J. Aust. Math. Soc. **91** (2011), 405–413
doi:10.1017/S1446788712000043

A REMARK ON PRIMALITY TESTING AND DECIMAL EXPANSIONS

TERENCE TAO

(Received 22 February 2008; accepted 4 July 2008)

Communicated by I. E. Shparlinski

Abstract

We show that for any fixed base a, a positive proportion of primes become composite after any one of their digits in the base a expansion is altered; the case where $a = 2$ has already been established by Cohen and Selfridge ['Not every number is the sum or difference of two prime powers', *Math. Comput.* **29** (1975), 79–81] and Sun ['On integers not of the form $\pm p^a \pm q^b$', *Proc. Amer. Math. Soc.* **128** (2000), 997–1002], using some covering congruence ideas of Erdős. Our method is slightly different, using a partially covering set of congruences followed by an application of the Selberg sieve upper bound. As a consequence, it is not always possible to test whether a number is prime from its base a expansion without reading all of its digits. We also present some slight generalisations of these results.

2010 *Mathematics subject classification*: primary 35J10.

Keywords and phrases: primality testing, sieve theory, covering congruences.

1. Introduction

In 1950, Erdős [5] used the method of covering congruences to show that there exists an infinite arithmetic progression of odd integers m with the property that $|m - 2^i|$ is composite for every i. Modifying this method, Cohen and Selfridge [3] exhibited an arithmetic progression of odd integers m such that $|m - 2^i|$ and $m + 2^i$ are both composite for every i. In [20], Sun gave an explicit arithmetic progression with this property, namely $\{m : m = M \pmod{\prod_{p \in \mathcal{P}} p}\}$, where

$$M := 47\,867\,742\,232\,066\,880\,047\,611\,079$$

and $\mathcal{P}$ is the finite set of primes

$$\mathcal{P} := \{2, 3, 5, 7, 11, 13, 17, 19, 31, 37, 41, 61, 73, 97, 109, 151, 241, 257, 331\},$$

and noted that integers in this progression are in fact not of the form $\pm p^a \pm q^b$ for any primes p, q and positive integers a, b. Since M is coprime to $\prod_{p \in \mathcal{P}} p$, we can

The author is supported by NSF grant CCF-0649473 and a grant from the MacArthur Foundation.

apply the prime number theorem in arithmetic progressions (see, for instance, [13, Corollary 11.17]) to obtain the following immediate corollary.

COROLLARY 1.1 [3, 20]. *For all sufficiently large integers n, there exist at least $c2^n/n$ primes p between 2^{n-1} and 2^n such that the integers $p-2^i$ and $p+2^i$ are composite for every $i \in [0, n-1)$. Here c is a positive absolute constant.*

We remark that primes p of the above form are initially rather rare; the first few primes of this form are

$$1973, 3181, 3967, 4889, 8363, 8923, 11\,437, 12\,517, 14\,489, \ldots.$$

On the other hand, from Corollary 1.1 and the prime number theorem, we see that a positive proportion of the primes in fact lie on this sequence.

As an immediate corollary of Corollary 1.1, we see that for sufficiently large n, there exist n-bit integers p which are prime, but such that any number formed from p by switching one of the bits is not prime; the first few primes of this form are $127, 173, 191, 223, 233, \ldots$ (a slight variant of sequence A065092 in [19], which is the subsequence in which $p+2^{n+1}$ is also required to be composite). In other words, if we let $P_n : \{0,1\}^n \to \{0,1\}$ be the Boolean function which returns 1 if and only if the n-bit integer corresponding to the input in $\{0,1\}^n$ is prime, then the *sensitivity* $s(P_n)$ of P_n is equal to n for sufficiently large n. Recall that the sensitivity (or *critical complexity*) $s(B)$ of a Boolean function $B : \{0,1\}^n \to \{0,1\}$ is the largest integer s for which there exists an input $x \in \{0,1\}^n$ such that $B(x) \neq B(x')$ for at least s inputs x' which are formed from x by switching exactly one bit. We remark that the lower bound $s(P_n) \geq \frac{1}{4}n + O(1)$ was previously established in [18, p. 307].

If p is as above, then clearly it is not possible for an algorithm to determine with absolute certainty whether p is prime or not without inspecting all of the digits in the binary expansion. In particular, any deterministic primality tester can require computational time at least logarithmic in the size of the number being tested, if that number is represented in binary. For comparison, it was shown in [21, Theorem 6] that any recursive algorithm which can decide the primality of an n-bit integer using the operations $=, <, +, -, 2\cdot, \frac{1}{2}\cdot$, and parity, has time complexity at least $\frac{1}{4}n$. We remark that for bounded depth circuits, much stronger lower bounds (of exponential type in n) on the spatial complexity are known; see [1, 22].

