Annals of Mathematics **191** (2020), 355–392
https://doi.org/10.4007/annals.2020.191.2.2

A conjecture of Erdős, supersingular primes and short character sums

By Michael A. Bennett and Samir Siksek

Abstract

If k is a sufficiently large positive integer, we show that the Diophantine equation

$$n(n+d)\cdots(n+(k-1)d) = y^\ell$$

has at most finitely many solutions in positive integers n, d, y and ℓ, with $\gcd(n,d) = 1$ and $\ell \geq 2$. Our proof relies upon Frey-Hellegouarch curves and results on supersingular primes for elliptic curves without complex multiplication, derived from upper bounds for short character sums and sieves, analytic and combinatorial.

1. Introduction

In 1975, Erdős and Selfridge [13] solved a long-open problem, originally posed by Liouville [26] in 1857, proving that the product of two or more consecutive nonzero integers can never be a perfect power:

Theorem 1 (Erdős - Selfridge, 1975). *The Diophantine equation*

$$n(n+1)\cdots(n+k-1) = y^\ell \tag{1}$$

has no solutions in positive integers n, k, y and ℓ with $k, \ell \geq 2$.

The proof, rather surprisingly, relies upon a combination of clever elementary and graph theoretic arguments. Earlier work on equation (1), from Liouville onwards, had either depended upon results from multiplicative number theory or upon Diophantine approximation (as, for example, in oft-cited but unpublished work of Erdős and Siegel, where a result similar to Theorem 1 was obtained for suitably large n).

Keywords: Superelliptic curves, Galois representations, Frey-Hellegouarch curve, modularity, level lowering

AMS Classification: Primary: 11D61; Secondary: 11D41, 11F80, 11F41.

The first author was supported by NSERC, while the second author was supported by an EPSRC *LMF*: *L-Functions and Modular Forms* Programme Grant EP/K034383/1.

An apparently rather more difficult problem is to derive an analogue of Theorem 1 for products of consecutive terms in arithmetic progression, and this is the subject of the following famous conjecture, widely attributed to Erdős (see, for example, [41]):

CONJECTURE (Erdős). *There is a constant k_0 such that the Diophantine equation*

$$n(n+d)(n+2d)\cdots(n+(k-1)d) = y^\ell, \qquad \gcd(n,d) = 1 \tag{2}$$

has no solutions in positive integers n, d, k, y, ℓ, with $\ell \geq 2$ and $k \geq k_0$.

Without the condition $\gcd(n,d) = 1$ it is easy to construct a plethora of artificial solutions. As pointed out by Erdős and Selfridge, equation (2) has infinitely many solutions for $(k,\ell) = (3,2)$ (satisfying $\gcd(n,d) = 1$). Note that if we permit negative values of n, we must modify this conjecture somewhat to allow for solutions corresponding to the identities

$$\prod_{j=-2m}^{2m-1}(2j+1) = \left(\prod_{j=0}^{2m-1}(2j+1)\right)^2$$

and

$$\prod_{j=-2m^2-2m}^{2m^2+2m}(2j+1) = \left((2m+1)\prod_{j=0}^{2m^2+2m-1}(2j+1)\right)^2,$$

where m is a positive integer.

The literature on equation (2) is extensive, dating back to work of Euler who proved that there are no nontrivial solutions with $(k,\ell) = (4,2)$. It is worth observing that, via an argument of Granville (unpublished, but reproduced in Laishram and Shorey [24]), Erdős' conjecture is a consequence of the *abc*-conjecture of Masser and Oesterlé. Currently, Erdős' conjecture has been verified unconditionally only subject to a variety of additional assumptions. By way of example, we now know it to be true if d is fixed (Marszalek [27]), if both ℓ and $\omega(d)$ (the number of distinct prime divisors of d) are fixed (Shorey and Tijdeman [41]), if $P(d)$ (the greatest prime divisor of d) is fixed and $\ell \geq 3$ (Shorey [38]), or if n is fixed and $\ell \geq 7$ (Shorey [39]). In subsequent work, a number of these results have been refined and, in a number of cases, made completely explicit (particularly for small values of k); the interested reader is directed to the fine survey of Shorey [40] for further details on the literature on this problem.

The papers we have mentioned so far rely upon either elementary arguments in the spirit of Erdős and Selfridge, or upon lower bounds for linear forms in logarithms (sometimes in conjunction with Diophantine inequalities

resulting from Padé approximation to binomial functions). More recently, we find a number of results that appeal to the modularity of Galois representations associated to certain Frey-Hellegouarch curves to show that equation (2) has at most finitely many solutions, again under certain additional constraints. The possibility of this approach is implicit in the work of Darmon and Granville [9] (where, in Corollary 2.1, the finiteness of the number of nontrivial solutions to (2) is proved provided k and ℓ are both fixed). Explicitly, via such methods, we find a complete solution of equation (2) in case $k = 3$ (Győry [17]), $k \in \{4, 5\}$ (Győry, Hajdu and Saradha [18]), $6 \leq k \leq 11$ (Bennett, Bruin, Győry and Hajdu [1]) and $12 \leq k \leq 34$ (Győry, Hajdu and Pintér [18]). In [1], it is further proved that (2) has at most finitely many nontrivial solutions for all $k \leq 82$.

In this paper, we prove a somewhat weakened version of the Erdős conjecture, which deals also with negative solutions:

THEOREM 2. *There is an effectively computable absolute constant k_0 such that if $k \geq k_0$ is a positive integer, then any solution in integers to equation (2) with prime exponent ℓ satisfies either $y = 0$ or $d = 0$ or $\ell \leq \exp(10^k)$.*

It follows from Faltings' Theorem that (2) has finitely many solutions with $k \geq k_0$ and $yd \neq 0$.

Our proof of Theorem 2 follows very different lines from prior work on this problem, and we emphasize that it bears little resemblance to an earlier result of the authors [3], where an analogous finiteness statement for rational points on curves corresponding to equation (1) is deduced. While our starting point shares much in common with [1], [3] and [18], in that one is led to study certain ternary equations with corresponding Frey-Hellegouarch curves, the information we derive from these equations is quite distinct from that previously considered. In particular, our proof of Theorem 2 makes essential use of a wide array of tools from arithmetic geometry, analytic number theory and additive combinatorics, including the following:

- the modularity of elliptic curves over $\mathbb{Q}$ due to Wiles, Breuil, Conrad, Diamond and Taylor;
- Ribet's level lowering theorem;
- known cases of Serre's uniformity conjecture, due to Mazur, to Bilu, Parent and Rebolledo, to Darmon and Merel, and to Lemos;
- a version of the large sieve inequality due to Selberg;
- the Prime Number Theorem for Dirichlet L-functions;
- gap principles for exceptional zeros of L-functions due Siegel and Landau;
- an explicit version of Roth's theorem on 3-term arithmetic progressions;
- theorems on short character sums due to Burgess and to Graham and Ringrose.

The outline of this paper is as follows. In Section 2, we state some now standard results deriving from the modularity of elliptic curves. In Section 3, we detail the correspondence between solutions to (2), related ternary Diophantine equations, and Frey-Hellegoaurch elliptic curves. We further discuss why the techniques of [1] and [18] (which lead to analogues of Theorem 2 for small values of k) will likely fail for all sufficiently large k. Sections 4 and 5 contain, respectively, an argument that guarantees that primes in $(k/2, k]$ necessarily divide d (for a solution to (2) with $y \neq 0$ and large exponent ℓ), and the consequence of this, that the primes $p \equiv 3 \pmod 4$ in this interval are in fact supersingular for a certain parametrized family of elliptic curves. In Section 6, we use this information to construct a (short) character sum that is unusually large, corresponding to each Frey-Hellegouarch curve. Section 7 contains an argument, based upon the Prime Number Theorem for Dirichlet characters, that ensures the desired conclusion, provided we have suitably many elliptic curves corresponding to our Frey-Hellegouarch curves with extremely smooth conductors. In Section 8, we attain a like conclusion, via upper bounds for short character sums and the large sieve, under the assumption that we have a somewhat larger number of rather less smooth conductors. Finally, in Sections 9 and 10, we complete the proof of Theorem 2, by using a variety of sieving arguments to show that our Frey-Hellegouarch curves correspond to sufficiently many Dirichlet characters to guarantee that we can appeal to at least one of the results from the preceding sections. Our addendum contains a streamlined version of the more analytic aspects of our proof (deriving a contradiction from Proposition 6.1 without recourse to estimates for short character sums or Roth's theorem) that was communicated to us by Andrew Granville [16] and is reproduced here with his kind permission.

Acknowledgements. We are grateful to Andrew Granville, Adam Harper, Roger Heath-Brown, Lillian Pierce and Trevor Wooley for useful conversations.

2. **Residual representations attached to elliptic curves**

Let E be an elliptic curve defined over $\mathbb{Q}$, with minimal discriminant Δ and conductor M. For a rational prime $\ell \geq 3$, we denote by

$$\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

the representation describing the action of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-torsion subgroup $E[\ell]$. Define

$$M_0 = M \Big/ \prod_{\substack{q \,\|\, M,\ q \text{ prime} \\ \ell \,|\, \mathrm{ord}_q(\Delta)}} q, \tag{3}$$

where we write $\mathrm{ord}_q(x)$ for the largest power of a prime q dividing a nonzero integer x.

The following theorem is a standard consequence of Ribet's level lowering theorem [33] (stated, for example, in [42, p. 157]). It was originally conditional on the modularity of elliptic curves over $\mathbb{Q}$, a result that was subsequently proved by Wiles, Breuil, Conrad, Diamond and Taylor (see [46] and [8]). Additionally, it is, in fact, a special case of Serre's Modularity Conjecture [37], now a theorem of Khare and Wintenberger ([20] and [21]).

THEOREM 3. *If $E[\ell]$ is irreducible, then there is a cuspidal newform $f = \sum_{n\geq 1} c_n q^n$ of weight 2 and level M_0 such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$, where $\lambda \mid \ell$ is a prime of the totally real field $K = \mathbb{Q}(c_1, c_2, \dots)$.*

Here, by $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{f,\lambda}$ we mean that, for almost all primes p, we have that

$$a_p(E) \equiv c_p \pmod{\lambda}.$$

In fact, by comparing the traces of Frobenius for $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{f,\lambda}$, we can be rather more precise.

LEMMA 2.1. *With notation as in Theorem 3, let p be a rational prime.*

(i) *If $p \nmid \ell M M_0$, then $a_p(E) \equiv c_p \pmod{\lambda}$.*
(ii) *If $p \nmid \ell M_0$ and $p \parallel M$, then $p + 1 \equiv \pm c_p \pmod{\lambda}$.*

The following lemma will be invaluable to us:

LEMMA 2.2. *With notation as above, suppose $p \neq \ell$ is a prime with $p \parallel M$ and, additionally, $\ell \mid \operatorname{ord}_p(\Delta)$. Then*

$$\ell \leq (\sqrt{p} + 1)^{(M_0+1)/6}.$$

Proof. From (3), we see that $p \nmid M_0$. Thus by Lemma 2.1 we have

$$\lambda \mid (p + 1 \mp c_p)$$

and so

$$\ell \mid \operatorname{Norm}_{K/\mathbb{Q}}(p + 1 \mp c_p).$$

As c_p is bounded by $2\sqrt{p}$ in all the real embeddings of K, we have

$$\ell \leq (p + 1 + 2\sqrt{p})^{[K:\mathbb{Q}]} = (\sqrt{p} + 1)^{2[K:\mathbb{Q}]}.$$

If we denote the dimension of $S_2^{\text{new}}(M_0)$ by $g_0^+(M_0)$, then $[K : \mathbb{Q}] \leq g_0^+(M_0)$. By Theorem 2 of Martin [28], we have

$$g_0^+(M_0) \leq \frac{M_0 + 1}{12}, \tag{4}$$

completing the proof. □

It is well known that if the residual characteristic ℓ is sufficiently large compared to the level M_0, then f has rational eigenvalues and so corresponds

to an elliptic curve over $F/\mathbb{Q}$. We shall have use of a quantitative version of this statement due to Kraus [23]. For a positive integer n, let

$$\mu(n) = n \prod_{\substack{q \mid n \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right). \tag{5}$$

Define

$$F(n) = \left(\sqrt{\frac{\mu(n)}{6}} + 1\right)^{2g_0^+(n)}, \quad G(n) = \left(\sqrt{\frac{\mu(\mathrm{lcm}(n,4))}{6}} + 1\right)^2,$$

and set

$$H(n) = \max(F(n), G(n)).$$

The following is Théorème 4 of [23].

THEOREM 4 (Kraus). *With notation as in Theorem 3, suppose E has full 2-torsion and that*

$$\ell > H(M_0).$$

Then there is an elliptic curve $F/\mathbb{Q}$ having full 2-torsion of conductor M_0 such that $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{F,\ell}$.

3. Frey-Hellegouarch curves associated to (2)

We shall call a solution (n, d, k, y, ℓ) of (2) *trivial* if $yd = 0$. We shall henceforth restrict our attention to nontrivial solutions. In this section, we will show how a nontrivial solution to equation (2) is simultaneously a solution to many generalized Fermat equations, both of signature (ℓ, ℓ, ℓ) and of signature $(\ell, \ell, 2)$. (In fact, we can actually derive ternary equations of signature (ℓ, ℓ, q) for values of $q > 2$, but these will not be of interest to us.) The following elementary lemma is an immediate consequence of the coprimality assumption for equation (2).

