analogous identity in the quaternions gives 3b). These observations were perhaps the motivation to Gauss's discovery of the Gaussian integers and to Hamilton's discovery of the quaternions.

4:
Any identity of the form
\[\sum_{n=1}^{N} p(n) = q(N)\]
with \(p\) and \(q\) polynomials, is routinely verifiable, since it is equivalent to
\[q(N) - q(N - 1) = p(N)\].

Unfortunately, many inane identities of this kind are assigned to students, expecting them to use mathematical induction. Many students who do not understand mathematical induction "prove" such identities by plugging in a few values. They are not that wrong. For example, in order to prove identity 4) all we need is check it in 5 different values, say \(N = 0, 1, 2, 3, 4\), since both sides are polynomials of degree 4.
5. Trigonometric identities are the bane of many a high school student. Using \( \cos x = (e^{ix} + e^{-ix})/2 \) and \( \sin x = (e^{ix} - e^{-ix})/2i \), they are all routine, and indeed trigonometric simplifications are built-in to most computer algebra systems.

6. Writing the Fibonacci numbers in terms of Binet's formula, identities like 6) are trivially verifiable, as are all identities involving sums and products of Fibonacci numbers, or more generally, solutions of constant coefficients homogeneous linear recurrences.

7. Thanks to the work of the Lotharingien school (Schützenberger, Foata, Viennot and their students), many combinatorial sequences are known to have generating functions that are algebraic formal power series. It is by now a routine matter to find the equation satisfied by such a generating function and to see whether two such sequences are equivalent. In fact it should be possible to find a priori bounds for the order of the equation satisfied by the generating function, as well as bounds for the degrees of the coefficients. Then it should be possible to find an a priori integer \( N \) such that if the two combinatorial sequences of the problem are equal up to \( N \), then they are identical. It follows that many theorems on trees, and on two- and three-dimensional lattice walks, are either routine or routineable. Of course it is nice to have nice proofs, preferably bijective, to prove such results, but if the proof is going to be ugly it may just as well be done by computer.

8. This statement is not only "routine" in the colloquial sense of the word, but is also technically routine, since it can be easily encoded in terms of an identity involving rational functions of a fixed number of variables.

Consider

\[ M(n) := \{(a_1, \ldots, a_m) : \text{ for some } m \geq 0, n \geq a_1 \geq a_2 \geq \cdots \geq a_m \geq 0\} . \]

(Note that we allow some trailing zeroes). Introduce the commuting indeterminates \( x_1, \ldots, x_n \) and \( t \), and define the weight

\[ \text{weight} (a_1, \ldots, a_m) = x_{a_1} \cdots x_{a_m} t^{e_m}, \]

with the convention that \( x_0 = 1 \). The subset of \( M(n) \) of partitions of length \( m \) (allowing zeroes) can be easily identified with Young's lattice \( L(m, n) \). It is easily seen that the total weight of \( M(n) \) ( i.e. the sum of the weights is )

\[ (1-t)^{-1}(1-x_1t)^{-1} \cdots (1-x_nt)^{-1}. \]

The total weight of the chain \( C_1(n) \), for a fixed \( n \) is

\[ (x_1^1 + x_2^1 x_1 + \cdots + x_2^{n-2} + x_2^{n-2} + x_2^{n-2} + \cdots x_2^{n-2} + 1) t^n, \]

which is some (simple) rational function, and summing with respect to \( n \) yields geometric series that are easily summed. Thus the statement that the chains \( C_i(n) \) cover \( L(2, n) \), for every \( n \), is equivalent to a simple identity among rational functions. Of course it is obvious by inspection that \( C_i(n) \) are symmetric chains.

By the same token, the verifications of West's [We] constructions of symmetric chain decomposition of \( L(4, n) \) and Riese's [Ri] for \( L(3, n) \) and \( L(4, n) \) are purely routine and could have been omitted. This does not take away from their achievements, because the hard part was to find the constructions. But once found, the verification is a purely routine matter and two pages of the European Journal of Combinatorics could have been spared.

On the other hand, a symmetric chain decomposition of \( L(m, n) \) for general \( m \) and \( n \) is not going to be routinely verifiable, at least not at present. Neither is O'Hara's [O'H] recent magnificent symmetric chain decomposition of the "complete" version of \( L(m, n) \) where any two partitions with different ranks are related.

