Nested Squares and Evaluations of Integer Products

Karl Dilcher

CONTENTS

The identity

$$\left((x^2-85)^2-4176\right)^2-2880^2 = (x^2-1^2)(x^2-7^2)(x^2-11^2)(x^2-13^2),$$

discovered by R. E. Crandall, allows the evaluation of a product of 8 integers by a succession of 3 squares and 3 subtractions. The question arises whether there exist formulas like Crandall's with more than 3 nested squares. It will be shown that this is not the case; however, there are infinitely many formulas of length 3.

1. INTRODUCTION

Crandall [1996, p. 109] found the following interesting identity:

$$\begin{aligned}\left((x^2-85)^2-4176\right)^2&-2880^2\\ &= (x^2-1^2)(x^2-7^2)(x^2-11^2)(x^2-13^2). \qquad (1\text{–}1)\end{aligned}$$

The potential significance of this identity, which resembles Horner's scheme for polynomial evaluation, lies in that a product of eight integers on the right of (1–1) can be evaluated as a succession of three squares and three subtracts.

Crandall [1996, p. 109] also asks whether there exist formulas like (1–1) with more than three (say k) nested squares which would produce a product of 2^k integers, or linear factors of the form $x \pm a_j$, $a_j \in \mathbb{N}$. Such formulas would have important consequences for the fast computation of factorials, with further consequences in the field of factorization, etc. (For a general discussion of factorial evaluation, see [Crandall 1996; Crandall et al. 1997].)

It is the main purpose of this note to show that such larger formulas cannot exist; this will be done in Section 3. However, we will first see, in Section 2, that it is easy to give infinitely many formulas of type (1–1), by means of sums of squares. By multiplying two or three such formulas together, one can obtain expressions for products of a relatively large number of integers in arithmetic progression.

Research supported in part by the Natural Sciences and Engineering Research Council of Canada.

1058-6458/2000 $0.50 per page

2. NESTED SQUARES OF LENGTH 3

The left-hand side of (1–1) can be factored in an obvious way. In fact, the two parts thus obtained can likewise be factored, and we get

$$\begin{aligned}&\big((x^2-85)^2-4176\big)^2-2880^2 =\\ &\quad= \big((x^2-85)^2-4176+2880\big)\big((x^2-85)^2-4176-2880\big)\\ &\quad= \big((x^2-85)^2-36^2\big)\big((x^2-85)^2-84^2\big)\\ &\quad= (x^2-85+36)(x^2-85-36)(x^2-85+84)(x^2-85-84)\\ &\quad= (x^2-7^2)(x^2-11^2)(x^2-1^2)(x^2-13^2).\end{aligned}$$

Note that $7^2+11^2 = 1^2+13^2 = 2\cdot 85$. This indicates that we should get a similar formula whenever an even number can be written as a sum of 2 squares in at least two ways. Indeed: we have

Proposition 1. *Suppose the even number n can be written in two different ways as a sum of two squares, say*

$$n = a_1^2 + b_1^2 = a_2^2 + b_2^2.$$

Then

$$\bigg(\Big(x^2-\frac{n}{2}\Big)^2-\Big(\frac{n^2}{4}-\frac{a_2^2b_2^2+a_1^2b_1^2}{2}\Big)\bigg)^2-\Big(\frac{a_2^2b_2^2-a_1^2b_1^2}{2}\Big)^2 = (x^2-a_1^2)(x^2-b_1^2)(x^2-a_2^2)(x^2-b_2^2). \qquad (2\text{–}1)$$

This can be verified by simple calculation, just as in the example above. Also note that

$$\frac{n^2}{4}-\frac{a_2^2b_2^2+a_1^2b_1^2}{2} = \tfrac{1}{8}\big((a_1^2-b_1^2)^2+(a_2^2-b_2^2)^2\big)$$

and

$$\frac{a_2^2b_2^2-a_1^2b_1^2}{2} = \tfrac{1}{8}\big((a_1^2-b_1^2)^2-(a_2^2-b_2^2)^2\big).$$

