Cyclic Cubic Fields of Given Conductor and Given Index

Alan K. Silvester, Blair K. Spearman, and Kenneth S. Williams

Abstract. The number of cyclic cubic fields with a given conductor and a given index is determined.

1 Introduction

Let $K$ be a cyclic cubic extension of $\mathbb{Q}$ so that $[K : \mathbb{Q}] = 3$ and $\text{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. By the Kronecker–Weber theorem [10, p. 289] there exists a positive integer $m$ such that the cyclotomic field $\mathbb{Q}(e^{2\pi i/m}) \supseteq K$. The smallest such $m$ is called the conductor of $K$ and is denoted by $f(K)$. The discriminant of $K$ is given by $d(K) = f(K)^2$ [8, p. 831]. The conductor $f(K)$ of a cyclic cubic field is of the form

\[(1.1) \quad f = p_1 p_2 \cdots p_r,\]

where $r \in \mathbb{N}$ and $p_1, \ldots, p_r$, are distinct integers from the set

\[(1.2) \quad P = \{9\} \cup \{p \text{ (prime) } \equiv 1 \pmod{3}\} = \{7, 9, 13, 19, 31, 37, \ldots\},\]

see [8, p. 831]. Moreover each positive integer $f$ of the form (1.1) is the conductor of some cyclic cubic field; indeed it is the conductor of $2^{r-1}$ cyclic cubic fields [8, p. 831]. For any cubic field $K$ it is known that its field index $i(K) = 1$ or $2$ [5, p. 234]. For $f$ of the form (1.1) and $i \in \{1, 2\}$, we define

\[(1.3) \quad N(f, i) = \text{number of cyclic cubic fields } K \text{ with } f(K) = f \text{ and } i(K) = i,\]

so that

\[(1.4) \quad N(f, 1) + N(f, 2) = 2^{r-1}.\]

In this paper we determine $N(f, 1)$ and $N(f, 2)$.

It is well known that each prime $p \equiv 1 \pmod{3}$ has a unique representation in the form

\[(1.5) \quad 4p = a^2 + 27b^2, \quad a, b \in \mathbb{N},\]
see [1, Theorem 3.1.3, p. 105; Lemma 3.0.1, p. 101]. Clearly for such a representation we have \(a \equiv b \pmod{2}\) and

\[
gcd(a, b) = 1 \text{ or } 2.
\]

It is a classical result of Gauss that 2 is a cubic residue \((\text{mod } p)\) if and only if \(\gcd(a, b) = 2\), see [1, Theorem 7.1.1, p. 213]. We set

\[
P_1 = \{9\} \cup \{p \text{ (prime) } \equiv 1 \pmod{3}, 4p = a^2 + 27b^2, \gcd(a, b) = 1\}
\]

and

\[
P_2 = \{p \text{ (prime) } \equiv 1 \pmod{3}, 4p = a^2 + 27b^2, \gcd(a, b) = 2\},
\]

so that

\[
P_1 \cup P_2 = P, \quad P_1 \cap P_2 = \emptyset.
\]

Clearly

\[
P_1 = \{7, 9, 13, 19, 37, \ldots\}, \quad P_2 = \{31, 43, 109, 127, \ldots\}.
\]

If \(p\) is a prime in \(P_1\), then \(a \equiv b \equiv 1 \pmod{2}\). Replacing \(b\) by \(-b\), if necessary, we may suppose that \(a \equiv b \pmod{4}\). Set \(x = (a - b)/4 \in \mathbb{Z}, y = b \in \mathbb{Z}\). Then \(4x^2 + 2xy + 7y^2 = p\). Conversely if \(p = 4x^2 + 2xy + 7y^2\) for some \(x, y \in \mathbb{Z}\) then \(y\) is odd, \(\gcd(x, y) = 1\) and \(4p = a^2 + 27b^2\) with \(a = |4x + y|, b = |y|\) and \(\gcd(a, b) = \gcd(4x + y, y) = \gcd(4x, y) = \gcd(x, y) = 1\). Thus the primes in \(P_1\) are precisely those which can be expressed in the form \(4x^2 + 2xy + 7y^2\) for some \(x, y \in \mathbb{Z}\). The primes in \(P_2\) are precisely those which can be expressed in the form \(x^2 + 27y^2\) for some \(x, y \in \mathbb{Z}\).

