New York Journal of Mathematics

New York J. Math. **17** (2011) 553–567.

Remarks on a paper of Ballot and Luca concerning prime divisors of $a^{f(n)} - 1$

Paul Pollack

Abstract. Let a be an integer with $|a| > 1$. Let $f(T) \in \mathbf{Q}[T]$ be a nonconstant, integer-valued polynomial with positive leading term, and suppose that there are infinitely many primes p for which f does not possess a root modulo p. Under these hypotheses, Ballot and Luca showed that almost all primes p do not divide any number of the form $a^{f(n)}-1$. More precisely, assuming the Generalized Riemann Hypothesis (GRH), their argument gives that the number of primes $p \le x$ which do divide numbers of the form $a^{f(n)} - 1$ is at most (as $x \to \infty$)

$$\frac{\pi(x)}{(\log\log x)^{r_f+o(1)}},$$

where r_f is the density of primes p for which the congruence $f(n) \equiv 0 \pmod{p}$ is insoluble. Under GRH, we improve this upper bound to $\ll x(\log x)^{-1-r_f}$, which we believe is the correct order of magnitude.

Contents

1. Introduction

Fix an integer a with $|a| > 1$. From Fermat's little theorem, we know that the set of primes which divide $a^n - 1$ for some n is precisely the set of primes not dividing a. Luca and Ballot [1] investigated what happens if we replace the exponent n here by a different polynomial expression in n: fix a

Received August 6, 2011.
2010 *Mathematics Subject Classification.* Primary: 11N37, Secondary: 11B83.
Key words and phrases. Prime factors, Chebotarev density theorem, orders modulo p.

ISSN 1076-9803/2011

nonconstant, integer-valued polynomial $f(T) \in \mathbf{Q}[T]$ with positive leading coefficient. Define

$$(1) \qquad \mathscr{P} := \{q : q \text{ prime}, f(n) \equiv 0 \pmod{q} \text{ has no solution}\}.$$

By the Chebotarev density theorem (see, e.g., [16]), the set $\mathscr{P}$ has a Dirichlet density; call this r_f. The following is the main result of [1]; we write GRH for the *Generalized Riemann Hypothesis*, which for us is the assertion that the nontrivial zeros of all Dedekind zeta functions lie on the line $\Re(s) = \frac{1}{2}$.

Theorem A. *Assume that f is irreducible of degree > 1. Then the number of primes $p \leq x$ which divide some number of the form $a^{f(n)} - 1$, where $n \in \mathbf{N}$, is at most*

$$\frac{\pi(x)}{(\log\log\log x)^{r_f + o(1)}},$$

as $x \to \infty$. Assuming GRH, the upper bound can be improved to

$$\frac{\pi(x)}{(\log\log x)^{r_f + o(1)}}.$$

A careful reading of the proof of Theorem A reveals that the stated estimates hold for all f, and that irreducibility is used only to guarantee that $r_f > 0$; see [1, Lemma 3]. (Of course, the estimates are trivial if $r_f = 0$.) By the density theorems in [16], one has $r_f > 0$ exactly when $\mathscr{P}$ is infinite. So as long as infinitely many primes do not divide values of $f(n)$, almost all primes (all but $o(\pi(x))$ of those in $[2, x]$, as $x \to \infty$) do not divide any expression of the form $a^{f(n)} - 1$. Moreover, replacing the use of inclusion-exclusion in the argument of [1] with a more powerful sieve, one quickly obtains an unconditional proof of the upper bound claimed under GRH. In fact, one gets an upper bound that is $\ll_a \pi(x)/(\log\log x)^{r_f}$; notice that we have removed the $o(1)$ in the exponent. See Remark 8 at the end of §2.

By a different method, we shall improve the conditional upper bound substantially:

Theorem 1. *Assume GRH. Let a be an integer with $|a| > 1$. Suppose that the set $\mathscr{P}$ defined in (1) is infinite, with Dirichlet density $r_f > 0$. For $x \geq 2$, the number of $p \leq x$ dividing some $a^{f(n)} - 1$ is $\ll_{a,f} x/(\log x)^{1+r_f}$.*

Remark. For later use, it will be helpful to observe that by the Chebotarev density theorem, f splits into linear factors modulo p for a set of primes p of positive density. Thus, $r_f < 1$ always.

Theorem 1 leaves open the question of what happens when $\mathscr{P}$ is finite. This turns out to be much simpler; indeed, we can establish an asymptotic formula.

Theorem 2. *If $\mathscr{P}$ is finite, then the set of primes dividing some $a^{f(n)} - 1$ possesses a positive relative density. In other words, the number of such $p \leq x$ is $\sim c_{a,f}\pi(x)$, as $x \to \infty$, for some constant $c_{a,f} > 0$.*

We prove Theorem 2 in §4. There we also give a formula for $c_{a,f}$ when $a > 0$, using explicit results of Wiertelak [19] (cf. Pappalardi [13], Moree [10]) concerning how often a given integer d divides the order of a mod p.

It seems difficult to prove a corresponding asymptotic formula in the case when $\mathscr{P}$ is infinite. On the basis of our work in §4, we propose such a formula in §5 (again, assuming $a > 0$). One consequence of this formula is that the primes p dividing some $a^{f(n)} - 1$ should have counting function asymptotic to a constant multiple of $x/(\log x)^{1+r_f}$. In §6, we conclude the paper with a discussion of the difficulties associated with proving a lower bound of the expected order of magnitude.

