Arch. Math. 83 (2004) 507–513
0003–889X/04/060507–07
DOI 10.1007/s00013-004-1043-x

Archiv der Mathematik

Density of integers which are discriminants of cyclic fields of odd prime degree

By

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

Abstract. An asymptotic formula is given for the number of integers $\leqq x$ which are discriminants of cyclic fields of odd prime degree.

Let q be a fixed odd prime. Let n be a positive integer. It is known that n is the discriminant of a cyclic field of degree q over $\mathbb{Q}$ if and only if

$$n = q^{2(q-1)}, \quad (q_1 \cdots q_r)^{q-1} \quad \text{or} \quad q^{2(q-1)}(q_1 \cdots q_r)^{q-1},$$

where r is a positive integer and $q_1, \ldots, q_r$ are distinct primes $\equiv 1 \pmod q$, see for example [1], [7]. Let $A(q)$ denote the set of positive integers which are the product of distinct primes $\equiv 1 \pmod q$ including the empty product $= 1$. Then the number $C_q(x)$ of $n \leqq x$ which are discriminants of cyclic fields of degree q is (for large enough x in terms of q)

$$C_q(x) = 1 + \sum_{\substack{1<n\leqq x^{1/(q-1)} \\ n\in A(q)}} 1 + \sum_{\substack{1<n\leqq x^{1/(q-1)}/q^2 \\ n\in A(q)}} 1$$

so that

$$C_q(x) = A_q(x^{1/(q-1)}) + A_q(x^{1/(q-1)}/q^2) - 1, \tag{1}$$

where

$$A_q(x) = \sum_{\substack{n\leqq x \\ n\in A(q)}} 1.$$

Mathematics Subject Classification (2000): 11R16, 11R21, 11R29.

Both authors were supported by grants from the Natural Sciences and Engineering Research Council of Canada.

Our purpose is to determine an asymptotic formula for $C_q(x)$ valid for large x. To do this we make use of the prime number theorem for arithmetic progressions, Mertens' theorem for arithmetic progressions, and a result, which under certain conditions, gives the asymptotic behavior of $\sum_{n \leqq x} f(n)$ from that of $\sum_{p \leqq x} f(p)$, where p runs through primes. This last result is a consequence of theorems of Wirsing [12, Satz 1, p. 76] and Odoni [3, Theorem II, p. 205; Theorem III, p. 206; Note added in proof, p. 216.]. Throughout this paper p denotes a prime number.

Proposition. *Let $f : \mathbb{N} \to \mathbb{R}$ be multiplicative with $0 \leqq f(n) \leqq 1$ for all $n \in \mathbb{N}$. Suppose that there are constants τ and β with $\tau > 0$ and $0 < \beta < 1$ such that*

$$\sum_{p \leqq x} f(p) = \tau \frac{x}{\log x} + O\left(\frac{x}{(\log x)^{1+\beta}}\right).$$

Then

$$\lim_{x \to \infty} \frac{1}{(\log x)^{\tau}} \prod_{p \leqq x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right)$$

exists, and

$$\sum_{n \leqq x} f(n) = Ex(\log x)^{\tau-1} + O(x(\log x)^{\tau-1-\beta})$$

with

$$E = \frac{e^{-\gamma\tau}}{\Gamma(\tau)} \lim_{x \to \infty} \frac{1}{(\log x)^{\tau}} \prod_{p \leqq x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right).$$

Proof. See [6, Proposition 5.5]. Here γ denotes Euler's constant. □

Prime number theorem for primes $p \equiv 1 (\mathrm{mod}\ q)$.

$$\sum_{\substack{p \leqq x \\ p \equiv 1 \ (\mathrm{mod}\ q)}} 1 = \frac{1}{q-1} \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

as $x \to \infty$.

