Chapter 4
Cyclotomic Cosets, the Mattson–Solomon Polynomial, Idempotents and Cyclic Codes

4.1 Introduction

Much of the pioneering research on cyclic codes was carried out by Prange [5] in the 1950s and considerably developed by Peterson [4] in terms of generator and parity-check polynomials. MacWilliams and Sloane [2] showed that cyclic codes could be generated from idempotents and the Mattson–Solomon polynomial, first introduced by Mattson and Solomon in 1961 [3]. The binary idempotent polynomials follow directly from cyclotomic cosets.

4.2 Cyclotomic Cosets

Consider the expansion of polynomial $a(x) = \prod_{i=0}^{m-1}(x - \alpha^{2^i})$. The coefficients of $a(x)$ are a cyclotomic coset of powers of α or a sum of cyclotomic cosets of powers of α. For example, if $m = 4$

$$a(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) \tag{4.1}$$

and expanding $a(x)$ produces

$$\begin{aligned} a(x) = x^4 &- (\alpha + \alpha^2 + \alpha^4 + \alpha^8)x^3 + (\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 + \alpha^5 + \alpha^{10})x^2 \\ &+ (\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11})x + \alpha^{15}. \end{aligned} \tag{4.2}$$

Definition 4.1 (*Cyclotomic Coset*) Let s be a positive integer, and the $2-$cyclotomic coset of $s \pmod{n}$ is given by

M. Tomlinson et al., *Error-Correction Coding and Decoding*,
Signals and Communication Technology,
DOI 10.1007/978-3-319-51103-0_4

$$C_s = \{2^i s \pmod{n} \mid 0 \leq i \leq t\},$$

where s is the smallest element in the set C_s and t is the smallest positive integer such that $2^{t+1}s \equiv s \pmod{n}$.

For convenience, we will use the term cyclotomic coset to refer to 2−cyclotomic coset. If $\mathscr{N}$ is the set consisting of the smallest elements of all possible cyclotomic cosets, then it follows that

$$C = \bigcup_{s \in \mathscr{N}} C_s = \{0, 1, 2, \ldots, n-1\}.$$

Example 4.1 The entire cyclotomic cosets of 15 are as follows:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8\} \\ C_3 &= \{3, 6, 12, 9\} \\ C_5 &= \{5, 10\} \\ C_7 &= \{7, 14, 13, 11\} \end{aligned}$$

and $\mathscr{N} = \{0, 1, 3, 5, 7\}$.

It can be seen that for $GF(2^4)$ above, Eq. (4.2), the coefficients of $a(x)$ are a cyclotomic coset of powers of α or a sum of cyclotomic cosets of powers of α. For example, the coefficient of x^3 is the sum of powers of α from cyclotomic coset C_1.

In the next step of the argument we note that there is an important property of Galois fields.

Theorem 4.1 *For a Galois field $GF(p^m)$, then*

$$\big(b(x) + c(x)\big)^p = b(x)^p + c(x)^p.$$

Proof Expanding $\big(b(x) + c(x)\big)^p$ produces

$$\begin{aligned} \big(b(x) + c(x)\big)^p = b(x)^p + \binom{p}{1} b(x)^{p-1} c(x) + \binom{p}{2} b(x)^{p-2} c(x)^2 + \\ \ldots + \binom{p}{p-1} b(x) c(x)^{p-1} + c(x)^p. \end{aligned} \tag{4.3}$$

As p modulo $p = 0$, then all of the binomial coefficients $\binom{p}{r} = 0$ and

$$\big(b(x) + c(x)\big)^p = b(x)^p + c(x)^p.$$

Another theorem follows.

Theorem 4.2 *The sum of powers of α that are from a cyclotomic coset C_i is equal to either 1 or 0.*

Proof The sum of powers of α that are from a cyclotomic coset C_i must equal to a field element, some power, j of α, α^j or 0. Also, from Theorem 1.1,

$$\left(\sum \alpha^{C_i}\right)^2 = \sum \alpha^{C_i}.$$

If the sum of powers of α is non-zero then

$$\left(\sum \alpha^{C_i}\right)^2 = \alpha^{2j} = \sum \alpha^{C_i} = \alpha^j.$$

The only non-zero field element that satisfies $\alpha^{2j} = \alpha^j$ is $\alpha^0 = 1$. Hence, the sum of powers of α that are from a cyclotomic coset C_i is equal to either 1 or 0.

