Journal of Number Theory **90**, 294–303 (2001)
doi:10.1006/jnth.2001.2667, available online at http://www.idealibrary.com on IDEAL®

On Kummer's Conjecture

M. Ram Murty and Yiannis N. Petridis[1]

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6
E-mail: murty@mast.queensu.ca, petridis@math.mcgill.ca

Communicated by A. Granville

Received June 13, 2000; published online July 23, 2001

Kummer conjectured the asymptotic behavior of the first factor of the class number of a cyclotomic field. If we only ask for upper and lower bounds of the order of growth predicted by Kummer, then this modified Kummer conjecture is true for almost all primes.

1. INTRODUCTION

Let p be an odd prime and h_p be the class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$, where ζ_p denotes a primitive p-root of unity. Let h_p^+ denote the class number of the maximal real subfield $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. It is well-known, e.g., [4, p. 213, VI 1.20] that $h_p^+ \mid h_p$ and so we can factor $h_p = h_p^+ h_p^-$. The number h_p^- is called the first factor of the class number of the cyclotomic field. In 1851, Kummer [12, p. 473] conjectured that

$$h_p^- \sim \frac{p^{(p+3)/4}}{2^{(p-3)/2}\pi^{(p-1)/2}} = G(p) \tag{1.1}$$

as $p \to \infty$. In fact he claimed to have a proof that he would publish later together with further developments. In 1949 Ankeny and Chowla [2, 3] proved that

$$\log(h_p^-/G(p)) = o(\log p) \tag{1.2}$$

[1] Current address: Department of Mathematics and Statistics, McGill University, Montreal, Quebec, Canada H3A 2K6. The first author was partially supported by a Killam Research Fellowship and the Bankers Trust Company Foundation by a grant to the Institute for Advanced Study.

0022-314X/01 $35.00

as $p \to \infty$. Unaware of the work of Ankeny and Chowla, Siegel [15] proved the weaker assertion

$$\log(h_p^-/G(p)) = O(p \log\log p). \tag{1.3}$$

He also cast doubt on the original Kummer conjecture and asked whether $h_p^-/G(p)$ is bounded above and below by positive constants. It follows from (1.2), (1.3) that

$$\log h_p^- \sim \tfrac{1}{4} p \log p \tag{1.4}$$

and that $\mathbf{Q}(\zeta_p)$ has class number 1 for only a finite set of primes p. In 1990 Granville [7] showed that assuming two standard conjectures of analytic number theory, namely the Elliott–Halberstam conjecture and the Hardy–Littlewood conjecture, Kummer's conjecture is false. More precisely, let $\pi(x, k, l)$ denote the number of primes $p \leqslant x$ with $p \equiv l \pmod k$. The Elliott–Halberstam conjecture predicts that for any $\varepsilon > 0$ and $A > 0$ we have

$$\sum_{k < x^{1-\varepsilon}} \max_{(l,k)=1} \max_{y \leqslant x} \left| \pi(y, k, l) - \frac{\operatorname{li} y}{\varphi(k)} \right| \ll_{\varepsilon, A} \frac{x}{\log^A x}. \tag{1.5}$$

The Hardy–Littlewood conjecture predicts that there are at least $\gg x/\log^2 x$ primes $p \leqslant x$ such that $2p+1$ is also prime. Assuming these two unproved conjectures, Granville shows that Kummer's conjecture (1.1) is false.

In this paper we prove the following theorem, which we call the weak Kummer conjecture.

THEOREM 1.1. *There exists a positive constant c such that for almost all primes*

$$c^{-1} \leqslant \frac{h_p^-}{G(p)} \leqslant c. \tag{1.6}$$

That is, there is a sequence of primes p_i such that (1.6) *holds and the number of primes $p_i \leqslant x$ is asymptotic to $x/\log x$ as $x \to \infty$.*

This theorem should be compared with further results of Granville in [7, Theorem 5, p. 325] that state that

$$1/c \leqslant h_p^-/G(p) \leqslant c$$

for a positive proportion $\rho(c)$ of primes $p \leqslant x$, where $\rho(c) \to 1$ as $c \to \infty$. The estimate

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

holds for all primes $p \notin S$, where $S = \varnothing$ under the Generalized Riemann Hypothesis (GRH), or S has density zero unconditionally.

Granville [7] conjectures that

$$(-\tfrac{1}{2} + o(1)) \log\log\log p \leqslant \log(h_p^-/G(p)) \leqslant (\tfrac{1}{2} + o(1)) \log\log\log p.$$

In fact he conjectures that they are the best possible bounds, in the sense that there are sequences of primes realizing the left and right equality.