Proof. See for example [4, Satz 7.6, p. 139]. □

The cyclotomic field $\mathbb{Q}(e^{2\pi i/q})$ is of degree $\phi(q) = q - 1$ over $\mathbb{Q}$. We denote its class number and regulator by $h(q)$ and $R(q)$ respectively. We also let

$$\omega := e^{\frac{2\pi i}{q-1}} \in \mathbb{C},$$

so that $\omega^{q-1} = 1$. The principal character $\chi_0 \pmod q$ is defined as follows: for $n \in \mathbb{Z}$ we have

$$\chi_0(n) = \begin{cases} 1, & \text{if } n \not\equiv 0 \pmod q, \\ 0, & \text{if } n \equiv 0 \pmod q. \end{cases}$$

Let g be a primitive root $\pmod q$. For $n \in \mathbb{Z}$ with $n \not\equiv 0 \pmod q$ the index $\mathrm{ind}_g(n)$ of n with respect to g is defined modulo $q-1$ by

$$n \equiv g^{\mathrm{ind}_g(n)} \pmod q.$$

We define a character $\chi_g \pmod q$ as follows: for $n \in \mathbb{Z}$ we set

$$\chi_g(n) = \begin{cases} \omega^{\mathrm{ind}_g(n)}, & \text{if } n \not\equiv 0 \pmod q, \\ 0, & \text{if } n \equiv 0 \pmod q. \end{cases}$$

There are exactly $\phi(q) = q-1$ characters $\pmod q$. They are

$$\chi_0,\ \chi_g,\ \chi_g^2, \ldots,\ \chi_g^{q-2},$$

where $\chi_g^{q-1} = \chi_0$. Let $r \in \{1, 2, \ldots, q-2\}$. We define the constant $C(q, r, \chi_g)$ by

$$C(q, r, \chi_g) = \prod_{\substack{p \\ \chi_g(p) = \omega^r}} \left(1 - \frac{1}{p^{\frac{q-1}{(r,q-1)}}}\right).$$

As $1 \leqq (r, q-1) \leqq \frac{1}{2}(q-1)$ for $r \in \{1, 2, \ldots, q-2\}$, we have

$$\frac{q-1}{(r, q-1)} \geqq 2,$$

so that the infinite product converges. It is shown in [6, Section 3] that the product

$$\prod_{r=1}^{q-2} C(q, r, \chi_g)^{(r,q-1)}$$

does not depend on the choice of the primitive root g. Thus we can define a constant $C(q)$ by

$$C(q) := \prod_{r=1}^{q-2} C(q, r, \chi_g)^{(r,q-1)}. \tag{2}$$

Then we define the constants $\lambda(q)$, $E(q)$ and $K(q)$ by

$$\lambda(q) = \left(\frac{e^{-\gamma} 2^{-(q-3)/2} q^{(q+2)/2} \pi^{-(q-1)/2}}{(q-1) h(q) R(q) C(q)}\right)^{\frac{1}{q-1}}, \tag{3}$$

$$E(q) = \frac{1}{\lambda(q)} \frac{e^{-\gamma/(q-1)}}{\Gamma(\frac{1}{q-1})} \prod_{p \equiv 1 (\mathrm{mod}\, q)} \left(1 - \frac{1}{p^2}\right)$$

$$= 2^{\frac{q-3}{2q-2}} q^{-\frac{q+2}{2q-2}} (q-1)^{\frac{1}{q-1}} \pi^{\frac{1}{2}} \left(\Gamma\left(\frac{1}{q-1}\right)\right)^{-1} \prod_{p \equiv 1 (\mathrm{mod}\, q)} \left(1 - \frac{1}{p^2}\right) \tag{4}$$

$$\times (h(q)R(q)C(q))^{\frac{1}{q-1}},$$

and

$$K(q) = E(q)(q-1)^{\frac{q-2}{q-1}} \left(1 + \frac{1}{q^2}\right)$$

$$= 2^{\frac{q-3}{2q-2}} q^{\frac{2-5q}{2q-2}} (q-1)(q^2+1)\pi^{\frac{1}{2}} \left(\Gamma\left(\frac{1}{q-1}\right)\right)^{-1} \prod_{p \equiv 1 (\mathrm{mod}\, q)} \left(1 - \frac{1}{p^2}\right) \tag{5}$$

$$\times (h(q)R(q)C(q))^{\frac{1}{q-1}}.$$

Mertens' theorem for primes $p \equiv 1 (\mathbf{mod}\ q)$. *Let q be an odd prime. Then*

$$\prod_{\substack{p \leqq x \\ p \equiv 1 \,(\mathrm{mod}\, q)}} \left(1 - \frac{1}{p}\right) = \lambda(q)(\log x)^{-1/(q-1)} + O((\log x)^{-q/(q-1)}),$$

as $x \to \infty$, where the constant implied by the O-symbol depends only on q.