Now suppose that \(f\) is of the form \((1.1)\) with

\[
p_1, p_2, \ldots, p_u \in P_1 \quad \text{and} \quad p_{u+1}, p_{u+2}, \ldots, p_r \in P_2,
\]

where \(u \in \{0, 1, \ldots, r\}\). In Section 5 we prove the following result.

**Theorem**  With the above notation, we have

\[
N(f, 1) = \frac{1}{3}(2^r - (-1)^u2^{r-u}), \quad N(f, 2) = \frac{1}{3}(2^{r-1} + (-1)^u2^{r-u}).
\]

In Sections 2, 3, 4 we give some results on representations of integers by binary quadratic forms which will be needed in the proof of this theorem.
2 The Form Class Group $H(d)$

Let $H(d)$ denote the set of classes of primitive, positive-definite, integral binary quadratic forms $(a, b, c) = ax^2 + bxy + cy^2$ of discriminant $d = b^2 - 4ac \equiv 0 \text{ or } 1 \pmod{4}$ under the action of the modular group. As $ax^2 + bxy + cy^2$ is positive-definite, we have $a > 0$ and $d < 0$. The class of the form $(a, b, c)$ is denoted by $[a, b, c]$. Multiplication of classes of $H(d)$ is due to Gauss and is described, for example, in [2]. With respect to multiplication, $H(d)$ is a finite abelian group called the form class group of discriminant $d$. The order of $H(d)$ is called the form class number of discriminant $d$ and is denoted by $h(d)$. The identity $I$ of the group $H(d)$ is the principal class

$$I = \begin{cases} [1, 0, -d/4] & \text{if } d \equiv 0 \pmod{4}, \\ [1, 1, (1 - d)/4] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

The inverse of the class $K = [a, b, c] \in H(d)$ is the class $K^{-1} = [a, -b, c] \in H(d)$. Each class of $H(d)$ contains one and only one form $(a, b, c)$ with

$$-a < b \leq a \leq c, \quad b \geq 0 \quad \text{if } a = c, \quad b^2 - 4ac = d, \quad \gcd(a, b, c) = 1,$$

see [4, pp. 68-71]. Let $n \in \mathbb{N}$. If $x$ and $y$ are integers such that $n = ax^2 + bxy + cy^2$, then $(x, y)$ is called a representation of the positive integer $n$ by the form $(a, b, c)$. As $(a, b, c)$ is a positive-definite form, the number $R_{(a, b, c)}(n)$ of representations of $n$ by the form $(a, b, c)$ is finite. If in addition the representation $(x, y)$ satisfies $\gcd(x, y) = 1$, then the representation is called primitive. The number of primitive representations of $n$ by the form $(a, b, c)$ is denoted by $P_{(a, b, c)}(n)$. Clearly,

$$R_{(a, b, c)}(n) = \sum_{c' \mid n} P_{(a, b, c)}(n/c^2).$$

If $(A, B, C)$ is a form equivalent to $(a, b, c)$ it is well known that $R_{(A, B, C)}(n) = R_{(a, b, c)}(n)$ and $P_{(A, B, C)}(n) = P_{(a, b, c)}(n)$. Hence we can define the number of representations of $n \in \mathbb{N}$ by the class $K \in H(d)$ by

$$R_K(n) = R_{(a, b, c)}(n) \quad \text{for any } (a, b, c) \in K,$$

and the number of primitive representations of $n \in \mathbb{N}$ by the class $K \in H(d)$ by

$$P_K(n) = P_{(a, b, c)}(n) \quad \text{for any } (a, b, c) \in K.$$

From (2.2)–(2.4) we deduce that for $n \in \mathbb{N}$ and $K \in H(d)$

$$R_K(n) = \sum_{c' \mid n} P_K(n/c^2).$$

In particular, if $n \in \mathbb{N}$ is squarefree, we have

$$R_K(n) = P_K(n).$$
As each representation \((x, y)\) of \(n\) by \((a, b, c)\) gives a representation \((x, -y)\) of \(n\) by \((a, -b, c)\) and conversely, we have for \(n \in \mathbb{N}\) and \(K \in H(d)\)

\[
R_K(n) = R_{K^{-1}}(n), \quad P_K(n) = P_{K^{-1}}(n).
\]

(2.7)