LEMMA 3.1. *Let (n, d, k, y, ℓ) be a nontrivial solution to (2) with ℓ prime.*

(i) *For $0 \le i < j \le k-1$,*

$$\gcd(n + id, n + jd) \mid (j - i).$$

(ii) *Let $0 \le i \le k-1$, and let $q \ge k$ be prime. Then*

$$\ell \mid \mathrm{ord}_q(n + id).$$

Thus we may write

$$n + id = A_i\, y_i^{\ell}, \qquad 0 \le i \le k-1, \tag{6}$$

where A_i are positive integers divisible only by primes $< k$, whereas y_i are divisible only by primes $\ge k$.

3.1. *Fermat equations of signature* (ℓ,ℓ,ℓ). In general, given any integers

$$0 \le i_1 < i_2 < i_3 \le k-1,$$

the identity

$$(i_3-i_2)(n+i_1d)+(i_1-i_3)(n+i_2d)+(i_2-i_1)(n+i_3d)=0$$

leads to a ternary Diophantine equations of signature (ℓ,ℓ,ℓ). This provides us with roughly $k^3/6$ generalized Fermat equations to consider. For our purposes, it will be convenient to restrict our attention to indices (i_1,i_2,i_3) in arithmetic progression (of which there are approximately $k^2/4$). Let

$$\mathcal{A}=\{(i,j,2j-i) : i,j,2j-i \in \{0,1,\dots,k-1\},\ \ i<j\}$$

denote the set of nontrivial 3-term arithmetic progressions in the set $\{0,1,\dots,k-1\}$. Associated to any such tuple $\mathfrak{a}=(i,j,2j-i)\in\mathcal{A}$ is the identity

$$(n+id)-2(n+jd)+(n+(2j-i)d)=0,$$

from which we see that $(r,s,t)=(y_i,y_j,y_{2j-i})$ is a solution to the following generalized Fermat equation of signature (ℓ,ℓ,ℓ):

$$A_ir^\ell-2A_js^\ell+A_{2j-i}t^\ell=0.$$

We may attach to this solution a Frey-Hellegouarch curve as in Kraus [23]. For convenience, we let

$$g=\gcd\left(n+id,\ 2(n+jd),\ n+(2j-i)d\right), \tag{7}$$

$$a_{\mathfrak{a}}=\frac{n+id}{g},\ \ b_{\mathfrak{a}}=\frac{-2(n+jd)}{g}\quad\text{and}\quad c_{\mathfrak{a}}=\frac{n+(2j-i)d}{g}. \tag{8}$$

Our corresponding Frey–Hellegouarch is

$$E_{\mathfrak{a}}: Y^2=X(X-a_{\mathfrak{a}})(X+c_{\mathfrak{a}}).$$

LEMMA 3.2. *The model $E_{\mathfrak{a}}$ is minimal and semistable at all odd primes. Its discriminant is*

$$\Delta_{\mathfrak{a}}=64(a_{\mathfrak{a}}b_{\mathfrak{a}}c_{\mathfrak{a}})^2=\frac{2^8}{g^6}(n+id)^2(n+jd)^2(n+(2j-i)d)^2.$$

In particular, for any prime $p\ge k$, we have $\ell \mid \operatorname{ord}_p(\Delta_{\mathfrak{a}})$.

Proof. The first part is a straightforward computation. The second follows from Lemma 3.1. □

LEMMA 3.3. *Let $\ell\ge 7$. Then $\overline{\rho}_{E_{\mathfrak{a}},\ell}\sim\overline{\rho}_{f,\lambda}$, where f is a newform of weight 2 and level $M_{\mathfrak{a}}$, with*

$$M_{\mathfrak{a}} \mid 2^8\cdot A_iA_jA_{2j-i} \tag{9}$$

and

$$M_{\mathfrak{a}}\le 2^7\cdot\exp(1.000081\cdot k).$$

Proof. As $E_{\mathfrak{a}}$ has full 2-torsion and $\ell \geq 7$, we know from the work of Mazur [29] that $E_{\mathfrak{a}}[\ell]$ is irreducible. It follows from Theorem 3 that $\overline{\rho}_{E_{\mathfrak{a}},\ell} \sim \overline{\rho}_{f,\lambda}$, where f is a newform of weight 2 and level M_0 given by (3). We write $M_{\mathfrak{a}} := M_0$. Equation (3) and Lemma 3.2 ensure that $M_{\mathfrak{a}}$ satisfies (9). Moreover, as the odd part of $M_{\mathfrak{a}}$ is squarefree, $M_{\mathfrak{a}}$ divides

$$2^7 \prod_{\substack{q \leq k \\ q \text{ prime}}} q.$$

From Schoenfeld [35, p. 160], we have

$$\sum_{q \leq k} \log q < 1.000081 \cdot k. \tag{10}$$

The lemma follows. □

3.2. *Fermat equations of signature* $(\ell, \ell, 2)$. Let

$$\mathcal{I} = \{(j_1, i_1, i_2, j_2) : i_1 + i_2 = j_1 + j_2, \;\; 0 \leq j_1 < i_1 \leq i_2 < j_2 \leq k-1\}.$$

To any fixed quadruple $\mathbf{i} = (j_1, i_1, i_2, j_2) \in \mathcal{I}$, we can associate the identity

$$(n + j_1 d)(n + j_2 d) - (n + i_1 d)(n + i_2 d) = (j_1 j_2 - i_1 i_2) d^2.$$

It follows that $(r, s, t) = (y_{j_1} y_{j_2}, y_{i_1} y_{i_2}, d)$ is a solution to the following generalized Fermat equation with signature $(\ell, \ell, 2)$:

$$A_{j_1} A_{j_2} \cdot r^\ell - A_{i_1} A_{i_2} \cdot s^\ell = (j_1 j_2 - i_1 i_2) \cdot t^2. \tag{11}$$

Following Bennett and Skinner [4], solutions to this equation also correspond to Frey-Hellegouarch elliptic curves defined over $\mathbb{Q}$. To simplify notation, write

$$A = (n + j_1 d)(n + j_2 d), \;\; B = (n + i_1 d)(n + i_2 d) \quad \text{and} \quad \kappa = j_1 j_2 - i_1 i_2, \tag{12}$$

so that

$$A - B = \kappa d^2. \tag{13}$$

Let

$$\mathcal{E}_{\mathbf{i}} : Y^2 = X(X^2 + 2\kappa d X + \kappa A).$$

LEMMA 3.4. *The model* $\mathcal{E}_{\mathbf{i}}$ *is minimal and semistable at all primes* $p \geq k$ *that also satisfy* $p \nmid \kappa$. *It has discriminant*

$$\Delta_{\mathbf{i}} = -64 \kappa^3 A^2 B.$$

In particular, for any prime $p \geq k$ *with* $p \nmid \kappa$, *we have* $\ell \mid \mathrm{ord}_p(\Delta_{\mathbf{i}})$.

Proof. This again follows from a straightforward computation with the help of Lemma 3.1. □

LEMMA 3.5. *Let $\ell \geq 11$. Then $\overline{\rho}_{\mathcal{E}_{\mathbf{i}},\ell} \sim \overline{\rho}_{f,\lambda}$, where f is a newform of weight 2 and level $M_{\mathbf{i}}$ satisfying*

$$M_{\mathbf{i}} \leq 2^7 \cdot 3^5 \cdot k^4 \cdot \exp(2.000162 \cdot k).$$

Proof. As $\mathcal{E}_{\mathbf{i}}$ has a rational point of order 2 and $\ell \geq 11$, we know from the work of Mazur [29] that $\mathcal{E}_{\mathbf{i}}[\ell]$ is irreducible. It follows from Theorem 3 that $\overline{\rho}_{\mathcal{E}_{\mathbf{i}},\ell} \sim \overline{\rho}_{f,\lambda}$ where f is a newform of weight 2 and level M_0 given by (3). We write $M_{\mathbf{i}} := M_0$. Equation (3), together with Lemma 3.4, ensures that $M_{\mathbf{i}}$ divides

$$2^7 \cdot 3^5 \cdot \kappa^2 \cdot \prod_{\substack{q \leq k \\ q \text{ prime}}} q^2.$$

As $|\kappa| < k^2$, the lemma follows from inequality (10). □

At this point, it is worth mentioning why the techniques of [1] and [18] are apparently insufficient to prove Theorem 2 (yet do allow one to show that equation (2) has at most finitely many nontrivial solutions for small values of k). Intrinsically, they rely upon the fact that for suitably small k, and each possible tuple

$$\mathbf{A} = (\mathrm{Rad}(A_0), \mathrm{Rad}(A_1), \ldots, \mathrm{Rad}(A_{k-1}))$$

(here, the A_i are as in (6); the number of such tuples depends only upon k and not ℓ or d), we can find $\mathbf{i} = (j_1, i_1, i_2, j_2) \in \mathcal{I}$ such that the corresponding polynomial-exponential equation

$$x + y = z^2, \tag{14}$$

where $z \in \mathbb{Q}$ and x, y are S-units, for

$$S = \{p \text{ prime} : p \mid A_{j_1} A_{j_2} A_{i_1} A_{i_2} (j_1 j_2 - i_1 i_2)\},$$

has only "trivial" solutions. As a first step, one applies an argument to guarantee that

$$p \mid A_1 A_2 \cdots A_{k-1} \implies p < \tau k$$

for certain $\tau \in (0, 1]$. That we may take $\tau = 1$ is immediate from the definition of A_i, while, for example, Lemma 4.1 of the next section implies a like result with $\tau = 1/2$. It is not especially difficult to improve this to $\tau = 1/3$, but it appears to be quite hard to reduce this significantly. From a result of Erdős, Stewart and Tijdeman (see, e.g., Theorem 4 of [14]), the number of solutions to equation (14) with x and y rational numbers supported on primes of size at most τk exceeds $\exp\left(3\frac{\sqrt{\tau k}}{\log k}\right)$ for large enough k. Since the number of tuples $\mathbf{A}$ to be treated also grows exponentially in τk, while the cardinality of $\mathcal{I}$ is

$$\sum_{j=2}^{k-1} (k-j)\,[j/2] = \frac{k^3}{12} - \frac{k^2}{8} - \frac{k}{12} + \frac{\delta}{8}, \quad \text{where} \quad \delta = \begin{cases} 0 & \text{if } k \text{ is even,} \\ 1 & \text{if } k \text{ is odd,} \end{cases}$$

our expectation is that for all sufficiently large k, there will correspond to each choice of $\mathbf{i} \in \mathcal{I}$ a tuple $\mathbf{A}$ for which the associated equation of the shape (14) has nontrivial solutions.

We will proceed in a very different direction. Rather than attempting to reduce the problem of treating equation (2) to that of solving associated ternary equations (which, as we have noted, is likely to be futile for large k), we will, in the next two sections, instead deduce from a nontrivial solution to (2) the existence of a large number of elliptic curves that, on some level, mimic the behaviour of elliptic curves with complex multiplication (despite not possessing this property).

4. A first result on primes $k/2 < p \le k$

We begin with an easy lemma that ensures that primes in the interval $(k/2, k]$ fail to divide $A_0 A_1 \cdots A_{k-1}$ for suitably large ℓ. This apparently innocuous result (a version of which first appeared in the proof of Theorem 1.5 of [1]) is actually the key first step in proving Theorem 2.

LEMMA 4.1. *Let $k \ge 10^8$, and suppose that (n, d, k, y, ℓ) is a nontrivial solution to (2) with prime exponent $\ell > \exp(10^k)$. Let p be a prime in the range $k/2 < p \le k$. Then $p \mid d$.*

Proof. Suppose that $p \nmid d$. Then p divides at least one and at most two of the terms $n + d, n + 2d, \ldots, n + kd$. Suppose first that p divides precisely one such term, say $p \mid n + id$. It follows from (2) that

$$\ell \mid \mathrm{ord}_p(n + id).$$

Let $\mathfrak{a}$ be any triple of indices in $\mathcal{A}$ containing i. It follows from Lemma 3.2 that $E_{\mathfrak{a}}$ is semistable at p with multiplicative reduction, and that $\ell \mid \mathrm{ord}_p(\Delta_{\mathfrak{a}})$. Applying Lemma 2.2, we see that

$$\ell \le (\sqrt{p} + 1)^{(M_{\mathfrak{a}}+1)/6}.$$

Now the bound in Lemma 3.3 for $M_{\mathfrak{a}}$ contradicts the assumption $\ell > \exp(10^k)$.

If instead p divides divides precisely two terms, say $p \mid n + id$ and $p \mid n + (i + p)d$, then we choose $\mathbf{i} = (i, i + 1, i + p - 1, i + p) \in \mathcal{I}$. Let A, B, κ and d be as in (3.2). From (2) and (12), we have

$$p \mid A, \quad \ell \mid \mathrm{ord}_p(A) \quad \text{and} \quad p \nmid B.$$

Equation (13) thus implies that $p \nmid \kappa$ and so the model $\mathcal{E}_{\mathbf{i}}$ has multiplicative reduction at p. Applying Lemma 2.2, we see that

$$\ell \le (\sqrt{p} + 1)^{(M_{\mathbf{i}}+1)/6}.$$

Now the bound in Lemma 3.5 for $M_{\mathbf{i}}$ contradicts the assumption $\ell > \exp(10^k)$, completing the proof of Lemma 4.1. □

5. A closer look at the Frey-Hellegouarch curve $E_{\mathfrak{a}}$

The Frey-Hellegouarch curves $\mathcal{E}_{\mathbf{i}}$ associated to $\mathbf{i} \in \mathcal{I}$ have been valuable in proving Lemma 4.1. We shall not, however, have further use for them and will instead focus, here and henceforth, solely on the Frey-Hellegouarch curves $E_{\mathfrak{a}}$ associated to the 3-term arithmetic progressions $\mathfrak{a} \in \mathcal{A}$.

