Squares from Products of Consecutive Integers

Alf van der Poorten and Gerhard Woeginger

1. INTRODUCTION. Notice that $1 \cdot 2 \cdot 3 \cdot 4 + 1 = 5^2, 2 \cdot 3 \cdot 4 \cdot 5 + 1 = 11^2, 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 19^2, \ldots$. Indeed, it is well known that the product of any four consecutive integers differs by 1 from a perfect square. However, a little experimentation readily leads one to guess that there is no integer n, other than four, so that the product of any n consecutive integers differs from a perfect square by some integer $c = c(n)$ depending only on n.

There are two issues here. The first is to explain the apparently special status of four. We show that this matter lies little deeper than the fact that any quadratic polynomial can be completed by the addition of a constant to become the square of a polynomial. Second, we give a proof that there can be no n larger than four with the stated property.

2. SQUARES FROM PRODUCTS OF JUST A FEW CONSECUTIVE INTEGERS. We study the polynomials $P_{n,c}(x) = x(x + 1)(x + 2) \cdots (x + n - 1) + c$ and find all n and c so that $P_{n,c}$ is the square of a polynomial. That suffices, given our concluding remarks proving that a polynomial taking "too many" square values at the integers must be the square of a polynomial. Accordingly, we suppose $n = 2m$ is even.

We will at first find it convenient to set $y = x - m + \frac{1}{2}$, turning $P_{n,c}$ into a product of the m factors $(y^2 - \frac{1}{4}(2k - 1)^2)$, $k = 1, \ldots, m$. The further substitution $2z = y^2 - \frac{1}{4}$ yields

$$P_{2m,c}(x) = 2^m z(z - 1)(z - 3) \cdots \left(z - \tfrac{1}{2}m(m - 1)\right) + c.$$

Plainly $P_{2,c}(x) = 2z + c = y^2 - \frac{1}{4} + c$ is a square if and only if $c = 1/4$; namely, $P_{2,1/4}(x) = x(x + 1) + \frac{1}{4} = (x + \frac{1}{2})^2$. Just so, $P_{4,c}(x) = 4z(z - 1) + c$ is a square, specifically $(2z - 1)^2$, if and only if $c = 1$. Thus, indeed,

$$P_{4,1}(x) = x(x + 1)(x + 2)(x + 3) + 1 = (x^2 + 3x + 1)^2$$

is the square of a polynomial.

It will turn out that $P_{2m,c}(x)$ is not again a square for larger m, no matter what c is. That should be no particular surprise, for once m is greater than 1, it is unusual for any polynomial of degree $2m$ to be a square, even up to a constant. In fact, let f be a polynomial of degree $2m$ with square leading coefficient. Suppose a is the *polynomial part* of its square root, in the sense that $r = f - a^2$ has degree less than m. Notice here that a has $m + 1$ coefficients, which may be chosen so that the $m + 1$ leading coefficients of a^2 match the $m + 1$ leading coefficients of f. The point is that r has $m - 1$ coefficients, other than its constant term, that need to vanish fortuitously for f to be a square. On the other hand, because our useful substitution shows that $P_{4,c}$ is a polynomial of degree $2l = 2$ in z (so $l - 1 = 0$), the fact that $P_{4,c}$ is a square for some c becomes evident as soon as one recognises the possibility of such a substitution.

3. THE PRINCIPAL ARGUMENT. We show that

$$P_{n,c}(x) = x(x+1)\cdots(x+n-1)+c$$

is not the square of a polynomial if n is different from 2 or 4.

Accordingly we suppose, to the contrary, that $P_{n,c} = a^2$, with $n = 2m$ and a of degree m. Then the identity

$$P_{n,c}(x+1) - P_{n,c}(x) = n(x+1)(x+2)\cdots(x+n-1)$$
$$= (a(x+1))^2 - (a(x))^2$$

entails $(a(x+1)-a(x))(a(x+1)+a(x)) = n(x+1)(x+2)\cdots(x+n-1)$.

But the graph $y = a(x+1)$ is simply that of $y = a(x)$ shifted to the left by 1. Thus each of the $m-1$ solutions of $a(x+1) = a(x)$ is between a pair of the m zeros of $a(x+1)+a(x)$. Hence $a(x+1) - a(x) = m(x+2)(x+4)\cdots(x+2m-2)$, while $a(x+1) + a(x) = 2(x+1)(x+3)\cdots(x+2m-1)$. Then, adding these two relations, we obtain

$$2a(x+1) = 2(x+1)(x+3)\cdots(x+2m-1) + m(x+2)(x+4)\cdots(x+2m-2);$$

and subtraction yields

$$2a(x) = 2(x+1)(x+3)\cdots(x+2m-1) - m(x+2)(x+4)\cdots(x+2m-2).$$

Replacing x by $x+1$ in the last expession gives

$$2a(x+1) = 2(x+2)(x+4)\cdots(x+2m) - m(x+3)(x+5)\cdots(x+2m-1).$$

However, the two allegations detailing $2a(x+1)$ are incompatible for m greater than 2. To see this, we check the constant terms variously attributed to $2a(x+1)$. The first claim alleges that

$$2a(1) = 2\,(1\cdot 3\cdots(2m-1)) + m\,(2\cdot 4\cdots(2m-2)),$$

while the second suggests that

$$2a(1) = 2(2\cdot 4\cdots 2m) - m\,(3\cdot 5\cdots(2m-1)).$$

The purported equality of these quantities amounts to

$$(m+2)\,(1\cdot 3\cdots(2m-1)) = 3m\,(2\cdot 4\cdots(2m-2)), \qquad (\ddagger)$$

which is absurd for m greater than 2 because a higher power of 2 divides the right-hand side of $(\ddagger)$ than divides the other side.

