Product of integers in an interval, modulo squares

Andrew Granville and J.L. Selfridge

Abstract: We prove a conjecture of Irving Kaplansky which asserts that between any pair of consecutive positive squares there is a set of distinct integers whose product is twice a square. This follows from our main theorem which asserts that if prime p divides some integer in $[z, z + 3\sqrt{z/2} + 1)$ (with $z \geq 11$) then there is a set of integers in the interval whose product is p times a square. This is essentially best possible because it seems that arbitrarily large counterexamples would exist if we shorten the interval to $[z, z + 3\sqrt{z})$.

1. Introduction

In several modern algorithms, such as the quadratic sieve, one gradually constructs a set of integers, and tries to efficiently find a (nonempty) subset whose product is a square. Recently researchers have been analyzing when it is likely that there is a subset of a given set whose product is a square. In [2] Pomerance shows that if we randomly select $\exp(\sqrt{(2+\epsilon)\log x \log\log x})$ integers up to x then, with probability $\to 1$ as $x \to \infty$, there is a subset of these integers whose product is a square; whereas if we only have $\exp(\sqrt{(2-\epsilon)\log x \log\log x})$ such integers then the probability $\to 0$ as $x \to \infty$. This allows him to give a plausible heuristic to analyze the running time of several important practical algorithms; however, this is only a heuristic since the sets of integers constructed are not really random numbers but rather are determined by some procedure. To unconditionally analyze these algorithms, we need to understand whether there is a subset of certain types of *given* sets whose product is a square, though this appears to be extremely difficult in the cases of interest. In this paper we study this type of problem, and variants, where our given set of integers is perhaps as simple as is possible, the integers in a short interval.

In July 1994, Irving Kaplansky conjectured that there is a set of distinct integers, between any pair of consecutive squares, whose product is twice a square. We deduce this as a (trivial) corollary to our

Theorem 1. *For every integer $u \geq 2$, there is a set of integers in the closed interval $[(u-1)^2, u^2]$ whose product is twice a square.*

Our proof uses the 'Walk method' of [1]. For the interval from 16 to 25, for example, we consider the sequence $5, 4, 6, 3, 7, 3, 8, 2, 9$. Note that the product of any two consecutive integers in this sequence lies in the closed interval $[16, 25]$. Therefore, as we 'walk' along the sequence from 4 to 2, we get the pairs $4.6, 6.3, 3.7, 7.3, 3.8, 8.2$ giving the integers $24, 18, 21, 21, 24, 16$ from the interval, whose product is $(4.6)(6.3)(3.7)(7.3)(3.8)(8.2) = 4(6.3.7.3.8)^2 2 = 2.6048^2$. To deduce Kaplansky's conjecture, we need to cull pairs of the same integer (21 and 24), as well as squares (16), from our sequence $24, 18, 21, 21, 24, 16$, to obtain the set $\{18\}$. In the proof of Theorem 1 we generalize this method to the interval between any pair of consecutive squares.

Kaplansky's problem is susceptible to various generalizations. For example, when is there a set of integers in $[(u-1)^2, u^2]$ whose product is 3 times a square? Or 5 times a square? etc. Alternatively, we might ask for 'large' intervals which do not contain a set of integers whose product is twice a square. In Theorem 1 there is no restriction placed on the size of our set of integers, though presumably one doesn't usually need more than a few; so, how small is the smallest such set of integers? We will attack these and related problems in the rest of this article.

Our main theorem is the following:

Theorem 2. *Fix real number $z \geq 10.22$. Suppose that p is a prime which divides some integer in the interval $J = [z, z + 3\sqrt{z/2} + 1)$. Then there is some set of integers in the interval J whose product equals p times a square.*

If we only allow z to run through integers, then the theorem holds for all integers $z \geq 1$. However, for $z = 10.21$ we have $J \subset (10, 18)$, and there is no set of integers in this interval whose product is twice a square.

We note that as an easy consequence of Theorem 2 we can deduce that there is some set of integers in the interval J whose product equals n times a square, for any squarefree n dividing the product of the integers in J. For if a and b are coprime, squarefree integers, and A and B are sets of integers such that the product of the elements in A (and in B) equals a (and b, respectively) times the square of an integer, then the product of the elements in $(A \cup B) \setminus (A \cap B)$ evidently equals ab times the square of an integer. The result follows by induction on the number of prime divisors of n. Thus in general we may restrict our attention to constructing sets of integers whose product is a prime times a square.

Next we show that the interval in Theorem 2 cannot be taken to be much shorter. If $z = p^2 - p + \epsilon$, where p is prime then $z + 2\sqrt{z} < p^2 + p$ if $\epsilon > 0$ is sufficiently small, so that p^2 is the only integer in $[z, z + 2\sqrt{z}] \subset (p^2 - p, p^2 + p)$ divisible by p. Thus p divides some integer in the interval, yet there does not exist any set of integers in the interval whose product is p times a square. This is a substantially shorter interval than that in Theorem

2, but similar ideas account for the construction in:

Corollary 4. *Suppose that for real number $z \geq 78$, there exists some prime p which divides an integer in the interval $J = [z, z + 3\sqrt{z/2})$, yet for which there is no set of integers in J whose product equals p times a square. Then*
Either there exist primes $q, 2q+1$, one of which is p, such that

$$2q^2 - q - 1 < z \leq 2q^2 < 2q^2 + q < z + 3\sqrt{z/2} \leq 2q^2 + 2q;$$

Or there exist primes $q, 2q-1$, one of which is p, such that

$$2q^2 - 2q < z \leq 2q^2 - q < 2q^2 < z + 3\sqrt{z/2} \leq 2q^2 + q - 1.$$

Thus if there are, as we expect, infinitely many prime pairs of the form $q, 2q+1$, or of the form $q, 2q-1$ then Theorem 2 is "best possible" in that it does not hold for infinitely many intervals of the form $[z, z + 3\sqrt{z/2})$.