For \(n_1, n_2 \in \mathbb{N}\) with \(n_1\) squarefree, \(n_2\) squarefree and gcd\((n_1, n_2) = 1\), it is known that

\[
R_K(n_1 n_2) = \frac{1}{w(d)} \sum_{K_1, K_2 \in K} R_{K_1}(n_1) R_{K_2}(n_2),
\]

(2.8)

where \(K_1, K_2\) run through all the classes of \(H(d)\) whose product is \(K\), and

\[
w(d) = 6, 4 \text{ or } 2 \text{ according as } d = -3, \; d = -4 \text{ or } d < -4,
\]

see [9, (29) and Lemma 5.5]. The largest positive integer \(f\) such that \(f^2 \mid d\) with \(\Delta = d/f^2 \equiv 0 \text{ or } 1 \pmod{4}\) is called the conductor of \(d\). By a theorem of Dirichlet, see [6], we have for gcd\((n, f) = 1\)

\[
\sum_{K \in H(d)} R_K(n) = w(d) \sum_{e \mid n} \left( \frac{d}{e} \right) = w(d) \sum_{e \mid n} \left( \frac{\Delta}{e} \right),
\]

(2.10)

where \(\left( \frac{d}{e} \right)\) is the Legendre–Jacobi–Kronecker symbol of discriminant \(d\). If \(p\) is a prime such that \(\left( \frac{d}{p} \right) = 1\), then there is at least one class \(C \in H(d)\) which represents \(p\). If \(C = C^{-1}\), then \(C\) is the only class of \(H(d)\) representing \(p\) and \(R_C(p) = 2w(d)\). If \(C \neq C^{-1}\), then \(C\) and \(C^{-1}\) are the only classes of \(H(d)\) representing \(p\) and \(R_C(p) = R_{C^{-1}}(p) = w(d)\). See [9, Lemma 5.5].

3 Representations of Integers by \([1,0,3]\)

From (2.1) with \(d = -12\) we find

\[
H(-12) = \{I\}, \quad h(-12) = 1,
\]

where

\[
I = [1, 0, 3].
\]

Here \(f = 2\) and \(\Delta = -3\).

Lemma 3.1 Let \(p_1, \ldots, p_t \; (t \geq 0)\) be distinct primes \(\equiv 1 \pmod{3}\). Then

\[
R_I(p_1 \cdots p_t) = 2^{t+1}, \quad P_I(p_1 \cdots p_t) = 2^{t+1},
\]

\[
R_I(9p_1 \cdots p_t) = 2^{t+1}, \quad P_I(9p_1 \cdots p_t) = 0.
\]
Proof If \( n \in \mathbb{N} \) is such that \( \gcd(n, 2) = 1 \), by (2.9) and (2.10) with \( d = -12 \), we have

\[
R_t(n) = 2 \sum_{e \mid n} \left( -\frac{3}{e} \right).
\]

Taking \( n = p_1 \cdots p_t \), as \( \left( \frac{-3}{p_i} \right) = 1 \) \( (i = 1, \ldots, t) \), we obtain

\[
R_t(p_1 \cdots p_t) = 2 \sum_{e \mid p_1 \cdots p_t} 1 = 2 \cdot 2^t = 2^{t+1}.
\]

Then, appealing to (2.6), we obtain

\[
P_t(p_1 \cdots p_t) = 2^{t+1}.
\]

Taking \( n = 9p_1 \cdots p_t \) in (3.1), since \( \left( \frac{-3}{3} \right) = 0 \) we obtain

\[
R_t(9p_1 \cdots p_t) = 2 \sum_{e \mid 9p_1 \cdots p_t} \left( -\frac{3}{e} \right) = 2 \sum_{e \mid p_1 \cdots p_t} \left( -\frac{3}{e} \right) = 2^{t+1}.
\]

Finally, by (2.5), we have

\[
R_t(9p_1 \cdots p_t) = R_t(p_1 \cdots p_t) + P_t(p_1 \cdots p_t),
\]

so that

\[
P_t(9p_1 \cdots p_t) = 2^{t+1} - 2^{t+1} = 0.
\]

This completes the proof of the lemma. \( \blacksquare \)

4 Representations of Integers by \([1,0,27]\) and \([4,2,7]\)

From (2.1) with \( d = -108 \) we find

\[
H(-108) = \{I, A, A^2\} \simeq \mathbb{Z}/3\mathbb{Z}, \quad h(-108) = 3,
\]

where

\[
I = [1, 0, 27], \quad A = [4, 2, 7], \quad A^2 = [4, -2, 7], \quad A^3 = I.
\]

Here \( f = 6 \) and \( \Delta = -3 \).