Notation. The unitalicized letter e denotes the base of the natural logarithm. We write ζ_m for the primitive mth root of unity $\mathrm{e}^{2\pi i/m}$. The letters p and q are reserved for primes. We use Erdős's notation $\ell_a(m)$ for the order of a modulo m; if a is understood, we often omit the subscript. We write $\omega(n) := \sum_{p|n} 1$ for the number of distinct prime factors of n. The notation $d \parallel n$ means that d is a *unitary* divisor of n, i.e., $d \mid n$ and $\gcd(d, n/d) = 1$. We employ the Landau–Bachmann O and o symbols, as well as Vinogradov's $\ll$ notation, with subscripts indicating any dependence of implied constants. We use Li for the usual *logarithmic integral*, so that $\mathrm{Li}(x) := \int_2^x dt/\log t$.

2. Sieving the numbers $\ell(p)$

Fix an integer a with $|a| > 1$. In this section, we prove an upper bound on the proportion of the time that $\ell(p)$ has a prime factor belonging to a prescribed set $\mathscr{Q}$. It seems that this result may be of some independent interest.

Theorem 3. *Assume GRH. Let $x \geq 2$, and let $\mathscr{Q}$ be a set of primes contained in $[2, x]$. The number of primes $p \leq x$ for which $\ell(p)$ is not divisible by any $q \in \mathscr{Q}$ is*

$$\ll_a \pi(x) \prod_{q \in \mathscr{Q}} (1 - 1/q), \tag{2}$$

uniformly in $\mathscr{Q}$ and x.

Remarks 4.

(i) As we will see in Theorem C below, apart from $O_a(1)$ exceptional primes q, the probability that q divides $\ell(p)$ is $q/(q^2 - 1)$. So from a psychological standpoint, it would appear more natural if the factors on the right-hand side of (2) were $1 - q/(q^2 - 1)$. However, replacing each term $1 - 1/q$ with the more cumbersome factor $1 - q/(q^2 - 1)$ would not change the magnitude of the right-hand side, and so would not affect the result. We have chosen to allow typography to trump psychology.

(ii) From Theorem 3, it is simple to deduce a (GRH-conditional) theorem of Murata and Pomerance [12, Theorem 4]: for $x \geq 2$, the number of odd primes $p \leq x$ for which $\ell_2(p)$ is prime is $\ll x/(\log x)^2$. (Briefly, take $\mathscr{Q}$ to be the set of primes $\leq x^{1/3}$, say, and recall that there are $o(x/(\log x)^2)$ primes $p \leq x$ with $\ell_2(p) \leq x^{1/3}$.) Our proof is similar in spirit to theirs.

Our argument rests on Lagarias and Odlyzko's explicit Chebotarev density theorem (on GRH) [8], as formulated by Serre [15, §2.4]:

Theorem B. *Assume GRH. Let K be a finite Galois extension of $\mathbf{Q}$ with Galois group G, and let C be a conjugacy class of G. The number of unramified primes $p \leq x$ whose Frobenius conjugacy class $(p, K/\mathbf{Q}) = C$ is given by*

$$\frac{\#C}{\#G}\mathrm{Li}(x) + O\left(\frac{\#C}{\#G}x^{1/2}(\log|\Delta_K| + [K:\mathbf{Q}]\log x)\right),$$

for all $x \geq 2$. Here Δ_K denotes the discriminant of K and the O-constant is absolute.

We also need an estimate extracted from Hooley's GRH-conditional proof of Artin's primitive root conjecture [5].

Lemma 5. *Assume GRH. Let $x \geq 2$. There are $\ll_a x/(\log x)^2$ primes $p \leq x$ which have the following property: For some prime $q \in (\log x, x^{1/2}(\log x)^{-2}]$,*

$$q \mid p-1 \quad \textit{and} \quad a^{\frac{p-1}{q}} \equiv 1 \pmod{p}.$$

Remark 6. Hooley's aim is to prove Artin's conjecture, and so he assumes from the start that a is not a perfect square. But Lemma 5 is valid without that restriction. It is enough that the number of $p \leq x$ which split completely in $K := \mathbf{Q}(\zeta_q, a^{1/q})$ is $\frac{\mathrm{Li}(x)}{[K:\mathbf{Q}]} + O_a(x^{1/2}\log(qx))$ and that $[K:\mathbf{Q}] \gg_a q\phi(q)$. This much holds without assuming that a is not a square (cf. the argument for Theorem 3 below).

Finally, we need a known estimate on the distribution of smooth numbers. Recall that a natural number n is said to be *y-smooth* if every prime divisor p of n satisfies $p \leq y$. We let $\Psi(x, y)$ denote the number of y-smooth natural numbers $n \leq x$.

Lemma 7. *Fix a real number $A \geq 1$. Then $\Psi(x, (\log x)^A) = x^{1-\frac{1}{A}+o(1)}$, as $x \to \infty$.*

For a proof of Lemma 7, see, e.g., [3, p. 291].

Proof of Theorem 3. There is no loss in assuming $\mathscr{Q} \subset [2, x^{1/2}(\log x)^{-2}]$, since $\prod_{x^{1/2}(\log x)^{-2} < q \leq x}(1 - 1/q) \asymp 1$. Let $p \leq x$ be a prime for which $\ell(p)$ is coprime to the members of $\mathscr{Q}$. The right-hand side of (2) is always $\gg x/(\log x)^2$, and so we can assume that p is not in the exceptional set considered in Lemma 5. Thus, if $q \in \mathscr{Q}$ is a divisor of $p-1$ with $q > \log x$, then $a^{(p-1)/q} \not\equiv 1 \pmod{p}$. Let M be the largest divisor of $p-1$ supported on primes belonging to $\mathscr{Q}$. Since $\ell(p)$ is coprime to the members of $\mathscr{Q}$, we must have $a^{(p-1)/M} \equiv 1 \pmod{p}$. It follows that M is supported entirely on primes not exceeding $\log x$.