The result in Theorem 1.1 is unconditional. If we assume the Elliott–Halberstam conjecture more can be deduced.

THEOREM 1.2. *Assume the Elliott–Halberstam conjecture* (1.5). *Then the Kummer conjecture holds for almost all primes in the following sense*: *For every* $\varepsilon > 0$ *there exists an* x_ε *such that*

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

holds for all primes $p \geqslant x_\varepsilon$ *with the exception of a set* $P(\varepsilon)$ *of zero density in the set of primes*: $|\{p \in P(\varepsilon), x_\varepsilon < p \leqslant x\}| = o(\pi(x))$.

Remark 1.3. There are a lot of computations related to Kummer's conjecture. Kummer himself [12] computed h_p^- for $p < 100$. M. Newman [13] extended the calculations to $p < 200$, after earlier efforts of G. Schrutka von Rechtenstamm [14] for $p < 256$. D. Lehmer and J. Masley [11] worked out the range $200 < p < 521$ and G. Fung, A. Granville and H. Williams [5] computed h_p^- for $p < 3000$. The best algorithm known is due to V. Jha [10].

2. PRELIMINARY MATERIAL

We first derive several reformulations and simplifications of Kummer's conjecture. Much of this material can be found in [3, 7]. Hasse showed that

$$h_p^- = G(p) \prod_{\chi \bmod p,\, \chi(-1) = -1} L(1, \chi); \tag{2.1}$$

see [4, Theorem 69, 5.13]. This formula follows from the analytic class number formula

$$\prod_{\chi \in \Theta_K,\, \chi \neq 1} L(1, \chi) = \frac{2^{s+t} \pi^t R_K h_K}{W_K \sqrt{|d_k|}}$$

applied to $\mathbf{Q}(\zeta_p)$ and $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ and the comparison of the regulators, discriminants and the roots of unity in these fields. Here Θ_K is the character group of the (abelian) Galois group of K, R_K is the regulator, W_K is the number of roots of unity in K, d_K is the discriminant and s, t are the number of real and complex imbeddings of K.

Thus

$$h_p^- = G(p)\exp\left(\frac{p-1}{2} f_p\right), \tag{2.2}$$

where

$$f_p = \lim_{x\to\infty} f_p(x), \qquad f_p(x) = \sum_{n\leqslant x} \frac{c(n)}{n} \tag{2.3}$$

with $c(n)=0$, unless n is a prime power q^m, in which case $c(q^m)=1/m$ if $q^m \equiv 1 (\mathrm{mod}\ p)$, and $-1/m$ if $q^m \equiv -1 (\mathrm{mod}\ p)$. Thus Kummer's conjecture is equivalent to the assertion $f_p = o(1/p)$. The weak Kummer conjecture (1.6) is equivalent to $f_p = O(1/p)$. As in [7], the Siegel–Walfisz theorem allows to write $f_p = f_p(2^p) + o(1/p)$, for odd primes p. Thus, we may restrict our attention to the finite sum $f_p(2^p)$. We will use the following results.

LEMMA 2.1 (Brun–Titchmarsh Theorem). *For $k<x$, $(k,l)=1$ we have*

$$\pi(x,k,l) < \frac{3x}{\varphi(k)\log(x/k)}. \tag{2.4}$$

Proof. See [8, Th. 3.8, p. 110]. ∎

LEMMA 2.2 [9, Hooley, p. 124]. *Let l be a fixed nonzero integer. Let also ε, A and B be any positive real numbers where $A \geqslant B+30$. Then for any numbers x and X such that $x^{1/2} \leqslant X < x\log^{-A} x$ and $x > x_0(\varepsilon, B)$, we have*

$$\pi(x,k,l) \leqslant \frac{(4+\varepsilon)\,x}{\varphi(k)\log X} \tag{2.5}$$

for all values of k satisfying $X \leqslant k \leqslant 2X$ and $(l,k)=1$, except for at most $X\log^{-B} x$ exceptional values of k.