Proof. This result is proved in [6, Proposition 6.3] from Mertens' theorem for primes in arithmetic progression [11] and the class number formula for abelian fields [2, Theorem 8.4, p. 436]. □

We are now ready to prove an asymptotic formula for $A_q(x)$.

Theorem 1. *Let $0 < \epsilon < 1$. Let q be an odd prime. Then*

$$A_q(x) = E(q)x(\log x)^{-\frac{q-2}{q-1}} + O(x(\log x)^{-\frac{2q-3}{q-1}+\epsilon}),$$

as $x \to \infty$, where the constant implied by the O-symbol depends only on q and ϵ.

Proof. We let

$$f(n) = \begin{cases} 1, & \text{if } n \in A(q), \\ 0, & \text{if } n \notin A(q). \end{cases}$$

Clearly $f(n)$ is a multiplicative function satisfying the conditions of the Proposition with $\tau = \frac{1}{q-1}$ and $\beta = 1 - \epsilon$, where $0 < \epsilon < 1$, by the prime number theorem for primes $p \equiv 1 \,(\mathrm{mod}\, q)$. Hence, by the Proposition, we obtain

$$A_q(x) = \sum_{\substack{n \leqq x \\ n \in A(q)}} 1 = \sum_{n \leqq x} f(n) = E(q) \frac{x}{(\log x)^{\frac{q-2}{q-1}}} + O\left(\frac{x}{(\log x)^{\frac{2q-3}{q-1}-\epsilon}}\right),$$

as $x \to \infty$, where

$$E(q) = \frac{e^{\frac{-\gamma}{q-1}}}{\Gamma(\frac{1}{q-1})} \lim_{x\to\infty} \frac{1}{(\log x)^{\frac{1}{q-1}}} \prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1+\frac{1}{p}\right).$$

Next, for $x \to \infty$, we have

$$\prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1+\frac{1}{p}\right) = \frac{R_q(x)}{S_q(x)},$$

where

$$R_q(x) = \prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1-\frac{1}{p^2}\right) = (1+o(1)) \prod_{p\equiv 1 (\mathrm{mod}\ q)} \left(1-\frac{1}{p^2}\right),$$

and by Mertens' theorem for primes $p \equiv 1\ (\mathrm{mod}\ q)$

$$S_q(x) = \prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1-\frac{1}{p}\right) = \lambda(q)(1+o(1)) \frac{1}{(\log x)^{\frac{1}{q-1}}},$$

so that

$$\prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1+\frac{1}{p}\right) = \frac{1}{\lambda(q)} \prod_{p\equiv 1 (\mathrm{mod}\ q)} \left(1-\frac{1}{p^2}\right)(1+o(1))(\log x)^{1/(q-1)}.$$

Hence

$$\lim_{x\to\infty} (\log x)^{-1/(q-1)} \prod_{\substack{p\leqq x\\ p\equiv 1 (\mathrm{mod}\ q)}} \left(1+\frac{1}{p}\right) = \frac{1}{\lambda(q)} \prod_{p\equiv 1 (\mathrm{mod}\ q)} \left(1-\frac{1}{p^2}\right)$$

and

$$E(q) = \frac{1}{\lambda(q)} \frac{e^{\frac{-\gamma}{q-1}}}{\Gamma(\frac{1}{q-1})} \prod_{p\equiv 1 (\mathrm{mod}\ q)} \left(1-\frac{1}{p^2}\right)$$

in agreement with (4). □

From (1), (5) and Theorem 1 we obtain

Theorem 2. *Let* $0 < \epsilon < 1$. *Then*

$$C_q(x) = K(q)x^{\frac{1}{q-1}}(\log x)^{-\frac{q-2}{q-1}} + O\left(x^{\frac{1}{q-1}}(\log x)^{-\frac{2q-3}{q-1}+\epsilon}\right),$$

as $x \to \infty$, *where the constant implied by the* O*-symbol depends only on* q *and* ϵ.

We conclude with an example.