For $m = 2$, however, $(\ddagger)$ is $4\cdot 3 = 6\cdot 2$; and $m = 1$ provides $3\cdot 1 = 3$. So all may be well in those instances, as had better be the case given our introductory observations.

We have proved a tiny bit more than we set out to show.

Theorem. *Suppose $c = c(n)$ and $d = d(n)$ are relatively prime integers such that d times every product of n consecutive integers $k, k+1, \ldots, k+n-1$ differs by c from a square. Then $n = 2$ with $(2k+1)^2 = 4k(k+1)+1$, or $n = 4$ with $(k^2+3k+1)^2 = k(k+1)(k+2)(k+3)+1$.*

4. CONCLUDING REMARKS. We promised to explain why a polynomial taking too many square values at the integers must be the square of a polynomial.

Proposition. *Let f be a monic polynomial with rational coefficients and of even degree. If $f(x)$ is not the square of a polynomial, then $f(x)$ takes square values (thus, is the square of a rational) for at most finitely many positive integer values of x.*

Proof. Suppose the polynomial f has degree $n = 2m$, and suppose a is the polynomial part of the square root of f, in the sense that $r = f - a^2$ is of degree at most $m - 1$. Let N be an integer large relative to the data, but suppose that, contrary to expectation, $f(N)$ *is* a square, say $f(N) = B^2$. Then $a(N) = A$ is of order N^m, whereas $r(N)$ is of order at most N^{m-1}. Because, by hypothesis, r does not vanish identically we may suppose that $r(N) \neq 0$. Then $B^2 - A^2$ is nonzero and is at most of order N^{m-1}, contradicting the identity $B^2 - A^2 = (B + A)(B - A)$, which says that $B^2 - A^2$ has at least the order of magnitude of A. ∎

Remarks. (1) Notice that any denominators occurring among the rational coefficients of f and a are part of the data and their effect is readily offset by choosing N large enough relative to those data. (2) What if $f(x)$ is of odd degree $2m + 1$, you ask? This case is actually more subtle. Nonetheless, $f(z^2)$ is of even degree in z, whereas $f(z^2)$ is a square only if $f(x)$ happened to have been x times a square. But according to the proposition, if $f(x)$ is not x times a square, then $f(N^2)$ is not a square for N large. Certainly, whether $f(x)$ is x times a square or not, if f has odd degree, then there are large N for which $f(N)$ is not a square. (3) There is a substantial literature on polynomials taking square values, and the like. For an introduction to the proper context of such results, see, for example, Davenport, Lewis, and Schinzel [1].

Rather more elegant proofs than that sketched for the proposition, demonstrating that a polynomial taking only kth power values of integers must be the kth power of a polynomial, appear as items VIII.114 and VIII.190 in [2].

The present study was provoked by a question put by Bob Silverman to the sci.math newsgroup.

REFERENCES

1. H. Davenport, D. J. Lewis, and A. Schinzel, Polynomials of certain special types, *Acta Arith.* **9** (1964) 107–116.
2. George Pólya and Gábor Szegő, *Problems and Theorems in Analysis*, vol. 2; Theory of functions, zeros, polynomials, determinants, number theory, geometry; revised and enlarged translation by C. E. Billigheimer of the fourth German edition, Springer-Verlag, New York, 1976.

ALFRED J. VAN DER POORTEN has written some 150 mathematical items, primarily on topics with a number-theoretical flavor, including *Notes on Fermat's Last Theorem* (Wiley-Interscience, 1996), awarded the Association of American Publishers Professional/Scholarly Publishing 1996 Award for Excellence in Mathematics [see *Notes on FLT* for his biography]. He is a reader of mysteries and of science fiction, and is generally a retainer/collector of books, including an extensive mathematical library. In real life—when not attending meetings overseas—Alf is a member of the senior executive of Macquarie University, Sydney.
ceNTRe for Number Theory Research, Macquarie, University, Sydney, Australia 2109
alf@math.mq.edu.au

GERHARD J. WOEGINGER spent most of his academic life at the TU Graz, Austria: the 1980s as a student of Mathematics and Computer Science, and the 1990s as a researcher first in the Department of Theoretical Computer Science and later in the Department of Mathematics. In 2001 he joined the Department of Mathematics at the University of Twente in the Netherlands. His research centers on algorithmical and combinatorial questions in discrete mathematics.
Department of Discrete Mathematics and Mathematical Programming, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands
g.j.woeginger@math.utwente.nl

Three Non-Independent Events

The usual example that pairwise independence of events does not imply independence, due to Bernstein (*On the Axiomatic Foundation of the Theory of Probability* (in Russian), Mitt. Math. Ges., Charkov, 1917), appears in many texts on probability theory. However, it is somewhat artificial, constructed only to demonstrate this fact. There is a simpler and more natural example in the following common dice experiment:

Roll two dice, independently. Let E = [the first die is a 3], F = [the second die is a 4], and G = [the sum is 7].

The events E and F are pairwise independent, by assumption. The fact that E and G are pairwise independent is a common exercise for students in a first course in probability theory (just verify that the multiplication rule $P(E \cap G) = P(E)P(G)$ holds). Similarly, F and G are pairwise independent.

But E and F together imply G, so E, F, and G are not independent.

Submitted by
Mark Finkelstein ·
University of California, Irvine