Corollary 4 follows from the much more general (and technical) Theorem 3 below, which classifies all such p when the interval length is $\geq 5\sqrt{z/6} + 1$.

Returning to the intervals $I_u = [(u-1)^2, u^2]$ considered by Kaplansky, but now thought of as subintervals of $[z, z + 3\sqrt{z/2})$ with $z = (u-1)^2$ for $u \geq 10$, we note that primes 911 and 1823 both divide $911 \cdot 1823$, which lies in the interval $[1288^2, 1289^2]$, yet there is no set of integers in the interval whose product is 911 times a square (this is an example of the type discussed in the first part of Corollary 4). We ask, for which of the primes p which divide an integer in I_u does there exist a set of integers in I_u whose product equals p times a square? In Proposition 2 we see that this is so for any prime $p \leq u^{3/4}/30$, and then show that this is so for any prime $p \leq Cu/\log u$, where C is some constant > 0, assuming:

Conjecture B. *There exists some constant $c > 0$ such that there is an integer, all of whose prime factors are $\leq \sqrt{x}$, in the interval $[x - c\log x, x]$, for all $x \geq 1$.*

As we shall discuss, Theorem 3 below suggests that we should be able to get a good estimate for the number of exceptional p:

Conjecture A. *There exists a constant $\kappa > 0$ such that there are $\sim \kappa u/\log^4 u$ primes $p \leq u$ for which there is no subset of the integers in $I = [(u-1)^2, u^2]$ whose product is p times a square.*

We can use Theorem 2 to improve our knowledge about a function defined by Erdős in a problem in the *American Mathematical Monthly*: For each positive integer n, define $g(n)$ to be the minimum integer $a_k \geq 0$ such that there exists a sequence of integers $n < n + a_1 < n + a_2 < \ldots < n + a_k$ for which $n(n+a_1)\ldots(n+a_k)$ is a square. For example, $g(2) = 4$, $g(3) = 5$, $g(5) = 5$ (taking 2.3.6, 3.6.8, 5.8.10 respectively). Our task is to obtain good estimates for $g(n)$. Define $p(n)$ to be the largest prime which divides n to an odd power. Evidently our sequence of numbers must contain an integer, other than n, which is divisible by $p(n)$; since that integer is $\geq n + p(n)$, we must have $g(n) \geq p(n)$. In particular, if p is prime then $g(p) \geq p$. Now it is easily shown that every interval $(p, 2p)$ contains an integer that is twice a square when $p > 3$, so that $g(p) = p$. For various other integers n we will show that $g(n) = p(n)$. In this paper we slightly re-focus our description of $g(n)$ by viewing it as the smallest integer such that there is some set of integers in the interval $(n, n + g(n)]$ whose product equals n times a square.

Corollary 1. *For any integer n, define $p(n)$ to be the largest prime divisor of n. If $p(n) > \sqrt{2n} + 1$ then $g(n) = p(n)$. Otherwise $p(n) \leq g(n) \leq 3\sqrt{n/2} + 1$.*

Proof: If $p = p(n) > \sqrt{2n}+1$ then write $n = ap$, so that $p > 2a+1$ since $p(p-1) > 2n = 2ap$. Then the product of the integers

$$n = ap < a(p+1), (2a+1)(p-1)/2, (2a+1)(p+1)/2, (a+1)(p-1) < (a+1)p$$

is a square, implying that $g(n) \leq p$. The result follows since we always have $g(n) \geq p(n)$.

On the other hand if $p(n) \leq \sqrt{2n} + 1$ then every prime p dividing n satisfies $p \leq p(n) \leq 3\sqrt{n/2} + 1$ so, by Theorem 2 with $z = n + \epsilon$, there is some set of integers in the interval $(n, n + 3\sqrt{n/2} + 1]$ whose product equals n times a square.

Corollary 1 is close to 'best possible'. For, if p and $2p + 1$ are both prime, with $p > 3$, then $g(n) \geq 3p(n)$ for $n = p(2p - 1)$ (note that $p(n) = p$ since $2p - 1$ is divisible by 3). By Corollary 1 we have $g(n) < 3p(n) + 1$ so $g(n) = 3p(n)$ $(\geq 3\sqrt{n/2} + 3/4)$.

