Glasgow Math. J. **52** (2010) 453–472. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S0017089510000340.

A GENERALISED KUMMER'S CONJECTURE

M. J. R. MYERS*
Department of Mathematics and Statistics, Calvin College, Grand Rapids, MI 49546, USA
e-mail: mjm49@calvin.edu

(Received 25 June 2008; revised 4 August 2009; accepted 10 April 2010)

Abstract. Kummer's conjecture predicts the rate of growth of the relative class numbers of cyclotomic fields of prime conductor. We extend Kummer's conjecture to cyclotomic fields of conductor n, where n is any natural number. We show that the Elliott–Halberstam conjecture implies that this generalised Kummer's conjecture is true for almost all n but is false for infinitely many n.

2010 *Mathematics Subject Classification.* Primary 11R18; Secondary 11M20.

1. Introduction. Let $\mathbb{Q}(\zeta_m)$ be the mth cyclotomic field, where ζ_m is a primitive mth root of unity for an integer $m \geq 1$. Let h_m denote the class number of $\mathbb{Q}(\zeta_m)$ and h_m^+ be the class number of its maximal real subfield $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Kummer proved that the relative class number $h_m^- = h_m/h_m^+$ is an integer, and in 1851 he claimed ([**7**, p. 473]) that the rule for the asymptotic growth of h_p^- as the prime $p \to \infty$ is given by the formula

$$\frac{p^{(p+3)/4}}{2^{(p-3)/2}\pi^{(p-1)/2}} =: G(p). \tag{1}$$

Kummer never published a proof of his claim, and the modern, rigourous reading of Kummer's assertion, that

$$\lim_{p\to\infty} \frac{h_p^-}{G(p)} = 1$$

has become well known as 'Kummer's conjecture'.

As it stands, Kummer's conjecture remains unproven; however, Ankeny and Chowla [**1**] showed that

$$\log(h_p^-/G(p)) = o(\log p)$$

as $p \to \infty$. Murty and Petridis [**9**] proved what they called the weak Kummer's conjecture. They showed that there exists a positive constant c such that

$$c^{-1} \leq \frac{h_p^-}{G(p)} \leq c$$

*Present address: School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland holds for a sequence of primes p_i, where the number of primes $p_i \le x$ is asymptotic to $x/\log x$ as $x \to \infty$. With the additional assumption of the Elliott–Halberstam conjecture, they were able to prove a stronger result. This conjecture says as follows.

CONJECTURE 1.1 (Elliott–Halberstam conjecture). For any $\delta > 0$ and any $A > 0$,

$$\sum_{k<x^{1-\delta}} \max_{(l,k)=1} \max_{y \le x} \left| \pi(y,k,l) - \frac{\operatorname{li} y}{\phi(k)} \right| \ll_{\delta,A} \frac{x}{\log^A x},$$

where $\pi(y,k,l)$ equals the number of primes $p \le y$ such that $p \equiv l \bmod k$, and $\operatorname{li} y = \int_2^y \frac{dt}{\log t}$.

Murty and Petridis showed that the Elliott–Halberstam conjecture implies that for every $\epsilon > 0$ there exists an x_ϵ such that

$$1 - \epsilon < \frac{h_p^-}{G(p)} < 1 + \epsilon$$

holds for all primes $x_\epsilon < p \le x$, with the exception of a set $P(\epsilon)$ such that

$$|\{p \in P(\epsilon) : x_\epsilon < p \le x\}| = o(\pi(x)).$$

Hence Kummer's conjecture concerning class numbers of cyclotomic fields is related to the density of primes in arithmetic progressions. Kummer's conjecture is also related to pairs of primes. The Hardy–Littlewood conjecture posits the existence of $\gg x/\log^2 x$ primes $p \le x$ such that $2p+1$ is also prime; in 1990 Granville [**3**] proved that the Elliott–Halberstam conjecture and the Hardy–Littlewood conjecture together imply that Kummer's conjecture is false. In that same paper Granville offered heuristic reasoning for believing that for all primes p

$$(\log\log p)^{-1/2+o(1)} \le h_p^-/G(p) \le (\log\log p)^{1/2+o(1)},$$

and that these bounds are the best possible.

More recently, Lu and Zhang [**8**] proved that for any fixed $\epsilon > 0$, there is a positive number Q depending only on ϵ such that for all primes $p \ge Q$,

$$e^{-1.4} p^{-\epsilon} (\log p)^{-1/3} \le h_p^-/G(p) \le e^{0.84} p^{\epsilon} (\log p)^{1/6}.$$

In this paper, we extend Kummer's conjecture to composite numbers; that is, for natural numbers n and a suitable function $G(n)$ (see (2.2)), the generalised Kummer's conjecture predicts that $\lim_{n\to\infty} h_n^-/G(n) = 1$. We prove a composite moduli analogue of Murty and Petridis' weak Kummer's conjecture:

THEOREM 1.2. *Let $\omega(n)$ the number of distinct prime divisors of n. Then*

$$e^{-\omega(n)} \ll \frac{h_n^-}{G(n)} \ll e^{\omega(n)}$$

holds for all but $o(x)$ natural numbers $n \le x$.

Moreover, assuming the Elliott–Halberstam conjecture, the generalised Kummer's conjecture is true for almost all n and is false for infinitely many n. More precisely, we have the following two results.

THEOREM 1.3. *Assume the Elliott–Halberstam conjecture. Then for every $\epsilon > 0$ there exists an x_ϵ such that*

$$1 - \epsilon < \frac{h_n^-}{G(n)} < 1 + \epsilon$$

holds for all natural numbers $n \geq x_\epsilon$ with the exception of $o(x)$ natural numbers $n < x$.

THEOREM 1.4. *Assume the Elliott–Halberstam conjecture. Then the generalised Kummer's conjecture fails for infinitely many natural numbers n.*

2. Generalised Kummer's conjecture. For the cyclotomic field $\mathbb{Q}(\zeta_n)$, one may obtain the formula (see [11, p. 42]):

$$h_n^- = \frac{Qw\sqrt{|d_n/d_n^+|}}{\pi^{\phi(n)/2}2^{\phi(n)/2}} \prod_{\substack{\chi \bmod n \\ \chi \text{ odd}}} L(1, \chi). \tag{2.1}$$

Here d_n is the discriminant of $\mathbb{Q}(\zeta_n)$ and d_n^+ is the discriminant of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Also, w is the number of roots of unity in $\mathbb{Q}(\zeta_n)$, and $Q = 1$ if n is a prime power p^r and $Q = 2$ otherwise.