LEMMA 5.1. *Let $k \geq 10^8$, and suppose that (n, d, k, y, ℓ) is a nontrivial solution to (2) with $\ell > \exp(10^k)$ prime. Let $\mathfrak{a} \in \mathcal{A}$. Then there is an elliptic curve $F_{\mathfrak{a}}/\mathbb{Q}$ having full rational 2-torsion and conductor $M_{\mathfrak{a}}$ such that $\overline{\rho}_{E_{\mathfrak{a}},\ell} \sim \overline{\rho}_{F_{\mathfrak{a}},\ell}$.*

Proof. By Theorem 4, it is sufficient to show that $\ell > H(M_{\mathfrak{a}})$. From Tenenbaum [44] (Theorem 9 and the remark following it), we have

$$\prod_{\substack{q \leq k \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right) \leq \exp\left(0.27 + \frac{5}{\log k}\right) \cdot \log k.$$

As $k \geq 10^8$, we obtain

$$\prod_{q \leq k} \left(1 + \frac{1}{q}\right) \leq 2 \log k.$$

This, together with Lemma 3.3 and its proof, shows that both $\mu(M_{\mathfrak{a}})$ and $\mu(\operatorname{lcm}(M_{\mathfrak{a}}, 4))$ are bounded by

$$2^8 \log k \cdot \exp(1.000081 \cdot k).$$

Using the previously cited estimate (4) to bound $g_0^+(M_{\mathfrak{a}})$, we easily deduce that $H(M_{\mathfrak{a}}) < \exp(10^k) < \ell$ as required. □

Throughout the remainder of the paper, we maintain the assumption $\ell > \exp(10^k)$. Further, $F_{\mathfrak{a}}$ will always denote the elliptic curve associated to $\mathfrak{a}$ by Lemma 5.1.

LEMMA 5.2. *With notation and assumptions as in Lemma 5.1, let p be a prime satisfying $k/2 < p \leq k$. Then p is a prime of good reduction for both $E_{\mathfrak{a}}$ and $F_{\mathfrak{a}}$, and we have $a_p(E_{\mathfrak{a}}) = a_p(F_{\mathfrak{a}})$. If, moreover, $p \equiv 3 \pmod 4$, then $a_p(F_{\mathfrak{a}}) = 0$ and hence p is a prime of supersingular reduction for $F_{\mathfrak{a}}$.*

Proof. By Lemma 4.1, we know that every prime $k/2 < p \leq k$ divides d. As $\gcd(n, d) = 1$ we see that $p \nmid (n + id)$ for all i. It follows from Lemma 3.2 that p is a prime of good reduction for $E_{\mathfrak{a}}$. Since the conductor $M_{\mathfrak{a}}$ of $F_{\mathfrak{a}}$ is a divisor of the conductor of $E_{\mathfrak{a}}$ (see equation (3)), it follows that p is a prime of good reduction for both elliptic curves. Hence, by Lemma 2.1, we know that $a_p(E_{\mathfrak{a}}) \equiv a_p(F_{\mathfrak{a}}) \pmod \ell$. By the Hasse–Weil bounds $|a_p(E_{\mathfrak{a}}) - a_p(F_{\mathfrak{a}})| \leq 4\sqrt{k}$, whereby the inequality $\ell > \exp(10^k)$ immediately implies that $a_p(E_{\mathfrak{a}}) = a_p(F_{\mathfrak{a}})$.

Let g be as in (7), so that the reduction of $E_{\mathfrak{a}}$ modulo p is

$$\tilde{E}_{\mathfrak{a}} : Y^2 = X(X - n/g)(X + n/g).$$

If $p \equiv 3 \pmod 4$, then, as is well known (see, e.g., page 41 of [22]), $a_p(E_{\mathfrak{a}}) = 0$ whereby also $a_p(F_{\mathfrak{a}}) = 0$. □

Before we proceed, it is worth remarking that Lemma 5.2 implies that the elliptic curve $F_{\mathfrak{a}}$ shares supersingular primes with elliptic curves with complex multiplication and j-invariant 1728, in the interval $k/2 < p \leq k$. As we shall later observe, $F_{\mathfrak{a}}$ cannot itself have complex multiplication. This alone, however, is not enough to imply a contradiction; indeed the curve with model

$$E : Y^2 = X^3 - X + \prod_{p \leq k} p \tag{15}$$

has precisely these properties. On the other hand, if we can deduce the existence of an $\mathfrak{a} \in \mathcal{A}$ for which the conductor of $F_{\mathfrak{a}}$ is suitably "small" (notice that E in (15) has conductor that is exponentially large in k), then we can apply an effective version of the Chebotarev density theorem to derive a contradiction for large k, solely from $F_{\mathfrak{a}}$ having a surplus of supersingular primes in the interval $(k/2, k]$. (See Serre [36] and Elkies [11] for upper bounds on the number of supersingular primes in intervals, for elliptic curves without complex multiplication, both conditional on the Generalized Riemann Hypothesis (GRH) and otherwise.) As we shall observe in Section 9, we can guarantee the existence of an $\mathfrak{a}$ for which the conductor of $F_{\mathfrak{a}}$ is bounded above by k^{λ} for some absolute positive constant λ. This is sufficient to contradict the Chebotarev density theorem under GRH, but not unconditionally. If we had an $\mathfrak{a} \in \mathcal{A}$ for which $F_{\mathfrak{a}}$ has conductor bounded by $(\log k)^{\lambda}$, say, then we would have an alternative proof of Theorem 2 via this approach. At present, we are unable to prove the existence of such an $\mathfrak{a}$.

6. On a character sum associated to $F_{\mathfrak{a}}$

Henceforth, $F_{\mathfrak{a}}$ will denote the elliptic curve over $\mathbb{Q}$ having full 2-torsion and conductor $M_{\mathfrak{a}}$ attached, via Lemma 5.1, to a 3-term arithmetic progression $\mathfrak{a} \in \mathcal{A}$, where $\mathcal{A}$ corresponds to a nontrivial solution of (2). For a positive integer N, we write $N^{\text{odd}} = N \cdot 2^{-\text{ord}_2(N)}$ for the odd part of N. As usual, we denote by Λ the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

PROPOSITION 6.1. *Let $k \geq 2 \times 10^{10}$, and let $\ell > \exp(10^k)$ be prime. Let (n, d, k, y, ℓ) be a nontrivial solution to equation (2), and suppose that $\mathfrak{a} \in \mathcal{A}$.*

Then there exists a quadratic character $\chi_{\mathfrak{a}}$ that is primitive of conductor $N_{\mathfrak{a}}$ such that

$$\left|\sum_{k/2<m\le k}\chi_{\mathfrak{a}}(m)\cdot\Lambda(m)\right| > 0.1239\,k. \tag{16}$$

Moreover, we have that $N_{\mathfrak{a}}^{\mathrm{odd}} \mid M_{\mathfrak{a}}$ and $N_{\mathfrak{a}}^{\mathrm{odd}} \neq 1$.

Remark. After proving Proposition 6.1, the key to the proof of Theorem 2 will be to show, for k suitably large, that if $N_{\mathfrak{a}}^{\mathrm{odd}} \neq 1$ for all $\mathfrak{a}$, then there is some $\mathfrak{a}$ for which the left-hand side of the inequality (16) is much smaller than $0.1239k$.

Legendre elliptic curves. Let $\lambda \in \mathbb{Q}\setminus\{0,1\}$, and write

$$F_\lambda : Y^2 = X(X-1)(X-\lambda), \tag{17}$$

often called a *Legendre elliptic curve with parameter* λ. For $\mathfrak{a}\in\mathcal{A}$, the elliptic curve $F_{\mathfrak{a}}$ has full 2-torsion, and hence is a quadratic twist of a Legendre elliptic curve F_λ, where there are in fact six possible choices for λ. Define

$$\mathfrak{S} = \{-t^2 : t\in\mathbb{Q}\}\cup\{2t^2 : t\in\mathbb{Q}\}.$$

We partition $\mathcal{A}$ into two disjoint subsets, $\mathcal{A}^{(I)}$ and $\mathcal{A}^{(II)}$.

$\mathcal{A}^{(I)}$: This consists of $\mathfrak{a}\in\mathcal{A}$ such that at least one of the λ-invariants of $F_{\mathfrak{a}}$ lies outside $\mathfrak{S}$.

$\mathcal{A}^{(II)}$: This consists of $\mathfrak{a}\in\mathcal{A}$ such that every λ-invariant of $F_{\mathfrak{a}}$ is in $\mathfrak{S}$.

The precise construction of the character $\chi_{\mathfrak{a}}$ in the proof of Proposition 6.1 depends on whether $\mathfrak{a}$ belongs to $\mathcal{A}^{(I)}$ or $\mathcal{A}^{(II)}$, but in either case it is closely related to the λ-invariants of $F_{\mathfrak{a}}$.

We require some preliminary results.

LEMMA 6.2. *Let $F/\mathbb{Q}$ be an elliptic curve of conductor M, semistable away from 2 (i.e., with M^{odd} squarefree), having full rational 2-torsion. Let $\lambda\in\mathbb{Q}$ be any of the six λ-invariants of F. Then the following hold*:

(i) $\mathrm{ord}_p(\lambda) = \mathrm{ord}_p(1-\lambda) = 0$ *for all odd primes p of good reduction for F.*

(ii) *Let $\omega\in\{\pm1,\pm2\}$, and let χ be the unique primitive quadratic character of conductor N that satisfies*

$$\chi(p) = \left(\frac{\omega\cdot\lambda}{p}\right) \tag{18}$$

for odd primes p with $\mathrm{ord}_p(\lambda)=0$. Then $N^{\mathrm{odd}} \mid M$.

Proof. As F has full rational 2-torsion and is semistable away from 2, it has a model of the form

$$F : Y^2 = X(X-a)(X-b),$$

where a, b, $a-b$ are nonzero integers with no odd prime common factors. The primes dividing M^{odd} are precisely the odd primes dividing $ab(a-b)$. Since the six associated λ-invariants are

$$b/a,\ \ a/b,\ \ (a-b)/a,\ \ a/(a-b),\ \ b/(b-a)\ \text{ and }\ (b-a)/b,$$

the lemma follows immediately. □

LEMMA 6.3. *Let $p \equiv 3 \pmod 4$ be prime, and suppose that $F/\mathbb{F}_p$ is an elliptic curve of the form*

$$F : Y^2 = X(X-1)(X-\eta^2)$$

for some $\eta \in \mathbb{F}_p \setminus \{0, 1, -1\}$. Then $F(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proof. Since F has full rational 2-torsion, it is enough to show that $F/\mathbb{F}_p$ has a point of order 4 or, in other words, that one of the three points of order 2 is 2-divisible. We know $(a, b) \in F(\mathbb{F}_p)$ is 2-divisible if a, $a-1$ and $a-\eta^2$ are all squares. Suppose $(1, 0)$ is not 2-divisible. Then $1-\eta^2$ is not a square. As $p \equiv 3 \pmod 4$, it follows that $\eta^2 - 1$ is a square. Thus the point $(\eta^2, 0)$ is 2-divisible. □

We are now ready to apply this to the elliptic curves $F_{\mathfrak{a}}$ that arise from solutions to (2).

LEMMA 6.4. *Let $k \geq 10^8$, and suppose that $\ell > \exp(10^k)$ is prime. Assume that (n, d, k, y, ℓ) is a nontrivial solution to equation (2). Let $\mathfrak{a} \in \mathcal{A}$, and let λ be any of the six λ-invariants of $F_{\mathfrak{a}}$. If $p \equiv 3 \pmod 8$ is a prime in the interval $k/2 < p \leq k$, then*

$$\left(\frac{\lambda}{p}\right) = -1.$$

Proof. From Lemma 5.2, we know that p is a prime of good supersingular reduction for $F_{\mathfrak{a}}$. Lemma 6.2 tells us that $\mathrm{ord}_p(\lambda) = \mathrm{ord}_p(1-\lambda) = 0$, whence p is a prime of good reduction for F_λ. Now F_λ is a quadratic twist of $F_{\mathfrak{a}}$ and so must also have supersingular reduction at p. In particular, $a_p(F_\lambda) = 0$, so that

$$\#F_\lambda(\mathbb{F}_p) = p + 1 \equiv 4 \pmod 8.$$

On the other hand, if we suppose that λ is a square modulo p, then we know from Lemma 6.3 that $8 \mid \#F_\lambda(\mathbb{F}_p)$. The resulting contradiction completes the proof. □

Proof of Proposition 6.1 for $\mathfrak{a} \in \mathcal{A}^{(I)}$. We are ready to prove Proposition 6.1 for $\mathfrak{a} \in \mathcal{A}^{(I)}$. Fix a λ-invariant of $F_{\mathfrak{a}}$ with $\lambda \notin \mathfrak{S}$. Suppose first that $\lambda = t^2$ or $\lambda = -2t^2$ for some nonzero rational t. By the results of [32], the assumption that $k \geq 2 \times 10^{10}$ forces the existence of (many) primes

$p \equiv 3 \pmod 8$ in the interval $k/2 < p \le k$. For each such prime, we have $\left(\frac{\lambda}{p}\right) = 1$, contradicting Lemma 6.4. We may therefore suppose

$$\lambda \notin \{\pm t^2 : t \in \mathbb{Q}\} \cup \{\pm 2t^2 : t \in \mathbb{Q}\}. \tag{19}$$