One can modify Erdős's problem to ask for $g_k(n)$, the minimum integer $a_k \geq 0$, such that there exists a sequence of integers $n < n + a_1 < n + a_2 < \ldots < n + a_k$ for which $n(n + a_1) \ldots (n + a_k)$ is a square. It is easy to determine $g_1(n)$ since if $n = rs^2$ with r squarefree then evidently $n + g_1(n) = r(s + 1)^2$. Conjecture 3 of [1] states that if n is not a square and $n \neq 8$ or 392 then $g_2(n) < g_1(n)$. In other words, there exist integers $a, b \in (rs^2, r(s+1)^2)$ for which rab is a square. (Note that if $n = s^2$ is a square and $uv^2 > n$ with $u > 1$ then $u(v + 1)^2 = n + 2uv + u > s^2 + 2s\sqrt{u} + 1 > (s + 1)^2$, so $g_2(s^2) > g_1(s^2)$.) The conjecture is proved in [1, Theorems 4,5,6] except when $r = 2$; and in this case except for intervals $(2s^2, 2(s + 1)^2)$ where $s = u_{2m\pm1}v_{2m}$ with $u_m + \sqrt{2}v_m = (1 + \sqrt{2})^m$. The first two examples here, $u_1v_2 = 2$ and $u_2v_2 = 14$ yield $n = 8$ and $n = 392$ respectively.

Acknowledgement: We would like to thank Aaron Meyerowitz for his careful reading of this paper.

2. The Key Proposition

For integers a and b we write $a \equiv b \pmod{\mathbf{Q}^2}$ if a/b is a rational square; it is easy to show that this is an equivalence relation. Any equivalence class is most naturally represented by the (unique) squarefree integer in that equivalence class. Given an interval I, we will denote by S_I the set of equivalence classes of products of integers in I. Note that S_I is closed under multiplication, a fact that we will repeatedly use.

Proposition 1. *Fix real numbers $1 \le x \le y$. Let $I = [x, y+1]$ and $J = [xy, xy+x+y+1)$, unless xy is an integer, in which case we take $J = [xy, xy + x + y)$.*
i) For any pair of integers $m < n$ in the interval I, there exists some set of integers in the interval J whose product is mn times a square (of an integer).
ii) Suppose that the interval I contains a square. If the product of some subset of the integers in I equals N times a square, then there is some set of integers in the interval J whose product equals N times a square.

Proof:

i) Suppose that a is an integer in the range $x \le a \le y$, and define b to be the smallest integer $\ge xy/a$ so that $xy/a \le b < xy/a + 1$, and $xy \le ab < xy + a$. Therefore $(a + 1)b = ab + b < (xy + a) + (xy/a + 1) \le xy + x + y + 1$ in this range for a. If xy is an integer then $ab \le xy + a - 1$, so that $(a + 1)b < xy + a + xy/a \le xy + x + y$. Thus both ab and $(a + 1)b$ are in J and therefore in S_J. But then $a(a + 1) \in S_J$ since S_J is closed under multiplication and $a(a + 1) \equiv ab \times (a + 1)b \pmod{\mathbf{Q}^2}$.

Since $x \le m \le n - 1 \le y$ we deduce from the paragraph above that $m(m + 1), (m + 1)(m + 2), \ldots, (n - 1)n \in S_J$, and so $mn \in S_J$ since $mn \equiv m(m + 1) \times (m + 1)(m + 2) \times \ldots \times (n - 1)n \pmod{\mathbf{Q}^2}$ and S_J is closed under multiplication.

ii) Let m_0 be a square in I, and let $m_1, m_2, \ldots, m_k$ be that subset of the integers in I whose product equals N times the square of a rational number. We may assume that $k = 2\ell$ is even, without loss of generality, for if not, we could remove m_i from the list if it equalled m_0, or add m_0 to the list if it does not already appear. We may also assume that the m_j are distinct (else we cull any pair of occurences of one number from the list) and so $m_1 < m_2 < \ldots < m_k$. But then, by i), we have $m_{2i-1}m_{2i} \in S_J$ for $i = 1, 2, \ldots, \ell$.

Now $N \equiv (m_1 m_2)(m_3 m_4)\dots(m_{2\ell-1}m_{2\ell}) \pmod{\mathbf{Q}^2}$, and thus $N \in S_J$, since S_J is closed under multiplication.

Proof of Theorem 1: Let $x = u - \sqrt{2u-1} > 1$ and $y = u + \sqrt{2u-1}$ in Proposition 1, so that $xy = (u-1)^2$ is an integer. Let a and b be the smallest positive integers for which $a^2, 2b^2 \geq x$, so that $(a-1)^2, 2(b-1)^2 < x$, implying that $a-1, \sqrt{2}(b-1) < \sqrt{x} < \sqrt{u} - 1/\sqrt{2}$. Therefore $a^2, 2b^2 \in I$ since

$$a^2 = (a-1)^2 + 2(a-1) + 1 < x + 2\sqrt{u} \leq y,$$
$$2b^2 = 2(b-1)^2 + 2\sqrt{2}(\sqrt{2}(b-1)) + 2 < x + 2\sqrt{2u} < y + 1.$$

The result follows from Proposition 1(i), by taking $\{m, n\}$ to be $\{a^2, 2b^2\}$.