By Proposition 2.7 in [**11**],

$$d_n = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}},$$

and by Lemma 4.19 in [**11**],

$$d_n = \begin{cases} p(d_n^+)^2 & \text{if } n = p^r \text{ with } p \neq 2, \\ 4(d_n^+)^2 & \text{if } n = 2^r, \\ (d_n^+)^2 & \text{otherwise.} \end{cases}$$

Hence, we see that

$$h_n^- = a_n \left(\frac{1}{2\pi} \sqrt{\frac{n}{\prod_{p|n} p}} \right)^{\phi(n)/2} \prod_{\substack{\chi \text{ odd} \\ \chi \bmod n}} L(1, \chi),$$

with

$$a_n = \begin{cases} 2p^{r+1/4} & \text{if } n = p^r \text{ with } p \neq 2, \\ 2^{r+1/2} & \text{if } n = 2^r, \\ 4n & \text{if odd } n \neq p^r \;, \\ 2n & \text{if even } n \neq 2^r \;. \end{cases}$$

Let

$$G(n) = a_n \left(\frac{1}{2\pi} \sqrt{\frac{n}{\prod_{p|n} p}} \right)^{\phi(n)/2}. \tag{2.2}$$

Then the composite moduli form of Kummer's conjecture may be stated as follows.

CONJECTURE 2.1 (Generalised Kummer's conjecture).

$$h_n^- \sim G(n)$$

as the natural number $n \to \infty$.

As in [**10**], we can rewrite the product of L-functions in (2.1) as

$$\prod_{\substack{\chi \bmod n \\ \chi \text{ odd}}} L(1, \chi) = \exp\left(\frac{\phi(n)}{2} f_n\right),$$

where $f_n = \lim_{x\to\infty} f_n(x)$ and $f_n(x)$ is the finite sum

$$f_n(x) = \sum_{r \le x} \frac{c_n(r)}{r}$$

with

$$c_n(r) = \begin{cases} 1 & \text{if } r = q^m \equiv 1 \bmod n, \\ -1 & \text{if } r = q^m \equiv -1 \bmod n, \\ 0 & \text{otherwise} \end{cases}$$

where q is a prime and $m \ge 1$.

Clearly, the generalised Kummer's conjecture is true if and only if $f_n = o(\frac{1}{\phi(n)})$.

3. Lemmas. We will need the following theorems which are also used in [**9**].

LEMMA 3.1 (Siegel–Walfisz theorem). *For any constant $A > 0$, there is a constant $c(A) > 0$ so that uniformly for $x \ge 3$, $1 \le k \le (\log x)^A$, $(k, l) = 1$, we have*

$$\pi(x, k, l) = \frac{\operatorname{li} x}{\phi(k)} + O\left(xe^{-c(A)\sqrt{\log x}}\right).$$

LEMMA 3.2 (Bombieri–Vinogradov theorem). *Assume $x \ge 2$. For any $A > 0$ there exists $B = B(A) > 0$ such that*

$$\sum_{k < \frac{x^{1/2}}{\log^B x}} E(x, k) \ll_A \frac{x}{\log^A x},$$

where

$$E(x, k) := \max_{y \le x} \max_{(k,l)=1} \left|\pi(y, k, l) - \frac{\operatorname{li} y}{\phi(k)}\right|.$$

LEMMA 3.3 (Brun–Titchmarsh theorem). *For $k < x$, $(k, l) = 1$,*

$$\pi(x, k, l) < \frac{2x}{\phi(k) \log(x/k)}.$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

LEMMA 3.4 ([**6**, p. 124]). *Let l be a fixed, non-zero integer, and ϵ, A, B positive real numbers, where $A > B + 30$. Then for any numbers x and X such that $x^{1/2} < X < x \log^{-A} x$ and $x > x_0(\epsilon, B)$, we have*

$$\pi(x, k, l) \le \frac{(4+\epsilon)x}{\phi(k) \log X}$$

for every k such that $X \le k \le 2X$, and $(l, k) = 1$, except for at most $X \log^{-B} x$ exceptional values of k.

LEMMA 3.5 ([**9**, p. 298]). *Fix l and k, $(l, k) = 1$. The number of primes $x < p \le 2x$ such that $kp + l$ is also prime is*

$$\ll \prod_{p_i | kl} \left(1 - \frac{1}{p_i}\right)^{-1} \frac{x}{\log^2 x},$$

uniformly for $k < x^2$.

LEMMA 3.6 ([**9**, p. 298]). *There is a constant c such that, as $T \to \infty$,*

$$\sum_{k \le T} \prod_{p_i | k} \left(1 - \frac{1}{p_i}\right)^{-1} \sim cT.$$

LEMMA 3.7 ([**10**, Corollary 3.6]). *The number of solutions $\bmod n$ to $x^m \equiv 1 \bmod n$ (or to $x^m \equiv -1 \bmod n$) is at most $2m^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisors of n.*

Let A be some constant greater than or equal to e. A slight modification of Hardy and Ramanujan's original proof in [**5**] of the normal order of $\omega(n)$ shows that the number of $n \le x$ such that $\omega(n) > A \log\log x$ is $o(\frac{x}{\log x})$. More specifically, we have

LEMMA 3.8. *For any constant $A \ge e$,*

$$|\{n \le x : \omega(n) > A \log\log x\}| \ll \frac{x}{(\log x)^{1 + A \log A - A} (\log\log x)^{1/2}}.$$

Proof. Let

$$\pi(x, k) = \sum_{\substack{n \le x \\ \omega(n) = k}} 1 \quad \text{and} \quad S = \sum_{k \ge A \log\log x} \pi(x, k+1).$$

Lemma B of [**5**] gives us the uniform upper bound

$$\pi(x, k+1) < \frac{Lx}{\log x} \frac{(\log\log x + D)^k}{k!},$$

where L and D are absolute constants. Clearly, then

$$S < \frac{Lx}{\log x} \sum_{k \ge A \log\log x} \frac{(\log\log x + D)^k}{k!}.$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Write $\xi = \log\log x + D$ and let k_1 be the smallest integer greater than $A\xi$. Then

$$\sum_{k\geq A\xi}\frac{\xi^k}{k!} < \frac{\xi^{k_1}}{k_1!}\left[1+\frac{\xi}{k_1+1}+\frac{\xi^2}{(k_1+1)(k_1+2)}+\dots\right]$$
$$< \frac{\xi^{k_1}}{k_1!}\left[1+\frac{1}{A}+\frac{1}{A^2}+\dots\right] = \frac{\xi^{k_1}}{k_1!}\left[\frac{A}{A-1}\right]$$
$$\ll \frac{e^{k_1(\log\xi-\log k_1+1)}}{\sqrt{k_1}}$$

by Stirling's formula. It follows, then, that

$$\sum_{k\geq A\xi}\frac{\xi^k}{k!} \ll \frac{e^{(A-A\log A)\xi}}{\sqrt{\xi}} \ll (\log x)^{A-A\log A}(\log\log x)^{-1/2}.$$