In this note we establish a similar result for general bases.

THEOREM 1.2. *Let K be a positive integer. Then for all sufficiently large N, the number of primes p between N and $(1+1/K)N$ such that $|kp \pm ja^i|$ is composite for all integers $a, j, k \in [1, K]$ and $i \in [1, K \log N]$ is at least $c_K N/\log N$; here c_K is a positive constant depending only on K.*

From this theorem we see that the above results for binary expansions are also valid in other bases as well. For instance, applying this theorem with K equal to 10, we conclude that a positive proportion of the primes have the property that if one changes

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

any one of the digits in the base 10 expansion, one necessarily obtains a composite number, and so any deterministic primality tester receiving the digits of this number as input must read all of these digits in order to determine its primality. The first few such primes are 294 001, 505 447, 584 141, . . . (sequence A050249 from [19]). The infinitude of this sequence was established previously by Erdős [15].

Our argument does not use a fully covering set of congruences. Instead, we use congruences modulo primes arising from Mersenne-type numbers (in which bases such as a have an unexpectedly low order) to sieve out most of the quadruples (a, j, k, i) appearing in the above theorem, leaving behind a small number which can be handled via standard upper bound sieves. It might be difficult to establish this result without such a preliminary sieving step, since without such a sieving one would expect each $|kp \pm ja^i|$ to be prime with probability comparable to $1/\log N$, which makes it moderately unlikely (especially for large K) that the $|kp \pm ja^i|$ are composite for all $a, j, k \in [1, K]$ and $i \in [1, K \log N]$ for any given prime p.

2. Proof of Theorem 1.2

We now prove Theorem 1.2. Fix K. We will need a large integer $M = M(K) \geq K$ to be chosen later. We will then use this integer M to generate a finite set $\mathcal{P}$ of primes, as follows.

LEMMA 2.1. *For any $M, K \geq 1$, there exists a finite set $\mathcal{P}$ of primes which can be partitioned into disjoint sets: $\mathcal{P} = \bigcup_{2 \leq a \leq K} \mathcal{P}_a$, with the following properties.*

(1) *If $p \in \mathcal{P}_a$ for some $a \in [2, K]$, then there exists a prime q_p such that*

$$q_p \geq Mp \tag{2.1}$$

and

$$a^p = 1 \mod q_p.$$

Furthermore, the primes q_p for $p \in \mathcal{P}$ are all distinct.

(2) *For each $a \in [2, K]$,*

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p} \geq M. \tag{2.2}$$

PROOF. The claim is trivial when $K = 1$, so assume inductively that $K \geq 2$ and that the claim has already been proven for $K - 1$. Thus we already have disjoint finite sets of primes $\mathcal{P}_1, \dots, \mathcal{P}_{K-1}$ with the stated properties.

Let W denote the product of all the numbers less than K that are coprime to K, and let A denote the multiplicative order of $K \bmod W^K$. Observe that if p is a prime and $p = 1 \bmod A$, then $K^p - 1 = K - 1 \bmod W^K$. In particular, if q is a prime and $q < K$, then q can divide $K^p - 1$ at most K times (since $K - 1$ is not a multiple of q^K, being a smaller integer). As a consequence, we see that the largest prime factor of $K^p - 1$ is greater than K if p is larger than some sufficiently large constant C_K.

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

By the prime number theorem in arithmetic progressions (see, for instance, [13, Corollary 11.17]), the sum of reciprocals of primes p such that $p = 1 \bmod A$ is divergent. From this and Corollary A.3 we may find an infinite collection $\mathcal{P}'$ of primes p such that $p = 1 \bmod A$ and $p > C_K$, disjoint from the finite sets $\mathcal{P}_1, \ldots, \mathcal{P}_{K-1}$, such that $\sum_{p \in \mathcal{P}'} 1/p = \infty$, and such that $mp + 1$ is composite for every $m \in [1, M]$. For any p in $\mathcal{P}'$, we set q_p equal to the largest prime factor of $K^p - 1$. Now $p > C_K$, and so $q_p > K$. In particular, the multiplicative order of $K \bmod q_p$ is exactly p, which forces all the q_p to be distinct. In particular, we can find a finite subset $\mathcal{P}_K$ of $\mathcal{P}'$ such that $\sum_{p \in \mathcal{P}_K} 1/p \geq M$ and the values of q_p for $p \in \mathcal{P}_K$ are distinct from all the values of q_p already assigned to p in $\mathcal{P}_1, \ldots, \mathcal{P}_{K-1}$.