We may assume that M does not exceed $\exp(\sqrt{\log x})$. Indeed, the total number of integers in $[1,x]$ divisible by some $(\log x)$-smooth integer $M > \exp(\sqrt{\log x})$ is at most

$$(3) \qquad \sum_{\substack{\exp(\sqrt{\log x})<M\leq x\\ p\mid M\Rightarrow p\leq \log x}} \left\lfloor \frac{x}{M}\right\rfloor \leq x\int_{\exp(\sqrt{\log x})}^{x} \frac{d\Psi(t,\log x)}{t}.$$

When $t \geq \exp(\sqrt{\log x})$, we have $\log x \leq (\log t)^2$, and so $\Psi(t,\log x) \ll t^{2/3}$, say, by taking $A=2$ in Lemma 7. Hence, the right-hand side of (3) is $\ll x/\exp(\frac{1}{3}\sqrt{\log x})$. This is negligible in comparison with the upper bound in the theorem statement.

We now fix a $(\log x)$-smooth integer $M \leq \exp(\sqrt{\log x})$ and use Selberg's Λ^2-sieve to count the number of corresponding $p \leq x$. Let

$$\begin{aligned} \mathscr{A} &:= \left\{p-1 : p\leq x, M \,\middle|\, p-1, a^{\frac{p-1}{M}} \equiv 1 \pmod{p}\right\},\\ \mathscr{Q}' &:= \{q\in\mathscr{Q} : q\nmid aM\}. \end{aligned}$$

Then the number of $p \leq x$ corresponding to M is bounded above by

$$S(\mathscr{A},\mathscr{Q}') := \#\left\{A\in\mathscr{A} : \gcd\left(A, \prod_{q\in\mathscr{Q}'} q\right) = 1\right\}.$$

We turn next to the preliminary estimates needed to apply the sieve.

Let $p \leq x$ be a prime not dividing $2a$. From a well-known theorem of Kummer–Dedekind, $p-1\in\mathscr{A}$ precisely when p splits completely in $K_1 := \mathbf{Q}(\zeta_M, a^{1/M})$. From [18, Proposition 4.1], we have $[K_1:\mathbf{Q}] \asymp_a M\phi(M)$. Since the discriminant of $\mathbf{Q}(\zeta_M)$ divides $M^{\phi(M)}$ and the discriminant of $\mathbf{Q}(a^{1/M})$ divides $(aM)^M$, we obtain from the relation

$$\Delta_{K_1} \mid \Delta_{\mathbf{Q}(a^{1/M})}^{[K_1:\mathbf{Q}(a^{1/M})]}\Delta_{\mathbf{Q}(\zeta_M)}^{[K_1:\mathbf{Q}(\zeta_M)]}$$

(cf. [14, p. 218, Proof of 7Q]) that

$$\begin{aligned} \log|\Delta_{K_1}| &\leq M\phi(M)\log(|a|M) + M\phi(M)\log M\\ &\ll_a M\phi(M)\log(\mathrm{e}M). \end{aligned}$$

So setting $X := \frac{\mathrm{Li}(x)}{[K_1:\mathbf{Q}]}$, Theorem B yields

$$\#\mathscr{A} := X + O_a(x^{1/2}\log(Mx)) = X + O_a(x^{1/2}\log x).$$

Next, let d be a squarefree natural number supported on primes belonging to $\mathscr{Q}'$. Set $\mathscr{A}_d := \{A\in\mathscr{A} : d\mid A\}$. If $p\leq x$ is a prime not dividing $2a$, then $p-1\in\mathscr{A}_d$ precisely when p splits completely in $K_2 := \mathbf{Q}(\zeta_{dM}, a^{1/M})$. View K_2 as the compositum of K_1 and $L := \mathbf{Q}(\zeta_d)$. The discriminant of L

divides $d^{\phi(d)}$, while the discriminant of K_1 is supported on primes dividing aM. Hence, $\gcd(\Delta_L, \Delta_{K_1}) = 1$. We deduce that

$$[K_2 : \mathbf{Q}] = [L : \mathbf{Q}][K_1 : \mathbf{Q}] = \phi(d)[K_1 : \mathbf{Q}]$$

and

$$\Delta_{K_2} = \Delta_{K_1}^{[L:\mathbf{Q}]} \Delta_L^{[K_1:\mathbf{Q}]},$$

so that

$$\begin{aligned} \log|\Delta_{K_2}| &\ll_a \phi(d)\log|\Delta_{K_1}| + M\phi(M)\log|\Delta_L| \\ &\ll_a \phi(d)M\phi(M)\log(\mathrm{e}M) + (M\phi(M))(\phi(d)\log d) \\ &\ll M\phi(dM)\log(\mathrm{e}dM). \end{aligned}$$

Applying Theorem B again, we find that

$$\begin{aligned} \#\mathscr{A}_d &= \frac{\mathrm{Li}(x)}{\phi(d)[K_1 : \mathbf{Q}]} + O_a\left(x^{1/2}\log x + x^{1/2}\log(\mathrm{e}dM)\right) \\ &= \frac{X}{\phi(d)} + O_a(x^{1/2}\log x), \end{aligned}$$

assuming $d \le x$ (say).