Thus the number of $n \leq x$ such that $\omega(n) > A\log\log x$ is

$$\ll \frac{x}{(\log x)^{1+A\log A-A}(\log\log x)^{1/2}},$$

as required. □

4. Unconditional composite moduli weak Kummer's conjecture. In this section, we will prove Theorem 1.2, the weak Kummer's conjecture for composite moduli. To remove the contributions of the prime powers q^m with $m \geq 2$ from the sum f_n, we will use the following lemma:

LEMMA 4.1.

$$\sum_{q\ prime}\sum_{m\geq 2}\frac{c_n(q^m)}{mq^m} = O\left(\frac{\omega(n)}{n}\right).$$

Proof. Write $S = \sum_{q \text{ prime}}\sum_{m\geq 2}\frac{c_n(q^m)}{mq^m}$. Then, clearly,

$$|S| \leq \sum_{q \text{ prime}}\sum_{\substack{m\geq 2\\ q^m\equiv\pm 1(n)}}\frac{1}{mq^m} = S_1 + S_2,$$

where

$$S_1 = \sum_{\substack{q \text{ prime}\\ q<n}}\sum_{\substack{m\geq 2\\ q^m\equiv\pm 1(n)}}\frac{1}{mq^m} \text{ and } S_2 = \sum_{\substack{q \text{ prime}\\ q>n}}\sum_{\substack{m\geq 2\\ q^m\equiv\pm 1(n)}}\frac{1}{mq^m}.$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Recall that $\pi(x)$ is the number of primes $p \leq x$. By the prime number theorem, we have

$$
\begin{aligned}
|S_2| \leq \sum_{\substack{q>n \\ q \text{ prime}}} \sum_{m \geq 2} q^{-m} &\ll \sum_{\substack{q>n \\ q \text{ prime}}} q^{-2} \\
&\ll \lim_{x\to\infty} \left[\frac{\pi(t)}{t^2}\right]_n^x + \int_n^x \frac{\pi(t)}{t^3} dt \\
&\ll \frac{1}{n\log n} + \int_n^\infty \frac{1}{t^2 \log t} dt \\
&\ll \frac{1}{n\log n} = o\left(\frac{1}{n}\right).
\end{aligned}
$$

We now consider $S_1 = S_3 + S_4$ with

$$
S_3 = \sum_{m\geq 2} \sum_{\substack{q<n \\ q^m \equiv 1(n)}} \frac{1}{mq^m} \text{ and } S_4 = \sum_{m\geq 2} \sum_{\substack{q<n \\ q^m \equiv -1(n)}} \frac{1}{mq^m}.
$$

For a fixed n, let $C(m)$ denote the number of solutions $x < n$ to the congruence $x^m \equiv 1 \bmod n$. By Lemma 3.7 $C(m) \leq 2m^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisors of n. This gives us the upper bound

$$
\left| \bigcup_{i=2}^{m} \{x < n : x^i \equiv 1 \bmod n\} \right| \leq \sum_{i=2}^{m} C(i) \leq \sum_{i=2}^{m} 2i^{\omega(n)} =: B(m).
$$

Observe that $B(m) \ll m^{\omega(n)+1}$.

Now for each solution $x < n$ to $x^m \equiv 1 \bmod n$, write $x^m = u_i n + 1$, where each u_i is a distinct positive integer for $i = A(m), \ldots, A(m) + C(m) - 1$. Here $A(2) = 1$, and for $m \geq 3$, $A(m) = B(m-1) + 1$. Then

$$
S_3 = \sum_{m\geq 2} \frac{1}{m} \sum_{\substack{q<n \\ q^m \equiv 1(n)}} \frac{1}{q^m} = \sum_{m\geq 2} \frac{1}{m} \left(\sum_{a=A(m)}^{B(m)} \frac{\theta_a}{u_a n + 1} \right),
$$

where for $A(m) \leq a \leq A(m) + C(m) - 1$,

$$
\theta_a = \begin{cases} 1 & \text{if } \sqrt[m]{u_a n + 1} \text{ is a prime,} \\ 0 & \text{otherwise.} \end{cases}
$$

For any $A(m) + C(m) \leq a \leq B(m)$, let $\theta_a = 0$ and $u_a = 1$. Thus

$$
S_3 < \frac{1}{n} \sum_{m\geq 2} \frac{1}{m} \left(\sum_{a=A(m)}^{B(m)} \frac{\theta_a}{u_a} \right).
$$

Let d_m be the inner sum $\sum_{a=A(m)}^{B(m)} \frac{\theta_a}{u_a}$, and write the partial sums

$$
D_2 = d_2, D_3 = d_2 + d_3, D_4 = d_2 + d_3 + d_4, \ldots.
$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Notice that for any two indices $a \neq a'$ such that θ_a and $\theta_{a'}$ are both non-zero, we must have $u_a \neq u_{a'}$, which implies that $D_r \leq \sum_{a=1}^{B(r)} a^{-1}$.

Now,

$$\sum_{m=2}^{x} \frac{d_m}{m} = \frac{D_x}{x} + \sum_{r=2}^{x-1} \frac{D_r}{r(r+1)},$$

and we get

$$\begin{aligned} 0 < S_3 &= \frac{1}{n} \sum_{m \geq 2} \frac{D_m}{m(m+1)} \\ &\ll \frac{1}{n} \sum_{m \geq 2} \frac{1}{m(m+1)} \left(\sum_{a=1}^{m^{\omega(n)+1}} \frac{1}{a} \right) \\ &\ll \frac{\omega(n)}{n} \sum_{m \geq 2} \frac{\log(m)}{m(m+1)} = O\left(\frac{\omega(n)}{n}\right). \end{aligned}$$

Similarly, we can express the sum $S_4 = \sum_{m \geq 2} \frac{1}{m} (\sum_{a=A(m)}^{B(m)} \frac{\phi_a}{v_a n - 1})$, where the values of v_a are positive integers and $\phi_a = 1$ or 0. Since

$$\sum_{a=A(m)}^{B(m)} \frac{\phi_a}{v_a n - 1} = \sum_{a=A(m)}^{B(m)} \frac{\phi_a}{v_a n + 1} + O(n^{-2}),$$

it follows that $S_4 \ll \frac{\omega(n)}{n}$ as well. $\square$

Define the sum

$$g_n(x) = \sum_{\substack{q \text{ prime} \\ q \leq x}} \frac{c_n(q)}{q},$$

and

$$g_n = \lim_{x \to \infty} g_n(x).$$

By Lemma 4.1, $f_n = g_n + O(\frac{\omega(n)}{n})$. An application of the Siegel–Walfisz Theorem (Lemma 3.1) reduces the infinite sum g_n to a finite one.