In the example of C_1 from $GF(2^4)$ we have

$$(\alpha + \alpha^2 + \alpha^4 + \alpha^8)^2 = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = \alpha^2 + \alpha^4 + \alpha^8 + \alpha$$

and so

$$\alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0 \text{ or } 1.$$

Returning to the expansion of polynomial $a(x) = \prod_{i=0}^{m-1}(x - \alpha^{2^i})$. Since the coefficients of $a(x)$ are a cyclotomic coset of powers of α or a sum of cyclotomic cosets of powers of α, the coefficients of $a(x)$ must be 0 or 1 and $a(x)$ must have binary coefficients after noting that the coefficient of x^0 is $\prod_{i=0}^{m-1} \alpha^{2^i} = \alpha^{2^m-1} = 1$, the maximum order of α. Considering the previous example of $m = 4$ ($GF(2^4)$), since $a(x)$ is constrained to have binary coefficients, we have the following possible identities:

$$\begin{aligned} \alpha^{15} &= 1 \\ \alpha + \alpha^2 + \alpha^4 + \alpha^8 &= 0 \text{ or } 1 \\ \alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11} &= 0 \text{ or } 1 \\ \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 + \alpha^5 + \alpha^{10} &= 0 \text{ or } 1. \end{aligned} \tag{4.4}$$

These identities are determined by the choice of primitive polynomial used to generate the extension field. This can be seen from the Trace function, $T_m(x)$, defined as

$$T_m(x) = \sum_{i=0}^{m-1} x^{2^i} \tag{4.5}$$

and expanding the product of $T_m(x)\big(1 + T_m(x)\big)$ produces the identity

$$T_m(x)\big(1 + T_m(x)\big) = x(1 - x^n). \tag{4.6}$$

α is a root of $(1 - x^n)$ and so α is a root of either $T_m(x)$ or $\big(1 + T_m(x)\big)$, and so either $T_m(\alpha) = 0$ or $\big(1 + T_m(\alpha)\big) = 0$. For $GF(2^4)$

$$T_m(x) = \sum_{i=0}^{3} x^{2^i} = x + x^2 + x^4 + x^8. \tag{4.7}$$

Factorising produces

$$x + x^2 + x^4 + x^8 = x(1 + x)(1 + x + x^2)(1 + x + x^4), \tag{4.8}$$

and

$$1 + T_m(x) = 1 + \sum_{i=0}^{3} x^{2^i} = 1 + x + x^2 + x^4 + x^8. \tag{4.9}$$

Factorising produces

$$1 + x + x^2 + x^4 + x^8 = (1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4). \tag{4.10}$$

It may be verified that

$$\begin{aligned} T_m(x)\big(1 + T_m(x)\big) &= (x + x^2 + x^4 + x^8)(1 + x + x^2 + x^4 + x^8) \\ &= x(1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4) \\ &\quad (1 + x + x^2 + x^3 + x^4) \\ &= x(1 - x^{15}). \end{aligned}$$

Consequently, if $1 + x + x^4$ is used to generate the extension field $GF(16)$ then $\alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0$ and if $1 + x^3 + x^4$ is used to generate the extension field $GF(16)$, then $1 + \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0$.

Taking the case that $a(x) = 1 + x + x^4$ is used to generate the extension field $GF(16)$ by comparing the coefficients given by Eq. (4.2), we can solve the identities of (4.4) after noting that $\alpha^5 + \alpha^{10}$ must equal 1 otherwise the order of α is equal to 5, contradicting α being a primitive root. All of the identities of the sum for each cyclotomic coset of powers of α are denoted by $S_{i\,m}$ and these are

$$
\begin{aligned}
S_{04} &= \alpha^0 = 1 \\
S_{14} &= \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0 \\
S_{34} &= \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1 \\
S_{54} &= \alpha^5 + \alpha^{10} = 1 \\
S_{74} &= \alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11} = 1 \\
S_{154} &= \alpha^{15} = 1.
\end{aligned} \tag{4.11}
$$

The lowest degree polynomial that has β as a root is traditionally known as a minimal polynomial [2], and is denoted as M_{im} where $\beta = \alpha^i$. With M_{im} having binary coefficients

$$
M_{im} = \prod_{j=0}^{m-1} (x - \alpha^{i2^j}). \tag{4.12}
$$

For $GF(2^4)$ and considering M_{34} for example,

$$
M_{34} = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9), \tag{4.13}
$$

and expanding leads to

$$
\begin{aligned}
M_{34} = x^4 &- (\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9)x^3 + (\alpha^9 + \alpha^3 + \alpha^6 + \alpha^{12})x^2 \\
&+ (\alpha^6 + \alpha^{12} + \alpha^9 + \alpha^3)x + 1.
\end{aligned} \tag{4.14}
$$