9. There are many identities in matrix algebra, of which 9) is one of the simplest. Writing the matrices in generic form, the statement \( \det(AB) = \det(A) \det(B) \), for a fixed \( n \) is nothing but a finite algebraic identity, but of course for \( n = 9000 \) we would have more than 9000!^2 terms! Of course identity 9c), for general \( n \), is non-Littlewoodian (at least today).

10. This is the celebrated Amitsur-Levitski identity, that was given an elegant proof by Rosset [Ro]. For general \( n \) it is non-Littlewoodian.

11. Identity 11c) is Dyson's ex-conjecture, that was proved by Wilson and Gunson and that was given a short and elegant proof by Good (see [An]). For general \( n \) this is certainly non-Littlewoodian, but for \( n = 3 \) (identity 11a) and for \( n = 1000 \) (11b) it is real time-Littlewoodian and zillion years-Littlewoodian respectively. This follows from my approach ([Zel]) to special functions identities that is based on I.N. Bernstein's theory of holonomic systems.

12. No one would argue with the assertion that 12a) is real time-Littlewoodian. That the binomial theorem is real time-Littlewoodian follows from my above mentioned approach ([Zel]), but the multinomial theorem, that involves an indefinite number of variables is not covered by this theory, and is thus non-Littlewoodian at present.

13. Identity 13b) was the starting point of Apery's incredible proof of the irrationality of \( \zeta(3) \) ([Poi]). At present such identities that state the equality of two infinite hypergeometric series (and whose summands only depend on the index of summation, and not on an auxiliary parameter) are non-Littlewoodian. On the other hand,
13b), which is the “finite form” of 13a), is nothing but a binomial coefficients identity and is certainly real-time-Littlewoodian. Note that from a human point of view, 13b) is a trivial consequence of 13a), upon taking \( n \to \infty \), and thus 13a) is “deeper” and more general.

14.

This final example illustrates the q-analog of the point made in the previous example. 14a) is one of the Rogers-Ramanujan identities, and involves the equality of an infinite q-hypergeometric series and an infinite q-hypergeometric product. Since we do not have any extra parameters to provide elbow room, it is, at present, non–Littlewoodian. On the other hand, the finite form of this identity, 14b) (that implies 14a) upon taking \( n \to \infty \) and using the Jacobi triple product identity) is nothing but a q-binomial identity, and as such is real-time-Littlewoodian ([Ze]). Given an infinite q-hypergeometric identity we still need, at present, a Schur, an Andrews, or a Bressoud to come up with a conjectured finite form, that my program can then do.

5. An Open Problem. It would be nice if identities like 13b) and 14a) would be provable by computer. Consider an identity

\[
\sum_{i=1}^{\infty} a(n) = \sum_{i=1}^{\infty} b(n),
\]

where \( a(n) \) and \( b(n) \) are hypergeometric sequences, i.e., there are polynomials \( P(n), Q(n), R(n), S(n) \) such that

\[
a(n+1)/a(n) = P(n)/Q(n), \quad b(n+1)/b(n) = R(n)/Q(n).
\]

It would be interesting to develop a decision procedure, in the style of [Go], that will decide whether such an identity is true or false.

Consider

\[
c(N) := \sum_{i=1}^{N} (a(n) - b(n)).
\]

The statement (*) is equivalent to the fact that \( c(N) \to 0 \) as \( N \to \infty \). It is not hard to find a second order linear recurrence equation (with polynomial coefficients) satisfied by \( a(n) - b(n) \), and hence a third order linear recurrence equation satisfied by \( c(N) \). The problem of deciding whether identities of the form (*) are true would follow from the following more general problem:

**Problem.** Given a homogeneous linear recurrence with polynomial coefficients:

\[
p_0(q^n)a(n) + p_1(q^n)a(n-1) + \cdots + p_i(q^n)a(n-i) + \cdots + p_K(q^n)a(n-K) = 0,
\]

and \( K \) initial conditions: \( a(0), \ldots, a(K-1) \), decide whether or not the solution \( a(n) \) of the equation, subject to the initial conditions, has the property that \( a(n) \to 0 \) as \( n \to \infty \).

The Birkhoff-Trijinski method (resurrected in [W-Z]) enables us to find the complete asymptotics of the dominant solution of a linear recurrence equation. What we need is some way to handle the asymptotics of an arbitrary solution, under prescribed initial conditions. On the other hand we are not asking for complete asymptotics but only whether or not it tends to zero.

q-Analogously, one may pose the q-problem, that will enable our machines to prove Rogers-Ramanujan style identities, and will free us humans to prove multivariate extensions, like the multi-variate extensions of Andrews, Gordon, and Bressoud (see [An], (3.45), (3.46)).