Selberg's upper bound sieve, in the form of [4, p. 133, Theorem 4.1], now yields that for $z := x^{1/5}$,

$$S(\mathscr{A}, \mathscr{Q}') \ll_a X \prod_{q \in \mathscr{Q}' \cap [2,z]} \left(1 - \frac{1}{\phi(q)}\right) + x^{1/2}\log x \sum_{\substack{d \le z^2 \\ p \mid d \Rightarrow p \in \mathscr{Q}' \\ d \text{ squarefree}}} 3^{\omega(d)}. \tag{4}$$

Using the universal upper bound $\omega(d) \ll \log d/\log\log(3d)$ and recalling the restriction $d \le z^2$, we see that $3^{\omega(d)} \ll x^{1/25}$, say. So the second term on the right-hand side of (4) is $\ll x^{0.95}$. Also,

$$\begin{aligned} X \prod_{q \in \mathscr{Q}' \cap [2,z]} \left(1 - \frac{1}{\phi(q)}\right) &\ll_a \frac{\mathrm{Li}(x)}{M\phi(M)} \prod_{q \in \mathscr{Q}'} \left(1 - \frac{1}{q}\right) \\ &= \frac{\mathrm{Li}(x)}{\phi(M)^2} \prod_{q \mid M} \left(1 - \frac{1}{q}\right) \prod_{q \in \mathscr{Q}'} \left(1 - \frac{1}{q}\right) \\ &\ll_a \frac{\pi(x)}{\phi(M)^2} \prod_{q \in \mathscr{Q}} \left(1 - \frac{1}{q}\right). \end{aligned}$$

Hence, the number of $p \le x$ corresponding to M is

$$\ll_a \frac{\pi(x)}{\phi(M)^2} \prod_{q \in \mathscr{Q}} \left(1 - \frac{1}{q}\right) + x^{0.95}.$$

Now sum over all $(\log x)$-smooth values of $M \le \exp(\sqrt{\log x})$. Since the infinite series $\sum_{M \ge 1} \frac{1}{\phi(M)^2}$ converges, and since we are summing over only $x^{o(1)}$ values of M, we obtain the estimate of the theorem. □

Remark 8. The idea of [1] is to sieve directly the sequence $\mathscr{A} := \{\ell(p)\}_{p \le x}$, where the requisite information on the number of terms of $\mathscr{A}$ divisible by a given d can be read off from a theorem of Pappalardi [13, Theorem 1.3]. That approach, in conjunction with the same form of Selberg's sieve employed above, gives an unconditional proof of Theorem 3 under the severe restriction that $\mathscr{Q} \subset [2, \log x]$.

3. The case when $\mathscr{P}$ is infinite: proof of Theorem 1

Assume that a and $f(T)$ satisfy the hypotheses of Theorem 1. If p divides $a^{f(n)} - 1$ for some n, then $\ell(p) \mid f(n)$, and so $\ell(p)$ cannot be divisible by any of the primes from the set $\mathscr{P}$ defined in (1). Applying Theorem B to the splitting field of f, we find that (on GRH) the counting function of $\mathscr{P}$ behaves like $r_f \cdot \mathrm{Li}(x)$ up to an error of $O_f(x^{1/2} \log x)$. By partial summation,

$$\sum_{q \in \mathscr{P} \cap [2,x]} \frac{1}{q} = r_f \log\log x + O_f(1). \tag{5}$$

(One could also prove this last estimate unconditionally, using, e.g., [15, Théorème 2].) Theorem 1 now follows from Theorem 3 with $\mathscr{Q}$ taken as $\mathscr{P} \cap [2, x]$.

4. The case when $\mathscr{P}$ is finite: proof of Theorem 2

We start by quoting a weakened form of a result of Wiertelak [19, Theorem 2] (see also Pappalardi [13, Theorem 1], whose notation is more similar to ours).

Theorem C. *Fix an integer a with $a > 1$. Write $a = b^h$, with b not a perfect power, and put $b = a_1 a_2^2$, where a_1 is squarefree. Let d be a fixed natural number. For $x \ge 3$, the number of primes $p \le x$ for which d divides $\ell_a(p)$ is*

$$\left(\frac{\nu_{a,d}}{d(h, d^\infty)} \prod_{q \mid d} \frac{q^2}{q^2 - 1}\right) \mathrm{Li}(x) + O_{a,d}\left(\frac{\mathrm{Li}(x)}{(\log x)^{1.9}}\right).$$

Here (h, d^∞) is the largest divisor of h supported on the primes dividing d, and

$$\nu_{a,d} := \begin{cases} 1 & \text{if } [2, a_1] \nmid d, \\ 1/2 & \text{if } [2, a_1] \mid d,\ a_1 \equiv 1 \pmod 4, \\ 1/2 & \text{if } [2, a_1] \mid d,\ a_1 \not\equiv 1 \pmod 4,\ 4(2, a_1) \mid dh, \\ 5/4 & \text{if } [2, a_1] \mid d,\ a_1 \not\equiv 1 \pmod 4,\ 2(2, a_1) \parallel dh, \\ 17/16 & \text{if } [2, a_1] \mid d,\ a_1 \not\equiv 1 \pmod 4,\ 2(2, a_1) \nmid dh. \end{cases}$$

Remark 9. It follows from Theorem C that for fixed positive integers a and d with $a > 1$, the primes p for which d divides $\ell_a(p)$ possess a relative density. This holds also if $a < -1$. To see this, first note that except in the case when $2 \parallel d$, one has that $d \mid \ell_a(p)$ precisely when $d \mid \ell_{-a}(p)$. If $2 \parallel d$, then it is easy to show that

$$\#\{p \le x : p \nmid 2a, d \mid \ell_a(p)\} = \#\{p \le x : p \nmid 2a, \frac{d}{2} \mid \ell_{-a}(p)\} + \#\{p \le x : p \nmid 2a, 2d \mid \ell_{-a}(p)\} - \#\{p \le x : p \nmid 2a, d \mid \ell_{-a}(p)\};$$

see, e.g., [19, p. 181]. Theorem C applies to estimate all three right-hand terms and so gives the relative density in this case also. Alternatively, one can consult [10, Theorem 2], which gives expressions for the density valid regardless of the sign of a.