Let \( p \) be a prime with \( p \equiv 1 \pmod{3} \). Then

\[
\left( \frac{d}{p} \right) = \left( \frac{-108}{p} \right) = \left( \frac{-2^2 \cdot 3^3}{p} \right) = \left( \frac{-3}{p} \right) = 1,
\]

so that \( p \) is represented by some class in \( H(-108) \). If \( p \) is represented by \( I \), then (as \( I = I^{-1} \)) \( I \) is the only class representing \( p \), and

\[
R_I(p) = 4, \quad R_A(p) = R_A^I(p) = 0.
\]
If \( p \) is represented by \( A \) or \( A^2 \), then (as \( A \neq A^{-1} \)) the only classes of \( H(-108) \) representing \( p \) are \( A \) and \( A^2 \), and

\[
(4.2) \quad R_I(p) = 0, \quad R_A(p) = R_{A^2}(p) = 2.
\]

Now let \( m \) be a product of distinct primes \( \equiv 1 \) (mod 3). By (2.9) and (2.10) we have

\[
R_I(m) + R_A(m) + R_{A^2}(m) = 2 \sum_{e | m} \left( \frac{-3}{e} \right) = 2^{\tau(m)+1},
\]

where \( \tau(m) \) denotes the number of primes dividing \( m \). As \( R_A(m) = R_{A-1}(m) = R_{A^2}(m) \) by (2.7), we deduce that

\[
(4.3) \quad R_A(m) = R_{A^2}(m) = 2^{\tau(m)} - \frac{1}{2} R_I(m).
\]

By (2.8) we have for \( p \nmid m \)

\[
(4.4) \quad R_I(pm) = \frac{1}{2} \left( R_I(p)R_I(m) + R_A(p)R_{A^2}(m) + R_{A^2}(p)R_A(m) \right).
\]

Appealing to (4.1)–(4.4), we obtain

\[
(4.5) \quad R_I(pm) = \begin{cases} 
2R_I(m) & \text{if } R_I(p) > 0, \\
2^{\tau(m)+1} - R_I(m) & \text{if } R_A(p) > 0.
\end{cases}
\]

We now use (4.5) to prove the following result.

**Lemma 4.1** Let \( p_1, \ldots, p_l \) be \( l \geq 0 \) distinct primes \( \equiv 1 \) (mod 3), which are represented by \( I = [1, 0, 27] \), and let \( q_1, \ldots, q_m \) be \( m \geq 0 \) distinct primes \( \equiv 1 \) (mod 3), which are represented by \( A = [4, 2, 7] \). Then

\[
R_I(p_1 \cdots p_lq_1 \cdots q_m) = \frac{1}{3} \left( 2^{l+m+1} + (-1)^m 2^{l+2} \right),
\]

\[
R_A(p_1 \cdots p_lq_1 \cdots q_m) = R_{A^2}(p_1 \cdots p_lq_1 \cdots q_m) = \frac{1}{3} \left( 2^{l+m+1} - (-1)^m 2^{l+1} \right).
\]
Proof
By (4.5) we obtain
\[
R_I(p_1 \cdots p_l q_1 \cdots q_m) = 2 R_I(p_1 \cdots p_{l-1} q_1 \cdots q_m) \\
= 2^2 R_I(p_1 \cdots p_{l-2} q_1 \cdots q_m) \\
= \cdots \\
= 2^l R_I(q_1 \cdots q_m) \\
= 2^l (2^m - R_I(q_1 \cdots q_{m-1})) \\
= 2^l (2^m - 2^{m-1} + R_I(q_1 \cdots q_{m-2})) \\
= \cdots \\
= 2^l (2^m - 2^{m-1} + 2^{m-2} - \cdots + (-1)^{m-2}2^2 + (-1)^{m-1} R_I(q_1)) \\
= 2^l (2^m - 2^{m-1} + 2^{m-2} - \cdots + (-1)^{m-2}2^2) \\
= \frac{1}{3} (2^{l+m+1} + (-1)^m 2^{l+2}),
\]
as required. Then, by (4.3), we obtain
\[
R_A(p_1 \cdots p_l q_1 \cdots q_m) = 2^{l+m} - \frac{1}{2} \left( \frac{1}{3} (2^{l+m+1} + (-1)^m 2^{l+2}) \right) \\
= \frac{1}{3} (2^{l+m+1} - (-1)^m 2^{l+1}),
\]
as asserted. \(\blacksquare\)