To obtain examples for (2–1), we let $N_2(n)$ be the number of integral solutions (x, y) of $x^2 + y^2 = n$ with $x > 0$ and $y \geq 0$. Then it is well-known that

$$N_2(n) = \prod_{p\equiv 1(4)} (1 + \operatorname{ord}_p(n)) \qquad (2\text{–}2)$$

if there are solutions at all, i.e., if prime factors $p \equiv 3 \pmod n$ of n occur only to even powers (see [Ireland and Rosen 1990, p. 279], for example). Note that in (2–2), (x, y) and (y, x) for $x \neq y$ count as two different solutions. This means that the smallest even n with two "essentially different" solutions, i.e., with $N_2(n) = 4$, is $n = 2\cdot 5\cdot 13 = 130$, the next one being $n = 2\cdot 5\cdot 17 = 170$. Since $170 = 1^2 + 13^2 = 7^2 + 11^2$, (2–1) specializes to (1–1) in this case. For $n = 130 = 3^2 + 11^2 = 7^2 + 9^2$ we get the smaller example

$$\begin{aligned}&\big((x^2-65)^2-1696\big)^2-1440^2\\ &\quad= (x^2-3^2)(x^2-7^2)(x^2-9^2)(x^2-11^2).\end{aligned} \qquad (2\text{–}3)$$

Table 1 shows the six smallest values of even n with two different representations, along with the solutions a_1, a_2, b_2, b_1. It lists only those representations for which all the a_i, b_i are distinct and nonzero, and have no factors in common. (Otherwise the right-hand side of (2–1) would have repeated factors, or (2–1) could be reduced to an equivalent formula with smaller coefficiencts).

n	a_1, a_2, b_2, b_1	A	B
130	3, 7, 9, 11	1696	1440
170	1, 7, 11, 13	4176	2880
250	5, 9, 13, 15	5968	4032
290	1, 11, 13, 17	10656	10080
370	3, 9, 17, 19	20896	10080
410	7, 11, 17, 19	15696	8640

TABLE 1. The six smallest values of n that have two nontrivially distinct representations as a sum of two squares, $n = a_1^2+b_1^2 = a_2^2+b_2^2$. The last two columns give the values of $A = \frac{1}{4}n^2 - \frac{1}{2}(a_2^2b_2^2 + a_1^2b_1^2)$ and $B = \frac{1}{2}(a_2^2b_2^2 - a_1^2b_1^2)$ in formula (2–1).

We see from Table 1 that if we multiply the formulas for $n = 250$ and for $n = 410$, we obtain

$$(x-19)(x-17)\dots(x-5)(x+5)(x+7)\dots(x+19).$$

This can be completed to form a product of 20 integers in arithmetic progression by way of the identity

$$(x-3)(x-1)(x+1)(x+3) = (x^2-5)^2 - 16,$$

which is a special case of a shorter and less interesting analogue of (2–1).

3. NESTED SQUARES OF LENGTH 4

If we follow the construction that led to (2–1), it is clear that we need two more distinct solutions of $n = x^2 + y^2$, say

$$n = a_3^2 + b_3^2 = a_4^2 + b_4^2.$$

Then we obtain an exact analogue of (2–1), with subscripts 3 and 4 instead of 1 and 2. Now in order for the two to combine to give a formula of the form

$$\left(\left(\left(x^2-\frac{n}{2}\right)^2-A\right)^2-B\right)^2-C^2=\prod_{j=1}^{8}(x^2-c_j^2), \quad (3\text{–}1)$$

for integers $A, B, C, c_1, \dots, c_8$, it is necessary (and sufficient) that

$$\frac{n^2}{4}-\frac{a_2^2b_2^2+a_1^2b_1^2}{2}=\frac{n^2}{4}-\frac{a_4^2b_4^2+a_3^2b_3^2}{2},$$

or, equivalently,

$$a_1^2b_1^2+a_2^2b_2^2=a_3^2b_3^2+a_4^2b_4^2. \quad (3\text{–}2)$$

Our aim is to show that (3–2) cannot have a solution in $a_1, \dots, a_4, b_1, \dots, b_4$ with $a_i^2+b_i^2=n$ for $i=1,\dots,4$. To do this, we define the difference

$$d:=a_1^2b_1^2+a_2^2b_2^2-a_3^2b_3^2-a_4^2b_4^2. \quad (3\text{–}3)$$

Note that d is not uniquely determined but depends on how the four solutions (a_i, b_i) of $n=x^2+y^2$ are combined to give the formulas (2–1) and its analogue with subscripts 3 and 4. In fact, up to sign, we get three different values of d by combining the four terms according to the patterns

$$++--\,,\quad +-+-\,,\quad +--+\,.$$

However, the nonvanishing of d is independent of this. In fact:

Proposition 2. *No quadruple $\{(a_i, b_i),\ i=1,\dots,4\}$ of distinct solutions of $n=x^2+y^2$ satisfies* (3–2).