Proof of existence of the density in Theorem 2. Let $\mathscr{Q}$ be the set of primes q for which not all of the congruences $f(n) \equiv 0 \pmod{q^e}$, with $e = 0, 1, 2, \dots$, are solvable. By Hensel's lemma, $\mathscr{Q} \setminus \mathscr{P}$ is finite, and so our assumption that $\mathscr{P}$ is finite gives that $\mathscr{Q}$ is also finite.

For each $q \in \mathscr{Q}$, there is a least positive integer e_q (say) for which the congruence $f(n) \equiv 0 \pmod{q^{e_q}}$ is insoluble. A prime p divides $a^{f(n)} - 1$ for some n precisely when no prime power of the form q^{e_q}, with $q \in \mathscr{Q}$, divides $\ell(p)$. That the set of such primes p possesses a relative density now follows immediately from inclusion-exclusion and Remark 9. $\square$

It remains to show that the density whose existence was just proved is positive. We will give an explicit expression for this density from which positivity follows by a straightforward check. Complete details are given only in the case when $a > 0$; the case $a < 0$ presents additional difficulties which we discuss at the end.

So suppose now that $a > 1$. We may assume that a is not a perfect power, since if $a = b^h$, then $a^{f(n)} - 1 = b^{h \cdot f(n)} - 1$, and we could replace a by b and f by hf. Thus, in the notation of Theorem C, we have $h = 1$ and $a = b$.

Let $\mathscr{Q}$ be the set introduced in the existence proof, and let $Q := \prod_{q \in \mathscr{Q}} q^{e_q}$. Inclusion-exclusion shows that our relative density is given by

$$c_{a,f} := \sum_{d \parallel Q} (-1)^{\omega(d)} \frac{\nu_{a,d}}{d} \prod_{q \mid d} \frac{q^2}{q^2 - 1}, \tag{6}$$

in the notation of Theorem C. If $[2, a_1] \nmid Q$, then each $\nu_{a,d} = 1$, and the sum admits the product expansion

$$\prod_{q \mid Q} \left(1 - \frac{q^2}{q^{e_q}(q^2 - 1)}\right).$$

Suppose now that $[2, a_1] \mid Q$. Write $Q = Q_1 Q_2$, where Q_1 is supported on the primes dividing $2a_1$. For unitary divisors d of Q, we see that $[2, a_1] \mid d$ if and only if $Q_1 \mid d$. This suggests splitting the sum in (6) into two pieces, $\sum_1$ and $\sum_2$, with $\sum_1$ corresponding to those d not divisible by Q_1 and $\sum_2$

corresponding to the remaining d. From $\sum_1$, we get a contribution of

$$\sum_{d \| Q} \frac{(-1)^{\omega(d)}}{d} \prod_{q|d} \frac{q^2}{q^2-1} - \sum_{\substack{d \| Q \\ Q_1 | d}} \frac{(-1)^{\omega(d)}}{d} \prod_{q|d} \frac{q^2}{q^2-1}$$

$$= \prod_{q|Q} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right) - (-1)^{\omega(Q_1)} \left(\prod_{q|Q_1} \frac{q^2}{q^{e_q}(q^2-1)}\right) \cdot \left(\prod_{q|Q_2} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right)\right).$$

It remains to treat $\sum_2$, corresponding to unitary divisors d of Q for which $Q_1 \mid d$. The key observation is that $\nu_{a,d}$ is constant for such d. In fact, putting

$$\nu := \begin{cases} 1/2 & \text{if } a_1 \equiv 1 \pmod 4, \\ 1/2 & \text{if } a_1 \not\equiv 1 \pmod 4,\ 4(2, a_1) \mid Q_1, \\ 5/4 & \text{if } a_1 \not\equiv 1 \pmod 4,\ 2(2, a_1) \parallel Q_1, \\ 17/16 & \text{if } a_1 \not\equiv 1 \pmod 4,\ 2(2, a_1) \nmid Q_1, \end{cases} \tag{7}$$

we have $\nu_{a,d} = \nu$ for all these d. Reasoning as above, we obtain a contribution from $\sum_2$ of

$$\nu \cdot (-1)^{\omega(Q_1)} \left(\prod_{q|Q_1} \frac{q^2}{q^{e_q}(q^2-1)}\right) \left(\prod_{q|Q_2} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right)\right).$$

Collecting the contributions from $\sum_1$ and $\sum_2$, we find that $c_{a,f}$ is equal to

$$\prod_{q|Q} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right) + (-1)^{\omega(Q_1)}(\nu - 1) \left(\prod_{q|Q_1} \frac{q^2}{q^{e_q}(q^2-1)}\right) \left(\prod_{q|Q_2} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right)\right).$$

Factoring out the first product appearing here, we complete the proof of the following proposition:

Proposition 10. *Assume $a > 1$ and not a perfect power. Then the constant $c_{a,f}$ in Theorem 2 is given by*

$$\left(1 + (\nu - 1)(-1)^{\omega(Q_1)} \prod_{q|Q_1} \frac{q}{q^{e_q+1} - q - q^{e_q-1}}\right) \prod_{q|Q} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right). \tag{8}$$

Here we take $\nu = 1$ if $[2, a_1] \nmid Q$.

Recalling the way the value of ν was selected, it is now straightforward to check directly that $c_{a,f} > 0$ in the cases when $a > 1$.