It will be noticed that this is the same as Eq. (4.2) with α replaced with α^3. Using the identities of Eq. (4.11), it is found that

$$
M_{34} = x^4 + x^3 + x^2 + x + 1. \tag{4.15}
$$

Similarly, it is found that for M_{54} substitution produces $x^4 + x^2 + 1$ which is $(x^2 + x + 1)^2$, and so

$$
M_{54} = x^2 + x + 1; \tag{4.16}
$$

similarly, it is found that

$$
M_{74} = x^4 + x^3 + 1 \tag{4.17}
$$

for M_{04} with $\beta = 15$, and substitution produces $x^4 + 1 = (1 + x)^4$ and

$$
M_{04} = x + 1. \tag{4.18}
$$

It will be noticed that all of the minimal polynomials correspond to the factors of $1 + x^{15}$ given above. Also, it was not necessary to generate a table of $GF(2^4)$ field elements in order to determine all of the minimal polynomials once $M_{1\,4}$ was chosen.

A recurrence relation exists for the cyclotomic cosets with increasing m for

$$M_{i\,m+1} = \Big(\prod_{j=0}^{m-1}(x - \alpha^{i2^j})\Big)x - \alpha^{i2^m}. \tag{4.19}$$

For $m = 4$,

$$M_{1\,4} = x^4 + S_{1\,4}x^3 + (S_{3\,4} + S_{5\,4})x^2 + S_{7\,4}x + \alpha^{15} \tag{4.20}$$

and so

$$M_{1\,5} = \Big(x^4 + S_{1\,4}x^3 + (S_{3\,4} + S_{5\,4})x^2 + S_{7\,4}x + \alpha^{15}\Big)(x + \alpha^{16}) \tag{4.21}$$

and

$$\begin{aligned} M_{1\,5} =& x^5 + (\alpha^{16} + S_{1\,4})x^4 + (\alpha^{16}S_{1\,4} + (S_{3\,4} + S_{5\,4}))x^3 \\ &+ \big(\alpha^{16}(S_{3\,4} + S_{5\,4}) + S_{7\,4}\big)x^2 + (\alpha^{16}S_{7\,4} + \alpha^{15})x + \alpha^{31} \end{aligned} \tag{4.22}$$

and we find that

$$\begin{aligned} M_{1\,5} =& x^5 + S_{1\,5}x^4 + (S_{3\,5} + S_{5\,5})x^3 \\ &+ (S_{7\,5} + S_{11\,5})x^2 + S_{15\,5}x + \alpha^{31}. \end{aligned} \tag{4.23}$$

We have the following identities, linking the cyclotomic cosets of $GF(2^4)$ to $GF(2^5)$

$$\begin{aligned} S_{3\,5} + S_{5\,5} &= \alpha^{16}S_{1\,4} + S_{3\,4} + S_{5\,4} \\ S_{7\,5} + S_{11\,5} &= \alpha^{16}(S_{3\,4} + S_{5\,4}) + S_{7\,4} \\ S_{15\,5} &= \alpha^{16}S_{7\,4} + \alpha^{15}. \end{aligned}$$

With $1 + x^2 + x^5$ used to generate the extension field $GF(32)$, then $\alpha + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = 0$. Evaluating the cyclotomic cosets of powers of α produces

$$\begin{aligned} S_{0\,5} &= \alpha^0 = 1 \\ S_{1\,5} &= \alpha + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = 0 \\ S_{3\,5} &= \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} + \alpha^{17} = 1 \\ S_{5\,5} &= \alpha^5 + \alpha^{10} + \alpha^{20} + \alpha^9 + \alpha^{18} = 1 \\ S_{7\,5} &= \alpha^7 + \alpha^{14} + \alpha^{28} + \alpha^{25} + \alpha^{19} = 0 \end{aligned}$$

$$\begin{aligned} S_{11\,5} &= \alpha^{11} + \alpha^{22} + \alpha^{13} + \alpha^{26} + \alpha^{21} = 1 \\ S_{15\,5} &= \alpha^{15} + \alpha^{30} + \alpha^{29} + \alpha^{27} + \alpha^{23} = 0. \end{aligned} \tag{4.24}$$