3. Iterating the key Proposition: The proof of Theorem 2

Corollary 2. *Fix real number $z \geq (\sqrt{2}-1)^2$. Suppose that the product of some subset of the integers in $I = [\sqrt{2z} - \sqrt{z}, \sqrt{2z} + \sqrt{z} + 1]$, equals N times the square of a rational number. Then there is some set of integers in the interval $J = [z, z + 2\sqrt{2z} + 1)$ whose product is N times the square of a rational number.*

Proof: This follows from Proposition 1(ii) by taking $x = \sqrt{2z} - \sqrt{z}$ and $y = \sqrt{2z} + \sqrt{z}$, provided we can show that there is a square in the interval I: If $(\sqrt{2}-1)^2 \leq z \leq (\sqrt{2}+1)^2$ then $1^2 \in I$. If $z > (\sqrt{2}+1)^2$ then select r to be the smallest positive integer for which $r^2 \geq \sqrt{2z} - \sqrt{z} > 1$. Since $r \geq 2$, thus $r \leq 2(r-1)$ and so $r^2 \in I$ as

$$r^2 \leq 4(r-1)^2 < 4(\sqrt{2}-1)\sqrt{z} < (\sqrt{2}+1)\sqrt{z} = \sqrt{2z} + \sqrt{z}.$$

Lemma 1. *Fix real number $z \geq (\sqrt{2}-1)^2$. If p is a prime $\leq \sqrt{2z} + \sqrt{z} + 1$ then there is an integer k such that $pk^2 \in I = [\sqrt{2z} - \sqrt{z}, \sqrt{2z} + \sqrt{z} + 1]$.*

Proof: If $p \in I$ take $k = 1$. Otherwise $p < \sqrt{2z} - \sqrt{z}$ in which case we select k to be the smallest integer for which $pk^2 \geq \sqrt{2z} - \sqrt{z}$; evidently $k \geq 2$. But then $k \leq 2(k-1)$ so that $pk^2 \leq 4p(k-1)^2 < 4(\sqrt{2z} - \sqrt{z}) < \sqrt{2z} + \sqrt{z}$, and the result follows.

Corollary 3. *Fix real number $z \geq 1$. Suppose that p is a prime which divides some integer in the interval $J = [z, z + 2\sqrt{2z} + 1)$. Then there is some set of integers in the interval J whose product equals p times a square.*

Proof: If $p \leq \sqrt{2z} + \sqrt{z} + 1$ then, by Lemma 1, there is an integer k such that $pk^2 \in I = [\sqrt{2z} - \sqrt{z}, \sqrt{2z} + \sqrt{z} + 1]$. The result follows from an immediate application of Corollary 2 with $N = p$.

If $p > \sqrt{2z} + \sqrt{z} + 1$ then write mp for the smallest integer in J which is divisible by p. Evidently

$$m \leq \frac{z + 2\sqrt{2z} + 1}{p} < \frac{z + 2\sqrt{2z} + 1}{\sqrt{2z} + \sqrt{z} + 1} \leq \sqrt{2z} + \sqrt{z} + 1,$$

so that all of the prime factors of m are certainly $\leq m \leq \sqrt{2z} + \sqrt{z} + 1$. But then, all of the prime factors of m belong to S_J (as we saw in the first paragraph of this proof), and so m belongs to S_J, since S_J is closed under multiplication. Moreover $mp \in J$ so that $mp \in S_J$, and so $p \in S_J$ since $p \equiv m \times mp \pmod{\mathbf{Q}^2}$ and S_J is closed under multiplication.

Proof of Theorem 2: For $10.22 \leq z < 128$, we proved the result by a computation. For $z \geq 128$, let $I = [x, 2x + 1]$ where $x = \sqrt{z/2}$. Let p be any prime $\leq 2x + 1$. Note that p divides some integer, call it mp, in I, for if not then evidently $p < x$, so select integer $a \geq 1$ to be the largest integer for which $ap < x$; then $(a + 1)p > 2x$ so that $2 \geq (a + 1)/a = (a + 1)p/ap > 2x/x = 2$ giving a contradiction.

Now $x + 2\sqrt{2x} + 1 \leq 2x + 1$ since $x \geq 8$. Therefore the interval I contains an interval of the form $[y, y+2\sqrt{2y}+1)$ containing mp; and so, by Corollary 3, there is a set of integers in $[y, y + 2\sqrt{2y} + 1) \subset I$ whose product equals p times a square.

We now apply Proposition 1(ii), noting that I contains a square, to deduce that there is some set of integers in the interval $J = [2x^2, 2x^2 + 3x + 1)$ whose product is p times a square. Therefore every prime $\leq 2x + 1$ belongs to S_J.

Now suppose p is some prime $> 2x + 1$ dividing an integer in J. Let's call that integer mp, and observe that $m < (2x^2 + 3x + 1)/(2x + 1) = x + 1 \leq 2x + 1$. Thus every prime factor of m is $\leq 2x + 1$, and so $m \in S_J$ (since S_J is closed under multiplication). By definition, $mp \in J$ and thus $mp \in S_J$; but then $p \in S_J$ since $p \equiv m \times mp \pmod{\mathbf{Q}^2}$ and S_J is closed under multiplication.

4. Classifying the exceptional primes

Theorem 3. *Fix real number $z \geq 78$, and let $K = [z, z + \Delta]$, where $5\sqrt{z/6} + 1 \leq \Delta < 3\sqrt{z/2} + 1$, Suppose that prime ℓ divides some integer in the interval K. There is no set of integers in the interval K whose product equals ℓ times a square if and only if one of the following cases holds:*

i) There exist primes $p, q, 2p + 1, 2q + 1$, one of which is ℓ, such that $p \geq q$ and

$$(2q + 1)(p - 1) < z \leq 2pq < p(2q + 1) < z + \Delta \leq q(2p + 2).$$

ii) There exist primes $p, q, 2p-1, 2q-1$, one of which is ℓ, such that $p \geq q$ and

$$(2q-1)(p+1) \geq z+\Delta > 2pq > p(2q-1) \geq z > q(2p-2).$$

Proof: For $78 \leq z < 357$. we proved the result by a computation. So assume $z \geq 357$. Let $x = \sqrt{2z/3}$ and $y = \sqrt{3z/2}$, so that $x > 46/3$. Note that $J := [xy, (x+1)(y+1)) \subseteq K \subset [xy, (x+2)(y+1))$.

