A BINARY ADDITIVE PROBLEM OF ERDŐS AND THE ORDER OF 2 MOD p^2

Andrew Granville and K. Soundararajan

We'd like to thank Paul Erdős for the questions

Abstract. We show that the problem of representing every odd positive integer as the sum of a squarefree number and a power of 2, is strongly related to the problem of showing that p^2 divides $2^{p-1}-1$ for "few" primes p.

Introduction

It is frustrating that there is no plausible known approach to the question of determining whether there are infinitely primes p for which p^2 does not divide $2^{p-1}-1$. We know very little of consequence; only the computational result [1] that p^2 divides $2^{p-1}-1$ for just the primes 1093 and 3511 of all $p \le 4.10^{12}$. Naive heuristics suggest that the number of primes up to x, for which p^2 divides $2^{p-1}-1$, should be $\sim \log\log x$; and so we believe that there are infinitely many primes for which p^2 divides $2^{p-1}-1$, and infinitely many primes p for which p^2 does not divide $2^{p-1}-1$.

In 1910, Wieferich [15] showed that if there are integers x, y, z satisfying $x^p+y^p = z^p$ and $(p, xyz) = 1$ then p^2 divides $2^{p-1}-1$; such primes p are thus known as "*Wieferich primes*". Of course, Fermat's Last Theorem is now proved [16] so this result has become a (delightful) historical curiosity.

Recently Paul Erdős has made the following, seemingly unrelated, conjecture (see section A19 in [9]):

Conjecture 1 (Erdős). *Every odd positive integer is the sum of a squarefree number and a power of 2.*

There is no significant loss of generality in Erdős's restriction to odd integers n. For if $n = m + 2^j$ then m is odd, so $2n = 2m + 2^{j+1}$, and vice-versa; and if $4n = m + 2^j$ then 4 divides m so it cannot be squarefree.

In this note, we show that these questions are indeed related.

Theorem 1. *Suppose that every odd positive integer can be written as the sum of a squarefree number and a power of 2. Then there are infinitely many primes p for which p^2 does not divide $2^{p-1}-1$. In fact there then exists a constant $c > 0$ such that there are arbitrarily large values of x for which*

$$\#\{\text{primes } p \le x : 2^{p-1} \not\equiv 1 \pmod{p^2}\} \ge c\#\{\text{primes } p \le x\}.$$

In the other direction we prove, at the suggestion of Neil Calkin:

The first author is a Presidential Faculty Fellow. He is also supported, in part, by the National Science Foundation. The second author is supported by an Alfred P. Sloan dissertation fellowship.

Theorem 2. *Assume that there are $\le 2\log x/(\log\log x)^2$ primes $p \le x$ for which p^2 does divide $2^{p-1}-1$, whenever $x \ge 3$. Then all but $O(x/\log x)$ of the odd integers $n \le x$ can be written as the sum of a squarefree number and a power of 2.*

Remark. Assuming $\sum_{p^2 \mid 2^{p-1}-1} 1/\mathrm{ord}_p(2) \le 5/8$ we can make the same deduction by the same proof.

It would be nicer to have an "if and only if" statement of some kind, rather than our two results above, which would probably require some strengthening of both of these results. We hope the reader will embrace this challenge.

Erdős's conjecture has been verified for all odd integers up to 10^7 by Andrew Odlyzko.

In Proposition 3 we give a result giving conditions under which we can guarantee that almost all integers, in certain arithmetic progressions, are the sum of a squarefree number and an element of a given sequence $\mathcal{A}$. This implies Theorem 2 and various other results. For example, there are no known primes for which $2^{p-1} \equiv 3^{p-1} \equiv 1 \pmod{p^2}$. If this is true, then we deduce:

Corollary 1. *Suppose that there does not exist a prime p for which p^2 divides both $2^{p-1}-1$ and $3^{p-1}-1$. Then almost all integers coprime to 6 are the sum of a squarefree number and an integer which is the product of a power of 2 and a power of 3.*

One might try to justify Erdős's conjecture by the following heuristic argument. The probability that a random odd integer is squarefree is $\prod_{p\ge 3}(1-1/p^2) = 8/\pi^2$. Thus the probability that none of $n-2, n-4, n-8, \dots, n-2^r$ is squarefree (under the assumption that these events are independent) is $(1-8/\pi^2)^r \asymp n^{-c}$ where $c = -\log(1-8/\pi^2)/\log 2$ (since $r = \log n/\log 2 + O(1)$). Since $8/\pi^2 < 4/5$, we have $c > \log 5/\log 2 > 2$. Hence, we 'deduce', by the Borel-Cantelli Lemma, that at most finitely many n fail to be the sum of a squarefree number and a power of 2. In fact, one can deduce from similar reasoning that if $r(n)$ denotes the number of positive integers i for which $n-2^i$ is a positive squarefree integer, then $r(n) \sim (8/\pi^2)\log n/\log 2$ for almost all integers n (we write that $r(n)$ has "normal order" $(8/\pi^2)\log n/\log 2$).

However, this reasoning is highly dubious, since the proof of Theorem 1 (in fact, of Proposition 1 below) rests, appropriately interpreted, on the fact that the events $n-2, n-4, \dots, n-2^r$ being squarefree, are not independent. By studying the first two moments of $r(n)$, we show below that $r(n)$ does not have a normal order. In fact our analysis extends to $r_{\mathcal{A}}(n)$, the number of ways of writing $n = m + a_i$ with m a positive squarefree number and $a_i \in \mathcal{A}$, where $\mathcal{A} = \{a_1 < a_2 < \dots\}$ is a sparse sequence of positive integers. Define $A(x)$ to be the number of $a_i \le x$.

Theorem 3. *Suppose we are given a sequence $\mathcal{A}$ of distinct positive integers for which $A(2x) \sim A(x)$, and an arithmetic progression $a \pmod{q^2}$ with $(a-a_i, q^2)$ squarefree for all $a_i \in \mathcal{A}$. Then $r_{\mathcal{A}}(n)$ has mean $\sim c_q A(x)$ when averaging over the integers $n \le x$, for which $n \equiv a \pmod{q^2}$, where $c_q := \prod_{p\nmid q}(1-1/p^2)$.*

Moreover, these $r_{\mathcal{A}}(n)$ have normal order $c_q A(n)$ if and only if $\mathcal{A}$ is equidistributed amongst the arithmetic progressions $\pmod{d^2}$, for every integer d which is coprime to q (that is, there are $\sim A(x)/d^2$ integers $a_i \le x$ with $a_i \equiv l \pmod{d^2}$ for each l).