5 Proof of Theorem
There is a one-to-one correspondence between cyclic cubic fields \(K\) and triples \((a, b, f) \in \mathbb{N}^3\) with
\[
a^2 + 27b^2 = 4f, \quad \gcd(a, b) = 1 \text{ or } 2, \quad f = p_1 \cdots p_r, \\
r \in \mathbb{N}, \quad p_1, \ldots, p_r \in P, \quad p_i \neq p_j \quad (1 \leq i < j \leq r),
\]
see [3, Section 6.4.6, pp. 336–343]. The cyclic cubic field corresponding to the triple \((a, b, f)\) is \(K = \mathbb{Q}(\theta)\), where \(\theta^3 - 3f\theta + fa = 0\). The conductor of \(K\) is \(f\). The index of \(K\) is
\[
i(K) = \begin{cases} 
2 & \text{if } a \text{ is even}, \\
1 & \text{if } a \text{ is odd}, 
\end{cases}
\]
see [7, Theorem 4, p. 585]. If \(a\) is even, then \(b\) is even and \(\left(\frac{a}{2}\right)^2 + 27\left(\frac{b}{2}\right)^2 = f\) with \(\gcd\left(\frac{a}{2}, \frac{b}{2}\right) = 1\). Thus
\[
N(f, 2) = \frac{1}{4} P_{\{1,0,27\}}(f).
\]
First suppose that $9 \nmid f$. We may suppose that $p_1, \ldots, p_u \in P_1$ (so they are represented by $[4, 2, 7]$) and $p_{u+1}, \ldots, p_r \in P_2$ (so they are represented by $[1, 0, 27]$) with $u \in \{0, 1, 2, \ldots, r\}$. Then, by (2.6) and Lemma 4.1 (with $l = r - u$ and $m = u$), we have

$$P_{[1,0,27]}(f) = R_{[1,0,27]}(f) = \frac{1}{3} (2^{r+1} + (-1)^u 2^{r-u+2}),$$

so that

$$N(f, 2) = \frac{1}{3} (2^{r-1} + (-1)^u 2^{r-u}), \quad 9 \nmid f.$$

Now suppose that $9 \mid f$. We may suppose that $p_1 = 9, p_2, \ldots, p_u \in P_1$ (so they are represented by $[4, 2, 7]$) and $p_{u+1}, \ldots, p_r \in P_2$ (so they are represented by $[1, 0, 27]$). As $9 \mid f$ we have

$$f = x^2 + 27y^2 \iff f/9 = (x/3)^2 + 3y^2$$

so that

$$R_{[1,0,27]}(f) = R_{[1,0,3]}(f/9).$$

As $f/9$ is squarefree, we have

$$R_{[1,0,27]}(f/9) = P_{[1,0,27]}(f/9).$$

From (2.5) we deduce

$$R_{[1,0,27]}(f) = P_{[1,0,27]}(f) + P_{[1,0,27]}(f/9).$$

Thus

$$P_{[1,0,27]}(f) = R_{[1,0,3]}(f/9) - R_{[1,0,27]}(f/9).$$

Appealing to Lemma 3.1 (with $t = r - 1$) and Lemma 4.1 (with $l = r - u$ and $m = u - 1$), we obtain

$$P_{[1,0,27]}(f) = 2^r - \frac{1}{3} (2^r + (-1)^u 2^{r-u+2}) = \frac{1}{3} (2^{r+1} + (-1)^u 2^{r-u+2})$$

so that

$$N(f, 2) = \frac{1}{3} (2^{r-1} + (-1)^u 2^{r-u}), \quad 9 \mid f.$$

Finally, from (1.4), we obtain in both cases

$$N(f, 1) = 2^{r-1} - N(f, 2) = \frac{1}{3} (2^r - (-1)^u 2^{r-u}).$$

This completes the proof of the theorem.
References