Substituting for the minimal polynomials, $M_{i,5}$ produces

$$\begin{aligned} M_{0\,5} &= x + 1 \\ M_{1\,5} &= x^5 + x^2 + 1 \\ M_{3\,5} &= x^5 + x^4 + x^3 + x^2 + 1 \\ M_{5\,5} &= x^5 + x^4 + x^2 + x + 1 \\ M_{7\,5} &= x^5 + x^3 + x^2 + x + 1 \\ M_{11\,5} &= x^5 + x^4 + x^3 + x + 1 \\ M_{15\,5} &= x^5 + x^3 + 1. \end{aligned} \tag{4.25}$$

For $GF(2^5)$, the order of a root of a primitive polynomial is 31, a prime number. Moreover, 31 is a Mersenne prime $(2^p - 1)$ and the first 12 Mersenne primes correspond to $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ and 127. Interestingly, only 49 Mersenne primes are known. The last known Mersenne prime being $2^{74207281} - 1$, discovered in January 2016. As $(2^5 - 1)$ is prime, each of the minimal polynomials in Eq. (4.25) is primitive.

If α is a root of $T_m(x)$ and m is even, then $1 + T_{2m}(x) = 1 + T_m(x) + \left(1 + T_m(x)\right)^{2^m}$ and $\alpha^{\frac{2^{2m}-1}{2^m-1}}$ is a root of $x^{2^{2m}}$. For example, if α is a root of $1 + x + x^2$, α is of order 3 and α^5 is a root of $x + x^2 + x^4 + x^8$. Correspondingly, $1 + x + x^2$ is a factor of $1 + x^3$ and also a factor of$1 + x^{15}$ and necessarily $2^{2m} - 1$ cannot be prime. Similarly, if m is not a prime and $m = ab$, then

$$\frac{2^m - 1}{2^a - 1} = 2^{b(a-1)} + 2^{b(a-2)} + 2^{b(a-3)} \ldots + 1 \tag{4.26}$$

and so

$$2^m - 1 = (2^{b(a-1)} + 2^{b(a-2)} + 2^{b(a-3)} \ldots + 1)2^a - 1. \tag{4.27}$$

Similarly

$$2^m - 1 = (2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} \ldots + 1)2^b - 1. \tag{4.28}$$

As a consequence

$$M_{(2^{b(a-1)} + 2^{b(a-2)} + 2^{b(a-3)} \ldots + 1) \times j\, m} = M_{j\, a} \tag{4.29}$$

for all minimal polynomials of $x^{2^a-1}-1$, and

$$M_{(2^{a(b-1)}+2^{a(b-2)}+2^{a(b-3)}\ldots+1)\times j\,m} = M_{j\,b} \tag{4.30}$$

for all minimal polynomials of $x^{2^b-1}-1$.

For $M_{1\,6}$, following the same procedure,

$$\begin{aligned} M_{1\,6} = x^6 + S_{1\,6}x^5 + (S_{3\,6} + S_{5\,6} + S_{9\,6})x^4 + (S_{7\,6} + S_{11\,6} + S_{13\,6} + S_{21\,6})x^3 \\ + (S_{15\,6} + S_{23\,6} + S_{27\,6})x^2 + S_{15\,6}x^2 + S_{31\,6}x + \alpha^{63}. \end{aligned} \tag{4.31}$$

Substituting for the minimal polynomials, $M_{i,6}$ produces

$$\begin{aligned} M_{0\,6} &= x+1 \\ M_{1\,6} &= x^6 + x + 1 \\ M_{3\,6} &= x^6 + x^4 + x^2 + x + 1 \\ M_{5\,6} &= x^6 + x^5 + x^2 + x + 1 \\ M_{7\,6} &= x^6 + x^3 + 1 \\ M_{9\,6} &= x^3 + x^2 + 1 \\ M_{11\,6} &= x^6 + x^5 + x^3 + x^2 + 1 \\ M_{13\,6} &= x^6 + x^4 + x^3 + x + 1 \\ M_{15\,6} &= x^6 + x^5 + x^4 + x^2 + 1 \\ M_{21\,6} &= x^2 + x + 1 \\ M_{23\,6} &= x^6 + x^5 + x^4 + x + 1 \\ M_{27\,6} &= x^3 + x + 1 \\ M_{31\,6} &= x^6 + x^5 + 1. \end{aligned} \tag{4.32}$$