If a and m are relatively prime integers, we write

$$\vartheta(X; a, m) = \sum_{\substack{p \le X \\ p \equiv a \bmod m}} \log p$$

for the first Chebychev function associated to the arithmetic progression a mod m. Here, the sum is over primes p. By [32], using the inequality $k \ge 2 \times 10^{10}$, we have

$$\sum_{\substack{k/2 < p \le k \\ p \equiv 3 \bmod 8}} \log p \;=\; \vartheta(k; 3, 8) - \vartheta(k/2; 3, 8) \ge (1 - 3\varepsilon) \cdot \frac{k}{8},$$

where $\varepsilon = 0.002811$. From Lemma 6.4, we thus have

$$\sum_{\substack{k/2 < p \le k \\ p \equiv 3 \bmod 8}} -\left(\frac{\lambda}{p}\right) \log p \;\ge\; (1 - 3\varepsilon) \cdot \frac{k}{8}. \tag{20}$$

Let μ_i be the primitive quadratic Dirichlet characters that on odd primes p away from the support of λ are given by

$$\mu_1(p) = \left(\frac{\lambda}{p}\right), \quad \mu_2(p) = \left(\frac{-\lambda}{p}\right), \quad \mu_3(p) = \left(\frac{2\lambda}{p}\right) \quad \text{and} \quad \mu_4(p) = \left(\frac{-2\lambda}{p}\right),$$

and observe that

$$\mu_1(p) - \mu_2(p) - \mu_3(p) + \mu_4(p) = \begin{cases} 4\left(\frac{\lambda}{p}\right) & \text{if } p \equiv 3 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

We may thus rewrite inequality (20) as

$$\sum_{k/2 < p \le k} (-\mu_1(p) + \mu_2(p) + \mu_3(p) - \mu_4(p)) \log p \;\ge\; (1 - 3\varepsilon) \cdot \frac{k}{2},$$

whereby there necessarily exists some $i \in \{1, 2, 3, 4\}$ such that

$$\left| \sum_{k/2 < p \le k} \mu_i(p) \log(p) \right| \ge (1 - 3\epsilon) \cdot \frac{k}{8}. \tag{21}$$

We let $\chi_{\mathfrak{a}} = \mu_i$ and write $N_{\mathfrak{a}}$ for its conductor. From (19), we have $N_{\mathfrak{a}}^{\text{odd}} \ne 1$. Moreover, by Lemma 6.2 we have $N_{\mathfrak{a}}^{\text{odd}} \mid M_{\mathfrak{a}}$. Finally, the left-hand side of (16) agrees with the left-hand side of (21), except on $m = q^r$ where q is prime and $r \ge 2$. Thus the difference between the two sums is bounded by

$$|\psi(k) - \vartheta(k) - \psi(k/2) + \vartheta(k/2)|,$$

where ϑ and ψ are the first and second Chebychev functions. From (5.3*) and (5.4*) of Theorem 6* of Schoenfeld [35], we have (16) as desired. This completes the proof of Proposition 6.1 in Case (I).

Legendre elliptic curves revisited. Let $\lambda \in \mathbb{Q} \setminus \{0, 1\}$, F_λ be as in (17), and suppose that p is an odd prime satisfying $\mathrm{ord}_p(\lambda) = \mathrm{ord}_p(1-\lambda) = 0$. We will need to use the 2-descent homomorphism:

$$\Theta_\lambda : F_\lambda(\mathbb{F}_p) \to \mathbb{F}_p^*/\mathbb{F}_p^{*2} \times \mathbb{F}_p^*/\mathbb{F}_p^{*2} \times \mathbb{F}_p^*/\mathbb{F}_p^{*2}, \qquad \Theta_\lambda(Q) = (\theta_1(Q), \theta_2(Q), \theta_3(Q)).$$

The kernel of Θ_λ is precisely $2F_\lambda(\mathbb{F}_p)$. If $Q \neq (0,0)$, then $\theta_1(Q) = x(Q)\mathbb{F}_p^{*2}$. If $Q \neq (1,0)$, then $\theta_2(Q) = (x(Q)-1)\mathbb{F}_p^{*2}$. If $Q \neq (\lambda, 0)$, then $\theta_3(Q) = (x(Q)-\lambda)\mathbb{F}_p^{*2}$. Moreover, $\theta_1(Q)\theta_2(Q)\theta_3(Q) = 1\mathbb{F}_p^{*2}$ for all $Q \in F_\lambda(\mathbb{F}_p)$, which allows us to compute Θ_λ even for the points of order 2.

LEMMA 6.5. *Let F_{-1} be as in (17) and $p \equiv 5 \pmod 8$ be prime. Then $2^3 \parallel \#F_{-1}(\mathbb{F}_p)$.*

Proof. We use the fact that 2 represents the class of nonsquares in $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$. The images of the points of order 2 under Θ_{-1} are

$$\Theta_{-1}(0,0) = (1,1,1), \qquad \Theta_{-1}(1,0) = (1,2,2), \qquad \Theta_{-1}(-1,0) = (1,2,2).$$

It follows that only $(0,0)$ is 2-divisible. We find that $2(i, 1-i) = (0,0)$ (where $i^2 = -1$ in $\mathbb{F}_p$). The points of order 4 are $(i, 1-i)$, $(i,1-i)+(0,0)$, $(i,1-i)+(1,0)$, $(i,1-i)+(-1,0)$. The images of all of these under Θ_{-1} have $i\mathbb{F}_p^{*2}$ as first coordinate. This is not a square in $\mathbb{F}_p$ (as $p \equiv 5 \pmod 8$) and hence none of the points of order 4 are 2-divisible. It follows that $2^3 \parallel \#F_{-1}(\mathbb{F}_p)$. □

Some preliminary results for $\mathfrak{a} \in \mathcal{A}^{(II)}$. Let $\mathfrak{a} \in \mathcal{A}^{(II)}$. The proof of Proposition 6.1 in this case is a little harder and requires some further preparation. By the definition of $\mathcal{A}^{(II)}$, every λ-invariant of $F_\mathfrak{a}$ belongs to the set $\mathfrak{S}$. Note that, if λ is any of the λ-invariants of $F_\mathfrak{a}$ and we write

$$\lambda_1 = \lambda, \quad \lambda_2 = 1 - \lambda \quad \text{and} \quad \lambda_3 = (\lambda - 1)/\lambda,$$

then the six λ-invariants of $F_\mathfrak{a}$ are precisely $\lambda_i^{\pm 1}$ with $i = 1, 2$ and 3. If we have that $\lambda = -t^2$ for some rational number t, it follows that necessarily there exists a rational number v such that $\lambda_2 = 2v^2$ (whence $\lambda_3 = 2(v/t)^2$). Similarly, if we have $\lambda = 2t^2$ for $t \in \mathbb{Q}$, then either λ_2 or λ_3 is of the shape $2v^2$ for rational v. In all cases, renaming if necessary, we deduce the existence of (positive) rational numbers t and v such that

$$\lambda = 2t^2 \quad \text{and} \quad 1 - \lambda = 2v^2, \tag{22}$$

whereby $2t^2 + 2v^2 = 1$.

LEMMA 6.6. *Let $k \geq 10^8$, and suppose that $\ell > \exp(10^k)$ is prime. Let (n, d, k, y, ℓ) be a nontrivial solution to equation (2) with corresponding $\mathcal{A}$. Let $\mathfrak{a} \in \mathcal{A}$, and suppose that λ, one of the six λ-invariants of $F_{\mathfrak{a}}$, satisfies (22) for positive rational numbers t and v. If $p \equiv 5 \pmod 8$ is prime with $k/2 < p \leq k$, then $\operatorname{ord}_p(t) = \operatorname{ord}_p(v) = 0$ and*

$$\left(\frac{tv}{p}\right) = 1.$$

Proof. Fix a prime $p \equiv 5 \pmod 8$ with $k/2 < p \leq k$. By Lemma 5.2, p is a prime of good reduction for both $E_{\mathfrak{a}}$ and $F_{\mathfrak{a}}$, and we have $a_p(E_{\mathfrak{a}}) = a_p(F_{\mathfrak{a}})$. By Lemma 6.2, $\operatorname{ord}_p(\lambda) = \operatorname{ord}_p(1-\lambda) = 0$ and so, from (22), $\operatorname{ord}_p(t) = \operatorname{ord}_p(v) = 0$. From the proof of Lemma 5.2, the reduction of $E_{\mathfrak{a}}$ modulo p is a quadratic twist of F_{-1}, whereby $a_p(F_{\mathfrak{a}}) = a_p(E_{\mathfrak{a}}) = \pm a_p(F_{-1})$. On the other hand, F_λ is a quadratic twist of $F_{\mathfrak{a}}$ and so $a_p(F_\lambda) = \pm a_p(F_{-1})$. If we consider also the quadratic twist of F_λ by 2,

$$F'_\lambda : Y^2 = X(X-2)(X-2\lambda),$$

since 2 is a nonsquare modulo p, it follows that $a_p(F'_\lambda) = -a_p(F_\lambda)$. Thus either $a_p(F_\lambda) = a_p(F_{-1})$ or $a_p(F'_\lambda) = a_p(F_{-1})$. Since Lemma 6.5 implies that $2^3 \parallel \#F_{-1}(\mathbb{F}_p)$, we may conclude that either $2^3 \parallel \#F_\lambda(\mathbb{F}_p)$ or $2^3 \parallel \#F'_\lambda(\mathbb{F}_p)$.

Now let Θ be the 2-descent map for $F_\lambda/\mathbb{F}_p$ as given previously. From (22), we find that

$$\Theta(0,0) = (2,1,2), \quad \Theta(1,0) = (1,2,2) \quad \text{and} \quad \Theta(\lambda,0) = (2,2,1).$$

It follows that none of the points of order 2 are 2-divisible, and so $2^3 \nmid \#F_\lambda(\mathbb{F}_p)$. Hence $2^3 \parallel \#F'_\lambda(\mathbb{F}_p)$.

We denote the 2-descent map for F'_λ by Θ'. The images of the points of order 2 in F'_λ are

$$\Theta'(0,0) = (2,2,1), \quad \Theta'(2,0) = (2,2,1) \quad \text{and} \quad \Theta'(2\lambda,0) = (1,1,1).$$

It follows that only $(2\lambda, 0)$ is 2-divisible. Let i be any square-root of -1 in $\mathbb{F}_p$ and set

$$P = \left(4ivt + 2\lambda, (128iv^5 - 64iv^3)t - 128v^6 + 96v^4 - 16v^2\right) \in E(\mathbb{F}_p).$$

Then $2P = (2\lambda, 0)$ and so P is a point of order 4. Writing $\Theta' = (\theta'_1, \theta'_2, \theta'_3)$, we have that $\theta'_3(P) = 4itv \cdot \mathbb{F}_p^{*2}$. Suppose

$$\left(\frac{4itv}{p}\right) = 1.$$

Then $\theta'_3(P) = 1$ and so $\Theta'(P) = (1,1,1)$ or $(2,2,1)$. (Recall that the product of the entries is a square.) Hence either $\Theta'(P) = (1,1,1)$ or $\Theta'(P + (0,0)) = (1,1,1)$. It follows that one of the points of order 4 is 2-divisible and so $F'_\lambda(\mathbb{F}_p)$

contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, contradicting the fact that $2^3 \,\|\, \#F'_\lambda(\mathbb{F}_p)$. We therefore have that

$$\left(\frac{4itv}{p}\right) = -1,$$

and hence the fact that i is a nonsquare modulo p completes the proof. □

Proof of Proposition 6.1 *for* $\mathfrak{a} \in \mathcal{A}^{(II)}$. By an easy modification of our earlier argument, but now using Lemma 6.6 in place of Lemma 6.4, the inequality (16) is satisfied, where now $\chi_\mathfrak{a}$ is a primitive quadratic character that for odd primes away from the support of tv is given by

$$\chi_\mathfrak{a}(p) = \left(\frac{\omega \cdot tv}{p}\right)$$

for some $\omega \in \{\pm 1, \pm 2\}$ that depends only on $\mathfrak{a}$. Again we write $N_\mathfrak{a}$ for the conductor of $\chi_\mathfrak{a}$.

We would like to show that $N_\mathfrak{a}^{\mathrm{odd}} \mid M_\mathfrak{a}$. We may choose a model for $F_\mathfrak{a}$ of the form $Y^2 = X(X-a)(X-b)$ where a, b and $a-b$ are nonzero integers, with no odd prime common factors, and we have

$$2t^2 = \lambda = b/a \quad \text{and} \quad 2v^2 = 1 - \lambda = (a-b)/a.$$

Thus the odd primes appearing in the support of $\omega \cdot tv$ are primes dividing a, b or $a-b$. As $\chi_\mathfrak{a}$ is quadratic, $N_\mathfrak{a}^{\mathrm{odd}}$, the odd part of its conductor, is squarefree. On the other hand, the primes dividing $M_\mathfrak{a}^{\mathrm{odd}}$ are precisely the odd primes dividing $ab(a-b)$, whereby $N_\mathfrak{a}^{\mathrm{odd}} \mid M_\mathfrak{a}$ as required.