Remark. Note that the condition $(a - a_i, q^2)$ is squarefree for all $a_i \in \mathcal{A}$ ensures that it is feasible that $n - a_i$ is squarefree for each a_i.

Take $\mathcal{A} = \{2, 4, 8, \dots\}$ with $q = 2$ and $a = 1$ or 3. Since the powers of 2 are not equi-distributed in residue classes $\pmod{d^2}$ for any odd d, we deduce by Theorem 3 that $r(n) = r_{\mathcal{A}}(n)$ cannot have a normal order.

We now give an example of a set $\mathcal{A}$ which is sparser than the powers of 2, but for which $r_{\mathcal{A}}(n)$ has a normal order.

Corollary 2. *Almost all integers are the sum of a squarefree number and an integer of the form* $1^1 + 2^2 + \cdots + k^k$. *In fact, if* $n \equiv 2, 3 \pmod 4$ *the number of such representations has normal order* $(8/\pi^2) \log n / \log\log n$; *and if* $n \equiv 0, 1 \pmod 4$, *the number of such representations has normal order* $(4/\pi^2) \log n / \log\log n$.

The genesis of Erdős's conjecture is from de Polignac's (incorrect) claim [10] (retracted in the second reference [10]) that every odd integer is the sum of a prime and a power of 2. The first counterexample is 127, though Euler had noted the counterexample 959 in a letter to Goldbach. In 1934, Romanoff [12] showed that a positive proportion of odd integers *can* be represented in this way, and in 1950 van der Corput [14] and Erdős [5] showed that a positive proportion of odd integers *cannot* be represented in this way. Romanoff's proof uses the Cauchy-Schwarz inequality, estimating the mean of the number of representations, and bounding the mean square; this last upper bound follows from Brun's sieve followed by showing that $\sum_d 1/d \operatorname{ord}_d(2) < \infty$. Erdős invented the elegant notion of a "covering system of congruences", which we describe in detail in the next section, to find an infinite arithmetic progression of odd values of n that cannot be written as a prime plus a power of 2. It is still an open question, of Erdős, as to whether there is a precise proportion of the odd integers that are so representable (asymptotically), and then even a informed prediction of what that proportion is (of course the Romanoff and Erdős results can be used to get non-trivial upper and lower bounds on that proportion).

Next one might perhaps replace "prime" by "squarefree number" in the above problem (as Erdős did); an alternative is to replace "a power of 2" by "two powers of 2". Unfortunately, Crocker [2] observed that for any odd integer $n = 2^{2^m} - 1$ with $m \geq 3$, the numbers $n - 2^a - 2^b$ with $1 \leq a < b < 2^m$ are never prime. To see this let 2^k be the highest power of 2 dividing $b - a$. Then $2^{2^k} + 1$ divides $2^{b-a} + 1$, which divides $2^b + 2^a$. Moreover $k \leq m - 1$ so that $2^{2^k} + 1$ divides n, and so $2^{2^k} + 1$ divides $n - 2^a - 2^b$. If these were equal then $2^{2^m} = 2^b + 2^a + 2^{2^k} + 2$, and this can be seen to be impossible by considering this equation mod 16 to restrict a and b. Thus it is not the case that every odd integer is the sum of a prime and two powers of 2, though Erdős predicted that perhaps almost all odd integers n can be so described. We conjecture that all odd integers > 1 are the sum of a prime and at most three powers of 2. Along these lines, Gallagher [8] showed that the proportion of odd integers that can be written as a prime plus the sum of k powers of two, tends to 1 as $k \to \infty$.

We take a lead from this line of investigation to discuss whether one can prove that almost all odd n are the sum of a squarefree integer plus at most k powers of 2, for some k. We prove:

Theorem 4. *Assume that* $\sum_{p^2|2^{p-1}-1} 1/\mathrm{ord}_p(2) < \infty$. *Then there exists an integer* k *such that almost every odd integer can be written as the sum of a squarefree number plus no more than* k *distinct powers of 2.*

It is completely straightforward to prove the analogy to Gallagher's result: Every integer up to 2^k is the sum of at most k powers of two. The number of integers amongst $n-1, n-2, \dots, n-2^k$ divisible by the square of a prime $p < 2^k$ is $\le \sum_{p<2^k}(2^k/p^2+1) < .49\times 2^k + O(2^k/k) < 2^{k-1}$ for k sufficiently large. Of the integers $n \le x$, the number for which more than 2^{k-1} of the integers $n-1, n-2, \dots, n-2^k$ are divisible by the square of a prime $p > 2^k$ is

$$\le 2^{1-k} \sum_{n\le x} \sum_{\sqrt{x}>p>2^k} \sum_{\substack{1\le i\le 2^k \\ p^2|n-i}} 1 \ll \sum_{\sqrt{x}>p>2^k} \frac{x}{p^2} \ll \frac{x}{k2^k}.$$

Thus all but $O(x/k2^k)$ of the odd integers $\le x$ can be written as the sum of a squarefree number and k powers of two.

There are many other intriguing questions of this type asked by Erdős (see section A19 of [9]): Erdős conjectured that 105 is the largest integer for which $n-2^k$ is prime whenever $2 \le 2^k < n$ (analogously it was shown in [3] that 210 is the largest integer $2n$ for which $2n-p$ is prime for every prime p, $n \le p < 2n$). He showed that there exist n for which $n-2^k$ is prime for $\gg \log\log n$ such values of k, and asked whether this could be improved. He also conjectured that for infinitely many n, all of the integers $n-2^k$, $2 \le 2^k < n$ are squarefree. Erdős conjectured that there are arbitarily large gaps between consecutive odd numbers that can be represented as the sum of a prime and a power of 2.

Erdős asked whether there are $\gg x^\epsilon$ odd integers $n \le x$ that are not equal to a prime plus two powers of two. By modifying Crocker's construction slightly, this is easily shown for arbitrarily large x if infinitely many Fermat numbers $F_k = 2^{2^k}+1$ are composite, and for all x if $\{k_{i+1}-k_i\}$ is bounded where F_{k_i} is the sequence of composite Fermat numbers.

Acknowledgements: We'd like to thank Neil Calkin, Jeff Lagarias, Tauno Metsankyla, Andrew Odlyzko and Carl Pomerance for helpful remarks incorporated into this paper.