LEMMA 4.2.

$$g_n = g_n(2^n) + O(n^{-2}).$$

Proof. For $x \geq y \geq 3$, Riemann–Stieltjes integration gives

$$g_n(x) - g_n(y) = \sum_{y < q \leq x} \frac{c_n(q)}{q} = \left[\frac{A_n(t)}{t} \right]_y^x + \int_y^x \frac{A_n(t)}{t^2} dt, \tag{4.3}$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

where $A_n(t) = \pi(t, n, 1) - \pi(t, n, -1)$. Using the Siegel–Walfisz theorem and taking $x > 2^n$, we obtain $A_n(x) \ll \frac{x}{n \log^2 x}$ and so

$$\begin{aligned}|g_n(x) - g_n(2^n)| &\ll \left[\frac{A_n(t)}{t}\right]_{2^n}^{x} + \int_{2^n}^{x} \frac{A_n(t)}{t^2} dt \\ &\ll \frac{1}{n \log^2 x} - \frac{1}{n(\log 2^n)^2} + \frac{1}{n}\left[\frac{1}{\log t}\right]_{2^n}^{x} \\ &\ll \frac{1}{n^2}.\end{aligned}$$

□

We have shown

$$f_n = g_n + O\left(\frac{\omega(n)}{n}\right) = g_n(2^n) + O\left(\frac{\omega(n)}{n}\right),$$

and have reduced the problem to one of studying the finite sum

$$g_n(2^n) = \sum_{\substack{q \text{ prime}, \\ q \leq 2^n}} \frac{c_n(q)}{q}.$$

We will now find bounds on $g_n(2^n)$ by using (4.3) to partition this sum into terms on which we may apply our various estimates for $\pi(t, n, 1) - \pi(t, n, -1)$. We are now in a position to prove Theorem 1.2.

Proof. Note that

$$|A_n(t)| = |\pi(t, n, 1) - \pi(t, n, -1)| \leq 2E(t, n)$$

as defined in Lemma 3.2, the conditions of which are satisfied for $x < n \leq 2x$ and $n^2 \log^{2B} n < q < 2^n$. Hence,

$$\begin{aligned}\sum_{x<n\leq 2x} \sum_{n^2 \log^{2B} n<q<2^n} \frac{c_n(q)}{q} &\ll \left[\frac{\sum_{x<n\leq 2x} E(t, n)}{t}\right]_{n^2 \log^{2B} n}^{2^n} + \int_{n^2 \log^{2B} n}^{2^n} \frac{\sum_{x<n\leq 2x} E(t, n)}{t^2} dt \\ &\ll \left[\frac{1}{\log^A t}\right]_{x^2 \log^{2B} x}^{\infty} + \int_{x^2 \log^{2B} x}^{\infty} \frac{1}{t \log^A t} dt \\ &\ll \log^{-A+1} x.\end{aligned}$$

If we set $D(n) = g_n(2^n) - g_n(n^2 \log^{2B} n)$, then we have shown

$$\sum_{x<n<2x} |D(n)| \ll \frac{1}{\log^{A-1} x}.$$

Thus for any constant $c > 0$,

$$\#\left\{x < n \leq 2x \;:\; |D(n)| > \frac{c}{n}\right\} \ll \frac{x}{\log^{A-1} x}.$$

Take $A > 3$ in Lemma 3.2.

By dyadic decomposition we discard at most $x \log^{-A+1} x$ natural numbers, and now we restrict our attention to primes q in the range $n^2/4 < q \le n^2 \log^{2B} n$. By Lemma 3.3,

$$\sum_{n^2/4<q\le n^2\log^{2B} n} \frac{c_n(q)}{q} \ll \frac{1}{\phi(n)\log n} + \int_{n^2/4}^{n^2\log^{2B} n} \frac{1}{t\phi(n)\log(t/n)}dt$$
$$\ll \frac{1}{\phi(n)} \log\left(1+\frac{\log(\log^{2B} n)}{\log(n/4)}\right)$$
$$= o\left(\frac{1}{\phi(n)}\right).$$

That is, $g_n(n^2\log^{2B} n) - g_n(n^2/4) = o(1/n)$, and now we consider the range $2^A n \log^A n < q \le n^2/4$.

Take $X < n < 2X$ and let $2^A n\log^A n < t < n^2/4$. The conditions of Lemma 3.4 are satisfied in this range, and so

$$\sum_{2^A n\log^A n<q\le n^2/4} \frac{c_n(q)}{q} \ll \frac{1}{\phi(n)\log n} + \frac{1}{\phi(n)}\int_{2^A n\log^A n}^{n^2/4} \frac{1}{t\log t}dt$$
$$\ll \frac{1}{\phi(n)}.$$

This holds for all natural numbers $X < n < 2X$ with the exception of a set of size $\ll \frac{X}{\log^B X}$. Using dyadic decomposition, we see the number of exceptional $n < x$ is $\ll \frac{x}{\log^B x}$.

To estimate $g_n(2^A n \log^A n) - g_n(n\log n)$, we apply Lemma 3.3 again to get

$$\sum_{n\log n<q\le 2^A n\log^A n} \frac{c_n(q)}{q} \ll \frac{1}{\phi(n)}\left[\log\left(\log\frac{t}{n}\right)\right]_{n\log n}^{2^A n\log^A n}$$
$$\ll \frac{1}{\phi(n)}\log\left(1+\frac{\log(2^A\log^{A-1} n)}{\log(\log n)}\right)$$
$$\ll \frac{1}{\phi(n)}.$$

Using Lemma 3.3 one more time:

$$\sum_{\epsilon n\log n/\log\log n<q<n\log n} \frac{c_n(q)}{q} \ll \int_{\epsilon n\log n/\log\log n}^{n\log n} \frac{dt}{\phi(n)t\log(t/n)}$$
$$\ll \frac{1}{\phi(n)}\log\left(\frac{\log(\log n)}{\log(\log n/\log\log n)}\right) = o\left(\frac{1}{\phi(n)}\right).$$

Finally, we need to analyse the sum

$$g_n(\epsilon n\log n/\log\log n) = \sum_{n<q<\epsilon n\log n/\log\log n} \frac{c_n(q)}{q}.$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

This sum is $\neq 0$ when there are summands; that is, when at least one of $n \pm 1, 2n \pm 1, \ldots, kn \pm 1$ is prime for $k < \epsilon \log x / \log\log x$. Hence we use the prime number theorem for arithmetic progressions and we see

$$\sum_{k < \frac{\epsilon \log x}{\log\log x}} \frac{k}{\phi(k)} \frac{x}{\log x} \ll \frac{x}{\log x} \cdot \frac{\epsilon \log x}{\log\log x} \ll \frac{\epsilon x}{\log\log x} = o(x).$$

The number of $n \leq x$ such that $g_n(\epsilon n \log n / \log\log n) \neq 0$ is $o(x)$, and Theorem 1.2 has been proved. $\square$

5. Conditional composite moduli weak Kummer's conjecture. We now prove Theorem 1.3 that Kummer's conjecture holds for almost all n. We will need natural numbers analogues of Proposition 1 and Proposition 2 from [**3**].