Example. We determine $C_3(x)$ for large x. The cyclotomic field $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$ has class number $h(3) = 1$ and regulator $R(3) = 1$. In [6, Lemma 3.1] it is shown that

$$C(3) = \prod_{p \equiv 2 \pmod 3}\left(1 - \frac{1}{p^2}\right).$$

Now

$$\begin{aligned}\left(1 - \frac{1}{3^2}\right)&\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)\prod_{p \equiv 2 \pmod 3}\left(1 - \frac{1}{p^2}\right)\\ &= \prod_p\left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}\end{aligned}$$

so that

$$C(3) = 2^{-2}3^3\pi^{-2}\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)^{-1}.$$

By (3) we have

$$\lambda(3) = e^{-\frac{\gamma}{2}}2^{-\frac{1}{2}}3^{\frac{5}{4}}\pi^{-\frac{1}{2}}C(3)^{-\frac{1}{2}} = e^{-\frac{\gamma}{2}}2^{\frac{1}{2}}3^{-\frac{1}{4}}\pi^{\frac{1}{2}}\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}}.$$

Then, by (4), we have as $\Gamma(\frac{1}{2}) = \pi^{\frac{1}{2}}$

$$\begin{aligned}E(3) &= e^{-\frac{\gamma}{2}}\pi^{-\frac{1}{2}}\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)\lambda(3)^{-1}\\ &= 2^{-\frac{1}{2}}3^{\frac{1}{4}}\pi^{-1}\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}}.\end{aligned}$$

Finally, by (5), we have

$$K(3) = E(3)2^{\frac{1}{2}}\left(1 + \frac{1}{3^2}\right) = 2 \cdot 3^{-\frac{7}{4}}5\pi^{-1}\prod_{p \equiv 1 \pmod 3}\left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}}$$

and Theorem 2 gives

$$C_3(x) = 2 \cdot 3^{-\frac{7}{4}} 5\pi^{-1} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}} \frac{x^{\frac{1}{2}}}{(\log x)^{\frac{1}{2}}} + O\left(\frac{x^{\frac{1}{2}}}{(\log x)^{\frac{3}{2}-\epsilon}}\right),$$

for $0 < \epsilon < 1$, as $x \to \infty$. This result without an error term was given in [5, Theorem 2].

We remark that Urazbaev [8], [9], [10] has determined asymptotic formulae for the number of cyclic fields of prime power degree with discriminant $\leqq x$.

References

[1] D. C. MAYER, Multiplicities of dihedral discriminants. Math. Comp. **58**, 831–847 (1992).

[2] W. NARKIEWICZ, Elementary and Analytic Theory of Algebraic Numbers. Berlin-Heidelberg-New York 1990.

[3] R. W. K. ODONI, A problem of Rankin on sums of powers of cusp-form coefficients. J. London Math. Soc. **44**, 203–217 (1991).

[4] K. PRACHAR, Primzahlverteilung. Berlin-Göttingen-Heidelberg 1957.

[5] B. K. SPEARMAN and K. S. WILLIAMS, Density of integers which are discriminants of cyclic cubic fields. Far East J. Math. Sci. (FJMS) **8**, 83–87 (2003).

[6] B. K. SPEARMAN and K. S. WILLIAMS, Values of the Euler phi function not divisible by a given odd prime. Submitted for publication.

[7] B. M. URAZBAEV, On the discriminant of a cyclic field of prime degree. Izv. Akad. Nauk Kazah. SSR 1950, no. 97, Ser. Mat Meh. **4**, 19–32 (1950). (in Russian)

[8] B. M. URAZBAEV, On the number of cyclic fields of prime degee with given discriminant. Izv. Akad. Nauk Kazah. SSR 1951, no. 62, Ser. Mat Meh. **5**, 53–67 (1951). (in Russian)

[9] B. M. URAZBAEV, On the density of distribution of cyclic fields of prime degree. Izv. Akad. Nauk Kazah. SSR 1951, no. 62, Ser. Mat Meh. **5**, 37–52 (1951). (in Russian)

[10] B. M. URAZBAEV, On an asymptotic formula in algebra. Dokl. Akad. Nauk SSSR (N.S.) **95**, 935–938 (1954). (in Russian)

[11] K. S. WILLIAMS, Mertens' theorem for arithmetic progressions. J. Number Theory **6**, 353–359 (1974).

[12] E. WIRSING, Das asymptotische Verhalten von Summen über multiplikativen Funktionen. Math. Ann. **143**, 75–102 (1961).

Received: 17 February 2004

Blair K. Spearman
Department of Mathematics and Statistics
Okanagan University College
Kelowna B.C.
Canada V1V 1V7
bspearman@ouc.bc.ca

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
williams@math.carleton.ca