Notation: Henceforth $\mathcal{A}$ will always denote a sequence $\{a_1 < a_2 < \dots\}$ of positive integers. We will let $A(x)$ be the number of $a_i \le x$, and $A(x;d,b)$ be the number of $a_i \le x$ for which $a_i \equiv b \pmod d$.

Covering systems and all that

The more detailed proof is that of Theorem 1, which stems from some modifications of constructions due to Paul Erdős. We will discuss here these constructions, beginning with the idea behind Erdős' disproof of de Polignac's "conjecture" [5].

A *covering system* for the integers is a finite set of arithmetic progressions, such that every integer belongs to at least one of these arithmetic progressions. For example $0 \pmod 2; 1 \pmod 2$ or $1 \pmod 2; 1 \pmod 3; 0 \pmod 6; 2 \pmod 6$.

Now suppose that we can find a covering system with arithmetic progressions like $a_i \pmod{\mathrm{ord}_{p_i}(2)}$, for $i = 1, 2, \dots, k$, where the p_i are distinct, odd primes.

Let n_0 be the smallest odd integer satisfying $n_0 \equiv 2^{a_i} \pmod{p_i}$ for each i (which is a well defined integer $\pmod{2\prod_{1\le i\le k} p_i}$ by the Chinese Remainder Theorem). For any $n \equiv n_0 \pmod{2\prod_{1\le i\le k} p_i}$ and for any integer j, we have that $j \equiv a_i \pmod{\mathrm{ord}_{p_i}(2)}$ for some i (since we have a covering system above), and so $n-2^j \equiv n_0 - 2^{a_i} \equiv 0 \pmod{p_i}$. Therefore $n-2^j$ is composite provided it is $> p_i$; and if this is so for each j with $2^j < n$, then n cannot be written as the sum of a prime and a power of 2.

There are several ways to get around the problem that we might have $n-2^j = p_i$ for some i and j. Usually one imposes an extra congruence on n. Alternately, note that if $n < 2^{m+1}$ can be so represented then $j \le m$ and $1 \le i \le k$, so that there are $\le mk$ such exceptional n. However the number of integers $n \equiv n_0 \pmod{2\prod_{1\le i\le k} p_i}$ in this range is $\ge 2^m/\prod_{1\le i\le k} p_i - 1$, so we certainly have non-exceptional such n if m is chosen sufficiently large.

The question reduces to producing such a covering system. This is easily done by taking $0 \pmod{\mathrm{ord}_3(2)=2}$, $0 \pmod{\mathrm{ord}_7(2)=3}$, $1 \pmod{\mathrm{ord}_5(2)=4}$, $3 \pmod{\mathrm{ord}_{17}(2)=8}$, $7 \pmod{\mathrm{ord}_{13}(2)=12}$, $23 \pmod{\mathrm{ord}_{241}(2)=24}$; so we end up with the arithmetic progression $n \equiv 7629217 \pmod{11184810}$.

Define $\omega(p)$ to be the order of $2 \pmod{p^2}$. If we were able to construct a covering system out of arithmetic progressions with moduli $\omega(p)$, then we could give a similar disproof of Conjecture 1.

Theorem 5. *Suppose that there exists a covering system $\{a_i \pmod{\omega(p_i)}\}_{1\le i\le m}$ where the p_i are distinct, odd primes. Then a positive proportion of the odd integers $n \le x$ cannot be written as the sum of a squarefree number and a power of 2.*

Proof. Let n be any odd integer $\equiv 2^{a_i} \pmod{p_i^2}$ for $1 \le i \le m$ (the density of such odd integers is $1/\left(\prod_{1\le i\le m} p_i\right)^2 > 0$ amongst the odd integers). For any positive integer j, select i, $1 \le i \le m$ so that $j \equiv a_i \pmod{\omega(p_i)}$ (which is possible by hypothesis), and thus $n-2^j$ is divisible by p_i^2. Therefore $n-2^j$ is never squarefree and so n cannot be written as the sum of a squarefree number and a power of 2.

However, we do not believe that such a covering system can exist:

Conjecture 2. *There is no finite set of distinct, odd primes $\{p_1, p_2, \dots, p_m\}$ and integers $a_1, a_2, \dots, a_m$ such that every integer belongs to at least one of the congruence classes $a_i \pmod{\omega(p_i)}$.*

Erdős remarked to us that, given that Theorems 1 and 2 suggest that it will probably be difficult to prove Conjecture 1, we might try for the weaker result that "almost all" odd n can be represented as the sum of a squarefree number and a power of 2. In Theorem 5 we saw that to prove this we will at least need to show that Conjecture 2 is true, which looks difficult. One encouraging remark is that, by a slight strengthening of Conjecture 2, we are able to deduce that "almost all" odd n can be represented as the sum of a squarefree number and a power of 2:

Conjecture 3. *There exists a constant $\delta > 0$ such that, for any finite set of primes $\{p_1, p_2, \dots, p_m\}$ and any choice of integers $a_1, a_2, \dots, a_m$, the proportion of positive integers which belong to at least one of the congruence classes $a_i \pmod{\omega(p_i)}$, is $< 1-\delta$.*

Theorem 6. *Assume that Conjecture 3 is true. Then "almost all" odd integers $n \le x$ can be written as the sum of a squarefree number and a power of 2.*

Proof. Fix integer K and consider odd n in the range $2^K < n \le 2^{K+1}$. Select $y = \log K$, so that the number of integers $n - 2^i$, $1 \le i \le K$ not divisible by the square of any prime $\le y$ is $> \delta K - 2^{\pi(y)} > \delta K/2$, using Conjecture 3 and the combinatorial sieve. Moreover, the total number of pairs (n, i) in these ranges, for which $n - 2^i$ is divisible by the square of a prime $> y$ is $\ll K \sum_{p>y} 2^{K+1}/p^2 \ll K2^K/y \log y$; and thus there are $< \delta K/2$ such values of i for all but $O(2^K/\log K \log\log K)$ of the values of n in our range. For these n, we have some i with $n - 2^i$ squarefree, and the number of failures is thus $\ll x/\log\log x$.

Note that the condition $\sum_p 1/\omega(p) < 1$ implies Conjecture 3 (with $\delta = 1 - \sum_p 1/\omega(p)$), which implies Conjecture 2.