PROPOSITION 5.1.

$$\sum_{m \geq 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 \bmod n \\ q \text{ prime}}} \frac{1}{q^m} = o\left(\frac{1}{n}\right)$$

for all but $o(\frac{x}{\log x})$ natural numbers $n \leq x$.

Proof. For any prime $q > n$,

$$\sum_{m \geq 2} \frac{1}{mq^m} \leq \frac{1}{2}\left(\frac{1}{q^2} + \frac{1}{q^3} + \ldots\right) \leq \frac{1}{q^2}.$$

Also, for any prime $q < n$,

$$\sum_{m \geq 2} \frac{1}{mq^m} \leq \frac{1}{2n^2}\left(1 + \frac{1}{q} + \frac{1}{q^2} + \ldots\right) \leq \frac{1}{n^2}.$$

Thus, if we list the primes q_i in order so that $q_k < n < q_{k+1}$,

$$\begin{aligned} \sum_{m \geq 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 \bmod n \\ q^m > n^2}} \frac{1}{q^m} &\leq \sum_{m \geq 2} \frac{1}{mq_1^m} + \cdots + \sum_{m \geq 2} \frac{1}{mq_k^m} + \sum_{m \geq 2} \frac{1}{mq_{k+1}^m} + \sum_{m \geq 2} \frac{1}{mq_{k+2}^m} + \cdots \\ &\leq \frac{1}{n^2} + \cdots \frac{1}{n^2} + \frac{1}{q_{k+1}^2} + \frac{1}{q_{k+2}^2} + \cdots \\ &= O\left(\frac{1}{n^2} \cdot \frac{n}{\log n}\right) = O\left(\frac{1}{n \log n}\right) \end{aligned}$$

by the prime number theorem.

Again, using Lemma 3.7, we have $\leq 4(2)^{\omega(n)}$ solutions mod n of the congruence $x^m \equiv \pm 1 \bmod n$. Also, by Lemma 3.8, the number of $n \leq x$ such that $\omega(n) > A \log\log x$ is $o(\frac{x}{\log x})$. (Here we choose $e \leq A < 2/\log 2$.)

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Hence

$$\frac{1}{2}\sum_{\substack{q^2\equiv\pm1 \bmod n\\ n\log^2 n<q^2\le n^2}}\frac{1}{q^2} \le \frac{1}{2n\log^2 n}\sum_{\substack{q^4\equiv1 \bmod n\\ q\le n}}1 \le \frac{2(2^{\omega(n)})}{n\log^2 n} = o\left(\frac{1}{n}\right) \tag{5.4}$$

for all but $o(\frac{x}{\log x})$ numbers $n \le x$.

Now if $q^m \le n^2$, then $m < 4\log n$. Let

$$S_n = \sum_{3\le m\le 4\log n}\frac{1}{m}\sum_{\substack{q^m\equiv\pm1 \bmod n\\ q^m\le n\log^2 n}}\frac{1}{q^m}.$$

Then

$$\begin{aligned}\sum_{x<n<2x}S_n &\ll \sum_{3<m<\log n}\frac{1}{m}\sum_{x\log^2 x<q^m<x^2}\frac{1}{q^m}\sum_{\substack{x<n<2x\\ n\mid q^m\pm1}}1\\ &\ll \sum_{3<m<\log n}\frac{1}{m}\sum_{\substack{q<x^{2/m}\\ q\text{ prime}}}\frac{1}{x\log^2 x}\cdot x^{\delta}\\ &\ll \log\log x\cdot\frac{x^{2/3}}{\log(x^{2/3})}\cdot\frac{1}{x^{1-\delta}\log^2 x}\\ &\ll \frac{\log\log x}{\sqrt[4]{x}\log^3 x},\end{aligned}$$

because the number of divisors of q^m+1 or of q^m-1 is $o(x^{\delta})$ for any $\delta>0$ (see [**2**, p. 296]).

The number of $x < S_n < 2x$ such that $S_n > \epsilon/n$ is $\ll x^{3/4}$, since otherwise

$$\sum_{x<n<2x}S_n \gg \frac{1}{x}\cdot x^{3/4} = \frac{1}{\sqrt[4]{x}}.$$

By dyadic decomposition together with (5.4), we see that

$$\sum_{m\ge2}\frac{1}{m}\sum_{\substack{q^m\equiv\pm1 \bmod n\\ n\log^2 n\le q^m\le n^2}}\frac{1}{q^m} = o(1/n)$$

for all but $o(x/\log x)$ natural numbers $n \le x$. It now suffices to show that

$$s_n = \sum_{m\ge2}\frac{1}{m}\sum_{\substack{q^m\equiv\pm1 \bmod n\\ q^m<n\log^2 n}}\frac{1}{q^m} = o(1/n)$$

for all but $o(x/\log x)$ numbers $n \le x$.

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Note that

$$
\begin{aligned}
\sum_{x<n<2x} s_n &\ll \sum_{m\geq 2}\frac{1}{m}\sum_{x<q^m<x\log^2 x}\frac{1}{q^m}\sum_{\substack{x<n<2x\\ q^m=\pm 1+kn}} 1\\
&\ll \sum_{m\geq 2}\frac{1}{m}\sum_{x<q^m<x\log^2 x}\frac{\log^2 x}{q^m}\\
&\ll \sum_{\substack{q \text{ prime}\\ q<x^{1/2}\log x}}\frac{\log^2 x}{x}\\
&\ll \frac{\log^2 x}{x}\cdot\frac{x^{1/2}\log x}{\log(x^{1/2}\log x)} \ll \frac{\log^2 x}{x^{1/2}}
\end{aligned}
$$

by the prime number theorem.

Thus if $s_n > \epsilon/n$ for $\gg x^{1/2}\log^3 x$ natural numbers $x < n \leq 2x$, then

$$
\sum_{x<n<2x} s_n \gg \frac{1}{x}(x^{1/2}\log^3 x) = \frac{\log^3 x}{x^{1/2}},
$$

a contradiction. By dyadic decomposition, $s_n = o(1/n)$ holds for $\ll x^{1/2}\log^3 x = o(x/\log x)$ numbers $n \leq x$. □

Recall $g_n = \lim_{x\to\infty} g_n(x)$, where

$$
g_n(x) = \sum_{\substack{q \text{ prime}\\ q\leq x\\ q\equiv 1 \bmod n}}\frac{1}{q} - \sum_{\substack{q \text{ prime}\\ q\leq x\\ q\equiv -1 \bmod n}}\frac{1}{q}.
$$

Then by Proposition 5.1 we have $f_n = g_n + o(1/n)$ for all but $o(x/\log x)$ numbers $n \leq x$.