Suppose now that $a < -1$. If 2 is not a unitary divisor of Q, then the situation is fairly simple: for $q \in \mathscr{Q}$, the number $\ell_a(p)$ is divisible by q^{e_q} precisely when the same is true for $\ell_{-a}(p)$. So replacing a with $-a$, we may derive an expression for $c_{a,f}$ analogous to that in Proposition 10 by essentially an identical argument. (We cannot assume now that $h = 1$, since $-a$ may be a perfect power, but the extra factor (h, d^∞), being multiplicative in d, does not cause any real difficulties.) Suppose now that $2 \parallel Q$, so that $2 \in \mathscr{Q}$ and $e_2 = 1$. Then we observe that

$$\begin{aligned}\#\{p \le x : p \nmid 2a, \ell_a(p) \text{ not divisible by any } q^{e_q}\} = \\ \#\{p \le x : p \nmid 2a, \ell_{a^2}(p) \text{ not divisible by any } q^{e_q}\} \\ - \#\{p \le x : p \nmid 2a, \ell_{-a}(p) \text{ not divisible by any } q^{e_q}\}.\end{aligned}$$

Since both a^2 and $-a$ are positive, we can now compute $c_{a,f}$ by using the previous argument to estimate both right-hand side terms. We omit the details, mentioning only that (by a straightforward but laborious check) the density $c_{a,f}$ so obtained is positive in every case.

5. An exercise in heuristic reasoning

In this section, we propose an asymptotic formula for the number of $p \le x$ which divide some $a^{f(n)} - 1$, where a and f are as in Theorem 1. For simplicity, we restrict ourselves to the case when $a > 0$, and we assume that a is not a perfect power.

We adopt some notation from the previous section. Namely, we let $\mathscr{Q}$ be the set of primes q for which f does not have a zero modulo every power of q. For each $q \in \mathscr{Q}$, we let e_q be the minimal positive integer for which the congruence $f(n) \equiv 0 \pmod{q^{e_q}}$ is insoluble. Since $\mathscr{Q} \setminus \mathscr{P}$ is finite, we have that $e_q = 1$ for all but finitely many $q \in \mathscr{Q}$. Let

$$Q_1 := \prod_{\substack{q \mid [2,a_1] \\ q \in \mathscr{Q}}} q^{e_q}.$$

If $[2, a_1] \nmid Q_1$, then put $\nu = 1$; otherwise, define ν by (7).

Let χ denote the characteristic function of those natural numbers n divisible by no prime power q^{e_q}, with $q \in \mathscr{Q}$. Then χ is multiplicative. Moreover, p divides some $a^{f(n)} - 1$ precisely when $\chi(\ell(p)) = 1$. One can approximate the condition that $\chi(\ell(p)) = 1$ by the condition that $\ell(p)$ be divisible by no q^{e_q}, with q up to some fixed large parameter z. For *fixed* z, there is no difficulty in computing the relative density of primes satisfying this latter condition; indeed, the proof of Proposition 10 shows that this proportion is given by (8), where now $Q := \prod_{q \in \mathscr{Q} \cap [2,z]} q^{e_q}$. We now (unjustifiably) replace

z with x to obtain the naive guess that

$$(9)\quad \frac{1}{\pi(x)}\#\{p \le x : \chi(\ell(p)) = 1\} \approx \left(1+(\nu-1)(-1)^{\omega(Q_1)} \prod_{q\mid Q_1} \frac{q}{q^{e_q+1} - q - q^{e_q-1}}\right) \prod_{q\in\mathscr{Q}\cap[2,x]} \left(1 - \frac{q^2}{q^{e_q}(q^2-1)}\right).$$

Let us compare this prediction with what the same naive heuristic suggests for the total number of $n \le x$ with $\chi(n) = 1$. Since $q^{e_q} \mid n$ with probability q^{-e_q}, our naive guess here is that

$$(10)\qquad \frac{1}{x}\#\{n \le x : \chi(n) = 1\} \approx \prod_{q\in\mathscr{Q}\cap[2,x]} \left(1 - \frac{1}{q^{e_q}}\right).$$

Dividing (9) by (10), we might conjecture that

$$(11)\qquad \frac{\frac{1}{\pi(x)}\#\{p \le x : \chi(\ell(p)) = 1\}}{\frac{1}{x}\#\{n \le x : \chi(n) = 1\}} \to C_{a,f} \qquad (\text{as } x \to \infty),$$

where

$$(12)\quad C_{a,f} = \left(1 + (\nu-1)(-1)^{\omega(Q_1)} \prod_{q\mid Q_1} \frac{q}{q^{e_q+1} - q - q^{e_q-1}}\right) \cdot \prod_{q\in\mathscr{Q}} \left(1 - \frac{1}{(q^2-1)(q^{e_q}-1)}\right).$$

As with $c_{a,f}$ in the last section, the definition of ν permits one to check in a straightforward way that $C_{a,f} > 0$.

To obtain our conjectured asymptotic formula, it remains to estimate the size of the denominator in (11), i.e., the number of $n \le x$ for which $\chi(n) = 1$. This can be obtained from a theorem of Wirsing [21, Satz 1]. We state his result in a weaker form that suffices for our application.

Theorem D. *Let f be a multiplicative function satisfying $0 \le f(n) \le 1$ for all n. Assume that for some positive constant τ, one has $\sum_{p\le x} f(p) \sim \tau x/\log x$, as $x \to \infty$. Then*

$$\frac{1}{x}\sum_{n\le x} f(n) \sim \frac{1}{\log x}\frac{\mathrm{e}^{-\gamma\tau}}{\Gamma(\tau)} \prod_{p\le x}\left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right) \qquad (\textit{as } x \to \infty).$$

Here γ is the Euler–Mascheroni constant and $\Gamma(z)$ is the classical Gamma function.