Lemma 1. *If Conjecture 3 is true then $\sum_p 1/\omega(p) < \infty$.*

Proof. Select a_p's by induction as follows: Let S_p be the set of positive integers $\le b_p := \mathrm{lcm}[\omega(q) : 2 < q < p]$ which do not belong to any of the arithmetic progressions $a_q \pmod{\omega(q)}$ for $q < p$, and note that $\delta_p := |S_p|/b_p$ is exactly the proportion of all positive integers not belonging to any of the congruence classes $a_q \pmod{\omega(q)}$ with $q < p$. Given the choices of a_q for each $q < p$, we select $a_p \pmod{\omega(p)}$ so that this arithmetic progression contains as many integers in S_p as possible. Evidently there must be one such arithmetic progression containing $\ge |S_p|/\omega(p)$ such integers, and thus $\delta_\ell \le (1 - 1/\omega(p))\delta_p$, where ℓ is the smallest prime $> p$. Starting with $a_3 = 0$, and then iterating the above procedure, we find that $\delta_p \le \prod_{q<p}(1 - 1/\omega(q))$. Now, Conjecture 3 implies that $\delta_p > \delta > 0$ for all p, and so $\sum_q 1/\omega(q)$ must converge.

Deduction of Theorems 1 and 2 from technical Propositions

Theorems 1 and 2 follow from stronger, but more technical, propositions.

Proposition 1. *Let $\omega(p)$ be the order of 2 $\pmod{p^2}$. Fix $\varepsilon > 0$. If there exist arbitrarily large values of y for which*

$$\prod_{p \le y} \left(1 - \frac{1}{\omega(p)}\right) \le \left(\frac{\log 2}{4} - \varepsilon\right) \frac{1}{\log y}$$

then there are infinitely many odd integers n which cannot be written as the sum of a squarefree number and a power of 2.

In the other direction we show

Proposition 2. *Suppose that*

$$\sum_p \frac{1}{\omega(p)} < 1.$$

Then all but $O(x/\log x)$ of the odd integers $n \le x$ can be written as the sum of a squarefree number and a power of 2.

One can see that there is a lot of difference in these hypotheses in their requirements for the average size of $1/\omega(p)$. Improving this paper would necessitate closing that gap.

Deduction of Theorem 1 from Proposition 1: Suppose that the conclusion of Theorem 1 is false so that

$$\#\{\text{primes } p \le x : 2^{p-1} \not\equiv 1 \pmod{p^2}\} = o(\#\{\text{primes } p \le x\}).$$

Thus almost all primes p satisfy $2^{p-1} \equiv 1 \pmod{p^2}$, implying that $\omega(p) \le p-1$. Moreover if $p \equiv \pm 1 \pmod 8$ then 2 is a quadratic residue $\pmod p$ so that $\omega(p) \le \frac{p-1}{2}$.

Now, as is well-known,

$$\prod_{p\le y}\left(1-\frac{1}{p-1}\right) \ll \frac{1}{\log y}$$

and

$$\prod_{\substack{p\le y\\ p\equiv\pm1 \pmod 8}}\left(1-\frac{1}{p-2}\right) \ll \frac{1}{(\log y)^{1/2}}.$$

Therefore

$$\begin{aligned}\prod_{p\le y}\left(1-\frac{1}{\omega(p)}\right) &\le \prod_{\substack{p\le y\\ 2^{p-1}\equiv1 \pmod{p^2}}}\left(1-\frac{1}{p-1}\right)\cdot\prod_{\substack{p\le y,\ p\equiv\pm1 \pmod 8\\ 2^{p-1}\equiv1 \pmod{p^2}}}\left(1-\frac{1}{p-2}\right)\\ &\ll \frac{1}{(\log y)^{3/2+o(1)}}\end{aligned}$$

The condition in Proposition 1 is thus satisfied and so there are infinitely many integers n which cannot be expressed as the sum of a squarefree number and a power of 2. Theorem 1 follows.

Remark. This argument can be used to show that one can take any constant c, in the range $1/4 > c > 0$, in Theorem 1. One can improve this by considering the appropriate products over those primes p for which 2 is a cubic residue mod p, or a quartic residue, or quintic residue, etc. The density of such primes is determined by the Cebotarev Density Theorem. By such methods we were able to show that $\left(\sum_{p\le y} 1/\mathrm{ord}_p(2)\right)/\log\log y \to \infty$ as $y \to \infty$. This leads us to ask:

$$\text{What is the true order of magnitude of } \prod_{p\le y}\left(1-\tfrac{1}{\mathrm{ord}_p(2)}\right) ?$$

As far as the averaged order of 2 $\pmod{p^2}$ is concerned, we certainly believe that $\sum_p \frac{1}{\omega(p)} < \infty$, and that even the hypothesis of Proposition 2 is true.

Deduction of Theorem 2 from Proposition 2: We write

$$\sum_{p \text{ prime}} \frac{1}{p \text{ ord}_p(2)} = \sum_{n\ge 2} \frac{1}{n} \sum_{\substack{p \text{ prime} \\ \text{ord}_p(2)=n}} \frac{1}{p}$$

Now, if $\text{ord}_p(2) = n$ then $p \equiv 1 \pmod n$. Thus $p > n$ and so the total number of such primes is $\le \log(2^n - 1)/\log(n+1) < n \log 2/\log n$.

Therefore, for $m = [n \log 2/\log n]$

$$\sum_{\substack{p \text{ prime} \\ \text{ord}_p(2)=n}} \frac{1}{p} \le \sum_{k=1}^{m} \frac{1}{kn+1} < \frac{1}{n} \sum_{k=1}^{m} \frac{1}{k}$$
$$\le \frac{1}{n}(\log m + 1) \le \frac{1}{n} \log\left(\frac{ne \log 2}{\log n}\right) < \frac{\log n}{n}$$

for $n \ge 7 > 2^e$. Thus for $N \ge 6$,

$$\sum_{n\ge N+1} \frac{1}{n} \sum_{\substack{p \text{ prime} \\ \text{ord}_p(2)=n}} \frac{1}{p} < \sum_{n\ge N+1} \frac{\log n}{n^2} \le \int_N^\infty \frac{\log t}{t^2} dt = \frac{1+\log N}{N}.$$

Using Maple, we have determined that

$$\sum_{n\le 100} \frac{1}{n} \sum_{\substack{p \text{ prime} \\ \text{ord}_p(2)=n}} \frac{1}{p} = 0.31586267847633\ldots$$