LEMMA 2.3. *Fix l, k, $(l, k) = 1$. The number of primes $x < p \leqslant 2x$ such that $kp + l$ is also prime is*

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

Proof. See [8, 2.4.1, p. 80]. ∎

LEMMA 2.4. *There is a constant c such that, as $T \to \infty$,*

$$\sum_{k \leqslant T} \prod_{p \mid k} \left(1 - \frac{1}{p}\right)^{-1} \sim cT. \tag{2.6}$$

Proof. We have $\prod_{p \mid k} (1 - p^{-1}) = \varphi(k)/k$. To analyze the asymptotics of $k/\varphi(k)$ we look at the Dirichlet series

$$g(s) = \sum_{k=1}^{\infty} \frac{k}{\varphi(k)} \frac{1}{k^s} = \prod_p \left(1 + \frac{p}{(p-1)(p^s - 1)}\right)$$

and apply the Wiener–Ikehara Tauberian theorem. We only need to notice that $g(s)/\zeta(s)$ is regular for $\Re s > 1$. ∎

Remark 2.5. Siegel's method [15] is based on the inequality $L(1, \chi) < 2 \log p$ for the upper bound and two inequalities for the lower bound: Landau's theorem $|L(1, \chi)| > c(\log p)^{-5}$ for nonreal characters and the analytic class number formula for a quadratic field

$$L(1, \chi) = \frac{2\pi h_{\mathbf{Q}(\sqrt{-p})}}{W\sqrt{p}} > p^{-1/2}, \qquad p \equiv 3 (\mathrm{mod}\ 4).$$

Siegel's theorem for real characters $L(1, \chi) > c(\varepsilon)\, p^{-\varepsilon}$ does not lead to an improvement. Siegel's doubts on whether Kummer had actually proved his conjecture are based on the fact that neither Kummer nor Dirichlet were aware of Siegel's theorem.

3. THE WEAK KUMMER CONJECTURE: PROOF OF THEOREM 1.1

We need to prove that for all but $o(x/\log x)$ primes $p \leqslant x$ we have (1.6). By the remarks of the preceding section, it suffices to consider $f_p(2^p)$. Moreover, in the definition of $f_p(x)$, we can confine our attention to primes

as the contribution of prime powers q^m with $m \geqslant 2$ is seen to be $O(1/p)$, see [3, p. 490]. Set

$$E(x, p) = \max_{y \leqslant x} \max_{(a, p)=1} \left| \pi(y, p, a) - \frac{\operatorname{li} y}{p-1} \right|. \tag{3.1}$$

The Bombieri–Vinogradov theorem [1] gives for any $A > 0$ a $B = B(A)$ such that

$$\sum_{p < x^{1/2}/\log^B x} E(x, p) \ll_A \frac{x}{\log^A x}. \tag{3.2}$$

We set

$$S(t, x) = \sum_{x < p \leqslant 2x} E(t, p)$$

and we can estimate

$$\sum_{x < p \leqslant 2x} \sum_{p^2 \log^{2B} p < q \leqslant 2^p} \frac{c(q)}{q}$$

$$\ll \left[\frac{S(t, x)}{t} \right]_{x^2 \log^{2B} x}^{\infty} + \int_{x^2 \log^{2B} x}^{\infty} \frac{S(t, x)}{t^2}\, dt \ll \log^{-A+1} x. \tag{3.3}$$

Therefore, if we write $f_p(2^p) = f_p(p^2 \log^{2B} p) + D(p)$, we see that the number of primes p, $x < p \leqslant 2x$, such that $|D(p)| > c/p$ is $O(x/\log^{A-1} x)$. Using a dyadic decomposition of the range $p \leqslant x$ into intervals $[2^{-i-1}x, 2^{-i}x]$, we exclude at most $x \log^{-A+1} x$ primes p, with $p \leqslant x$ and we choose $A > 2$ in the Bombieri–Vinogradov theorem.

Thus, we may restrict our attention to $f_p(p^2 \log^{2B} p)$. We use Lemma 2.1 to observe that

$$\sum_{p^2/4 < q < p^2 \log^{2B} p} \frac{c(q)}{q} \ll \int_{p^2/4}^{p^2 \log^{2B} p} \frac{dt}{pt \log(t/p)} = o(1/p),$$

so that we may restrict our attention to $f_p(p^2/4)$.

We apply Lemma 2.2 in the range $[2^A p(\log p)^A, p^2/4]$. We take $k = p$ in the Lemma and we easily see that, if $X \leqslant p \leqslant 2X$, this range is included in the range $x^{1/2} \leqslant X \leqslant x \log^{-A} x$ required in the Lemma. It follows that $\pi(x, p, \pm 1) \ll x/(p \log p)$, except for a set of primes p of size at most

$X \log^{-B} X$. Again using a dyadic decomposition we exclude at most $X \log^{-B} X$ primes p, with $p \leqslant X$. We take $B > 2$ in Lemma 2.2 and get

$$\sum_{2^A p \log^A p < q < p^2/4} \frac{c(q)}{q} \ll \int_{2^A p \log^A p}^{p^2/4} \frac{x}{x^2 p \log p}\, dx \ll \frac{1}{p}$$

for all but $O(X/\log^B X)$ primes p with $p \leqslant X$.