Notice that $M_{9\,6} = M_{3\,4}$ because $\alpha^9 + \alpha^{18} + \alpha^{36} = 1$ and $M_{27\,6} = M_{1\,4}$ because $\alpha^9 + \alpha^{18} + \alpha^{36} = 0$. $M_{21\,6} = M_{1\,3}$ because $\alpha^{21} + \alpha^{42} = 1$. The order of α is 63 which factorises to $7 \times 3 \times 3$ and so $x^{63} - 1$ will have roots of order 7 (α^9) and roots of order 3 ($\alpha^2 1$). Another way of looking at this is the factorisation of $x^{63} - 1$. $x^7 - 1$ is a factor and $x^3 - 1$ is a factor

$$\begin{aligned} x^{63} - 1 = (x^7 - 1)(1 + x^7 + x^{14} + x^{21} \\ + x^{28} + x^{35} + x^{42} + x^{49} + x^{56}) \end{aligned} \tag{4.33}$$

also

$$\begin{aligned} x^{63} - 1 = (x^3 - 1)(1 + x^3 + x^6 + x^9 + x^{12} + x^{15} + x^{18} + x^{21} \\ + x^{24} + x^{27} + x^{30} + x^{33} + x^{36} + x^{39} + x^{42} + x^{45} \\ + x^{48} + x^{51} + x^{54} + x^{57} + x^{60}) \end{aligned} \tag{4.34}$$

and

$$\begin{aligned} x^3 - 1 &= (x+1)(x^2+x+1) \\ x^7 - 1 &= (x+1)(x^3+x+1)(x^3+x^2+1) \\ x^{63} - 1 &= (x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1)(x^6+x+1) \\ &\quad (x^6+x^4+x^2+x+1)\ldots(x^6+x^5+1). \end{aligned} \tag{4.35}$$

For $M_{1\,7}$

$$\begin{aligned} M_{1\,7} = x^7 &+ S_{1\,7}x^6 + (S_{3\,7} + S_{5\,7} + S_{9\,7})x^4 + (S_{7\,7} + S_{11\,7} + S_{13\,7} + S_{19\,7} + S_{21\,7})x^3 \\ &+ (S_{15\,7} + S_{23\,7} + S_{27\,7} + S_{29\,7})x^3 + (S_{15\,7} + S_{31\,7} + S_{43\,7} + S_{47\,7} + S_{55\,7})x^2 \\ &+ S_{63\,7}x + \alpha^{127}. \end{aligned} \tag{4.36}$$

Although the above procedure using the sums of powers of α from the cyclotomic cosets may be used to generate the minimal polynomials $M_{i\,m}$ for any m, the procedure becomes tedious with increasing m, and it is easier to use the Mattson Polynomial or combinations of the idempotents as described in Sect. 4.4.

4.3 The Mattson–Solomon Polynomial

The Mattson–Solomon polynomial is very useful for it can be conveniently used to generate minimal polynomials and idempotents. It also may be used to design cyclic codes, RS codes and Goppa codes as well as determining the weight distribution of codes. The Mattson–Solomon polynomial [2] of a polynomial $a(x)$ is a linear transformation of $a(x)$ to $A(z)$. The Mattson–Solomon polynomial is the same as the inverse Discrete Fourier Transform over a finite field. The polynomial variables x and z are used to distinguish the polynomials in either domain.

Let the splitting field of $x^n - 1$ over $\mathbb{F}_2$ be $\mathbb{F}_{2^m}$, where n is an odd integer and $m > 1$, and let a generator of $\mathbb{F}_{2^m}$ be α and an integer $r = (2^m - 1)/n$. Let $a(x)$ be a polynomial of degree at most $n - 1$ with coefficients over $\mathbb{F}_{2^m}$.

Definition 4.2 (*Mattson–Solomon polynomial*) The Mattson–Solomon polynomial of $a(x)$ is the linear transformation of $a(x)$ to $A(z)$ and is defined by [2]