Also $(1 + \log 100)/100 = 0.05605170185988\ldots$ so that

$$\sum_{p \text{ prime}} \frac{1}{p \text{ ord}_p(2)} < 0.372$$

Note that if p^2 divides $2^{p-1} - 1$ then $\omega(p) = \text{ord}_p(2)$; otherwise $\omega(p) = p \text{ ord}_p(2)$. Therefore

$$\sum_{p \text{ prime}} \frac{1}{\omega(p)} = \sum_{p \text{ prime}} \frac{1}{p \text{ ord}_p(2)} + \sum_{p^2 \mid 2^{p-1}-1} \frac{p-1}{p \text{ ord}_p(2)}$$
$$< 0.372 + \sum_{p^2 \mid 2^{p-1}-1} \frac{1}{\text{ord}_p(2)}.$$

Now we know that $\text{ord}_p(2) > \log p/\log 2$ and that only $p = 1093$ and $p = 3511$ satisfy $p^2 \mid 2^{p-1} - 1$ when $p < 4 \cdot 10^{12}$. Also $\#\{p \le x : p^2 \mid 2^{p-1} - 1\} \le$

$2\log x/(\log\log x)^2$ by the hypothesis of Theorem 2, so that

$$\sum_{p^2\mid 2^{p-1}-1}\frac{1}{\mathrm{ord}_p(2)} \le \frac{1}{\mathrm{ord}_{1093}(2)}+\frac{1}{\mathrm{ord}_{3511}(2)}+\sum_{\substack{p>4\cdot 10^{12}\\ p^2\mid 2^{p-1}-1}}\frac{\log 2}{\log p}$$

$$\le \frac{1}{364}+\frac{1}{1755}+\frac{\log 2}{\log(4\cdot 10^{12})}\frac{2\log(4\cdot 10^{12})}{(\log\log(4\cdot 10^{12}))^2}+ \\ +\int_{4\cdot 10^{12}}^{\infty}\frac{\log 2}{\log t}d\left(\frac{2\log t}{(\log\log t)^2}\right)$$

$$\le 0.00332+\frac{2\log 2}{(\log\log(4\cdot 10^{12}))^2}+\int_{4\cdot 10^{12}}^{\infty}\frac{2\log 2}{t\log t(\log\log t)^2}dt$$

$$\le 0.1255361175+\frac{2\log 2}{\log\log(4\cdot 10^{12})}=0.5371568161\ldots .$$

Thus

$$\sum_p\frac{1}{\omega(p)}<.9091\ldots$$

and the hypothesis of Proposition 2 is satisfied.

The Proof of Proposition 1: Two constructions of Erdős

Let $m=\prod_{p\le 2y}p$ and select N so that $2y=\left(\frac{1}{2}-\varepsilon\right)\log N$. We shall construct an arithmetic progression $\ell \pmod{m^2}$, such that if $n\le N$ and $n\equiv \ell \pmod{m^2}$ then $(n-2^i,m^2)$ is divisible by a square of a prime for $1\le i\le r$, where $2^r\le N<2^{r+1}$. Since $m^2\ll N^{1-\varepsilon}$ (by the Prime Number Theorem) there exist such integers n, and the result follows.

We shall actually select arithmetic progressions $a_p \pmod{\omega(p)}$ for each prime $p\le 2y$ so that every integer in $[1,r]$ belongs to at least one of these arithmetic progressions (rather like in the "Erdős-Rankin method" [4,11]). Then we select $\ell\equiv 2^{a_p} \pmod{p^2}$ for each $p\le 2y$, constructing $\ell \pmod{m^2}$ by the Chinese Remainder Theorem (rather like in Erdős's use of covering congruences [5] in the de Polignac problem). If we can do all this then we have proved our result; for if $1\le i\le r$ then $i\equiv a_p \pmod{\omega(p)}$ for some prime $p\le 2y$. But then $2^i\equiv 2^{a_p} \pmod{p^2}$ and so $n-2^i\equiv \ell-2^{a_p}\equiv 0 \pmod{p^2}$.

We shall partition the odd primes $\le 2y$ into the sequence of odd primes $p_1=3,\ p_2=5,\ldots,\ p_k\le y$ and the set Q of odd primes in the range $(y,2y]$. We select our a_p's in the style of the Erdős-Rankin method:

Let S_1 be the set of positive integers $\le r$. For $j=1,\ldots,k$, select $a_{p_j} \pmod{\omega(p_j)}$ so that $\#\{n\in S_j : n\equiv a_{p_j} \pmod{\omega(p_j)}\}$ is maximized and then let $S_{j+1}=S_j\setminus\{n\in S_j : n\equiv a_{p_j} \pmod{\omega(p_j)}\}$. Evidently $|S_{j+1}|\le |S_j|(1-\frac{1}{\omega(p_j)})$ so that

$$|S_{k+1}|\le r\cdot\prod_{j=1}^{k}\left(1-\frac{1}{\omega(p_j)}\right)\le\frac{\log N}{\log 2}\prod_{p\le y}\left(1-\frac{1}{\omega(p)}\right)$$

$$<\left(\frac{1}{2}-2\varepsilon\right)\frac{\log N}{2\log y}<(1-\varepsilon)\frac{y}{\log y}<|Q|$$

by hypothesis. We complete our construction by selecting, for each integer $a \in S_{k+1}$, a different prime $p_a \in Q$ and taking $a_{p_a} \equiv a \pmod{\omega(p_a)}$.

Remark. By a slight modification of the above proof one can prove an analogous result about representing n in any arithmetic progression of odd numbers (that is $n \equiv 2a+1 \pmod{2q}$ for any positive integers a, q).

The Proof of Proposition 2: Easy sieving

The proof of Proposition 2 is based on a simple sieving procedure. We develop this in a very general form, as it will be useful in proving Theorem 4 and other generalizations.

Proposition 3. *Suppose that for a given sequence of positive integers $\mathcal{A}$, there is an absolute constant $c > 0$ such that for any sufficiently large x, for every prime p there is a non-empty set of arithmetic progressions $M_p(x)$, each with modulus p^2, and an absolute constant $\delta_p > 0$, such that*

$$A(x; p^2, m) \le \delta_p A(x) + c \text{ for all } m \in M_p(x).$$

Let $N(x)$ be the set of all integers n in the interval $x < n \le 2x$ for which $n \in M_p(x)$ for every prime p; and assume that $|N(x)| \gg x$. If $\sum_p \delta_p < 1$, then almost all integers $n \in N(x)$ can be written in $\gg A(x)$ different ways as the sum of a squarefree number and some a_i in the sequence.