Finally, by Lemma 2.3, the number of primes $x < p \leqslant 2x$ such that $pk \pm 1$ is also prime is

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

for a fixed k. Let the number of primes $p \in (x, 2x]$ such that $pk \pm 1$ is also prime for $k \leqslant \varepsilon \log x/\log\log x$ be $N(x)$. Then

$$N(x) \ll \sum_{k \leqslant \varepsilon \log x/\log\log x} \prod_{p \mid k} \left(1 - \frac{1}{p}\right)^{-1} \frac{x}{\log^2 x} \ll \frac{\varepsilon x}{\log x \log\log x},$$

in which we use the estimate (2.6). So we are excluding at most $x/(\log x \log\log x)$ primes $p \leqslant x$. We may therefore suppose that in our summation we have $q > \varepsilon p \log p/\log\log p$. Thus we need only to consider

$$\begin{aligned} \sum_{\varepsilon p \log p/\log\log p < q < 2^A p \log^A p} \frac{c(q)}{q} &\ll \int_{\varepsilon p \log p/\log\log p}^{2^A p \log^A p} \frac{dt}{tp \log(t/p)} \\ &\ll \frac{1}{p} \log\left(\frac{\log(2^A \log^A p)}{\log(\varepsilon \log p/\log\log p)}\right) \\ &= O(1/p) \end{aligned} \tag{3.4}$$

using Lemma 2.1 again. This completes the proof of Theorem 1.1.

Remark 3.1. We see that the exceptional set of primes $p \leqslant x$ is $\ll x/(\log x \log\log x)$.

4. PROOF OF THEOREM 1.2

Proposition 1 in [7] shows that the contribution for $m > 1$ is $o(1/p)$ with the exception of a set of primes $p \leqslant x$ which are at most $\ll x^{1/2} \log^2 x$. As in Corollary 1 in [7] the Elliott–Halberstam conjecture (1.5) implies

$f_p = f_p(p^{1+\delta}) + o(1/p)$ for all but $O_\delta(x/\log^3 x)$ primes $p \leqslant x$. We prove that for almost all primes p we have

$$\sum_{\varepsilon p \log p/\log\log p < q < 2^A p \log^A p} \frac{c(q)}{q} = o(1/p). \tag{4.1}$$

We set $q = kp \pm 1$ and see that, when q varies in the range $\varepsilon p \log p/\log\log p < q < 2^A p \log^A p$ and $x < p \leqslant 2x$, k varies in the range $(\varepsilon/2)\log x/\log\log x < k < 2^{A+1}\log^A(2x)$. We have

$$\sum_{x<p\leqslant 2x} \sum_{q\equiv \pm 1 \bmod p} \frac{1}{q} \ll \sum_{k} \sum_{x<p\leqslant 2x,\, q=kp\pm 1} \frac{1}{kp}.$$

We use Lemma 2.3 to estimate the number of primes p between x and $2x$ with $kp \pm 1$ also prime by $\prod_{p\mid k}(1-p^{-1})^{-1}\, x/\log^2 x$. Using a summation by parts together with (2.6) we easily get that

$$\sum_{k\leqslant T} \frac{1}{k} \prod_{p\mid k}\left(1-\frac{1}{p}\right)^{-1} \ll \log T.$$

The estimates above give

$$\sum_{x<p\leqslant 2x} \sum_{q\equiv \pm 1 \bmod p} \frac{1}{q} \ll \sum_{k\ll \log^A(2x)} \frac{1}{kx} \prod_{p\mid k}\left(1-\frac{1}{p}\right)^{-1} \frac{x}{\log^2 x} \ll \frac{\log\log x}{\log^2 x}.$$

From this it follows that the number of primes p with $x < p \leqslant 2x$ with

$$\sum_{q\equiv \pm 1 \bmod p} \frac{c(q)}{q} > \frac{c_1}{p\log\log p}$$

is $\ll x(\log\log x)^2/\log^2 x$. Using a dyadic decomposition again we get at most $\ll x(\log\log x)^2/\log^2 x$ exceptional primes p, $p \leqslant x$.