Finally, we must prove that $N_\mathfrak{a}^{\mathrm{odd}} \neq 1$. Suppose $N_\mathfrak{a}^{\mathrm{odd}} = 1$. Then $tv = \pm\alpha^2$ or $tv = \pm 2\alpha^2$ for some positive rational α. We have chosen t and v positive, whereby necessarily $tv = \alpha^2$ or $tv = 2\alpha^2$. Write $t = T/U$ and $v = V/U$ where, without loss of generality, T, V and U are positive integers with $\gcd(U, V, T) = 1$. Then, from (22),

$$2T^2 + 2V^2 = U^2,$$

and hence T and V are odd and coprime, while $U \equiv 2 \pmod 4$. In particular, $2 \mid \mathrm{ord}_2(tv)$, and so we may conclude that $tv = \alpha^2$. It follows that TV is a positive integer square and hence, since T and V are coprime and positive, each is itself an integer square, say $T = T_0^2$ and $V = V_0^2$, where T_0 and V_0 are positive. Writing $U = 2U_0$, we thus have

$$T_0^4 + V_0^4 = 2U_0^2,$$

whereby, from a classical descent argument, $T_0 = V_0 = U_0 = 1$, and so $\lambda = 1/2$. In particular, $F_\mathfrak{a}$ is isomorphic (possibly over a quadratic extension) to the elliptic curve $Y^2 = X(X-1)(X-1/2)$ with j-invariant 1728 and complex multiplication by $\mathbb{Z}[i]$. It follows that $F_\mathfrak{a}$ has complex multiplication and hence the image of $\overline{\rho}_{F_\mathfrak{a},\ell}$ is contained in the normalizer of a Cartan subgroup of

$\mathrm{GL}_2(\mathbb{F}_\ell)$. As $\overline{\rho}_{E_{\mathfrak{a}},\ell} \sim \overline{\rho}_{F_{\mathfrak{a}},\ell}$, the same is trivially true for $\overline{\rho}_{E_{\mathfrak{a}},\ell}$. It follows from the work of Lemos [25] (building on the results of Darmon and Merel [10] and of Bilu, Parent and Rebolledo [5]) that $E_{\mathfrak{a}}$ also has complex multiplication. If we let $a = a_{\mathfrak{a}}$, $b = b_{\mathfrak{a}}$ and $c = c_{\mathfrak{a}}$ be as in (8), we find that the j-invariant of $E_{\mathfrak{a}}$ is

$$j = 2^8 \frac{(a^2 - bc)^3}{a^2 b^2 c^2}.$$

Since $E_{\mathfrak{a}}$ has complex multiplication, j is integral. The fact that a, b and c are coprime thus implies that each of a, b and c is not divisible by odd primes. As $a + b + c = 0$, we quickly deduce that two out of a, b and c are equal. If $a = b$ or $c = b$, then

$$n + id = -2(n + jd) \quad \text{or} \quad n + (2j - i)d = -2(n + jd),$$

which imply that

$$3n = -(2j + i)d \quad \text{or} \quad 3n = (i - 4j)d.$$

Since $\gcd(n, d) = 1$, it follows that $d \mid 3$, contradicting Lemma 4.1. We thus have $a = c$ and so $n + id = n + (2j - i)d$, whence $d = 0$. The resulting contradiction completes the proof of Proposition 6.1.

7. The Prime Number Theorem

Henceforth we fix a nontrivial solution (n, d, k, y, ℓ) to equation (2) (with corresponding $\mathcal{A}$) and suppose that ℓ and k satisfy the assumptions of Proposition 6.1. By this proposition, $N_{\mathfrak{a}}^{\mathrm{odd}} \neq 1$, and therefore $\chi_{\mathfrak{a}}$ is *nontrivial* for each $\mathfrak{a} \in \mathcal{A}$, a fact that will be crucial in obtaining a bound for k.

We shall make use of the Prime Number Theorem for Dirichlet characters. Let us begin by defining what we mean by *exceptional conductors* and *exceptional zeros* for Dirichlet L-functions; here we combine Theorems 5.26 and 5.28 of [19].

PROPOSITION 7.1. *There exists an effectively computable absolute constant $c^* > 0$ such that the following hold*:

(i) *If χ_1 and χ_2 are distinct real, primitive quadratic characters of conductor N_1 and N_2, respectively, with associated L-functions $L(s, \chi_1)$ and $L(s, \chi_2)$ having real zeros β_{χ_1} and β_{χ_2}, respectively, then*

$$\min\{\beta_{\chi_1}, \beta_{\chi_2}\} < 1 - \frac{3c^*}{\log(N_1 N_2)}. \tag{23}$$

(ii) *If χ is any primitive, quadratic character of conductor N, then $L(s, \chi)$ has at most a single real zero β_χ with*

$$1 - \frac{c^*}{\log N} < \beta_\chi < 1. \tag{24}$$

If such a zero exists, then χ is necessarily real and β_χ is a simple zero. We term β_χ an exceptional zero and N an exceptional conductor.

From this, if $N_1 < N_2$ are two exceptional conductors, with corresponding exceptional zeros β_{χ_1} and β_{χ_2}, then, combining (23) and (24),

$$1 - \frac{c^*}{\log N_1} < \min\{\beta_{\chi_1}, \beta_{\chi_2}\} < 1 - \frac{3c^*}{\log(N_1 N_2)},$$

and so

$$N_2 > N_1^2. \tag{25}$$

The following quite explicit version of the Prime Number Theorem for Dirichlet characters is Theorem 5.27 of [19].

THEOREM 5. *Let χ be a primitive Dirichlet character of conductor N. Then*

(26)

$$\sum_{m \le X} \chi(m)\Lambda(m) = \delta_\chi X - \frac{X^{\beta_\chi}}{\beta_\chi} + O\left(X \exp\left(\frac{-c \log X}{\sqrt{\log X} + \log N}\right) \cdot (\log N)^4\right).$$

Here $\delta_\chi = 0$ unless χ is trivial, in which case $\delta_\chi = 1$. Moreover, $c > 0$ is an absolute effective constant, and the implied constant is absolute. Also β_χ denotes the exceptional zero if present, otherwise the term $-X^{\beta_\chi}/\beta_\chi$ is to be omitted.

It is worth observing at this point that the "error term" here is actually smaller than the main term (so that the statement in nontrivial), only for suitably small conductor N, relative to the interval of summation X; i.e., only when $\log N \ll \log^\kappa X$ for some $\kappa < 1$. We wish to apply this result to characters of conductor roughly $N_{\mathfrak{a}}$, over an interval of length $k/2$. The difficulty we encounter is that, a priori, the $N_{\mathfrak{a}}$ can be as large as e^k and, even on average, are of size that grows polynomially in k. Further, the potential presence of an exceptional (Siegel-Landau) zero β_χ additionally complicates matters, even when we have $N_{\mathfrak{a}}$ much smaller than k, as the term on the right-hand side of (26) corresponding to β_χ can, potentially, be very close to k in size. If, however, we are able to show that we can find sufficiently many $\mathfrak{a}$ for which $N_{\mathfrak{a}}$ is "tiny," we can use the fact that exceptional conductors are rare (as quantified in inequality (25), a "repulsion principle" due to Landau), to reach the desired conclusion:

PROPOSITION 7.2. *Let us suppose that $0 < c_1 < 1$ is fixed and, further, that there is a subset $\mathcal{D}$ of $\mathcal{A}$ such that the following hold*:

(i) $P(N_{\mathfrak{a}}) \neq P(N_{\mathfrak{a}'})$ *whenever* $\mathfrak{a} \neq \mathfrak{a}'$ *belong to* $\mathcal{D}$;
(ii) $P(N_{\mathfrak{a}}) < (\log k)^{1-c_1}$ *for all* $\mathfrak{a} \in \mathcal{D}$;

(iii) *we have*

$$\sum_{\mathfrak{a}\in\mathcal{D}} \frac{1}{P(N_{\mathfrak{a}})} \geq 0.166. \tag{27}$$

Then there exists an effectively computable constant k_1, depending only upon c_1, such that $k \leq k_1$.

We will later apply this proposition with $c_1 = 10^{-4}$. The constant 0.166 is chosen so that, in our argument, we have enough progressions $\mathfrak{a}$ to guarantee that either one corresponds to a nonexceptional conductor, or, through appeal to (25), that the smallest exceptional conductor $N_{\mathfrak{a}}$ we encounter satisfies $N_{\mathfrak{a}} \leq 400000$, contradicting work of Platt [30].

To prove Proposition 7.2, it is convenient for us to be able to deduce an explicit upper bound upon $N_{\mathfrak{a}}$, given one for $P(N_{\mathfrak{a}})$.

LEMMA 7.3. *Let N the conductor of a quadratic character, and let $P(N)$ be the largest prime factor of N. Then $P(N) > 0.94 \log N$.*

Proof. We can write $N = 2^{\kappa} N_1$, where N_1 is squarefree and $\kappa \in \{0, 1, 2\}$. Then

$$\log N \leq \kappa \log 2 + \sum_{p \leq P(N)} \log p < \kappa \log 2 + 1.000081 P(N),$$

via work of Schoenfeld [35, p. 160]. We thus have

$$\frac{P(N)}{\log(N)} > 0.9999 \left(1 - \frac{\kappa \log 2}{\log(N)}\right).$$

The desired result is then immediate if $\kappa = 0$ (i.e., unless $4 \mid N$). If $\kappa = 1$, we have the claimed inequality, unless $N \leq 105932$, while, for $\kappa = 2$, the conclusion follows for all $N \geq 1.2 \times 10^{10}$. A (relatively) short computation, checking values of $N \equiv 4 \pmod 8$ up to 105932 and $N \equiv 8 \pmod{16}$ to 1.2×10^{10} with, in each case, the odd part of N squarefree, completes the proof; the minimum value of $P(N)/\log(N)$ is attained at $N = 24$. □

Proof of Proposition 7.2. Suppose there is some $\mathfrak{a} \in \mathcal{D}$ such that the character $\chi_{\mathfrak{a}}$ is nonexceptional. By assumption (ii) and Lemma 7.3, $\log N_{\mathfrak{a}} < 1.07 (\log k)^{1-c_1}$. Applying Theorem 5, we have

$$\sum_{k/2 < m \leq k} \chi_{\mathfrak{a}}(m) \Lambda(m) = O\left(k \exp\left(-c'(\log k)^{c_1}\right) \cdot (\log k)^4\right)$$

for some effectively computable positive constant c', contradicting (16) for k sufficiently large.

We may therefore suppose that $\chi_{\mathfrak{a}}$ is exceptional for every $\mathfrak{a} \in \mathcal{D}$. We obtain, from assumption (i), a sequence of exceptional conductors

$$N_1 < N_2 < \cdots < N_s,$$

where $s = \#\mathcal{D}$. From inequality (25), $N_j > N_1^{2^{j-1}}$, whence, via Lemma 7.3,

$$P(N_j) > 0.94 \cdot 2^{j-1} \log N_1$$

for each j. By assumption (27),

$$0.166 \leq \sum_{j=1}^{s} \frac{1}{P(N_j)} < \frac{2.13}{\log N_1},$$

whereby

$$N_1 \leq 373743,$$

contradicting work of Platt [30], which rules out exceptional zeros corresponding to Dirichlet characters, for every conductor smaller than 400000. □

8. Consequences of having enough characters $\chi_{\mathfrak{a}}$ with smooth, small conductors

In the previous section, we stated a result (Proposition 7.2) that guarantees an effective upper bound upon k, provided we have suitably many $\mathfrak{a}$ with $P(N_{\mathfrak{a}})$ "tiny," i.e., with $N_{\mathfrak{a}}$ very smooth. In this section, we will show that, in fact, we can reach the same conclusion if we have a (potentially) much larger number of somewhat less smooth conductors corresponding to $\mathfrak{a} \in \mathcal{A}$.

PROPOSITION 8.1. *Suppose that $c_2 > 10$ is a constant and that there exists a subset $\mathcal{B} \subset \mathcal{A}$ such that*

(i) $\#\mathcal{B} > 17 \log k$;
(ii) *for every distinct pair* $\mathfrak{a}$, $\mathfrak{a}' \in \mathcal{B}$ *we have* $\chi_{\mathfrak{a}} \neq \chi_{\mathfrak{a}'}$;
(iii) $P(N_{\mathfrak{a}}) \leq k^{7/16}$ *for all* $\mathfrak{a} \in \mathcal{B}$;
(iv) $N_{\mathfrak{a}} < k^{c_2}$.

Then there is an effectively computable constant k_2, depending only upon c_2, such that $k \leq k_2$.

Here, the constants 17 and 7/16 can be slightly sharpened, but this is not of great importance for our argument.

The proof of Proposition 8.1 relies upon a combination of ingredients, including the large sieve and upper bounds for character sums over short intervals. We begin with the latter.

8.1. *Character sums over short intervals.* We shall need a standard theorem on short character sums to a smooth modulus, a variant of some results of Graham and Ringrose [15]. Specifically, we will appeal to [19, Th. 12.13].

THEOREM 6. *Let π_i be characters of conductor q_i for $1 \leq i \leq r$. Write $q = q_1$, and suppose that $q > 1$ is squarefree with $\gcd(q, q_2 q_3 \cdots q_r) = 1$.*

Suppose, moreover, that π_1 is primitive. Then, for $R \geq R_0$, where

$$R_0 = \max(q_2, \dots, q_r, q^{1/4})\, q^{5/4},$$

we have

$$\left| \sum_{M < m \leq M+R} \pi_1 \cdots \pi_{r-1}\pi_r(m) \right| \leq 4R \cdot \left(\tau(q)^{r^2}/q\right)^{2^{-r}},$$

where $\tau(q)$ is the number of divisors of q.