From Fermat's little theorem, we see that p divides $q_p - 1$ for all $p \in \mathcal{P}_K$. On the other hand, $mp + 1$ is composite for every $m \in [1, M]$. Thus $q_p \geq Mp$ as required. Hence $\mathcal{P} := \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_K$ has all the desired properties. □

Remark 2.2. In [6] it is shown that the largest prime factor of $2^p - 1$ is at least $cp \log p$ for some positive absolute constant c (see also [14] for additional refinements and further discussion). Slightly weaker results for more general bases may be found in [11]. By using these results one can avoid the use of Corollary A.3.

Henceforth we write $\mathcal{P} = \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_K$, and use the primes q_p where $p \in P$ as in the above lemma.

We let N be a sufficiently large integer parameter. We use the asymptotic notation $o(1)$ to denote any quantity that goes to zero as $N \to \infty$ (with K, M, and $\mathcal{P}$ fixed), and similarly $X \ll Y$ or $X = O(Y)$ to denote the estimate $X \leq CY$ for some C depending on K but independent of $N, M, \mathcal{P}$. We write $X \sim Y$ when $X \ll Y \ll X$.

By reducing the sets $\mathcal{P}_a$ if necessary, we may assume from (2.2) that

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p} \sim M.$$

Let S denote the finite set of pairs

$$S := \{(j, k) \in \mathbf{Z}^2 : -K \leq j \leq K; 1 \leq k \leq K; j \neq 0\}.$$

By (2.2) and a simple greedy argument, we may partition $\mathcal{P}_a$ as $\bigcup_{(j,k) \in S} \mathcal{P}_{a,j,k}$ in such a way that

$$\sum_{p \in \mathcal{P}_{a,j,k}} \frac{1}{p} \sim M \tag{2.3}$$

for all $a \in [2, K]$ and $(j, k) \in S$.

Define the quantity W by

$$W := \prod_{p \in \mathcal{P}} q_p.$$

By the Chinese remainder theorem, we can find b coprime to W such that $kb + j = 0 \bmod q_p$ for all $p \in \mathcal{P}_{a,j,k}$, where $2 \leq a \leq K$ and $(j, k) \in S$. (Note from (2.1) and the hypothesis that $M \geq K$ that all integers between 1 and K are coprime to W.)

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

To establish Theorem 1.2, it will suffice to show that the quantity X, given by

$$\begin{aligned} X = \#\{m \in [N, (1+1/K)N] : m = b \bmod W;\ m \text{ is prime, but} \\ |km + ja^i| \text{ is composite for all } i \in [0, K\log N),\ a \in [1, K] \text{ and } (j,k) \in S\}, \end{aligned}$$

satisfies $X \gg N/\log N$. Note that when $a = 1$, the value of i is irrelevant (and so can be set to zero, for instance). We can thus crudely bound X from below:

$$X \geq Q_N - \sum_{a\in[2,K]} \sum_{(j,k)\in S} \sum_{i\in[0,K\log N)} Q_{N,i,a,j,k} - \sum_{(j,k)\in S} Q_{N,0,1,j,k} - O(\log N) \tag{2.4}$$

where

$$Q_N := \#\{m \in [N, (1+1/K)N] : m = b \bmod W\}$$

and

$$Q_{N,i,a,j,k} := \#\{m \in [N, (1+1/K)N] : m = b \bmod W;\ m, |km \pm ja^i| \text{ both prime}\}.$$

(The $O(\log N)$ error arises from the small number of cases in which $|km + ja^i|$ is equal to zero or one.)

From the prime number theorem in arithmetic progressions (see, for instance, [13, Corollary 11.17]),

$$Q_N \gg \frac{N}{\phi(W)\log N}$$

where

$$\phi(W) = W \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{q_p}\right)$$

is the Euler totient function of W. (More precise asymptotics for Q_N are available, but we will not need them here.)