An application of Lemma 2.2 similar to the previous section shows that for all but $O(x/\log^B x)$ primes p with $p \leqslant x$ we have

$$\sum_{2^A p\log^A p < q < p^{1+\delta}} \frac{c(q)}{q} \ll \int_{2^A p\log^A p}^{p^{1+\delta}} \frac{dt}{pt\log p} \ll \frac{\delta\log p}{p\log p}.$$

Collecting the above estimates and exponentiating, we deduce that there is a constant $c > 0$ such that for every $\delta > 0$ and for all primes p with the exception of a set $P(\delta)$ of zero density in the set of all primes we have

$$c^{-\delta} < \frac{h_p^-}{G(p)} < c^{\delta}$$

as $p \to \infty$. The result of Theorem 1.2 follows easily.

5. CONCLUDING REMARKS

It is clear from the previous sections that Kummer's conjecture is related to the difference of the number of primes congruent to 1 and -1 modulo p.

From the analysis of the previous sections we see that Kummer's conjecture for almost all primes is a consequence of the following condition (unproven)

$$\int_{p \log^A p}^{p^2} \frac{E_1(t, p)}{t^2}\, dt = o(1/p),$$

where $E_1(x, d) = \pi(x, d, 1) - \pi(x, d, -1)$.

Remark 5.1. L. Goldstein [6] proved the analogue of (1.4) for $\mathbf{Q}(\zeta_{p^r})$. As $r \to \infty$ and for fixed odd p

$$\log h_{p^r}^- \sim \frac{1}{4}\left(1 - \frac{1}{p}\right) p^r r \log p.$$

In this case the analogue of (2.1) is

$$h_{p^r}^- = \frac{p^{r+1/4+t(p,r)/4}}{2^{\varphi(p^r)/2-1}\pi^{\varphi(p^r)/2}} \prod_{\chi(-1)=-1} L(1, \chi) \tag{5.1}$$

with $t(p, r) = \log |d_{\mathbf{Q}(\zeta_{p^r})}|/\log p = rp^r - (r+1)\, p^{r-1}$, and the product is over the odd characters of the Galois group of $\mathbf{Q}(\zeta_{p^r})$. It is interesting to investigate this product as $r \to \infty$.

ACKNOWLEDGMENT

The authors thank the referee for helpful comments concerning Theorem 1.2.

REFERENCES

1. E. Bombieri, On the large sieve, *Mathematika* **12** (1965), 201–225.
2. N. C. Ankeny and S. Chowla, The class number of the cyclotomic field, *Proc. Natl. Acad. Sci. U.S.A.* **35** (1949), 529–532.
3. N. C. Ankeny and S. Chowla, The class number of the cyclotomic field, *Canadian J. Math.* **3** (1951), 486–494.

4. A. Fröhlich and M. Taylor, "Algebraic Number Theory," Cambridge Studies in Advanced Mathematics, Vol. 27, Cambridge Univ. Press, Cambridge, UK, 1991.
5. G. Fung, A. Granville, and H. Williams, Computation of the first factor of the class number of cyclotomic fields, *J. Number Theory* **42** (1992), 297–312.
6. L. Goldstein, On the class numbers of cyclotomic fields, *J. Number Theory* **5** (1973), 58–63.
7. A. Granville, On the size of the first factor of the class number of a cyclotomic field, *Invent. Math.* **100** (1990), 321–338.
8. H. Halberstam and H. E. Richert, "Sieve Methods," London Mathematical Society Monographs, No. 4, Academic Press, London/New York, 1974.
9. C. Hooley, On the Brun–Titchmarsh Theorem, II, *Proc. London Math. Soc. (3)* **30** (1975), 114–128.
10. V. Jha, Faster computation of the first factor of the class number of $Q(\zeta_p)$, *Math. Comp.* **64**, No. 212 (1995), 1705–1710.
11. D. Lehmer and J. Masley, Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, *Math. Comp.* **32**, No. 142 (1978), 577–582.
12. E. Kummer, Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers, *J. Math. Pures Appl.* **16** (1851), 377–498. Collected Works, Vol. 1, pp. 363–484.
13. M. Newman, A table of the first factor for prime cyclotomic fields, *Math. Comp.* **24** (1970), 215–219.
14. G. Schrutka von Rechtenstamm, Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren φ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist, *Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech.* **1964**, No. 2 (1964).
15. C. L. Siegel, Zu zwei Bemerkungen Kummers, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* **6** (1964), 51–57.