We will prove the following:

PROPOSITION 8.2. *Let $c_2 > 0$ be a constant. Then there exist effectively computable positive constants k_3 and c_3, each depending only on c_2, such that the following holds. Let $k \geq k_3$ be an integer, and suppose that χ_1 and χ_2 are distinct primitive quadratic characters modulo N_1 and N_2, respectively, where the N_i satisfy*

$$P(N_i) \leq k^{7/16} \quad \text{and} \quad N_i \leq k^{c_2} \quad \text{for } i \in \{1, 2\}. \tag{28}$$

Then

$$\left| \sum_{k/2 < m \leq k} \chi_1(m)\chi_2(m) \right| \leq k^{1-c_3}. \tag{29}$$

Proof. Let $\chi = \chi_1\chi_2$, and write $M = \operatorname{lcm}(N_1, N_2)$ for the conductor of χ. We can thus rewrite $\chi = \eta\psi$, where η is *primitive* of conductor M_1 and ψ is *principal* of conductor M_2 with $M = M_1M_2$ and $\gcd(M_1, M_2) = 1$. As η is quadratic, we see that M_1^{odd} is squarefree. Clearly, $M_2 \mid \gcd(N_1, N_2)$, and so M_2^{odd} is also squarefree. From (28),

$$P(M) \leq k^{7/16} \quad \text{and} \quad M \leq k^{2c_2}. \tag{30}$$

We shall consider two cases, according to whether $M_1 \geq 8k^{7/32}$ or $M_1 < 8k^{7/32}$.

Case 1. Suppose first that

$$M_1 \geq 8k^{7/32}, \tag{31}$$

so that

$$M_1^{\text{odd}} \geq k^{7/32}.$$

We can write

$$\eta = \pi_1 \cdots \pi_s \quad \text{and} \quad \psi = \pi_{s+1} \cdots \pi_r,$$

where π_i is primitive of modulus q_i for $i = 1, \dots, s$ and principal of modulus q_i for $i = s+1, \dots, r$. Moreover, the q_i (which could be composite) may be chosen to satisfy

(a) $q_1q_2 \cdots q_s = M_1$ and $q_{s+1}q_{s+2} \cdots q_r = M_2$;
(b) $q_1 \mid M_1^{\text{odd}}$ and so $\gcd(q_1, q_2q_3 \cdots q_r) = 1$;

(c) $k^{7/32} \le q_i \le k^{7/16}$, for $i = 1, \dots, s-1$ and $i = s+1, \dots, r-1$;
(d) $1 < q_r \le k^{7/16}$; and
(e) $s \ge 1$, and if $s > 1$, then $1 \le q_s \le k^{7/16}$.

Now, from property (c) and (30),

$$r - 2 \le \log M / \log(k^{7/32}) < 10c_2,$$

whence $r < 10c_2 + 2$. In the notation of Theorem 6, we have that

$$R_0 \le k^{7/16} \cdot (k^{7/16})^{5/4} \le k^{63/64} < k/2.$$

Notice here that, at least in this argument, we cannot replace the exponent 7/16 in (28) with one larger than 4/9.

We will now apply Theorem 6. Let $q = q_1$ and note that we have (see, e.g., page 334 of [19])

$$\tau(q) \le q^{1/\log\log 3q}$$

for all $q \ge 1$. As $q \ge k^{7/32}$ and $r < 10c_2 + 2$, we see that for k suitably large,

$$\tau(q)^{r^2} < q^{1/2}.$$

Appealing to Theorem 6, we thus have

$$\left| \sum_{k/2 < m \le k} \chi_1(m)\chi_2(m) \right| \le \frac{2k}{q^{1/2^{r+1}}},$$

whence inequality (29) follows from $q \ge k^{7/32}$ and $r < 10c_2 + 2$. Explicitly, we may take $c_3 = 2^{-10c_2-6}$. This completes the proof of Proposition 8.2 in Case 1.

Case 2. Next, suppose instead that

$$M_1 < 8k^{7/32}.$$

Since χ_1 and χ_2 are distinct, it follows that $\chi = \chi_1\chi_2$ is not principal, and so

$$\left| \sum_{k/2 < m \le k} \chi_1(m)\chi_2(m) \right| < M = M_1 M_2.$$

To complete the proof of (29), we may thus certainly suppose that

$$M_2 > k^{3/4}.$$

Write μ for the Möbius function, and recall that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Now we can write

$$\begin{aligned}\sum_{k/2<m\le k}\chi_1(m)\chi_2(m) &= \sum_{k/2<m\le k}\eta(m)\psi(m)\\ &= \sum_{\substack{k/2<m\le k\\ \gcd(m,M_2)=1}}\eta(m)\\ &= \sum_{k/2<m\le k}\eta(m)\sum_{d\mid\gcd(m,M_2)}\mu(d)\\ &= \sum_{d\mid M_2}\sum_{k/2<nd\le k}\eta(nd)\mu(d)\\ &= \sum_{d\mid M_2}\eta(d)\mu(d)\sum_{k/(2d)<n\le k/d}\eta(n).\end{aligned}$$

As η is nonprincipal and has conductor $M_1 < 8k^{7/32}$, we have

$$\left|\sum_{k/(2d)<n\le k/d}\eta(n)\right| < M_1 < 8k^{7/32}.$$

Thus

$$\left|\sum_{k/2<m\le k}\chi_1(m)\chi_2(m)\right| < \tau(M_2)\cdot 8k^{7/32} \le M_2^{1/\log\log 3M_2}\cdot 8k^{7/32}.$$

The proof is complete for k sufficiently large as $k^{3/4} < M_2 < k^{c_2}$. □

8.2. *Proof of Proposition* 8.1: *The large sieve.* We make use of the following inequality of Bombieri (Proposition 1 of [6], attributed there to Selberg).

THEOREM 7. *If* $\mathbf{x}, \mathbf{y}_1, \dots, \mathbf{y}_m$ *are vectors in an inner product space, then*

$$\sum_{i=1}^{m}|\mathbf{x}\cdot\mathbf{y}_i|^2 \le \|\mathbf{x}\|^2\cdot\max_{1\le i\le m}\left\{\sum_{j=1}^{m}|\mathbf{y}_i\cdot\mathbf{y}_j|\right\}.$$

In view of (16), to prove Proposition 8.1, it clearly suffices to show that

$$\frac{1}{\#\mathcal{B}}\sum_{\mathfrak{a}\in\mathcal{B}}\left|\sum_{k/2<m\le k}\chi_{\mathfrak{a}}(m)\cdot\Lambda(m)\right|^2 \le \varpi\cdot k^2 \tag{32}$$

for k sufficiently large, where $\varpi = 0.1239^2$.

Let $\mathbf{x} = (\Lambda(m))_{k/2<m\le k}$ and, for each $\mathfrak{a}\in\mathcal{B}$, choose corresponding $\mathbf{y}_{\mathfrak{a}} = (\chi_{\mathfrak{a}}(m))_{k/2<m\le k}$ so that the desired inequality (32) can be rewritten as

$$\frac{1}{\#\mathcal{B}}\sum_{\mathfrak{a}\in\mathcal{B}}|\mathbf{x}\cdot\mathbf{y}_{\mathfrak{a}}|^2 \le \varpi\cdot k^2. \tag{33}$$

Applying the large sieve (Theorem 7), we have

$$\frac{1}{\#\mathcal{B}}\sum_{\mathfrak{a}\in\mathcal{B}}|\mathbf{x}\cdot\mathbf{y}_{\mathfrak{a}}|^2 \le \|\mathbf{x}\|^2\cdot\max_{\mathfrak{a}\in\mathcal{B}}\left\{\frac{1}{\#\mathcal{B}}\sum_{\mathfrak{a}'\in\mathcal{B}}|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}'}|\right\}. \tag{34}$$

Let us begin by noting that

$$\begin{aligned}\|\mathbf{x}\|^2 &= \sum_{k/2<m\le k}\Lambda(m)^2\\ &\le \log k\sum_{k/2<m\le k}\Lambda(m)\\ &= \frac{k\log k}{2}+O(k),\end{aligned}$$

from the Prime Number Theorem. Further, for each $\mathfrak{a}\in\mathcal{B}$, we have

$$|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}}|\le\frac{k+1}{2}.$$

As $\#\mathcal{B}\ge 17\log k$ (assumption (i)), it follows that

$$\frac{|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}}|}{\#\mathcal{B}}\le\frac{k+1}{34\log k}.$$

Next, we would like to estimate $\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}'}$ for $\mathfrak{a}\ne\mathfrak{a}'$ belonging to $\mathcal{B}$. Assumptions (ii), (iii), (iv) ensure that $\chi_{\mathfrak{a}}$, $\chi_{\mathfrak{a}'}$ satisfy the conditions of Proposition 8.2, which gives

$$|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}'}| = \left|\sum_{k/2<m<k}\chi_1(m)\chi_2(m)\right|\le k^{1-c_3}.$$

Hence, from (34),

$$\begin{aligned}\frac{1}{\#\mathcal{B}}\sum_{\mathfrak{a}\in\mathcal{B}}|\mathbf{x}\cdot\mathbf{y}_{\mathfrak{a}}|^2 &\le \|\mathbf{x}\|^2\cdot\max_{\mathfrak{a}\in\mathcal{B}}\left\{\frac{|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}}|}{\#\mathcal{B}}+\max_{\mathfrak{a}'\ne\mathfrak{a}}|\mathbf{y}_{\mathfrak{a}}\cdot\mathbf{y}_{\mathfrak{a}'}|\right\}\\ &\le \left(\frac{k\log k}{2}+O(k)\right)\cdot\left(\frac{k+1}{34\log k}+k^{1-c_3}\right)\\ &= \frac{k^2}{68}\cdot(1+o(1)).\end{aligned} \tag{35}$$

As $1/68<\varpi^2$, we have inequality (33), as desired, for k suitably large. This completes the proof of Proposition 8.1.

9. **Generating enough characters**

We now wish to sieve the set $\mathcal{A}$ carefully, hoping to guarantee the existence of suitably many corresponding characters $\chi_{\mathfrak{a}}$ with conductors smooth enough and small enough to enable us to employ either Proposition 7.2 or Proposition 8.1. There are (at least) two approaches we can take here to find a

reasonable quantity of smooth characters, both dependent upon leaving a positive proportion of elements in $\mathcal{A}$ after application of our sieve. We could, for example, appeal to a theorem of Varnavides [45] that guarantees that a set of positive density in $\{0, 1, \dots, k-1\}$ contains $\gg k^2$ nontrivial 3-term arithmetic progressions, and then average over these progressions. Instead, we will rely upon an explicit version of a theorem of Roth on 3-term arithmetic progressions, together with an old argument of Erdős. An apparent (small) advantage of this approach is that it will lead to explicit and reasonably small values for c_2 in Proposition 8.1. We begin by stating

THEOREM 8 (Roth). *Let $0 < \delta < 1$. Then there exists a positive constant $K_0(\delta)$ such if $k \geq K_0(\delta)$ and $J \subset \{0, 1, \dots, k-1\}$ with $\#J \geq \delta k$, then there is at least one nontrivial 3-term arithmetic progressions in J; i.e., there exist integers $0 \leq i < j$ such that i, j and $2j - i$ all belong to J.*

Note here that, following work of Rahman [31], for example, we may take

$$K_0(\delta) = \exp(\exp(132 \log(2) \cdot \delta^{-1})). \tag{36}$$

Let us define our index set $I = \{0, 1, \dots, k-1\}$ and recall that $\mathcal{A}$ is the set of 3-term arithmetic progressions $(i, j, 2j - i)$ in I, i.e., the set of integer triples $(i, j, 2j - i)$, satisfying $0 \leq i < j$ and $2j - i < k$. For a prime p, write

$$I_p = \{i \in I : p \mid (n + id)\},$$

so that

$$\#I_p = \delta_p \left(\frac{k}{p} + \theta_p \right),$$

where $|\theta_p| < 1$ and

$$\delta_p = \begin{cases} 1 & \text{if } p \nmid d, \\ 0 & \text{if } p \mid d. \end{cases}$$

We will now use Theorem 8, together with an elementary argument of Erdős, to find an element of $\mathfrak{a} \in \mathcal{A}$ with corresponding conductor $N_{\mathfrak{a}}$ that is smooth, small, and coprime to a given "thin" set of primes. We will do this in completely explicit form to provide an indication of the size of the constants involved here (and, in particular, to demonstrate an admissible value for c_2 in Proposition 8.1).

PROPOSITION 9.1. *Let us suppose that*

$$k \geq \exp(\exp(10^6)) \tag{37}$$

is an integer and that $S \subset [1, k]$ is a set of primes satisfying

$$\sum_{p \in S} \frac{1}{p} < 0.17. \tag{38}$$

Then there exists an $\mathfrak{a} \in \mathcal{A}$ *satisfying the following*:

(I) $p \nmid N_{\mathfrak{a}}$ *for* $p \in S$;
(II) $P(N_{\mathfrak{a}}) \le k^{7/16}$;
(III) $N_{\mathfrak{a}}$ *is not divisible by primes in the range* $((\log k)^{1-10^{-4}}, 10^4 \log k]$;
(IV) $N_{\mathfrak{a}} < k^{418}$.

Proof. Suppose k satisfies (37). Let us define T as the set of primes in the interval $(k^{7/16}, k]$ and U as the primes in the interval $((\log k)^{1-10^{-4}}, 10^4 \log k]$. Set

$$J = I \setminus \bigcup_{p \in S \cup T \cup U} I_p.$$

Notice that if $\mathfrak{a} = (i, j, 2j - i)$ is an arithmetic progression in J, then $(n + id)$, $(n + jd)$ and $(n + (2j - i)d)$ are each not divisible by any prime p in S, T or U. By (9) and Proposition 6.1, the conductor $N_{\mathfrak{a}}$ therefore satisfies (I), (II) and (III).