From Corollary A.2,

$$Q_{N,i,a,j,k} \ll \frac{N}{W\log^2 N} \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{q_p}\right)^{-2} \tag{2.5}$$

whenever $a \in [1, K]$, $i \in [0, K\log N]$ and $(j,k) \in S$. Applying this to dispose of the terms $Q_{N,0,1,j,k}$ in (2.4), we conclude that

$$X \gg \frac{N}{W\log N} \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{q_p}\right)^{-1} - O\left(\sum_{a=2}^{K} \sum_{(j,k)\in S} \sum_{0\leq i<K\log N} Q_{N,i,a,j,k}\right) \tag{2.6}$$

when N is sufficiently large.

Now suppose that $a \in [2, K]$ and $(j,k) \in S$. Observe that if $i = 0 \bmod p$ for any $p \in \mathcal{P}_{a,j,k}$, then $|km + ja^i|$ is divisible by q_p, and thus is prime for at most one value of m. Thus (paying a negligible factor of $O(\log N)$) we may restrict attention to those $i \in [0, n-1)$ such that $i \neq 0 \bmod p$ for all $p \in \mathcal{P}_{a,j,k}$. By the Chinese

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

remainder theorem, the number of such i is $O(\log N \prod_{p \in \mathcal{P}_{a,j,k}}(1 - 1/p))$. Using the approximations

$$\prod_{n \in A}\Big(1 - \frac{1}{n}\Big) \sim \exp\Big(-\sum_{n \in A}\frac{1}{n}\Big),$$

which are valid for any finite set A since $\sum_{n \in A} 1/n^2 = O(1)$, we conclude from the above discussion and (2.5) that

$$\sum_{0 \le i < K \log N} Q_{N,i,a,j,k} \ll \frac{N}{W \log^2 N}\prod_{p \in \mathcal{P}}\Big(1 - \frac{1}{q_p}\Big)^{-1} \exp\Big(\sum_{p \in \mathcal{P}}\frac{1}{q_p} - \sum_{p \in \mathcal{P}_{a,j,k}}\frac{1}{p}\Big).$$

But from (2.1) and (2.2), $\sum_{p \in \mathcal{P}} 1/q_p = O(1)$, while from (2.3), $\sum_{p \in \mathcal{P}_{a,j,k}} 1/p \gg M$. Inserting all these bounds into (2.6), we conclude that

$$X \gg \frac{N}{W \log N}(1 - O(\exp(-cM)))\prod_{p \in \mathcal{P}}\Big(1 - \frac{1}{q_p}\Big)^{-1}$$

where c depends on K but not on M. Taking M sufficiently large (depending on K), we obtain the claim.

3. Remarks

An inspection of the proof of Theorem 1.2 allows us to establish a strengthened version in which the numbers $|kp \pm ja^i|$ not only are composite, but also contain at least two distinct prime factors greater than K. More precisely, the cases in which $|kp \pm ja^i|$ is the product of a prime power q^b and some primes less than or equal to K can be disposed of by suitable variants of Corollary A.2 (and in the case where $b \ge 2$, the total contribution here is $O(\sqrt{N})$ which is easily discarded); we omit the details. Recently in [16], it was shown that one can in fact ensure that the numbers $kp \pm ja^i$ contain at least $C(\log\log N)^{1/3-\varepsilon}$ prime factors each for any fixed ε.

In a somewhat different direction, it should also be possible to strengthen the conclusion of Theorem 1.2 to assert that $|kp \pm ja^i + l|$ is composite for all l in some set $L = L_N \subset \{-KN, \ldots, KN\}$ of cardinality at most K. A new difficulty arises here due to an additional factor of $\prod_{p | \pm ja^i + l; p \nmid W}(1 - 1/p)^{-1}$ arising from the use of Corollary A.2, but it seems likely that this quantity should be bounded for the overwhelming majority of values of a, i, j, l, which should allow one to continue the argument; we will not pursue this matter here. If one is able to carry out this generalisation, one should be able to obtain the conclusion that for any base $a \ge 2$ and any $r \ge 1$, a positive proportion of the primes p have the property that if one modifies any single one of its digits in the base a expansion, *and* appends or deletes up to r digits to/from the end and/or beginning of the digit string, one necessarily obtains a composite number.

In a similar spirit, it was recently established in [7] that there exist infinitely many composite numbers which remain composite after inserting a single digit in their base 10 expansion. It seems likely that one should now also be able to find infinitely many prime numbers with the same property (that is, they become composite after inserting any digit at any place).