Proof. Consider $n \in N(x)$, and let $y := A(x)$. We shall try to write $n = m + a_i$ where $a_i \le x$ and m is squarefree. Then the number of integers $a_i \le x$ for which p^2 does not divide $n - a_i$ for any prime $p < y$, is $> y - \sum_{p<y}(\delta_p y + c)$, by the conditions on the sequence $\{a_i\}$ above. This amount is $> \left(1 - \sum_{p<y} \delta_p - O(1/\log y)\right) y \gg y$, by hypothesis.

On the other hand, the number of n in the range $x < n \le 2x$, for which $n - a_i$ is divisible by p^2 for some prime $p \ge y$, is, (noting that we must have $p^2 \le 2x$),

$$\le \sum_{y \le p \le 2x^{1/2}} \sum_{n \le 2x,\ p^2 | n - a_i} 1 \ll \sum_{y \le p \le 2x^{1/2}} x/p^2 \ll x/y \log y.$$

Thus there are $O(x/y \log y)$ integers n in the range $x < n \le 2x$, for which there are $\gg y$ values of $a_i \le x$ with $n - a_i$ divisible by the square of a prime $> y$. The result follows.

Deduction of Proposition 2. We choose our sequence to be the powers of 2; and take $N(x)$ to be all the odd numbers less than x. Thus, $\delta_2 = 0$ and $\delta_p = 1/\omega(p)$ for all odd primes p. Proposition 2 now follows from Proposition 3, and from its proof noting that $A(x) \asymp \log x$.

Corollary 1 follows from Proposition 3 by taking $\delta_p = 1/\max\{\omega_p(2), \omega_p(3)\}$, which will be $\le \log 2/p \log p$ under hypothesis, and by taking $N(x)$ to be all integers coprime to 6.

A variant, easily proved by modifying the argument in Proposition 3, is

Corollary 3. *Suppose that $\sum_p 1/\omega(p) < \infty$. Then almost all odd integers are the sum of a power of two and the product of a squarefree number and a bounded powerful number.*

Deduction of Theorem 4

Lemma 2. *Given $\mathcal{A}$ and squarefree integer ν, assume that for any prime p which does not divide ν, there are infinitely many integers in $\mathcal{A}$ which are not divisible by p. Then, for any given arithmetic progression $b \pmod d$ with $(d,\nu)=1$ there is a finite subset of elements of $\mathcal{A}$ whose sum is $\equiv b \pmod d$ and $\equiv 0 \pmod \nu$.*

Proof. Suppose p^α is the exact power of p which divides d. By the pigeonhole principle there exists a congruence class $\beta \pmod{\nu d}$, with $p \nmid \beta$, such that there is an infinite subsequence of integers in $\mathcal{A}$ which are all $\equiv \beta \pmod{\nu d}$. Let k_p be a positive integer $\equiv b/\beta \pmod{p^\alpha}$ and $\equiv 0 \pmod{\nu d/p^\alpha}$. The sum of the first k integers of our subsequence is $\equiv b \pmod{p^\alpha}$ and $\equiv 0 \pmod{\nu d/p^\alpha}$. We do this for each prime p dividing d, in turn, omitting from the sequence $\mathcal{A}$ those elements already used. The sum of all of these subsequences is thus $\equiv b \pmod d$ and $\equiv 0 \pmod \nu$, as required.

Proposition 4. *Suppose that we are given a sequence of positive integers $\mathcal{A}$ and squarefree integer ν. If prime p does not divide ν then assume there are infinitely many integers in $\mathcal{A}$ which are not divisible by p. For all primes p assume that $A(x;p^2,m) \le \delta_p A(x)$ for all m, if x is sufficiently large, for some absolute constant $\delta_p > 0$. If $\sum_p \delta_p < \infty$ then, for some integer $k \ge 1$ and all large x, almost all integers n, which are coprime to ν, can be written as the sum of a squarefree number plus at most k distinct elements from $\mathcal{A}$.*

Proof. Let x be sufficiently large and prime $q > \nu$ such that $\sum_{p>q} \delta_p < 1/2$. Let $d\nu$ be the product of the primes $\le q$. If $p > q$ then let M_p be all residue classes $\pmod{p^2}$; if $p \le q$ and $p \nmid \nu$ then let $M_p(x)$ be that residue class $m \pmod{p^2}$ for which $A(x;p^2,m)$ is minimal. For primes p dividing ν we select M_p to be all congruence classes $b \pmod{p^2}$ where p does not divide b.

By Proposition 3 (with δ_p as above for $p > q$, and equal to $1/p^2$ for $p \le q$) we find that there is an arithmetic progression $B \pmod d$, such that almost every integer $n \equiv B \pmod d$ with $(n,\nu)=1$ and $x < n \le 2x$ can be written in $\gg A(x)$ different ways as the sum of a squarefree number and some a_i in the sequence.

Now select any congruence class $b \bmod d$, and consider integers n in this congruence class which are coprime to ν and in the range $x < n \le 2x$. By Lemma 2 there is a finite subset of elements of $\mathcal{A}$ whose sum, s, is $\equiv b-B \pmod d$ and $\equiv 0 \pmod \nu$. Thus $n - s \equiv B \pmod d$ and is coprime to ν. Since s is absolutely bounded (as a function of the set $\mathcal{A}$), we may use the result in the paragraph above to deduce that almost all such $n-s$ may be written as the sum of a squarefree number and some a_i in the sequence. The result follows

Theorem 4 is an immediate corollary with $\nu = 2$ and $\delta_p = 1/\omega(p)$.

Unconditional results

As is well-known, there are $\sim 4x/\pi^2$ odd integers $n \le x$ such that $n-2$ is squarefree. Thus a positive proportion of odd integers can be written as the sum of a squarefree number and a power of 2. With a little work we can show that there are $c_r x/2$ odd integers $n \le x$ such that $n - 2^i$ is squarefree, for some i in the

range $1 \le i \le r$, where $c_r > 0$ is a computable constant. For examples, defining $d_k = \prod_{p \ge 3}(1 - k/p^2)$:

$$\begin{aligned}
c_1 &= d_1 = 8/\pi^2 = 0.810569\ldots\\
c_2 &= 2d_1 - d_2 = 0.975870\ldots\\
c_3 &= 3d_1 - 3d_2 + d_3 = 0.997851\ldots\\
c_4 &= 4d_1 - 6d_2 + 4d_3 - d_4 = 0.999860\ldots\\
c_5 &= 5d_1 - 10d_2 + 10d_3 - 5d_4 + d_5 = 0.999993\ldots\\
c_6 &= 6d_1 - 15d_2 + 20d_3 - 15d_4 + 6d_5 - d_6 = 0.999999\ldots.
\end{aligned}$$

In fact c_r will always be the sum of multiples of such Euler products, and those multiples are easily determined for a given r. However the multiples will not persist in being binomial coefficients, as above, since the order of 2 $(\mathrm{mod}\ p^2)$ will play a significant role for $r \ge 7$ (since then 3^2 can feasibly divide both $n-2$ and $n-2^7$). Thus we are unable to prove that $c_r \to 1$ as $r \to \infty$, for much the same reasons as those behind the proof of Theorem 5, although the numerical evidence above is striking. Of course if we could prove that $c_r \to 1$ as $r \to \infty$, this would allow us to deduce unconditionally that "almost all" odd integers may be written as a sum of a squarefree number and a power of 2.