Our initial goal will be to show that the set J has positive density in I. Note that

$$\# \bigcup_{p \in S \cup T \cup U} I_p \le \sum_{p \in S} \# I_p + \sum_{p \in T} \# I_p + \sum_{p \in U} \# I_p.$$

Now

$$\sum_{p \in T} \# I_p = \sum_{k^{7/16} < p \le k} \delta_p \left(\frac{k}{p} + \theta_p \right),$$

and hence we have

$$\sum_{p \in T} \# I_p < k \sum_{k^{7/16} < p \le k/2} \frac{1}{p} + \frac{0.6k}{\log k},$$

where we have used the fact that $\delta_p = 0$ for all $k/2 < p \le k$, Theorem 1 of Rosser and Schoenfeld [34], which yields the inequalities

$$\frac{x}{\log x} \left(1 + \frac{1}{2 \log x} \right) < \pi(x) < \frac{x}{\log x} \left(1 + \frac{3}{2 \log x} \right),$$

provided $x \ge 59$, and (37). From Theorem 5 of Rosser and Schoenfeld [34], we have

$$\left| \sum_{p \le x} \frac{1}{p} - \log \log x - \tau \right| < \frac{1}{2 \log^2 x},$$

valid for $x \ge 286$, where τ is an absolute constant (explicitly, $\tau = 0.26149\ldots$), and hence

$$\sum_{k^{7/16} < p \le k/2} \frac{1}{p} < \log(16/7) + \log \left(1 - \frac{\log 2}{\log k} \right) + \frac{1}{2 \log^2 (k/2)} + \frac{128}{49 \log^2 k}.$$

From (37), we thus have

$$\sum_{k^{7/16}<p\le k/2}\frac{1}{p}<\log(16/7)-\frac{0.6}{\log k}$$

and hence

$$\sum_{p\in T}\#I_p\le\log(16/7)\cdot k.$$

Moreover,

$$\sum_{p\in U}\frac{1}{p}<\log\left(\frac{\log\log k+\log 10^4}{(1-10^{-4})\log\log k}\right)+\frac{1}{\log^2\left((\log k)^{1-10^{-4}}\right)}$$

and so, from (37),

$$\sum_{p\in U}\frac{1}{p}<\log\left(1/(1-10^{-4})\right)+\frac{5\log 10}{\log\log k},$$

whence

$$\sum_{p\in U}\#I_p\le\log\left(1/(1-10^{-4})\right)k+\frac{5\log(10)\,k}{\log\log k}+10^4\log k.$$

From (38), we have, crudely,

$$\sum_{p\in S}\#I_p\le 0.17\,k+\pi(k)<0.17k+\frac{1.1k}{\log k}.$$

Thus

$$\#\bigcup_{p\in S\cup T\cup U}I_p\le(\log(16/7)+\log(1/(1-10^{-4}))+0.17)k+\frac{12k}{\log\log k}f,$$

and hence, from (37), we have

$$\#\bigcup_{p\in S\cup T\cup U}I_p<0.9968\,k.$$

It follows that

$$\#J=\#I-\#\bigcup_{p\in S\cup T\cup U}I_p>0.0032k,$$

so that, in particular, J is nonempty (and, as noted earlier, possesses the property that any arithmetic progression $\mathfrak{a}=(i,j,2j-i)$ in J has corresponding $N_{\mathfrak{a}}$ satisfying (I), (II) and (III)). From Theorem 8, it is immediate that there exist nontrivial 3-term arithmetic progressions $\mathfrak{a}$ in J; it remains to show that at least one of them has property (IV), i.e., satisfies $N_{\mathfrak{a}}\le k^{418}$.

We now follow a classic argument of Erdős (see, e.g., Lemma 3 of [12], or, in the context of arithmetic progressions, displayed equation (3.6) of [24]),

defining a set $J_1 \subset J$, obtained by deleting from J, for each prime $p \le k$, an index i_p with the property that $\mathrm{ord}_p(A_{i_p})$ is maximal. It follows that

$$\#J_1 > 0.0032k - \pi(k) > 0.00319k$$

and, more importantly for our purposes, that

$$\prod_{i \in J_1} A_i \mid (k-1)!.$$

Since no prime $p \ge k^{7/16}$ divides any of these A_i, Stirling's formula (see, e.g., [43] for a suitably explicit version) thus implies that

$$\prod_{i \in J_1} A_i \le \sqrt{2\pi(k-1)}((k-1)/e)^{k-1} e^{1/(12(k-1))} \prod_{k^{7/16} < p \le k} p^{-\mathrm{ord}_p((k-1)!)}.$$

Now

$$\log\left(\prod_{k^{7/16} < p \le k} p^{\mathrm{ord}_p((k-1)!)}\right) \ge \sum_{k^{7/16} < p \le k} \left(\frac{k-1}{p} - 1\right) \log p \ge \frac{9}{16} k \log k - 5k$$

using Theorem 5 of [44], Theorem 6 of [34] and our assumption (37). Hence, after a little work,

$$\prod_{i \in J_1} A_i < k^{0.44k}.$$

It follows, if we define $J_2 \subset J_1$ to be the set of indices $i \in J_1$ with the property that $A_i \le k^{139}$, that $\#J_2 > 0.00001k$. Checking that in (36) we have

$$K_0(10^{-5}) < \exp(\exp(10^6)),$$

we may thus apply Theorem 8 (Roth's theorem) to deduce the existence of a nontrivial 3-term arithmetic progression of indices $\mathfrak{a} = (i, j, 2j-i)$ in J_2. By (9)

$$N_{\mathfrak{a}} \le 2^8 \cdot A_i A_j A_{2j-i} \le 2^8 \cdot (k^{139})^3 < k^{418}.$$

This concludes the proof of Proposition 9.1. □

10. **Proof of Theorem 2**

We are now ready to prove Theorem 2. To begin, note that there exists a nonempty subset $\mathcal{B} \subset \mathcal{A}$ satisfying

(i) $P(N_{\mathfrak{a}}) \ne P(N_{\mathfrak{a}'})$ whenever $\mathfrak{a} \ne \mathfrak{a}'$ in $\mathcal{B}$;
(ii) $P(N_{\mathfrak{a}}) \le k^{7/16}$ for all $\mathfrak{a} \in \mathcal{B}$;
(iii) $N_{\mathfrak{a}}$ is not divisible by primes in the range $[(\log k)^{1-10^{-4}}, 10^4 \log k]$, for all $\mathfrak{a} \in \mathcal{B}$;
(iv) $N_{\mathfrak{a}} < k^{418}$ for all $\mathfrak{a} \in \mathcal{B}$.

Indeed to generate such a $\mathcal{B}$ with one element, we may simply apply Proposition 9.1 with $S = \emptyset$. Now let $\mathcal{B}$ be a *maximal* nonempty subset of $\mathcal{A}$ satisfying (i)–(iv). If $\#\mathcal{B} > 17 \log k$, then k is effectively bounded by Proposition 8.1. We may thus suppose that $\#\mathcal{B} \le 17 \log k$. Assume first that

$$\sum_{\mathfrak{a} \in \mathcal{B}} \frac{1}{P(N_{\mathfrak{a}})} < 0.17.$$

It follows, if we let $S = \{P(N_{\mathfrak{a}}) : \mathfrak{a} \in \mathcal{B}\}$, that S satisfies (38). Proposition 9.1 thus yields the existence of some $\mathfrak{a} \in \mathcal{A}$ that satisfies (ii), (iii), (iv) and, moreover, has the property that $N_{\mathfrak{a}}$ is not divisible by any prime in S. Thus $P(N_{\mathfrak{a}}) \neq P(N_{\mathfrak{a}'})$ for $\mathfrak{a}' \in \mathcal{B}$. Now the set $\mathcal{B}' = \mathcal{B} \cup \{\mathfrak{a}\}$ is strictly larger than $\mathcal{B}$ and satisfies conditions (i)–(iv), contradicting the maximality of $\mathcal{B}$.

We may thus assume that

$$\sum_{\mathfrak{a} \in \mathcal{B}} \frac{1}{P(N_{\mathfrak{a}})} \ge 0.17.$$

Define

$$\mathcal{C} = \{\mathfrak{a} \in \mathcal{B} : P(N_{\mathfrak{a}}) > 10^4 \log k\}$$

and

$$\mathcal{D} = \{\mathfrak{a} \in \mathcal{B} : P(N_{\mathfrak{a}}) < (\log k)^{1-10^{-4}}\}.$$

Then, by condition (iii), $\mathcal{B}$ is the disjoint union of $\mathcal{C}$ and $\mathcal{D}$. It follows that

$$\sum_{\mathfrak{a} \in \mathcal{C}} \frac{1}{P(N_{\mathfrak{a}})} \le \frac{\#\mathcal{C}}{10^4 \log k} \le \frac{\#\mathcal{B}}{10^4 \log k} \le \frac{17 \log k}{10^4 \log k} = 0.0017,$$

whereby

$$\sum_{\mathfrak{a} \in \mathcal{D}} \frac{1}{P(N_{\mathfrak{a}})} \ge 0.1683.$$

We now apply Proposition 7.2 with $c_1 = 10^{-4}$ to deduce that k is bounded. This completes the proof of Theorem 2.

11. **Concluding remarks**

Much of the literature on (2) has, in fact, dealt with the somewhat more general equation

$$n(n+d)\cdots(n+(k-1)d) = by^{\ell}, \tag{39}$$

where b is an integer, all of whose prime factors are bounded above by k. The arguments we have presented here do not permit us to treat quite such a general situation, but can be extended to handle equation (39) where $P(b)$, the greater prime factor of b, is at most τk, for $\tau < 1/2$.

While we have given our results in Section 6 on characters attached to nontrivial solutions to (2) only for large values of k, analogous statements

are readily obtained for smaller k. These provide us with a way to prove that the number of nontrivial solutions to (2) is finite that is much more computationally efficient than that described in [1]. Since the lower bound upon k in Theorem 2 is so large, however, there is little chance we can treat all the remaining cases $k \leq k_0$ by such an approach, without the introduction of fundamentally new ideas.

12. **Addendum**

In this addendum, we will sketch an approach that leads from Proposition 6.1 to a contradiction, while avoiding many of our more delicate analytic and combinatorial arguments. This was communicated to the authors by Andrew Granville [16] and is reproduced here with his permission.

To start, we note that via Theorem 5.26 of [19] (a result dating back to Landau and Page), there exists a positive constant c such that every zero of every Dirichlet L-function corresponding to a primitive character of modulus $q \leq T$ (where $T \geq 2$) necessarily has real part β satisfying

$$\beta < 1 - \frac{c}{\log T},$$

with at most a single exception, corresponding to, say, $q_1 \leq T$. For a given large positive integer k, let us define

$$T = \exp\left(\frac{c \log k}{3 \log\log k}\right). \tag{40}$$

Further let $\mathcal{Q}(k)$ denote the set of integers $q \leq Q := k^4$ for which there exists a primitive character $\chi \pmod q$ for which $L(s,\chi)$ has a zero $\beta + it$ with $|t| \leq T$ and

$$\beta > 1 - \frac{3 \log\log k}{\log k} = 1 - \frac{c}{\log T}. \tag{41}$$

PROPOSITION 12.1. *The set $\mathcal{Q}(k)$ contains $\ll (\log k)^{61}$ elements. Its smallest element is $\geq \log k$, and all of its other elements are $\geq k^{\delta/\log\log k}$ for some constant $\delta > 0$.*

Proof. Let $N(\sigma, T, \chi)$ count the number of zeros $\rho = \beta + it$ of $L(s,\chi)$ with $\beta \geq \sigma$ and $|t| \leq T$. From a result of Selberg (referenced immediately below the statement of Théorème 14 of [7]), we have that, for $T \geq 2$ and $\epsilon > 0$,

$$\sum_{q \leq Q} \sum_{\substack{\chi \pmod q \\ \chi \text{ primitive}}} N(\sigma, T, \chi) \ll_\epsilon \left(Q^{5+\epsilon} T^{3+\epsilon}\right)^{1-\sigma}.$$

Choosing $\sigma = 1 - \frac{3 \log\log k}{\log k}$ and ϵ suitably small thus implies that

$$\#\mathcal{Q}(k) \ll (\log k)^{61}.$$

From the choice of c, there is at most a single value $q_1 \le T$ with a zero with real part satisfying (41). If this zero exists, it must be real and, via Proposition 1.11 of [2], is bounded above by $1 - \frac{40}{\sqrt{q_1}\log^2 q_1}$, whence

$$1 - \frac{3\log\log k}{\log k} < 1 - \frac{40}{\sqrt{q_1}\log^2 q_1}.$$

It follows then that $q_1 > \log k$ for suitably large k. All of the other elements of $\mathcal{Q}(k)$ are necessarily at least $T = k^{\delta/\log\log k}$ with $\delta = c/3$. □

PROPOSITION 12.2. *If $q \le Q = k^4$ and $q \notin \mathcal{Q}(k)$, then*

$$\sum_{k/2<m\le k} \chi(m)\cdot\Lambda(m) \ll \frac{k}{\log k}.$$

Proof. From Proposition 5.25 of [19], if χ is a nonprincipal character modulo q with corresponding L-function $L(s,\chi)$, we have that

$$\sum_{m\le k} \chi(m)\cdot\Lambda(m) = -\sum_{\substack{L(\beta+it,\chi)=0\\ \beta>0,\ |t|\le T}} \frac{k^\rho}{\rho} + O\left(\log k + \frac{k(\log qk)^2}{T}\right),$$

where T is as in (40). Since $q \notin \mathcal{Q}(k)$,

$$|k^\rho| \le k^{1-\frac{3\log\log k}{\log k}} = k/(\log k)^3,$$

whereby it follows that

$$\left|\sum_{\substack{L(\beta+it,\chi)=0\\ \beta>0,\ |t|\le Q}} \frac{k^\rho}{\rho}\right| \le \frac{k}{(\log k)^3} \sum_{\substack{L(\beta+it,\chi)=0\\ \beta>0,\ |t|\le Q}} \frac{1}{|\rho|} \ll \frac{k}{\log k};$$

here, the last inequality follows from the standard proof of the Prime Number Theorem in Arithmetic Progressions (see, e.g., [2]). □

From this result, in conjunction with Proposition 6.1, it suffices to show that, for some $\mathfrak{a} \in \mathcal{A}$, the corresponding conductor $N_\mathfrak{a} \notin \mathcal{Q}(k)$ while also $N_\mathfrak{a} \le k^4$.