Any prime $\ell \leq x/2+1 = (y+1)-x$ evidently divides some integer in $I = [x, y+1]$ since the interval is longer than ℓ. Moreover if $x/2 \leq \ell \leq (y+1)/2$ then $2\ell \in I$, and if $x \leq \ell \leq y+1$ then $\ell \in I$. This accounts for all primes ℓ that divide some integer in I.

Suppose that ℓ divides some integer in the interval I; since $y \geq x + 3\sqrt{x/2} > 18$ for $x \geq 18$, we see that this integer is contained in some interval $[v, v+3\sqrt{v/2}+1) \subset I$ and so $\ell \in S_I$ by Theorem 2. If $18 > x \geq 46/3$ then $18, 24, 20 \in I$ so that $2, 3, 5 \in S_I$; moreover if $\ell \geq 7$ and $m\ell \in I$ then $m\ell \leq 28$ so that $m \leq 4$: thus $m \in S_I$ and so $\ell \in S_I$. Since I contains a square, we deduce from Proposition 1(ii) that there is some set of integers in the interval $J \subseteq K$ whose product equals ℓ times a square. This contradicts the hypothesis, and thus either $\ell \in ((y+1)/2, x)$ or $\ell > y+1$.

Suppose that $\ell > y+1$ and it divides $\ell\lambda \in K$. Evidently $\lambda \notin S_K$, for if it were then $\ell \in K$ (contradicting the hypothesis) since S_K is closed under multiplication. Moreover $\ell\lambda \leq (x+2)(y+1)$ so that $\lambda \leq (x+2)(y+1)/\ell < (x+2)$. Therefore λ is prime, otherwise all of its prime factors are $< (x+2)/2 < (y+1)/2$ and so belong to S_K, so that $\lambda \in S_K$ (since S_K is closed under multiplication), giving a contradiction. We also note that ℓ then divides only one integer in K; otherwise the second such integer would be $\ell(\lambda \pm 1)$ but $\lambda \pm 1$ cannot be a prime since λ is, and $2, 3 \in S_K$.

If $\ell > y+1$ we take $p = \lambda$ (defined as in the paragraph above); otherwise we take $p = \ell$. Therefore $p \in ((y+1)/2, x+2)$ and $p \notin S_K$.

Note that if $pm \in K$ then $m = r$ or $2r$ for some prime r. For, if not then $m = ab$ for some integers $a, b \geq 3$, and $abp \leq (x+2)(y+1)$, so that $a, b \leq (x+2)(y+1)/3p < 2(x+2)/3 < (y+1)/2$. Therefore all of the prime factors of $m = ab$ are $< (y+1)/2$ and thus in S_K, so that $m \in S_K$ (as S_K is closed under multiplication). But then $p \in S_K$ since $pm \in S_K$, and $p \equiv m \times pm \pmod{\mathbf{Q}^2}$, which contradicts the hypothesis. We also note that $r \notin S_K$, for if it were then we would have $m \in S_K$, and thus $p \in S_K$ (since S_K is closed under multiplication).

Since $2p$ is less than Δ, the length of the interval K, we see that p divides at least two integers in that interval. In fact p divides exactly two integers in K, for if it divided three, call them $pm, p(m+1), p(m+2)$, then one of them must be divisible by 3, contradicting what we proved in the previous paragraph.

Suppose that the two integers in K that p divides are $pm, p(m+1)$. Evidently 2 divides one of m and $m+1$, and we have already seen that these two numbers must each be either prime or twice a prime, so they can be written as $2q$ and $2q \pm 1$, where q and $2q \pm 1$ are both prime but not in S_K. Since $q \notin S_K$ and $q \leq (x+2)(y+1)/2p < x+2 < y+1$ we can draw the same conclusions for q as we did for p above: that is, q divides exactly two integers in S_K, namely $2pq$, and $q(2p+1)$ or $q(2p-1)$, where $2p+1$ or $2p-1$ (respectively) is prime and not in S_K (note that we already knew that q divides $2pq \in K$). We claim that if we have $2pq, p(2q+\delta), q(2p+\epsilon) \in K$ above (where $\delta, \epsilon = \pm 1$), then we must have $\delta = \epsilon$: For, if $q < p$ then $q(2p+\delta)$ lies between $2pq$ and $p(2q+\delta)$ so must be in K; similarly if $p < q$ then $p(2q+\epsilon)$ lies between $2pq$ and $q(2p+\epsilon)$ so must be in K. Note that either $\ell = p$ or $\ell = 2q+\delta$.