We take $f = \chi$ in Theorem D. By the Chebotarev density theorem (in the form of [15, Théorème 2], say), the hypothesis on $\sum_{p\le x} f(p)$ is satisfied with $\tau = 1 - r_f$. (Recall from the introduction that $1 - r_f > 0$.) Moreover, a short computation shows that

$$\prod_{p \le x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right) = \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} \prod_{q \in \mathscr{Q} \cap [2,x]} \left(1 - \frac{1}{q^{e_q}}\right).$$

Invoking Mertens's theorem, we deduce that (as $x \to \infty$)

$$\frac{1}{x} \#\{n \le x : \chi(n) = 1\} \sim \frac{e^{r_f \gamma}}{\Gamma(1 - r_f)} \prod_{q \in \mathscr{Q} \cap [2,x]} \left(1 - \frac{1}{q^{e_q}}\right).$$

Comparing this with (11), and recalling that $\pi(x) \sim x/\log x$, we arrive at our conjecture:

Conjecture 11. *With the above notation and hypotheses, the number of primes $p \le x$ which divide $a^{f(n)} - 1$ for some n is*

$$\sim C_{a,f} \frac{\mathrm{e}^{r_f \gamma}}{\Gamma(1 - r_f)} \frac{x}{\log x} \prod_{q \in \mathscr{Q} \cap [2,x]} \left(1 - \frac{1}{q^{e_q}}\right) \qquad (\textit{as } x \to \infty), \tag{13}$$

where $C_{a,f}$ is given by (12).

Remark 12. Lest the reader be misled, we should note that our heuristic does not depend on interpreting the symbol "$\approx$" appearing in (9) and (10) as asymptotic equality. In fact, we expect that both naive predictions (9) and (10) are off by a constant factor; the hope is that this anomalous factor disappears upon dividing (9) by (10). More colloquially, we are hoping that two wrongs make a right!

In defense of this reasoning, we point out that an exactly analogous procedure leads to a number of widely accepted conjectures, including the quantitative form of the twin prime conjecture, the Murata–Pomerance conjecture on the number of $p \le x$ for which $\ell_2(p)$ is prime [12], and Motohashi's conjecture [11, Conjecture J*] on the number of $p \le x$ of the form $x^2 + y^2 + 1$, in the corrected form of Iwaniec [7].

Example 13. We give an example where the product appearing in (13) can be put in a more satisfactory form. Take $a = 2$ and $f(T) = T^2 + 1$. Then $\mathscr{Q}$ consists of 2 together with the primes $q \equiv 3 \pmod 4$; also, $e_q = 1$ for all $q \in \mathscr{Q}$ except $q = 2$, where $e_2 = 2$. We have $Q_1 = 4$, and so $\nu = 5/4$. From (12), we find that

$$C_{2,T^2+1} = \frac{7}{9} \prod_{q \equiv 3 \pmod 4} \left(1 - \frac{1}{(q^2 - 1)(q - 1)}\right).$$

Also, $r_f = \frac{1}{2}$, $\Gamma(1 - r_f) = \Gamma(\frac{1}{2}) = \sqrt{\pi}$, and by a theorem of Uchiyama [17],

$$\prod_{\substack{q \le x \\ q \equiv 3 \pmod 4}} \left(1 - \frac{1}{q}\right) \sim \mathrm{e}^{-\gamma/2} \sqrt{\frac{\pi}{2}} \left(\prod_{q \equiv 3 \pmod 4} \left(1 - \frac{1}{q^2}\right)^{1/2}\right) (\log x)^{-1/2}.$$

So Conjecture 11 predicts that the number of $p \le x$ dividing some $2^{n^2+1}-1$ is asymptotically

$$\frac{7}{12\sqrt{2}}\left(\prod_{q\equiv 3 \pmod 4}\left(1-\frac{1}{q^2}\right)^{1/2}\left(1-\frac{1}{(q^2-1)(q-1)}\right)\right)\frac{x}{(\log x)^{3/2}}.$$

An analogous simplification of the product appearing in (13) is possible whenever the splitting field of f has an abelian Galois group; see [20, 9].

6. Concluding remarks

As noted by Ballot and Luca, classical results on primitive prime divisors imply that for every choice of a and f, infinitely many primes p divide some $a^{f(n)}-1$. But this argument gives only a very weak lower bound on the number of such $p \le x$. Can we do better?

Conjecture 11 is probably intractable at present. Even obtaining a lower bound of the form $\gg x/(\log x)^{1+r_f}$ seems difficult in general. It is more or less equivalent to asking for lower bounds of the expected order when one sieves the sequence $\{\ell(p)\}_{p\le x}$ by the set of primes $\mathscr{P}$ defined in (1). One may compare the situation with Hooley's GRH-conditional resolution of Artin's primitive root conjecture [5], which depends on sifting the corresponding sequence of indices $\{(p-1)/\ell(p)\}_{p\le x}$. We expect our problem to be at least as difficult as Hooley's. Indeed, as we saw in the proof of Theorem 1, under GRH the numbers $(p-1)/\ell(p)$ have only very small prime factors. This means that Hooley has only to sieve by a set of very small primes, which is quite convenient. We do not have this luxury.