**q-Problem.** Given a homogeneous linear recurrence with polynomial coefficients

\[
p_0(q^n)a(n) + p_1(q^n)a(n-1) + \cdots + p_i(q^n)a(n-i) + \cdots + p_K(q^n)a(n-K) = 0,
\]

and \( K \) initial conditions: \( a(0), \ldots, a(K-1) \), (certain polynomials in \( q \)) decide whether or not the solution \( a(n) \) of the equation, subject to the initial conditions, has the property that \( a(n) \to 0 \) as \( n \to \infty \), in the sense of formal power series in \( q \).

I am offering 50 dollars for a solution of the problem, and an additional \( (1 - q^{50})/(1 - q) \) dollars for a solution of the q-problem (where, for this one, I adopt the analyst’s ways of taking \( |q| < 1 \)).

6. Concluding Remarks. The computer is here to stay, for better or for worse, and as Marshal McLuhan has taught us, it will shape our practices, problems, ways of thinking and even our tastes. This was put beautifully by Ruelle [Ru]:

My guess is that, within fifty or hundred years (or it might be one hundred and fifty) computers will successfully compete with the human brain in doing mathematics, and that their mathematical style will be rather different from ours. Fairly long computational verifications (numerical or combinatorical) will not bother them at all, and this should lead not just to different sort of proofs, but more importantly to different sort of theorems being proved.

Most mathematicians nowadays still consider computer-assisted proofs as “cheating”, and a priori “ugly” and “not giving any insight”, as was manifested by the cold and hostile reception of Appel and Haken's marvelous tour-de-force. But I am not worried for Appel and Haken. In a hundred years, their proof will be considered as elegant as any human proof, and its only drawback will be the fact that it involves too much human effort.

In the future, given a “conjecture”, one would try to embed it into a class of statements having a given format, and then develop an effective method for deciding the truth of the statements in this class, or whether it is “undecidable” or “intractable”.

Given an algorithm to decide the truth of such a class of statements, nobody would care if the computer-generated proof, in every given instance, is long and ugly, and this is just as well. What is perhaps sad is that nobody would probably care whether the algorithm itself is elegant or not, and everything will be judged by
IN THE LAND OF OZ*
DAVID M. BRESSOUD†

This paper presents a proof and investigation of a curious identity which is implicit in work of K. O’Hara [7] and which was extracted and first explicitly stated by D. Zeilberger [8]. Zeilberger has referred to this identity as KOH, but in view of his contribution, it seems more appropriate to call it OZ:

\[
\binom{n+j}{j} = \sum_{m_1 + \cdots + m_j = m} \frac{(n+2)j - M_{i-1} - M_{i+1}}{m_i - m_{i+1}},
\]

where the Gaussian polynomial is defined by

\[
\binom{n+j}{j} = \prod_{i=1}^{j} \frac{1 - q^{n-i}}{1 - q^i} \quad \text{if} \quad n \in \mathbb{Z}, \ n \geq 0
\]

\[= 0 \quad \text{otherwise}
\]

Elsewhere in these Proceedings [8] and also in [4] there are discussions of the applications of OZ to proving unimodality of the Gaussian polynomials and to the proof of a conjecture proposed by A. Odlyzko. There is also discussion of the surprising fact that OZ remains valid if we adopt the product definition of the Gaussian polynomial when \( n \) is negative. In this paper I shall restrict my attention to explaining the right side of OZ as a generating function. Actually, we’ll be looking at a more general function:

\[
c_{n,k}(n_1, \ldots, n_k; j)
\]

\[= \sum_{m_1 + \cdots + m_k = m} \prod_{i=1}^{k} \frac{n_i - M_{i-1} - M_{i+1}}{m_i - m_{i+1}},
\]

where

\[M_0 = 0, \ M_i = m_1 + \cdots + m_i, \ M_k = j.
\]

Since the left side of OZ is known to be the generating function for partitions into at most \( j \) parts, each part at most \( n \) (see [1], thm. 3.1), OZ can be restated as the following theorem.

*Partially supported by the National Science Foundation, the National Security Administration, and the Institute for Mathematics and its Applications.
†The Pennsylvania State University, University Park, PA 16802