Large strings of consecutive smooth integers

Filip Najman

Abstract

In this note we improve an algorithm from a recent paper by Bauer and Bennett for computing a function of Erdös that measures the minimal gap size $f(k)$ in the sequence of integers at least one of whose prime factors exceeds k. This allows us to compute values of $f(k)$ for larger k and obtain new values of $f(k)$.

Keywords Pell equation, Compact representations, Smooth numbers
Mathematics subject classification (2000) 11N25, 11D09.

1 Introduction

For any integer m we let $P(m)$ be the largest prime factor of m with the convention $P(0) = P(\pm 1) = 1$. Let $\Pi_{n,k}$ be the product of k consecutive integers, starting with n, i.e.

$$\Pi_{n,k} = n(n+1)\cdots(n+k-1).$$

By a theorem of Sylvester (see [15]) $\Pi_{n,k}$ is divisible by a prime $p > k$, and thus, following Erdös [7], we define $f(k)$ to be the least integer with the property that

$$P\left(\Pi_{n,f(k)}\right) > k.$$

Standard heuristics for the size of gaps between consecutive primes lead one to expect that order of magnitude of $f(k)$ is $(\log k)^2$.

The following table gives known values of $f(k)$:

k	$f(k)$	k	$f(k)$	k	$f(k)$
1	1	$13-40$	6	$61-113$	14
2	2	$41-46$	7	114	13
$3-4$	3	$47-58$	8	$115-150$	12
$5-12$	4	$59-60$	9	$151-178$	14

The values of $f(k)$ for $k \leq 10$ were computed by Utz [16] and extended to $k \leq 42$ by Lehmer [11], to $k \leq 46$ by Ecklund and Eggleton [4], to $k \leq 73$ by Ecklund, Eggleton and Selfridge [5], [6] and finally to $k \leq 178$ by Bauer and Bennett [1]. Bauer and Bennett in the same paper also disproved an assertion of Utz that f is monotone.

In this paper we compute the values of $f(k)$ for $k \leq 268$. Our results can be summarized in the following theorem.

Theorem 1. *For* $179 \leq k \leq 268$ *the values of* $f(k)$ *are as follows:*

k	$f(k)$
$179 - 222$	14
$223 - 268$	16

Note that Bauer and Bennett, although greatly extending the set of k such that $f(k)$ is known, by 105 values of k, did not find any values of $f(k)$ such that $f(k) > 14$. In Theorem 1 we find the new largest proven value of $f(k)$, the first after nearly 40 years (the previous being [6]).

2 The algorithm

Lemher [10] searched for two consecutive smooth integers, satisfying $P(z(z+1)) \leq p_t$, where p_t is the t-th prime. One can write $x = 2z + 1$, and see that $P(z(z+1)) \leq p_t$ iff $P(x^2 - 1) \leq p_t$. Writing $x^2 - 1 = dy^2$, where d is squarefree, this leads to the Pell equation

$$x^2 - dy^2 = 1, \tag{1}$$

where $P(dy) \leq p_t$. This implies that the solutions $x + y\sqrt{d}$ we are searching for are powers of the fundamental solution $u + v\sqrt{d}$, i.e

$$x + y\sqrt{d} = (u + v\sqrt{d})^n.$$

By classic results on primitive divisors (see [3]) and the work of Lehmer (see [9]) if we want $P(y) \leq p_t$, then

$$n \leq \max\left\{\frac{p_t + 1}{2}, 12\right\}.$$

Thus one needs to consider only finitely many Pell equations and for each one only some of the first solutions.

After finding all pairs of smooth consecutive integers in this way, one can search through the results and find larger strings of consecutive integers.

Bauer and Bennett [1] improve on this strategy by the following clever argument: for fixed $m \leq 3$ and t suppose we are searching for all integers n satisfying

$$P(\Pi_{n,m}) \leq p_t. \tag{2}$$

We can split the indices $0, \ldots, m-1$ into $\lfloor \frac{m}{4} \rfloor + \lfloor \frac{m+1}{4} \rfloor$ disjoint pairs $(i, i+2)$, where $i \equiv 0, 1 \pmod 4$. Set $t_0 = \pi(m-1)$. By the Dirichlet principle, we can find an index i such that $(n+i)(n+i+2)$ is divisible by at most

$$N = \left\lfloor \frac{t - t_0}{\lfloor \frac{m}{4} \rfloor + \lfloor \frac{m+1}{4} \rfloor} \right\rfloor$$

of the primes from the set

$$\{p_{t_0+1}, \ldots, p_t\}. \tag{3}$$

Now one writes $X = n + i + 1$ and $Y = (n + i)(n + i + 2)$, and gets

$$X^2 - DY^2 = 1,$$

where D is squarefree and divisible only by some of the first t_0 primes and at most N of the primes from the set (3). Then one proceeds exactly as Lehmer, with the difference that in this approach $P(X) \leq p_t$ also has to hold. This lowers the number of Pell equations one needs to consider from $2^t - 1$ to

$$M = -1 + 2^{t_0} \sum_{j=0}^{N} \binom{t - t_0}{j},$$

and equally important, reduces the size of the Pell equations.

The bottleneck of both the algortihms of Lehmer and Bauer and Bennett is solving the Pell equaiton. The main difficulty in solving the Pell equaiton is the size of the solutions, as it grows exponentially in respect to the size of the coefficient d form (1). This means that just *writing down* the solution in standard representation takes exponential time. In [12], Luca and the author used *compact representations* of the solutions to the Pell equations to overcome this difficulty and managed to extend Lehmer's results (see also [14] for another application of this approach). Note that the algorithm described in [12] is still the best up to date if one wants to find 2 or 3 consecutive smooth integers.