Since (under GRH) the numbers $p-1$ and $\ell(p)$ have the same set of large prime factors, our problem is intimately related to the problem of sifting the set of shifted primes $p-1$ by a set like our $\mathscr{P}$. Here it seems very few lower bound results are known, apart from what can be derived from the half-dimensional sieve. To take a case that is favorable for us, consider the polynomial $f(T)=T^2+1$: From the half-dimensional sieve (as applied in [6]; cf. [2, p. 282, Theorem 14.8]), one obtains (unconditionally) $\gg x/(\log x)^{3/2}$ primes $p\le x$ for which $\frac{p-1}{2}$ is supported on primes $\equiv 1 \pmod 4$. For such primes, $\ell(p) \mid p-1 \mid n^2+1$ for some n, and so $p \mid a^{n^2+1}-1$ (provided that $p \nmid a$). Since $r_f = \frac{1}{2}$, the lower bound agrees with the conjectured order of magnitude. Unfortunately, this unconditional proof appears not to generalize very far, not even to all pairs a and f with f quadratic. It would be interesting to know the extent to which extra hypotheses, like GRH, would allow us to extend the list of pairs a and f for which the conjecture can be proved.

Acknowledgements. The author thanks Greg Martin for useful conversations. He also thanks the referee for a careful reading of the manuscript and for numerous helpful suggestions which made this a stronger and more readable paper.

References

[1] Ballot, Christian; Luca, Florian. Prime factors of $a^{f(n)} - 1$ with an irreducible polynomial $f(x)$. *New York J. Math.* **12** (2006), 39–45. MR2217162 (2007b:11140), Zbl 1197.11127.

[2] Friedlander, J.; Iwaniec, H. Opera de cribro. American Mathematical Society Colloquium Publications, 57. *American Mathematical Society, Providence, RI*, 2010. xx+527 pp. MR2647984 (2011d:11227), Zbl pre05757681.

[3] Granville, Andrew. Smooth numbers: computational number theory and beyond. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 267–323. Math. Sci. Res. Inst. Publ., 44. *Cambridge Univ. Press, Cambridge*, 2008. MR2467549 (2010g:11214), Zbl pre05532105.

[4] Halberstam, H.; Richert, H.-E. Sieve methods. London Mathematical Society Monographs, 4. *Academic Press, London-New York*, 1974. xiv+364 pp. MR0424730 (54 #12689), Zbl 0298.10026.

[5] Hooley, Christopher. On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220. MR0207630 (34 #7445), Zbl 0221.10048.

[6] Huxley, M. N.; Iwaniec, H. Bombieri's theorem in short intervals, *Mathematika* **22** (1975), 188–194. MR0389790 (52 #10620), Zbl 0317.10048.

[7] Iwaniec, Henryk. Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form. *Acta Arith.* **21** (1972), 203–234. MR0304331 (46 #3466), Zbl 0215.35603.

[8] Lagarias, J. C.; Odlyzko, A. M. Effective versions of the Chebotarev density theorem. *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464. *Academic Press, London*, 1977. MR0447191 (56 #5506), Zbl 0362.12011.

[9] Languasco, Alessandro; Zaccagnini, Alessandro. On the constant in the Mertens product for arithmetic progressions. I. Identities. *Funct. Approx. Comment. Math.* **42** (2010), 17–27. MR2640766 (2011b:11127), Zbl 1206.11112.

[10] Moree, Pieter. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.* **33** (2005), 85–95. MR2274151 (2007j:11131), Zbl pre05135205.

[11] Motohashi, Yoichi. On the distribution of prime numbers which are of the form $x^2 + y^2 + 1$. *Acta Arith.* **16** (1969/1970), 351–363. MR0288086 (44 #5284), Zbl 0205.06801.

[12] Murata, Leo; Pomerance, Carl. On the largest prime factor of a Mersenne number. *Number theory*, 209–218. CRM Proc. Lecture Notes, 36. *Amer. Math. Soc., Providence, RI*, 2004. MR2076597 (2005i:11137), Zbl 1077.11003.

[13] Pappalardi, Francesco. Square free values of the order function. *New York J. Math.* **9** (2003), 331–344. MR2028173 (2004i:11116), Zbl 1066.11044.

[14] Ribenboim, Paulo. Algebraic numbers. Pure and Applied Mathematics, 27. *Wiley-Interscience, New York-London-Sydney*, 1972. x+300 pp. MR0340212 (49 #4968), Zbl 0247.12002.

[15] Serre, Jean-Pierre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR0644559 (83k:12011), Zbl 0496.12011.

[16] Stevenhagen, P.; Lenstra, H. W., Jr. Chebotarëv and his density theorem. *Math. Intelligencer* **18** (1996), no. 2, 26–37. MR1395088 (97e:11144), Zbl 0885.11005.

[17] Uchiyama, S. On some products involving primes. *Proc. Amer. Math. Soc.* **28** (1971), 629–630. MR0277494 (43 #3227), Zbl 0212.07901.

[18] Wagstaff, Samuel S., Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.* **41** (1982), 141–150. MR0674829 (83m:10004), Zbl 0496.10001.

[19] Wiertelak, K. On the density of some sets of primes. IV. *Acta Arith.* **43** (1984), 177–190. MR0736730 (86e:11081), Zbl 0531.10049.

[20] Williams, Kenneth S. Mertens' theorem for arithmetic progressions. *J. Number Theory* **6** (1974), 353–359. MR0364137 (51 #392), Zbl 0286.10022.

[21] Wirsing, Eduard. Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Ann.* **143** (1961), 75–102. MR0131389 (24 #A1241), Zbl 0104.04201.

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

Simon Fraser University, Department of Mathematics, Burnaby, BC Canada V5A 1S6
pollack@math.ubc.ca

This paper is available via http://nyjm.albany.edu/j/2011/17-23.html.