PROPOSITION 5.2. *Assume the Elliott–Halberstam conjecture is true, and fix $\delta > 0$. For a constant $C \geq 3$, the equation $g_n - g_n(n^{1+\delta}) = o(1/n)$ holds for all but $\ll x/\log^C x$ natural numbers $n \leq x$.*

Proof. Set $S(t, x) = \sum_{x<n<2x} |\pi(t, n, 1) - \pi(t, n, -1)|$; then the Elliott–Halberstam conjecture gives

$$
\begin{aligned}
\sum_{x<n<2x} |g_n - g_n(n^{1+\delta})| &\ll \left[\frac{S(t,x)}{t}\right]_{x^{1+\delta}}^{\infty} + \int_{x^{1+\delta}}^{\infty}\frac{S(t,x)}{t^2}dt\\
&\ll \frac{1}{\log^5 x} + \int_{x^{1+\delta}}^{\infty}\frac{dt}{t\log^5 t} \ll \frac{1}{\log^{A-1} x}.
\end{aligned}
$$

Take $A \geq 3$ in the Elliott–Halberstam conjecture.

If the inequality

$$
\sum_{x<n<2x} |g_n - g_n(n^{1+\delta})| > \frac{\epsilon}{n}
$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

holds for $\gg x/\log^{A-2} x$ numbers $x < n \le 2x$, then

$$\sum_{x<n<2x} |g_n - g_n(n^{1+\delta})| \gg \frac{1}{x} \cdot \frac{x}{\log^{A-2} x} = \frac{1}{\log^{A-2} x},$$

a contradiction. The result follows by dyadic decomposition. □

COROLLARY 5.3. *Assume the Elliott–Halberstam conjecture. Then for any* $\delta > 0$ *and* $C \ge 3$,

$$f_n = g_n(n^{1+\delta}) + o(1/n)$$

for all but $o(x/\log x)$ *numbers* $n \le x$.

Proof. This follows from Propositions 5.1 and 5.2. □

We will also need the following result.

LEMMA 5.4 ([**4**, Theorem 5.7]). *Let* g *be a natural number, and let* $a_i, b_i(1 = 1, \ldots, g)$ *be integers satisfying*

$$E := \prod_{i=1}^{g} a_i \prod_{1 \le r < s \le g} (a_r b_s - a_s b_r) \ne 0.$$

Let $\rho(p)$ *denote the number of solutions of*

$$\prod_{i=1}^{g} (a_i n + b_i) \equiv 0 \bmod p,$$

and suppose that $\rho(p) < p$ *for all* p. *Let* y *and* x *be real numbers satisfying* $1 < y \le x$. *Then*

$$\begin{aligned} &|\{n : x - y < n \le x, a_i n + b_i \text{ prime for } i = 1, \ldots, g\}| \\ &\le 2^g g! \prod_p \left(1 - \frac{\rho(p) - 1}{p - 1}\right)\left(1 - \frac{1}{p}\right)^{-g+1} \frac{y}{\log^g y} \\ &\times \left\{1 + O\left(\frac{\log\log 3y + \log\log 3|E|}{\log y}\right)\right\}, \end{aligned}$$

where the implied constant depends at most on g.

We are now ready to prove Theorem 1.3.

Proof. We are left to deal with the finite sum

$$g_n(n^{1+\delta}) = \sum_{q<n^{1+\delta}} \frac{c_n(q)}{q} = \sum_{q<(1+\delta)n\log^2 n} \frac{c_n(q)}{q} + \sum_{(1+\delta)n\log^2 n<q<n^{1+\delta}} \frac{c_n(q)}{q}.$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

For $X < n < 2X$, and $(1+\delta)^A n \log^A n < x < n^{1+\delta}$, the conditions of Lemma 3.4 are satisfied, and

$$\sum_{(1+\delta)^A n \log^A n < q < n^{1+\delta}} \frac{c_n(q)}{q} \ll \int_{(1+\delta)^A n \log^A n}^{n^{1+\delta}} \frac{t}{\phi(n)\log n} \frac{dt}{t^2}$$
$$\ll \frac{1}{\phi(n)\log n}[\delta \log n - A\log(1+\delta) - A\log n]$$
$$\ll \frac{\delta}{\phi(n)}.$$

Now we put bounds on the sum

$$\sum_{q<(1+\delta)^A n \log^A n} \frac{c_n(q)}{q}.$$

For the range $(1+\delta)n\log^2 n < q < (1+\delta)^A n \log^A n$, we use the Brun–Titchmarsh theorem:

$$\sum_{\substack{(1+\delta)n\log^2 n<q \\ <(1+\delta)^A n\log^A n}} \frac{c_n(q)}{q} \ll \int_{(1+\delta)n\log^2 n}^{(1+\delta)^A n \log^A n} \frac{dt}{\phi(n)t\log(t/n)} \ll \frac{1}{\phi(n)}.$$

For $\epsilon n \log n < q < (1+\delta)n\log^2 n$,

$$\sum_{\substack{\epsilon n\log n<q \\ <(1+\delta)n\log^2 n}} \frac{c_n(q)}{q} \ll \sum_{\substack{\epsilon n<t<(1+\delta)\log^2 n, \\ nt\pm 1 \text{ prime}}} \frac{1}{nt}.$$

On average,

$$\sum_{x<n<2x} \sum_{\substack{\epsilon \log n<t<(1+\delta)\log^2 n, \\ nt\pm 1 \text{ prime}}} \frac{1}{nt} \ll \sum_{\epsilon \log x<t<(1+\delta)\log^2 x} \frac{1}{tx} \sum_{\substack{x<n<2x, \\ nt\pm 1 \text{ prime}}} 1$$
$$\leq \sum_{\epsilon \log x<t<(1+\delta)\log^2 x} \frac{1}{tx} \frac{x}{\phi(t)\log x}$$
$$\ll \frac{\log\log x}{\log x}.$$

Therefore the number of $n \leq x$ such that

$$\sum_{\substack{\epsilon \log n<t<\log^2 n, \\ nt\pm 1 \text{ prime}}} \frac{1}{nt} > \frac{\epsilon}{n}$$

is $\ll \frac{x\log\log x}{\log x} = o(x)$. That is, $|g_n(\epsilon n \log n) - g_n((1+\delta)n\log^2 n)| = o(n)$ for all but $o(x)$ natural numbers $n \leq x$.