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

In all of the above results, the total number of possible modifications of the digit string remains comparable to $\log p$ and so the cases in which a number is unexpectedly prime can be handled by the upper bound sieve after performing the preliminary sieving to eliminate most of the cases. The problem becomes significantly more difficult, however, if one asks that the number p become composite after allowing one to modify any *two* of the digits in the digit string, as the number of possible modifications is now comparable to $\log^2 p$. Indeed, standard heuristics from the prime tuples conjecture [8] now lead one to predict that for a sufficiently large base, there should only be finitely many numbers of this form, although there is a slim chance (especially in small bases) that Mersenne-type primes provide enough congruences to fully cover all the modifications for primes in a certain infinite arithmetic progression, as was the case with Theorem 1.1. We remark that in [23] it was shown that there are infinitely many integers n such that $n - 2^a - 2^b$ is not a prime power for any a, b (an earlier result in [4] establishes the weaker statement with 'prime power' replaced by 'prime'). The base 2 was generalised to other bases recently in [2], and lower bounds on the density of such integers were obtained in [2, 17] (the latter result using the methods in this paper).

Using the circle method and bounds on prime exponential sums, there are several further results known relating primes to binary digits, or to powers of 2. For instance, in [9] the distribution of a bounded number of fixed digits of a large prime was studied. In [12] it was shown that the binary digit sum of a large prime was equally likely to be even as it was to be odd. In a slightly different direction, it was shown in [10] that all sufficiently large even numbers are the sum of two primes, together with at most 13 powers of 2.

Acknowledgements

The author is indebted to Yiannis Moschovakis for suggesting this question, and to Jens Kruse Andersen, Yong-Gao Chen, Bjorn Poonen, Florian Luca, Paul Pollack, Igor Shparlinski, Zhi-Wei Sun, and several anonymous commenters on my blog for helpful comments and references.

Appendix A. Some sieve theory

We recall a standard application of the Selberg sieve to twin prime type problems.

THEOREM A.1 (Selberg sieve upper bound). *Suppose that $y \geq 4$, and let $P := \prod_{p<\sqrt{y}} p$. Let $\mathcal{B}(p)$ be the union of $b(p)$ arithmetic progressions with common difference p, and put $\mathcal{B} := \bigcup_{p|P} \mathcal{B}(p)$. If $b(2) \leq 1$ and $b(p) \leq 2$ for $p > 2$, then the number of integers r in $[0, y]$ such that $r \notin \mathcal{B}$ is bounded by*

$$C \frac{y}{\log^2 y} \prod_{p|P} \Big(1 - \frac{b(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-2},$$

for some absolute constant C.

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

PROOF. See [13, Theorem 3.13]. As shown there, one may replace the constant C with $8 + O((\log\log y)/(\log y))$, but we will not need this improvement here. □

COROLLARY A.2. *Let x, W, b be positive integers with W even, and let h, k be nonzero integers. Then if x is sufficiently large ('sufficiently large' depends on W, b),*

$$\begin{aligned}&\#\{m \in [1, x] : m = b \bmod W;\ m, |km + h| \text{ both prime}\}\\ &\quad \ll \frac{x}{W\log^2 x}\bigg(\prod_{p|W}\Big(1-\frac{1}{p}\Big)^{-2}\bigg)\bigg(\prod_{p|h;p\nmid W}\Big(1-\frac{1}{p}\Big)^{-1}\bigg)\end{aligned}$$

where the implied constant can depend on k.

PROOF. By reversing the signs of k and h if necessary, and increasing the size of the implied constant by a factor of 2 if necessary, we may replace $|km + h|$ by $km + h$. We may assume that b and $kb + h$ are both coprime to W, otherwise the number of m for which $km, km + h$ are both prime is bounded uniformly in x and the claim is trivial. For similar reasons we may assume that k and h are coprime. Write $m = Wr + b$ and $y = x/W$, thus $0 \le r \le y$. We can restrict attention to the case where $r > \sqrt{y}$, since the case where $r \le \sqrt{y}$ only contributes $O(\sqrt{y})$ elements, which is acceptable. If p is a prime and $p \le \sqrt{y}$, then the constraints that m and $m + h$ both be prime force $Wr + b$ and $kWr + kb + h$ to both be coprime to p. If $p \mid W$, then this condition is vacuous; if $p \mid h$, $p \nmid W$, and $p \nmid k$, then this excludes one residue class modulo p from the space of possible r; and if $p \nmid h$, $p \nmid W$ and $p \nmid k$ then this excludes two residue classes modulo p from the space of possible r. Finally, if $p \nmid W$ and $p \mid k$ then either one or two residue classes modulo p are excluded. The claim now follows from Theorem A.1 (note that $\log x \sim \log y$ for x large enough, and that $\prod_p (1 - 2/p)(1 - 1/p)^{-2} \sim 1$). □