Proof. By (2–2) we can write $n=n_1n_2$, where n_2 has at least one representation $n_2=a^2+b^2$ and n_1 has at least two essentially distinct representations

$$n_1=c_1^2+d_1^2=c_2^2+d_2^2, \quad (3\text{–}4)$$

which combine, by way of the well-known formula

$$(a^2+b^2)(c_j^2+d_j^2)=(ac_j\pm bd_j)^2+(ad_j\mp bc_j)^2,$$

to give the four solutions (a_i, b_i) of the proposition. Hence with (3–3) we get

$$\begin{aligned}
d &= \big((ac_1+bd_1)(ad_1-bc_1)\big)^2 \\
&\quad +\big((ac_1-bd_1)(ad_1+bc_1)\big)^2 \\
&\quad -\big((ac_2+bd_2)(ad_2-bc_2)\big)^2 \\
&\quad -\big((ac_2-bd_2)(ad_2+bc_2)\big)^2 \\
&= \big(c_1d_1(a^2-b^2)-ab(c_1^2-d_1^2)\big)^2 \\
&\quad +\big(c_1d_1(a^2-b^2)+ab(c_1^2-d_1^2)\big)^2 \\
&\quad -\big(c_2d_2(a^2-b^2)-ab(c_2^2-d_2^2)\big)^2 \\
&\quad -\big(c_2d_2(a^2-b^2)+ab(c_2^2-d_2^2)\big)^2 \\
&= 2c_1^2d_1^2(a^2-b^2)+2a^2b^2(c_1^2-d_1^2) \\
&\quad -2c_2^2d_2^2(a^2-b^2)^2-2a^2b^2(c_2^2-d_2^2)^2 \\
&= 2c_1^2d_1^2(a^2+b^2)^2+2a^2b^2(c_1^2+d_1^2)^2-16a^2b^2c_1^2d_1^2 \\
&\quad -2c_2^2d_2^2(a^2+b^2)-2a^2b^2(c_2^2+d_2^2)+16a^2b^2c_2^2d_2^2 \\
&= 2(c_2^2d_2^2-c_1^2d_1^2)(8a^2b^2-n_2^2).
\end{aligned}$$

Now we have $c_1^2d_1^2\neq c_2^2d_2^2$, since otherwise the two representations in (3–4) would be the same. Also,

$$8a^2b^2-n_2^2\neq 0$$

since both $4a^2b^2$ and n_2^2 are squares while 2 is not. Hence $d\neq 0$, which completes the proof. □

4. CONCLUDING REMARKS

1. Although a formula of the type (3–1) is not possible, there are formulas that are "close" to (3–1) in the following sense: If the even integer n has four essentially distinct representations as sum of two squares, then it is not difficult to show, using the methods of this note, that a product of 16 linear factors (as on the right of (3–1)) can be written as nested squares of length four (as on the left of (3–1)), plus a certain polynomial of degree four with integer coefficients, as "error term".

2. More generally, given 2^k essentially different respresentations of n, a product of 2^{k+2} linear factors can be written as nested squares of length $k+2$, with an error term of degree $2^{k+2}-12$. These formulas, however, become increasingly unpleasant.

3. The differences d, as defined in (3–3), have some interesting arithmetical properties. For instance, it can be shown that d is always divisible by $1152=2^7\cdot 3^2$, and by $28800=2^7\cdot 3^2\cdot 5^2$ whenever 5 does not divide n.

REFERENCES

[Crandall 1996] R. E. Crandall, *Topics in advanced scientific computation*, TELOS, The Electronic Library of Science, Springer, New York, 1996.

[Crandall et al. 1997] R. Crandall, K. Dilcher, and C. Pomerance, "A search for Wieferich and Wilson primes", *Math. Comp.* **66**:217 (1997), 433–449.

[Ireland and Rosen 1990] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Math. **84**, Springer, New York, 1990.

Karl Dilcher, Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada (dilcher@mathstat.dal.ca)

Received August 27, 1999; accepted in revised form October 31, 1999