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Finally, for the range $q < \epsilon n \log n$, we will use Lemma 5.4. Fix some $t < \epsilon \log x$. Then the number of $n < x$ such that $nt + 1$ or $nt - 1$ is a prime is $\leq x/\log x + O(\frac{x \log\log x}{\log^2 x})$, and so

$$\sum_{t<\epsilon \log x} \#\{n < x : \; nt \pm 1 \text{ prime}\} \leq \epsilon x + O\left(\frac{x \log\log x}{\log x}\right).$$

So the number of $n < x$ for which

$$\sum_{q<\epsilon n \log n} \frac{c_n(q)}{q} \neq 0$$

is $o(x)$, and we may assume $g_n(\epsilon n \log n) = 0$ for almost all n, and the proof of Theorem 1.3 is complete. □

6. Conditional disproof of generalised Kummer's conjecture. Recall that

$$h_n^- = G(n) \exp\left(\frac{\phi(n)}{2} f_n\right)$$

and that the generalised Kummer's conjecture predicts that $h_n^- \sim G(n)$ as $n \to \infty$. In this section, we will prove Theorem 1.4, that the Elliott–Halberstam conjecture implies that the generalised Kummer's conjecture fails for infinitely many natural numbers n. Here we wish to show that $f_n = o(1/\phi(n))$ fails for infinitely many n.

By Corollary 5.3, the Elliott–Halberstam conjecture implies that for any $\delta > 0$ and $C \geq 3$,

$$f_n = g_n(n^{1+\delta}) + o(1/n)$$

for all but $o(x/\log x)$ numbers $n \leq x$. We wish to find bounds on $g_n(n^{1+\delta}) - \frac{1}{n+1}$ and so estimate the contribution of the primes q of the form $n + 1$.

Lemma 6.1. *Fix $\lambda > 0$ and $\epsilon > 0$. There exists some $\delta > 0$ such that for all sufficiently large values of x, there are $\leq \frac{\lambda x}{\log x}$ natural numbers $n \leq x$ such that $n + 1$ is prime and*

$$\left| g_n(n^{1+\delta}) - \frac{1}{n+1} \right| \geq \frac{\epsilon}{2n}.$$

Proof. Define

$$N_k^{\pm}(x) = |\{x < n \leq 2x : n+1 \text{ and } kn \pm 1 \text{ both prime}\}|.$$

Then for $k \geq 2$,

$$N_k^+(x) \ll \left(\prod_{p|k(k-1)} \frac{p}{p-1}\right) \frac{x}{\log^2 x} \tag{6.5}$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

and

$$N_k^-(x) \ll \left(\prod_{p|k(k+1)} \frac{p}{p-1}\right) \frac{x}{\log^2 x} \tag{6.6}$$

by Theorem 3.5.

Thus

$$\sum_{\substack{x<n\le 2x\\ n+1 \text{ prime}}} n \left| g_n(n^{1+\delta}) - \frac{1}{n+1} \right| \ll \sum_{\substack{x<n\le 2x\\ n+1 \text{ prime}}} \sum_{\substack{q\equiv \pm 1 \bmod n\\ q\le n^{1+\delta}\\ q \text{ prime},\ q\ne n+1}} \frac{n}{q\mp 1} \ll \sum_{k=2}^{(2x)^\delta} \frac{N_k^+}{k} + \sum_{k=2}^{(2x)^\delta} \frac{N_k^-}{k}$$

$$\ll \frac{x}{\log^2 x} \sum_{k=2}^{(2x)^\delta} \left(\frac{1}{k} \prod_{p|k(k-1)} \frac{p}{p-1} \right)$$

$$+ \frac{x}{\log^2 x} \sum_{k=2}^{(2x)^\delta} \left(\frac{1}{k} \prod_{p|k(k+1)} \frac{p}{p-1} \right)$$

$$\ll \frac{x}{\log^2 x} \cdot \delta \log x = \frac{\delta x}{\log x}$$

by Lemmas 3.5 and 3.6.

Hence there exists a constant $c_1 > 0$ such that

$$\sum_{\substack{x<n\le 2x\\ n+1 \text{ prime}}} \left| g_n(n^{1+\delta}) - \frac{1}{n+1} \right| \le \frac{1}{n} c_1 \delta \frac{x}{\log x} = \frac{\epsilon}{2n} \cdot \frac{\lambda x}{\log x}$$

for $\delta = \frac{\epsilon\lambda}{2c_1}$. By dyadic decomposition, there exists $\le \frac{\lambda x}{\log x}$ numbers $n \le x$ such that $n+1$ is prime and

$$\left| g_n(n^{1+\delta}) - \frac{1}{n+1} \right| \ge \frac{\epsilon}{2n},$$

as required. □

Proposition 6.2. *Suppose the Elliott–Halberstam conjecture is true. Then for a fixed* $\epsilon > 0$ *there exist* $\gg x/\log x$ *natural numbers* $n \le x$ *such that* $f_n = (1 \pm \epsilon)\frac{1}{n}$.

Proof. By the prime number theorem, there are $\ge c_2 x/\log x$ numbers $n \le x$ such that $n+1$ is prime. Fix $\epsilon > 0$ and let $\lambda = c_2/2$ in Lemma 6.1. Then there exist $\ge c_2 x/2 \log x$ numbers $n \le x$ such that $n+1$ is prime and

$$\left| g_n(n^{1+\delta}) - \frac{1}{n+1} \right| < \frac{\epsilon}{2n}.$$

By Corollary 5.3, there exist $\ge c_2 x/2 \log x$ numbers $n \le x$ such that $n+1$ is prime and

$$\left| f_n - \frac{1}{n} \right| < \frac{\epsilon}{n}.$$

□

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

We have shown that with the assumption of the Elliott–Halberstam conjecture,

$$\frac{h_n^-}{G(n)} = \exp\left(\frac{\phi(n)}{2} f_n\right) = \exp\left(\frac{\phi(n)}{4n}(1 \pm \epsilon)\right)$$

for $\gg \frac{x}{\log x}$ numbers $n \leq x$. We now wish to prove that for infinitely many of these n, $\frac{\phi(n)}{n}$ is bounded away from 0. This must be verified, of course, because $\liminf_{n\to\infty} \frac{\phi(n)}{n} = 0$.

LEMMA 6.3.

$$\sum_{\substack{n\leq x \\ 2n+1 \text{ prime}}} \frac{\phi(n)}{n} \sim \frac{cx}{\log x}, \qquad \textit{as } x \to \infty,$$

where $c = \frac{3}{2}\prod_{p \text{ odd}}\left(1 - \frac{1}{p(p-1)}\right) \neq 0.$

Proof. Since

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d},$$

we have

$$\sum_{\substack{n\leq x \\ 2n+1 \text{ prime}}} \frac{\phi(n)}{n} = \sum_{\substack{n\leq x \\ 2n+1 \text{ prime}}} \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d\leq x} \frac{\mu(d)}{d} \sum_{\substack{t\leq x/d \\ 2dt+1 \text{ prime}}} 1.$$

The inner sum is $\pi(2x+1, 2d, 1)$.