COROLLARY A.3 (Brun's theorem). *Let m, j be any positive integers. Then the sum of the reciprocals of the primes p for which $mp + j$ is also prime is convergent.*

PROOF. By Corollary A.2, the number of primes of the above form which are less than x is $O(x/(\log^2 x))$ (where the implied constant can depend on m). The claim easily follows. □

References

[1] E. Allender, M. Saks and I. E. Shparlinski, 'A lower bound for primality', *J. Comput. System Sci.* **62** (2001), 356–366.

[2] Y.-G. Chen, R. Feng and N. Templier, 'Fermat numbers and integers of the form $a^k + a^l + p^\alpha$', *Acta Arith.* **135** (2008), 51–61.

[3] F. Cohen and J. L. Selfridge, 'Not every number is the sum or difference of two prime powers', *Math. Comput.* **29** (1975), 79–81.

[4] R. Crocker, 'On the sum of a prime and two powers of two', *Pacific J. Math.* **36** (1971), 103–107.

[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 and T. N. Shorey, 'On the greatest prime factor of $2^p - 1$ for a prime p and other expressions', *Acta Arithm.* **30** (1976), 257–265.

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press

[7] M. Fileseta, M. Kozek, C. Nicol and J. Selfridge, ‘Composites that remain composite after changing a digit’, *J. Comb. Number Theory* **2** (2010), 25–36.

[8] G. H. Hardy and J. E. Littlewood, ‘Some problems of “partitio numerorum” III: On the expression of a number as a sum of primes’, *Acta Math.* **44** (1923), 1–70.

[9] G. Harman, ‘Primes with preassigned digits’, *Acta Arith.* **125** (2006), 179–185.

[10] D. R. Heath-Brown and J.-C. Puchta, ‘Integers represented as a sum of primes and powers of two’, *Asian J. Math.* **6** (2002), 535–565.

[11] Z. Łuszczki, ‘On the prime factors of $\prod_{n=1}^{x}(a^{\tau_n}+1)$’, *Funct. Approx. Comment. Math.* **2** (1976), 115–120.

[12] C. Mauduit and J. Rivat, ‘Sur un problème de Gelfond: la somme de chiffres des nombres premiers’, *Ann. of Math.* (2) **171** (2010), 1591–1646.

[13] H. Montgomery and R. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Studies in Advanced Mathematics, 97 (Cambridge University Press, Cambridge, 2007).

[14] L. Murata and C. Pomerance, ‘On the largest prime factor of a Mersenne number’, in: *Number Theory*, CRM Proceedings Lecture Notes, 36 (American Mathematical Society, Providence, RI, 2004), pp. 209–218.

[15] P. Orno *et al.*, ‘Problems’, *Math. Mag.* **52** (1979), 179–184.

[16] H. Pan, ‘On the number of distinct prime factors of $nj + a^h k$’, arXiv:0907.1940.

[17] H. Pan, ‘On the integers not of the form $p + 2^a + 2^b$’, *Acta Arith.* **148** (2011), 55–61.

[18] I. Shparlinski, *Cryptographic Applications of Analytic Number Theory* (Birkhaüser, Basel, 2003).

[19] N. J. A. Sloane, ‘The On-Line Encyclopedia of Integer Sequences’, published electronically at www.research.att.com/~njas/sequences/, 2007.

[20] Z. W. Sun, ‘On integers not of the form $\pm p^a \pm q^b$’, *Proc. Amer. Math. Soc.* **128** (2000), 997–1002.

[21] L. van der Dries and Y. Moschovakis, ‘Is the Euclidean algorithm optimal among its peers?’, *Bull. Symbolic Logic* **10** (2004), 390–418.

[22] A. Woods, ‘Subset sum “cubes” and the complexity of prime testing’, *Theor. Comp. Sci.* **322** (2004), 203–219.

[23] P. Yuan, ‘Integers not of the form $c(2^a + 2^b) + p^\alpha$’, *Acta Arith.* **115** (2004), 23–28.

TERENCE TAO, Department of Mathematics, UCLA, Los Angeles,
CA 90095-1555, USA
e-mail: tao@math.ucla.edu

https://doi.org/10.1017/S1446788712000043 Published online by Cambridge University Press