Normal order

Proof of Theorem 3. First note that the condition $A(2x) \sim A(x)$ implies that $A(x) \sim A(x/2) \sim A(x/4) \sim \cdots \sim A(x/2^r)$ for any fixed r. Thus $\sum_{a_i \le x} a_i \le A(x/2^r)x/2^r + (A(x) - A(x/2^r))x \ll xA(x)/2^r$, and therefore $\sum_{a_i \le x} a_i = o(xA(x))$.

We have

$$\sum_{\substack{n \le x\\ n \equiv a \ (\mathrm{mod}\ q^2)}} r_{\mathcal{A}}(n) = \sum_{a_i \le x} \sum_{\substack{a_i < n \le x\\ n \equiv a \ (\mathrm{mod}\ q^2)}} \mu^2(n - a_i) = \sum_{a_i \le x} \sum_{\substack{m \le x - a_i\\ m \equiv a - a_i \ (\mathrm{mod}\ q^2)}} \mu^2(m).$$

Since p^2 does not divide $a_i - a$ for all i, and all primes p dividing q, and by using the combinatorial sieve, the sum over m above is $\sim c(x - a_i)/q^2 + O(1)$. Inserting this above, using the fact that $\sum_{a_i \le x} a_i = o(xA(x))$, gives that the average order of $r(n)$ with $n \le x,\ n \equiv a \ (\mathrm{mod}\ q^2)$, is $\sim cA(x)$.

Note that $r_{\mathcal{A}}(n) \le A(x)$, so that $|r_{\mathcal{A}}(n) - cA(x)| \le A(x)$. Therefore if $r_{\mathcal{A}}(n)$ is to have "normal order" then it must be $\sim cA(x)$. Moreover this is so if and only if the mean square of $|r_{\mathcal{A}}(n) - cA(x)|^2$ is $o(A(x)^2)$.

To compute the mean of the second moment of $r_{\mathcal{A}}(n)$ we proceed as above:

$$\sum_{\substack{n \le x\\ n \equiv a \ (\mathrm{mod}\ q^2)}} r_{\mathcal{A}}(n)^2 = \sum_{a_i, a_j \le x} \sum_{\substack{\max(a_i, a_j) < n \le x\\ n \equiv a \ (\mathrm{mod}\ q^2)}} \mu^2(n - a_i)\mu^2(n - a_j).$$

Again using the hypothesis and the combinatorial sieve, the inner sum over n is

$$\sim \left(\frac{x-\max(a_i,a_j)}{q^2}+O(1)\right)\prod_{p\nmid q}\left(1-\frac{2}{p^2}\right)\prod_{\substack{p^2\mid a_i-a_j\\ p\nmid q}}\frac{p^2-1}{p^2-2}$$
$$= \left(\frac{x-\max(a_i,a_j)}{q^2}+O(1)\right)\prod_{p\nmid q}\left(1-\frac{2}{p^2}\right)\sum_{\substack{a_i\equiv a_j \pmod{d^2}\\ (d,q)=1}} f(d),$$

where $f(d)=\mu^2(d)/\prod_{p\mid d}(p^2-2)$. Inserting this above, and using the fact that $\sum_{a_i\le x} a_i = o(xA(x))$, gives that the mean of the second moment of $r(n)$ is

$$\sim \prod_{p\nmid q}\left(1-\frac{2}{p^2}\right)\sum_{\substack{d=1\\ (d,q)=1}}^{\infty} f(d)\sum_{\substack{a_i,a_j\le x\\ a_i\equiv a_j \pmod{d^2}}} 1+o(A(x)^2).$$

Now

$$\sum_{\substack{a_i,a_j\le x\\ a_i\equiv a_j \pmod{d^2}}} 1 = \left(\frac{A(x)}{d}\right)^2+\sum_{l=1}^{d^2}\left(A(x;d^2,l)-\frac{A(x)}{d^2}\right)^2,$$

so that the mean of the second moment is

$$\sim (cA(x))^2+\prod_{p\nmid q}\left(1-\frac{2}{p^2}\right)\sum_{\substack{d=1\\ (d,q)=1}}^{\infty} f(d)\sum_{l=1}^{d^2}\left(A(x;d^2,l)-\frac{A(x)}{d^2}\right)^2.$$

Now, the contribution to the sum, for each d, is $\le f(d)A(x)^2$; and so the contribution of the terms with $d>D$ is $\ll \sum_{d>D} A(x)^2/d^2 \ll A(x)^2/D$. Therefore, taking D to be a large integer, we get

$$\frac{1}{x/q^2}\sum_{\substack{n\le x\\ n\equiv a \pmod{q^2}}}|r_{\mathcal{A}}(n)-cA(x)|^2 \asymp \sum_{\substack{d\le D\\ (d,q)=1}}\frac{\mu^2(d)}{d^2}\sum_{l=1}^{d^2}\left(A(x;d^2,l)-\frac{A(x)}{d^2}\right)^2 + O\left(\frac{A(x)^2}{D}\right).$$

Now if $A(x;d^2,l)\sim A(x)/d^2$ for each l and $(d,q)=1$, then the right hand side is $o(A(x)^2)$, letting $D\to\infty$. On the other hand if $A(x;d^2,l)\not\sim A(x)/d^2$ then this one term contributes $\gg A(x)^2$ to the right hand side. The theorem is thus proved.

Deducing Corollary 2. Let $\mathcal{A}$ to be the integers $a_k := 1^1+2^2+\ldots+k^k$ and let $q=2$. The results of [13] imply that the hypotheses of Theorem 3 are satisfied for $a=2$ or $a=3$, and that if d is odd then there are $\sim A(x)/d^2$ integers $a_i\le x$ with $a_i\equiv l \pmod{d^2}$, for every l. Corollary 2 follows in these cases noting that $A(x)\sim \log x/\log\log x$.