We deduce then that $p, q, 2p+\delta, 2q+\delta$ must all be prime, and that the only multiples of these primes that belong to K are $2pq, p(2q+\delta), q(2p+\delta)$. To guarantee that these are the only such multiples belonging to K we need to verify that certain inequalities are satisfied. If $\epsilon = 1$ these are:

$$z \leq 2pq, p(2q+1), q(2p+1) < z + \Delta$$
$$p(2q-1), q(2p-1), (2p+1)(q-1), (2q+1)(p-1) < z$$
$$p(2q+2), q(2p+2), (2p+1)(q+1), (2q+1)(p+1) \geq z + \Delta.$$

Now, by swapping the roles of p and q in the argument above if necessary, we may assume that $p \geq q$. Then we need only check that

$$(2q+1)(p-1) < z \leq 2pq, p(2q+1) < z + \Delta \leq q(2p+2).$$

A similar argument works when $\epsilon = -1$.

It is easy to check that none of the primes $p, q, 2p+\delta, 2q+\delta$ belong to S_K if $2pq, p(2q+\delta), q(2p+\delta)$ are their only multiples in K, since no subset of $pq, p(2q+\delta), q(2p+\delta)$ multiplies together to give $p, q, 2p+\delta$ or $2q+\delta$ times a square.

Remark: For $z = 77.05$ we have $I = [z, z + 5\sqrt{z/6} + 1) \subset (77, 96)$. It turns out that all primes that divide some number in I, belong to S_I, except $3, 7, 13, 29, 31$.

Proof of Corollary 4: Take $K = J$, $z \geq 78$ and $\Delta = 3\sqrt{z/2}$ in Theorem 3, so that either (i) or (ii) there holds. We note that $q = p$, otherwise $q = p - 2a$, for some positive integer

a. In case (i) this implies that $3p+1-8a = 4q+1-p = q(2p+2)-(2q+1)(p-1) > \Delta$, and in case (ii) this implies that $3p-1-8a = 4q-p-1 = (2q-1)(p+1)-q(2p-2) > \Delta$. Therefore $p > \sqrt{z/2}+(8a-1)/3 > \sqrt{z/2}+2$ and $q > \sqrt{z/2}+(2a-1)/3 > \sqrt{z/2}$. We thus have $z+3\sqrt{z/2} = z+\Delta > 2pq > z+4\sqrt{z/2}$, giving a contradiction.

5. The interval $I_u = [(u-1)^2, u^2]$ revisited

It is intriguing to determine exactly what primes belong to the set S_I. When u is small we can easily show that if prime p divides an integer in I, then $p \in S_I$:

For $u=2$ we have $2 = 2\times 1^2,\ 3 = 3\times 1^2$.

For $u=3$ we have $8 = 2\times 2^2,\ 6\times 8 = 3\times 4^2,\ 5 = 5\times 1^2,\ 7 = 7\times 1^2$.

For $u=4$ we have $10\times 12\times 15 = 2\times 30^2,\ 12 = 3\times 2^2,\ 12\times 15 = 5\times 6^2,\ 10\times 12\times 14\times 15 = 7\times 60^2,\ 11 = 11\times 1^2,\ 13 = 13\times 1^2$.

If we assume widely believed conjectures about the distribution of prime pairs, then from Corollary 4, it seems likely that there are infinitely many integers u, such that there is some prime p dividing an integer in I_u, yet $p \notin S_I$. Computations in Maple yielded the following prime pairs $p, 2p+1$ with $p(2p-1) < (u-1)^2 < 2p^2 < p(2p+1) < u^2 < 2p(p+1)$ and $u < 10^4$:

$(u,p) = (1289, 911), (3597, 2543), (3894, 2753), (4191, 2963), (4751, 3359), (5345, 3779),$
$(6779, 4793), (7076, 5003), (7636, 5399), (9961, 7043).$

In each case here neither p nor $2p+1$ belong to S_I, by Corollary 4.

The construction in Theorem 3(i) can be used here, if there are primes $q < p < 2q+1 < 2p+1$ for which

$$(2q+1)(p-1) < (u-1)^2 \le 2pq < p(2q+1) < u^2 \le q(2p+2).$$

We consider primes p in the interval $[30u/41, 5u/7]$ for which $2p+1$ is also prime. Then select q to be the largest integer such that $2q+1 < u^2/p$. So if $\lambda = u/p$, then $q \sim \lambda u/2$ and we need, essentially, $\lambda^2 - 1 > u^2/p > 2\lambda - \lambda^2$, which should hold for a positive proportion of such primes p. Standard heuristics suggest that the "probability" that q and $2q+1$ are both prime is $\asymp 1/\log^2 u$. Thus we expect that there should be $\gg u/\log^4 u$ such prime quadruplets, and so we propose Conjecture A.

On the other hand, we can prove that many primes do belong to S_I. As an immediate consequence of the following result we see that every prime $p \le u^{3/4}/30$ belongs to S_I.

Proposition 2. *Let $u \geq 4$ be an integer. If prime p divides some integer in the interval $[u - u^{3/4}/30, u)$ then there is some set of integers in the interval $I = [(u-1)^2, u^2]$ whose product equals p times the square of an integer.*

We shall prove this result below after a discussion of what we expect to be true. As we shall see, in the proof of Proposition 2 we show that there exists an integer in any interval $[x - 3x^{1/4} + 1, x]$, all of whose prime factors are $\leq 2\sqrt{x}$. If this could be strengthened as suggested in Conjecture B then we deduce that every prime $p \leq Cu/\log u$ belongs to S_I, for some constant $C > 0$: For if $u^{3/4}/30 < p \leq Cu/\log u$ then let $x = [u^2/p]$ and select integer $m \in [x - c\log x, x]$, as in Conjecture B, so that all prime factors of m are $\leq \sqrt{x} \leq u/\sqrt{p} \leq u^{3/4}/30$, and so belong to S_I. Thus $m \in S_I$, and $mp \in [u^2 - p(1 + c\log(u^2/p)), u^2] \subset I$; therefore $p \in S_I$.