A compact representation of an algebraic number $\beta \in \mathbb{Q}(\sqrt{d})$ is a representation of β of the form

$$\beta = \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j} \right)^{2^{k-j}}, \tag{4}$$

where $d_j \in \mathbb{Z},\ \alpha_j = (a_j + b_j\sqrt{d})/2 \in \mathbb{Q}(\sqrt{d}),\ a_j, b_j \in \mathbb{Z},\ j = 1, \ldots, k$, and k, α and d_j have $O(\log d)$ digits. A detailed description of compact representations and their use can be found in [8]. Using compact representations, the Pell equation is solved in two steps. First, the regulator of the apropriate quadratic field is computed, and after that from the regulator a compact representation is obtained. As, once the regulator is known, one can obtain a compact representation in polynomial time, by far the harder part of this process is the computation of the regulator. The fastest unconditional algorithms are still exponential in respect to d and the fastest known algorithm, Buchmann's subexponential algorithm (see [2]) depends on the Generalized Riemann Hypothesis.

For our purposes, the only algorithm fast enough is Buchmann's algorithm. We will perform a simple check, using continued fractions, that will for each case tell us either that the output of Buchmann's algorithm is unconditionally correct or that we can disregard this case. In other words, although we cannot unconditionally solve the Pell equation in subexponential time, we can determine unconditionally whether it has a smooth solution (and find any smooth solutions) in subexponential time. This removes the dependence of our results on the Generalized Riemann Hypothesis. This check is explained in detail in [12] in step 6 on page 5, and for this reason we will not repeat it here.

Using compact representation cuts down the space needed from exponential to polynomial in respect to d and the time needed to solve the Pell equation from exponential to subexponential.

In essence, our algorithm combines the clever approach of [1] and the powerful methods for finding smooth solutions of the Pell equations from [12].

3 Results

We run our algorithm for two pairs of parameters (m, t), these pairs being $(47, 14)$, and $(56, 16)$. Note thet $p_{47} = 211$, $p_{56} = 263$ and $P(\Pi_{318,13}) = 163$, $P(\Pi_{1330,15}) = 223$, implying

$$f(k) \geq 14 \text{ for } 178 \leq k \leq 222 \text{ and } f(k) \geq 16 \text{ for } 224 \leq k \leq 268 \qquad (5)$$

By proving that there is no integer $n > k$ for $178 \leq k \leq 222$ satisfying $P(\Pi_{n,14}) \leq k$ implies $f(k) = 14$ for $178 \leq k \leq 222$. In the same way one proves that $f(k) = 16$ for $224 \leq k \leq 268$.

The case $(m, t) = (47, 14)$ makes us solve

$$M_1 = -1 + 2^6 \sum_{j=0}^{6} \binom{41}{j} = 342948991$$

Pell equaitons, while the case $(m, t) = (56, 16)$ makes us solve

$$M_2 = -1 + 2^6 \sum_{j=0}^{6} \binom{50}{j} = 1168680703$$

Pell equaitons.

We obtain that there do not exist such integers n, thus proving Theorem 1.

Acknowledgements.
These materials are based on work financed by the National Foundation for Science, Higher Education and Technological Development of the Republic of Croatia.

References

[1] M. Bauer and M. A. Bennett, *Prime factors of consecutive integers*, Math. Comp., **77** (2008), 2455–2459.

[2] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres (1990), 27–41.

[3] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of. Math. **15** (1913), 30–70.

[4] E. F. Ecklund, Jr. and R. B. Eggleton, *Prime factors of consecutive integers*, Amer. Math. Monthly **79** (1972), 1082-1089.

[5] E. F. Ecklund, Jr., R. B. Eggleton and J. L. Selfridge, *Factors of consecutive integers*, Proc. Man. Conference Numerical Maths., Winnipeg (1971), 155-157.

[6] E. F. Ecklund, Jr., R. B. Eggleton and J. L. Selfridge *Consecutive integers all of whose prime factors belong to a given set*, Proc. Man. Conference Numerical Maths., Winnipeg (1971), 161-162.

[7] P. Erdös, *On consecutive integers*, Nieuw Arch. Wisk. **3** (1955), 124-128.

[8] M. J. Jacobson Jr., H. C. Williams, *Solving the Pell Equation*, Springer, 2009.

[9] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. Math. **31** (1930), 419-448.

[10] D. H. Lehmer, *On a problem of Störmer*, Illinois J. Math **8** (1964), 57–79.

[11] D. H. Lehmer, *The prime factors of consecutive integers* Amer. Math. Monthly **72** (1965), 19-20.

[12] F. Luca and F. Najman, *On the largest prime factor of* $x^2 - 1$, Math. Comp., to appear.

[13] F. Najman, *Compact representation of quadratic integers and integer points on some elliptic curves*, Rocky Mountain J. Math., to appear.

[14] F. Najman, *Smooth values of some quadratic polynomials*, Glasnik Mat. Ser III, to appear.

[15] J. J. Sylvester, *On arithmetical series*, Messenger Math. **21** (1892), 1-19, 87-120.

[16] W. R. Utz, *A conjecture of Erdos concerning consecutive integers*, Amer. Math. Monthly **68** (1961), 896-897.

MATHEMATISCH INSTITUUT, P.O. BOX 9512, 2300 RA LEIDEN, THE NETHERLANDS

AND

DEPARTMENT OF MATHEMATICS, UNIVERISTY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

E-mail address: fnajman@math.hr