Every $a_{4k-1} \equiv a_{4k} \equiv 0 \pmod 4$ and $a_{4k+1} \equiv a_{4k+2} \equiv 1 \pmod 4$. Thus when considering $a = 0$ or 1, we restrict attention to $\mathcal{A}_{\text{odd}}$ or $\mathcal{A}_{\text{even}}$, respectively, the odd or even, elements of $\mathcal{A}$. Once again, the results of [13] imply that the hypotheses of Theorem 3 are satisfied, and that if d is odd then there are $\sim A(x)/d^2$ integers $a_i \le x$ with $a_i \equiv l \pmod{d^2}$, for every l. Corollary 2 follows in these cases now noting that $A(x) \sim \log x/2 \log\log x$.

Squarefree numbers plus powers of odd primes

Lagarias asks about analogous results with powers of 3 or larger primes. One needs to be a little careful here since the analogy to Conjecture 2, and thus the obvious analogy to Conjecture 1, are often false: For example, if $n \equiv 1 \pmod 4$ then $n-5^i$ is divisible by $4 = 2^2$ for every positive integer; in other words, $\omega_5(2) = 1$ so we get the "covering system" of congruences $0 \pmod{\omega_5(2)}$. Another, less trivial example, would be that if $n \equiv 17 \pmod{36}$ then $n - 71^i$ is divisible by 4 whenever i is odd, and $n - 71^i$ is divisible by 9 whenever i is even. Thus we need to avoid the integers n in those arithmetic progressions that arise from counterexamples to the analogy of Conjecture 2:

For given integer $q > 1$, define $\omega(p) = \omega_q(p)$ to be the order of $q \pmod{p^2}$ for each prime p that does not divide q. Let S_q be the set of finite lists of arithmetic progressions $\{a_i \pmod{\omega_q(p_i)}, i = 1, 2, \dots, m\}$ which form a "covering system", but for which no sublist forms a "covering system".

Define a set T_q of arithmetic progressions, as follows: First we include each $a \pmod q$ where $(a, q) > 1$. Next, for each list $\{a_i \pmod{\omega_q(p_i)}, i = 1, 2, \dots, m\}$ in S_q, let $B = \prod_{1 \le i \le m} p_i^2$ and take $A \equiv q^{a_i} \pmod{p_i^2}$ for each i; we then include $A \pmod B$ in T_q. Note that if $n \equiv A \pmod B$ then $n - q^j$ is never squarefree, because $j \equiv a_i \pmod{\omega_q(p_i)}$ for some i (since we have a covering system of congruences), and thus p_i^2 divides $n - q^j$.

Note that Conjecture 2 implies that $T_2 = \{0 \pmod 2\}$.

Conjecture 4. *Fix squarefree integer $q > 1$. Then S_q is finite so that T_q is also finite. Further, if n is a sufficiently large integer, which does not belong to any of the arithmetic progressions in T_q, then n can be written as the sum of a squarefree positive integer and a power of q.*

Note that if T_q is finite as conjectured, then the set of integers n, which can possibly be written as the sum of a squarefree integer and a power of q, can be partitioned into a finite set of arithmetic progressions. Restrict n to one of these "good" arithmetic progresions and argue as in Theorem 1 and Proposition 1. The main differences are that we now restrict the product in Proposition 1 to be only over primes coprime to the modulus of our arithmetic progression, and we replace the constant there by some sufficiently small constant, depending on q. In the deduction of the appropriate analogue of Theorem 1 we take our second product to be over those primes p for which q is a quadratic residue $\pmod p$. In this way, we obtain:

Theorem 7. *Fix squarefree integer $q > 1$, and suppose that Conjecture 4 is true. Then there are arbitrarily large values of x for which*

$$\#\{\text{primes } p \le x : q^{p-1} \not\equiv 1 \pmod{p^2}\} \ge c\#\{\text{primes } p \le x\},$$

where c is a positive constant.

In the other direction we might again ask how often integers n (in a good arithmetic progression) can be written as the sum of a squarefree number and a power of q. One can prove (using Proposition 3) conditional results analogous to Theorems 2 and 4. For these, we require, at the very least, the following conjecture:

Conjecture 5. *Fix squarefree integer $q > 1$. Let $\omega_q(p)$ be the order of $q \pmod{p^2}$ for each prime p that does not divide q. Then $\sum_{p \nmid q} 1/\omega_q(p)$ is bounded.*

References

1. R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp (to appear).
2. R. Crocker, *On a sum of a prime and two powers of two*, Pacific J. Math. **36** (1971), 103-107.
3. J.-M. Deshouillers, A. Granville, W. Narkiewicz and C. Pomerance, *An upper bound in Goldbach's problem*, Math. Comp. **617** (1993), 209-213.
4. P. Erdős, *On the difference of consecutive primes*, Quart. J. Pure & Appl. Math., Oxford **6** (1935), 124-128.
5. P. Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa. Brasil. Math **2** (1950), 113-123.
6. P. Erdős, *On some problems of Bellman and a theorem of Romanoff*, J. Chinese Math. Soc **1** (1951), 409-421.
7. P. Erdős, *On the sum $\sum_{d|2^n-1} d^{-1}$*, Israel J. Math **9** (1971), 43-48.
8. P.X. Gallagher, *Primes and powers of 2*, Invent. Math. **29** (1975), 125-142.
9. R.K. Guy, *Unsolved problems in number theory (2nd. ed.)*, Springer-Verlag, New York, 1994.
10. A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris Math **29** (1849), 397-401, 738-739.
11. R.A. Rankin, *The difference between consecutive prime numbers, V*, Proc. Edinburgh Math. Soc **13 (2)** (1962/63), 331-332.
12. N. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **57** (1934), 668-678.
13. K. Soundararajan, *Primes in a sparse sequence*, J. Number Theory **43** (1993), 220-227.
14. J.G. van der Corput, *On de Polignac's conjecture*, Simon Stevin **27** (1950), 99-105.
15. A. Wieferich, *Zum letzten Fermat'schen Satz*, J. Reine Angew. Math **136** (1909), 293-302.
16. A. Wiles, *Modular curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), 443-551.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu

Department of Mathematics, Princeton University, Princeton, New Jersey 08544, USA
E-mail address: skannan@math.princeton.edu