We now proceed to the proof of Proposition 2:

Corollary 5. *Fix integer $u \geq 4$, and suppose that p is a prime which divides some integer in the interval $J = [u - \sqrt{2u-1}, u + \sqrt{2u-1} - 1)$. (In particular any prime $p < 2\sqrt{2u-1} - 1$ divides some integer in the interval.) Then there is some set of integers in the interval $[(u-1)^2, u^2]$ whose product equals p times the square of an integer.*

Proof: Let $z = u - \sqrt{2u-1}$, so that $z > 1$ and $z + 2\sqrt{2z} + 1 = u + \sqrt{2u-1} - 1$. By Corollary 3 we know that there is some set of integers in J whose product equals p times the square of a rational number. The result then follows from Proposition 1(i) by taking $x = z > 1$ and $y = z + 2\sqrt{2z} + 2 = u + \sqrt{2u-1}$ (so that $xy = (u-1)^2$ is an integer), and noting that in the above proof of Theorem 1 we proved that there is a square in the interval $[x, y+1]$.

Lemma 2. *There is always an integer n, all of whose prime factors are $\leq 2\sqrt{x}$, in the interval $[x - 3x^{1/4} + 1, x]$ when $x \geq 1$.*

Proof: For $x \leq 2000$ we proved the result by direct computation. When $x > 2000$ we select a to be the smallest integer $\geq \sqrt{x}$, and then b to be the smallest positive integer $\geq \sqrt{a^2 - x}$. We find that $a < 1 + \sqrt{x}$, so that $a^2 - x < 1 + 2\sqrt{x} \leq \frac{1}{4}(3x^{1/4} - 1)^2$, and thus $b - 1 < \sqrt{a^2 - x} < (3x^{1/4} - 1)/2$. Let $n = a^2 - b^2 = (a-b)(a+b)$, so that the prime factors of n are $\leq a + b < 1 + \sqrt{x} + 1 + (3x^{1/4} - 1)/2 < 2\sqrt{x}$. Moreover $x - n = b^2 - (a^2 - x)$ so that, by definition of b, $0 \leq x - n \leq 2(b-1) \leq 3x^{1/4} - 1$.

Proof of Proposition 2: The result follows directly from Corollary 5 in the range $4 \leq u \leq 3 \times 10^6$ since then $u^{3/4}/30 < \sqrt{2u-1}$. We may thus assume that $u > 3 \times 10^6$.

Suppose that p divides $u-a$ where a is a positive integer $\leq u^{3/4}/30$. If $p \leq \sqrt{u}$ then we know that $p \in S_I$ by Corollary 5. If $p > \sqrt{u}$ then $(u-a)/p \leq \sqrt{u}$ and so belongs to S_I. Thus, since S_I is closed under multiplication, we see that $p \in S_I$ if and only if $u-a \in S_I$.

Note that the result follows from Corollary 5 if $a \leq \sqrt{2u-1}$; so we assume henceforth that $a > \sqrt{2u-1}$. Let n be the largest integer $\leq 3u^{1/4}-1$. By Lemma 2 there are integers, in both of the intervals $[u-a-n, u-a]$ or $[u-a, u-a+n]$, which have all of their prime factors $\leq 2\sqrt{u}$ (we will call such an integer $u-b$ below). By Corollary 5 $u-b \in S_I$. We shall show that for one of these choices of $u-b$, we have $(u-b)(u-a) \in S_I$. Thus $(u-a) \in S_I$ (and so $p \in S_I$), since S_I is closed under multiplication.

Select k to be the greatest integer $\leq a^2/(u-a)$ so that $u^2-(u-a) < (u-a)(u+a+k) \leq u^2$. We note that $n+1 \leq 3u^{1/4}$ and $k \leq u^{1/2}/(900-30u^{-1/4}) \leq u^{1/2}/870$.

If $(u-a)(u+a+k) \geq u^2 - \frac{u-a}{2}$ then for $A = a, a+1, \dots, a+n$ we have

$$\begin{aligned} u^2 &\geq (u-a)(u+a+k) \geq (u-A)(u+A+k) > (u-A-1)(u+A+k) \\ &\geq (u-a-(n+1))(u+a+k+n) \geq u^2 - \frac{3(u-a)}{2} - (n+1)(2a+k+n). \end{aligned}$$

Now

$$(n+1)(2a+k+n) < 3u^{1/4}\left(\frac{u^{3/4}}{15} + \frac{u^{1/2}}{870} + 3u^{1/4}\right) \leq \frac{u}{5} + \frac{u^{3/4}}{290} + 9u^{1/2} < \frac{u}{2}$$

for $u \geq 904$ and so the lower bound above is $\geq (u-1)^2$. Therefore $(u-A)(u+A+k)$ and $(u-A-1)(u+A+k)$ both belong to I and so to S_I. Multiplying these together gives $(u-A-1)(u-A) \in S_I$; and then multiplying together this result for $A = a, a+1, \dots, b-1$ to get that $(u-b)(u-a) \in S_I$ and the result follows.