Thus we need to evaluate

$$\sum_{d\leq x} \frac{\mu(d)}{d}\pi(2x+1, 2d, 1) = \sum_{d<\log^A x} \frac{\mu(d)}{d}\pi(2x+1, 2d, 1) + \sum_{\log^A x\leq d\leq x} \frac{\mu(d)}{d}\pi(2x+1, 2d, 1).$$

For the second sum, we have the estimate

$$\sum_{\log^A x\leq d\leq x} \frac{\mu(d)}{d}\pi(2x+1, 2d, 1) \ll \sum_{d\geq \log^A x} \frac{x}{d^2} \ll \frac{x}{\log^A x}.$$

For the first sum, we use the Siegel–Walfisz theorem 3.1 to get

$$\sum_{d<\log^A x} \frac{\mu(d)}{d}\pi(2x+1, 2d, 1) \ll \sum_{d\leq \log^A x} \frac{\mu(d)}{d\phi(d)} \operatorname{li} 2x + O\left(\frac{x}{\log^A x}\right).$$

The first term is

$$(\operatorname{li} 2x)\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d\phi(2d)} + O\left(\frac{1}{\log^{A-1} x}\right)\right).$$

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

Since

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d\phi(d)}=\sum_{\substack{d=2d_1\\ d_1\ \text{odd}}}\frac{\mu(d)}{d\phi(2d)}+\sum_{d\ \text{odd}}\frac{\mu(d)}{d\phi(2d)}$$

$$=\sum_{d\ \text{odd}}\frac{\mu(2d)}{2d2\phi(d)}+\sum_{d\ \text{odd}}\frac{\mu(d)}{d\phi(d)}=-\frac{1}{4}\sum_{d\ \text{odd}}\frac{\mu(d)}{d\phi(d)}+\sum_{d\ \text{odd}}\frac{\mu(d)}{d\phi(d)}$$

$$=\frac{3}{4}\sum_{d\ \text{odd}}\frac{\mu(d)}{d\phi(2d)}=\frac{3}{4}\sum_{d\ \text{odd}}\mu(d)\prod_{p\mid d}\left(\frac{p}{p-1}\right)\frac{1}{d^2}$$

$$=\frac{3}{4}\prod_{p\ \text{odd}}\left(1-\frac{1}{p(p-1)}\right)$$

and

$$\operatorname{li}2x\sim\frac{2x}{\log x},$$

this completes the proof of the lemma. □

LEMMA 6.4. *Let $\delta>0$ and $x\geq 1$. Then*

$$\sum_{\substack{n\leq x\\ n+1\ \textit{prime}\\ kn\pm 1\ \textit{both prime for some}\\ 2\leq k\leq\delta\log x}}\frac{\phi(n)}{n}\ll\frac{\delta x}{\log x},\tag{6.7}$$

where the implied constant is absolute.

Proof. Since $\frac{\phi(n)}{n}\leq 1$, we have that the sum in (6.7) is bounded by

$$\sum_{2\leq k\leq\delta\log x}N_k^{\pm}(x),$$

where

$$N_k^{\pm}(x)=|\{n\leq x: n+1\ \text{ and } kn\pm 1\text{ both prime}\}|.$$

By dyadic decomposition and equations (6.5) and (6.6),

$$N_k^{+}(x)\ll\left(\prod_{p\mid k(k-1)}\frac{p}{p-1}\right)\frac{x}{\log^2 x}$$

and

$$N_k^{-}(x)\ll\left(\prod_{p\mid k(k+1)}\frac{p}{p-1}\right)\frac{x}{\log^2 x}.$$

Inserting this estimate into the sum, we get the sum is $\ll\frac{\delta x}{\log x}$, as claimed. □

https://doi.org/10.1017/S0017089510000340 Published online by Cambridge University Press

We now prove Theorem 1.4.

Proof. By Proposition 6.2, the Elliott–Halberstam conjecture implies that

$$\frac{h_n^-}{G(n)} = \exp\left(\frac{\phi(n)}{2} f_n\right) = \exp\left(\frac{\phi(n)}{2n}(1 \pm \epsilon)\right)$$

for $\gg \frac{x}{\log x}$ numbers $n \leq x$. By Lemmas 6.3 and 6.4, for a sufficiently small δ we have

$$\sum_{\substack{\frac{x}{2} \leq n \leq x \\ n+1 \text{ prime} \\ \text{neither } kn\pm 1 \text{ is prime for any} \\ 2 \leq k \leq \delta \log x}} \frac{\phi(n)}{n} \gg \frac{x}{\log x}.$$

From this we deduce that there are infinitely many n such that

$$\frac{h_n^-}{G(n)} \geq \exp(\eta)$$

for some fixed $\eta > 0$. Thus if the Elliott–Halberstam conjecture is true, then the generalised Kummer's conjecture (2.1) fails for infinitely many natural numbers. □

ACKNOWLEDGEMENTS. The author would like to thank Robert Osburn and Larry Washington, and to give special thanks to M. Ram Murty. The author would also like to thank Pieter Moree at MPI for his helpful comments. This work was partially supported by IRCSET's Embark Postdoctoral Fellowship Scheme.

REFERENCES

1. N. C. Ankeny and S. Chowla, The class number of the cyclotomic field. *Canad. J. Math.* **3** (1951), 486–494.

2. T. M. Apostol, *Introduction to analytic number theory* (Springer-Verlag, New York, 1995).

3. A. Granville, On the size of the first factor of the class number of a cyclotomic field, *Invent. Math.* **100** (1990), 321–338.

4. H. Halberstam and H. E. Richert, *Sieve methods* (Academic Press, London, 1974).

5. G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Q. J. Math.* **48** (1917), 76–92.

6. C. Hooley, On the Brun–Titchmarsh theorem, II, *Proc. Lond. Math. Soc. (3)* **30** (1975), 114–128.

7. E. E. Kummer, *Collected papers* (Springer-Verlag, New York, 1975).

8. Y. Lu and W. Zhang, On the Kummer conjecture, *Acta Arith.* **131** (2008), 87–102.

9. M. R. Murty and Y. N. Petridis, On Kummer's conjecture, *J. Number Theory* **90** (2001), 294–303.

10. M. J. R. Myers, A prime power variation of Kummer's conjecture, *J. Ramanujan Math. Soc.* (submitted).

11. L. C. Washington, *Introduction to cyclotomic fields* (Springer-Verlag, New York, 1982).