PROPOSITION 12.3. *For any given coprime nonzero integers a and d, let $\mathcal{N}_{a,d}$ denote the set of integers n, $0 \le n \le k-1$ for which $a+nd$ is divisible by some integer r, where r is a divisor of some $q \in \mathcal{Q}(k)$ with $r \ge q^{1/3}/2$. Then $\#\mathcal{N}_{a,d} \ll k/(\log k)^{1/4}$.*

Proof. The number of integers in the progression

$$a, a+d, \ldots, a+(k-1)d$$

divisible by r is at most $k/r + O(1) \ll k/r$, which is $\ll k/q^{1/3}$ if $r \geq q^{1/3}/2$. Therefore the number divisible by some integer r, where r is a divisor of some q with $r \geq q^{1/3}/2$, is $\ll \tau(q)k/q^{1/3} \ll k/q^{1/4}$, where $\tau(q)$ denotes the number of divisors of q. Therefore

$$\#\mathcal{N}_{a,d} \ll \frac{k}{q_1^{1/4}} + \sum_{\substack{q \in \mathcal{Q}(k), \\ q > k^{\delta/\log\log k}}} \frac{k}{q^{1/4}} \ll \frac{k}{(\log k)^{1/4}} + (\log k)^{61} k^{1 - \frac{\delta}{4\log\log k}},$$

where the latter inequality is a consequence of Proposition 12.1. The result thus follows. □

From the last result, almost all 3-term arithmetic progressions of integers $\leq k$ contain no element of $\mathcal{N}_{a,d}$. We can select one such progression, say, $\mathfrak{a}$, corresponding to

$$n + id = A_i y_i^\ell,\ n + jd = A_j y_j^\ell,\ n + (2j - i)d = A_{2j-i} y_{2j-i}^\ell,$$

where, appealing to the aforementioned argument of Erdős (as in, say, [24]), we may suppose that, say,

$$N_\mathfrak{a} \leq 8 A_i A_j A_{2j-i} \leq k^4.$$

Since $N_\mathfrak{a}^{\text{odd}}$ is the largest odd squarefree divisor of $A_i A_j A_{2j-i}$, it follows that

$$\gcd(N_\mathfrak{a}, A_i) \cdot \gcd(N_\mathfrak{a}, A_j) \cdot \gcd(N_\mathfrak{a}, A_{2j-i}) \geq N_\mathfrak{a}/8$$

and so at least one of $\gcd(N_\mathfrak{a}, A_i), \gcd(N_\mathfrak{a}, A_j)$ or $\gcd(N_\mathfrak{a}, A_{2j-i})$ is a divisor of $N_\mathfrak{a}$ that is at least $N_\mathfrak{a}^{1/3}/2$ in size. Since we have chosen $\mathfrak{a}$ to contain no element of $\mathcal{N}_{a,d}$, we necessarily have that $N_\mathfrak{a} \notin \mathcal{Q}(k)$, whereby Proposition 12.2 contradicts Proposition 6.1.

References

[1] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu, Powers from products of consecutive terms in arithmetic progression, *Proc. London Math. Soc.* (3) **92** no. 2 (2006), 273–306. MR 2205718. Zbl 1178.11033. https://doi.org/10.1112/S0024611505015625.

[2] M. A. Bennett, G. Martin, K. O'Bryant, and A. Rechnitzer, Explicit bounds for primes in arithmetic progressions, *Illinois J. Math.* **62** no. 1-4 (2018), 427–532. MR 3922423. Zbl 07036793. https://doi.org/10.1215/ijm/1552442669.

[3] M. A. Bennett and S. Siksek, Rational points on Erdős-Selfridge superelliptic curves, *Compos. Math.* **152** no. 11 (2016), 2249–2254. MR 3577894. Zbl 1407.11081. https://doi.org/10.1112/S0010437X16007569.

[4] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* **56** no. 1 (2004), 23–54. MR 2031121. Zbl 1053.11025. https://doi.org/10.4153/CJM-2004-002-2.

[5] Y. Bilu, P. Parent, and M. Rebolledo, Rational points on $X_0^+(p^r)$, *Ann. Inst. Fourier* (*Grenoble*) **63** no. 3 (2013), 957–984. MR 3137477. Zbl 1307.11075. https://doi.org/10.5802/aif.2781.

[6] E. Bombieri, A note on the large sieve, *Acta Arith.* **18** (1971), 401–404. MR 0286773. Zbl 0219.10055. https://doi.org/10.4064/aa-18-1-401-404.

[7] E. Bombieri, Le grand crible dans la théorie analytique des nombres, *Astérisque* no. 18 (1987), 103 pp. MR 0891718. Zbl 0618.10042. Available at http://www.numdam.org/item/AST_1987__18__1_0/.

[8] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** no. 4 (2001), 843–939. MR 1839918. Zbl 0982.11033. https://doi.org/10.1090/S0894-0347-01-00370-8.

[9] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** no. 6 (1995), 513–543. MR 1348707. Zbl 0838.11023. https://doi.org/10.1112/blms/27.6.513.

[10] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem, *J. Reine Angew. Math.* **490** (1997), 81–100. MR 1468926. Zbl 0976.11017. https://doi.org/10.1515/crll.1997.490.81.

[11] N. D. Elkies, Distribution of supersingular primes, in *Journées Arithmétiques*, 1989 (Luminy, 1989), *Astérisque* no. 198-200, Soc. Math. France, Paris, 1991, pp. 127–132 (1992). MR 1144318. Zbl 0754.14019. Available at http://www.numdam.org/item/AST_1991__198-199-200__127_0/.

[12] P. Erdős, On the product of consecutive integers. III, *Nederl. Akad. Wet., Proc. Ser. A.* **58** (1955), 85–90. MR 0067915. Zbl 0068.03704.

[13] P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301. MR 0376517. Zbl 0295.10017. https://doi.org/10.1215/ijm/1256050816.

[14] P. Erdös, C. L. Stewart, and R. Tijdeman, Some diophantine equations with many solutions, *Compositio Math.* **66** no. 1 (1988), 37–56. MR 0937987. Zbl 0639.10014. Available at http://www.numdam.org/item?id=CM_1988__66_1_37_0.

[15] S. W. Graham and C. J. Ringrose, Lower bounds for least quadratic nonresidues, in *Analytic Number Theory* (*Allerton Park, IL*, 1989), *Progr. Math.* **85**, Birkhäuser Boston, Boston, MA, 1990, pp. 269–309. MR 1084186. Zbl 0719.11006. https://doi.org/10.1007/978-1-4612-3464-7_18.

[16] A. Granville, personal communication.

[17] K. Győry, Power values of products of consecutive integers and binomial coefficients, in *Number Theory and its Applications* (Kyoto, 1997), *Dev. Math.* **2**, Kluwer Acad. Publ., Dordrecht, 1999, pp. 145–156. MR 1738813. Zbl 1074.11502.

[18] K. Győry, L. Hajdu, and A. Pintér, Perfect powers from products of consecutive terms in arithmetic progression, *Compos. Math.* **145** no. 4 (2009), 845–864. MR 2521247. Zbl 1194.11043. https://doi.org/10.1112/S0010437X09004114.

[19] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, *Amer. Math. Soc. Colloq. Publ.* **53**, Amer. Math. Soc., Providence, RI, 2004. MR 2061214. Zbl 1059.11001. https://doi.org/10.1090/coll/053.

[20] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I, *Invent. Math.* **178** no. 3 (2009), 485–504. MR 2551763. Zbl 1304.11041. https://doi.org/10.1007/s00222-009-0205-7.

[21] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. II, *Invent. Math.* **178** no. 3 (2009), 505–586. MR 2551764. Zbl 1304.11042. https://doi.org/10.1007/s00222-009-0206-6.

[22] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, *Grad. Texts in Math.* **97**, Springer-Verlag, New York, 1984. MR 0766911. Zbl 0804.11039. https://doi.org/10.1007/978-1-4684-0255-1.

[23] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* **49** no. 6 (1997), 1139–1161. MR 1611640. Zbl 0908.11017. https://doi.org/10.4153/CJM-1997-056-2.

[24] S. Laishram and T. N. Shorey, Perfect powers in arithmetic progressions, *J. Comb. Number Theory* **7** no. 2 (2015), 95–110. MR 3537553. Zbl 1386.11062.

[25] P. Lemos, Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies, *Trans. Amer. Math. Soc.* **371** no. 1 (2019), 137–146. MR 3885140. Zbl 06993229. https://doi.org/10.1090/tran/7198.

[26] J. Liouville, Sur le produit $m(m+1)(m+2)\dots(m+n-1)$, *J. Math. Pures Appl.* **2** (1857), 277–278. Available at https://gallica.bnf.fr/ark:/12148/bpt6k164012/f285n2.capture.

[27] R. Marszałek, On the product of consecutive elements of an arithmetic progression, *Monatsh. Math.* **100** no. 3 (1985), 215–222. MR 0812613. Zbl 0582.10011. https://doi.org/10.1007/BF01299269.

[28] G. Martin, Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$, *J. Number Theory* **112** no. 2 (2005), 298–331. MR 2141534. Zbl 1095.11026. https://doi.org/10.1016/j.jnt.2004.10.009.

[29] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** no. 2 (1978), 129–162. MR 0482230. Zbl 0386.14009. https://doi.org/10.1007/BF01390348.

[30] D. J. Platt, Numerical computations concerning the GRH, *Math. Comp.* **85** no. 302 (2016), 3009–3027. MR 3522979. Zbl 1345.11064. https://doi.org/10.1090/mcom/3077.

[31] M. Rahman, Roth's theorem on 3-term arithmetic progressions. Available at https://pdfs.semanticscholar.org/34d5/e5d802d1107b68f1aa76dff994e8b23341c2.pdf.

[32] O. Ramaré and R. Rumely, Primes in arithmetic progressions, *Math. Comp.* **65** no. 213 (1996), 397–425. MR 1320898. Zbl 0856.11042. https://doi.org/10.1090/S0025-5718-96-00669-2.

[33] K. A. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** no. 2 (1990), 431–476. MR 1047143. Zbl 0773.11039. https://doi.org/10.1007/BF01231195.

[34] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94. MR 0137689. Zbl 0122.05001. https://doi.org/10.1215/ijm/1255631807.

[35] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II, *Math. Comp.* **30** no. 134 (1976), 337–360. MR 0457374. Zbl 0326.10037. https://doi.org/10.2307/2005976.

[36] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR 0644559. Zbl 0496.12011. Available at http://archive.numdam.org/article/PMIHES_1981__54__123_0.pdf.

[37] J-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** no. 1 (1987), 179–230. MR 0885783. Zbl 0641.10026. https://doi.org/10.1215/S0012-7094-87-05413-5.

[38] T. N. Shorey, Some exponential Diophantine equations, in *New Advances in Transcendence Theory* (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 352–365. MR 0972011.

[39] T. N. Shorey, Perfect powers in products of arithmetical progressions with fixed initial term, *Indag. Math.* (*N.S.*) **7** no. 4 (1996), 521–525. MR 1620124. Zbl 0874.11034. https://doi.org/10.1016/S0019-3577(97)89137-9.

[40] T. N. Shorey, Diophantine approximations, Diophantine equations, transcendence and applications, *Indian J. Pure Appl. Math.* **37** no. 1 (2006), 9–39. MR 2254063. Zbl 1207.11074.

[41] T. N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetical progression, *Compositio Math.* **75** no. 3 (1990), 307–344. MR 1070417. Zbl 0708.11021. Available at http://www.numdam.org/item?id=CM_1990__75_3_307_0.

[42] S. Siksek, The modular approach to Diophantine equations, in *Explicit Methods in Number Theory*, *Panor. Synthèses* **36**, Soc. Math. France, Paris, 2012, pp. 151–179. MR 3098134. Zbl 1343.11042. https://doi.org/10.1007/978-0-387-49894-2_7.

[43] K. R. Stromberg, *Introduction to Classical Real Analysis*, *Wadsworth Internat. Math. Ser.*, Wadsworth International, Belmont, Calif., 1981. MR 0604364. Zbl 0454.26001.

[44] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, *Cambridge Stud. Adv. Math.* **46**, Cambridge Univ. Press, Cambridge, 1995, translated from the second French edition (1995) by C. B. Thomas. MR 1342300. Zbl 0831.11001.

[45] P. Varnavides, On certain sets of positive density, *J. London Math. Soc.* **34** (1959), 358–360. MR 0106865. Zbl 0088.25702. https://doi.org/10.1112/jlms/s1-34.3.358.

[46] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* (2) **141** no. 3 (1995), 443–551. MR 1333035. Zbl 0823.11029. https://doi.org/10.2307/2118559.

(Received: September 4, 2017)

University of British Columbia, Vancouver, B.C., Canada
E-mail: bennett@math.ubc.ca

Mathematics Institute, University of Warwick, Coventry, United Kingdom
E-mail: S.Siksek@warwick.ac.uk