If $(u-a)(u+a+k) \leq u^2 - \frac{u-a}{2}$ then note that $(u-a)(u+a+k-1) = (u-a)(u+a+k) - (u-a) > u^2 - 2(u-a) > (u-1)^2$. Thus for $A = a, a-1, \dots, a-n$ we have

$$\begin{aligned} (u-1)^2 &\leq (u-a)(u+a+k-1) \leq (u-A)(u+A+k-1) \\ &< (u-A+1)(u+A+k-1) \leq (u-a+(n+1))(u+a+k-(n+1)) \\ &\leq u^2 - \frac{u-a}{2} + (n+1)(2a+k-(n+1)). \end{aligned}$$

Now, proceeding as above, we have

$$(n+1)(2a+k) + a/2 < \frac{u}{5} + \frac{7u^{3/4}}{348} < \frac{u}{2}$$

for $u \geq 923$ and so the upper bound here is $\leq u^2$. Therefore $(u-A)(u+A+k-1)$ and $(u-A+1)(u+A+k-1)$ both belong to I and so to S_I. Multiplying these together gives

$(u-A)(u-A+1) \in S_I$; and then multiplying together this result for $A = b+1, \dots, a$ to get that $(u-a)(u-b) \in S_I$ and the result follows.

6. Minimal sets whose product is twice a square

It is interesting to consider what is the smallest set of integers $S \subset I_u$ whose product is twice a square:

Suppose that $|S| = 1$: That is, there exists an integer m such that $(u-1)^2 < 2m^2 < u^2$. This is equivalent to requiring that the fractional part of $u/\sqrt{2}$ is $< 1/\sqrt{2}$. It is well known that this occurs for $\sim U/\sqrt{2}$ of the integers $u \leq U$.

Suppose that $|S| = 2$: That is, there exist integers g, m, n, with g odd and squarefree, such that $(u-1)^2 \leq 2gm^2, gn^2 \leq u^2$. Notice that the $|S| = 1$ case is just the case $g = 1$ here. Do we get all intervals I_u covered with the constructions so far? We ran a program to check this; simply for each u we took each odd and squarefree $g \leq 2u$ and then looked to see if there are such integers m and n with $(u-1)^2 \leq 2gm^2, gn^2 \leq u^2$. There are 123 exceptional values of $u < 10^4$, namely $4, 14, 21, 79, 86, 93, 100, \dots, 7368, 7423, 7846, 8044, 8758$.

Now, for a fixed g, the existence of an integer n for which $(u-1)^2 < gn^2 < u^2$, is equivalent to having that $\{u/\sqrt{g}\} < 1/\sqrt{g}$, where $\{t\}$ denotes the fractional part of t. If we randomly choose a value of $u \leq U$, then the probability that this happens for one given odd, squarefree value of g is $\sim 1/\sqrt{g}$. By ergodic theory we know that such probabilities are independent so that the 'probability' that a randomly chosen value of u satisfies $\{u/\sqrt{g}\} < 1/\sqrt{g}$ and $\{u/\sqrt{2g}\} < 1/\sqrt{2g}$ simultaneously is $1/g\sqrt{2}$. Indeed, for any fixed G, we can prove that the number of integers $u \leq U$ for which there is no triple g, m, n satisfying $(u-1)^2 \leq 2gm^2, gn^2 \leq u^2$, where $g \leq G$ is odd and squarefree, is $\sim U \prod_g (1 - 1/g\sqrt{2})$ where the product is over odd, squarefree integers $g \leq G$. Now, it is easily shown that $\prod_g (1 - 1/g\sqrt{2}) = G^{-2\sqrt{2}/\pi^2 + o(1)}$ as $G \to \infty$. Thus there are $o(U)$ exceptional $u \leq U$. If we were to suppose that our formula held with appropriate uniformity (i.e. taking $G = 2U$ above) then we'd expect that the number of integers $u \leq U$, such that there are no two integers in $[(u-1)^2, u^2]$ whose product is twice a square, is $U^{1-2\sqrt{2}/\pi^2 + o(1)}$, and we note that this exponent is $.71342041\dots$. We'd thus expect about 138 such integers $u \leq 10^4$, whereas we found above that the correct number is 123, so our heuristic is more-or-less borne out in practice.

Scott Contini then wrote a program checking that for each u in the above list, there does exist three numbers in $((u-1)^2, u^2)$ whose product is twice a square; for examples,

$3^2 < 2.5 < 3.2^2 < 3.5 < 4^2$, then $13^2 < 19.3^2 < 5.6^2 < 2.5.19 < 14^2$, and $8757^2 < 2.11.1867^2 < 7.11.998^2 < 7.3310^2 < 8758^2$. Thus we can conclude that there is a nonempty set of integers, with no more than three elements, in any I_u for $u < 10^4$, whose product is twice a square. Presumably this is true for all $u \geq 2$.

References

[1] P. Erdős, J.L. Malouf, J.L. Selfridge and E. Szekeres, Subsets of an interval whose product is a power, Disc. Math. **200** (1999), 137–147.

[2] C. Pomerance, The role of smooth numbers in number theoretic algorithms, Proc. Int. Cong. Math., Birkhäuser Verlag, Basel (1994), 411–422.

Granville (andrew@math.uga.edu) Department of Mathematics, University of Georgia, Athens, Georgia 30602-7403.
Selfridge (selfridg@math.niu.edu) Department of Mathematics,Northern Illinois University, De Kalb, Illinois 60115.