$$A(z) = \mathrm{MS}(a(x)) = \sum_{j=0}^{n-1} a(\alpha^{-rj}) z^j. \tag{4.37}$$

The inverse Mattson–Solomon transformation or Fourier transform is

Table 4.1 $GF(16)$ extension field defined by $1+\alpha+\alpha^4=0$

$\alpha^0 = 1$
$\alpha^1 = \alpha$
$\alpha^2 = \alpha^2$
$\alpha^3 = \alpha^3$
$\alpha^4 = 1+\alpha$
$\alpha^5 = \alpha+\alpha^2$
$\alpha^6 = \alpha^2+\alpha^3$
$\alpha^7 = 1+\alpha+\alpha^3$
$\alpha^8 = 1+\alpha^2$
$\alpha^9 = \alpha+\alpha^3$
$\alpha^{10} = 1+\alpha+\alpha^2$
$\alpha^{11} = \alpha+\alpha^2+\alpha^3$
$\alpha^{12} = 1+\alpha+\alpha^2+\alpha^3$
$\alpha^{13} = 1+\alpha^2+\alpha^3$
$\alpha^{14} = 1+\alpha^3$

$$a(x) = \mathrm{MS}^{-1}(A(z)) = \frac{1}{n}\sum_{i=0}^{n-1} A(\alpha^{ri})x^i. \tag{4.38}$$

The integer r comes into play when 2^m-1 is not a prime, that is, 2^m-1 is not a Mersenne prime, otherwise $r=1$. As an example, we will consider $\mathbb{F}_{2^4}$ and the extension field table of non-zero elements is given in Table 4.1 with $1+\alpha+\alpha^4=0$, modulo $1+x^{15}$.

Consider the polynomial $a(x)$ denoted as

$$a(x) = \sum_{i=0}^{n-1} a_i x^i = 1+x^3+x^4. \tag{4.39}$$

We will evaluate the Mattson–Solomon polynomial coefficient by coefficient:

$A(0) = a_0 + a_3 + a_4 = 1+1+1 = 1$

$A(1) = a_0 + a_3\alpha^{-3} + a_4\alpha^{-4} = 1+\alpha^{12}+\alpha^{11} = 1+1+\alpha+\alpha^2+\alpha^3+\alpha+\alpha^2+\alpha^3 = 0$

$A(2) = a_0 + a_3\alpha^{-6} + a_4\alpha^{-8} = 1+\alpha^9+\alpha^7 = 1+\alpha+\alpha^3+1+\alpha+\alpha^3 = 0$

$A(3) = a_0 + a_3\alpha^{-9} + a_4\alpha^{-12} = 1+\alpha^6+\alpha^3 = 1+\alpha^2+\alpha^3+\alpha^3 = \alpha^8$

$A(4) = a_0 + a_3\alpha^{-12} + a_4\alpha^{-16} = 1+\alpha^3+\alpha^{14} = 1+\alpha^3+1+\alpha^3 = 0$

$A(5) = a_0 + a_3\alpha^{-15} + a_4\alpha^{-20} = 1+1+\alpha^{10} = \alpha^{10}$

$A(6) = a_0 + a_3\alpha^{-18} + a_4\alpha^{-24} = 1+\alpha^{12}+\alpha^6 = \alpha$

$A(7) = a_0 + a_3\alpha^{-21} + a_4\alpha^{-28} = 1+\alpha^9+\alpha^2 = 1+\alpha+\alpha^3+\alpha^2 = \alpha^{12}$

$A(8) = a_0 + a_3\alpha^{-24} + a_4\alpha^{-32} = 1+\alpha^6+\alpha^{13} = 0$

$$
\begin{aligned}
A(9) &= a_0 + a_3\alpha^{-27} + a_4\alpha^{-36} = 1 + \alpha^3 + \alpha^9 = 1 + \alpha = \alpha^4 \\
A(10) &= a_0 + a_3\alpha^{-30} + a_4\alpha^{-40} = 1 + 1 + \alpha^5 = \alpha^5 \\
A(11) &= a_0 + a_3\alpha^{-33} + a_4\alpha^{-44} = 1 + \alpha^{12} + \alpha = \alpha^6 \\
A(12) &= a_0 + a_3\alpha^{-36} + a_4\alpha^{-48} = 1 + \alpha^9 + \alpha^{12} = \alpha^2 \\
A(13) &= a_0 + a_3\alpha^{-39} + a_4\alpha^{-52} = 1 + \alpha^6 + \alpha^8 = \alpha^3 \\
A(14) &= a_0 + a_3\alpha^{-42} + a_4\alpha^{-56} = 1 + \alpha^3 + \alpha^4 = \alpha^9.
\end{aligned} \tag{4.40}
$$

It can be seen that $A(z)$ is

$$
\begin{aligned}
A(z) = 1 &+ \alpha^8 z^3 + \alpha^{10} z^5 + \alpha z^6 + \alpha^{12} z^7 + \alpha^4 z^9 + \alpha^5 z^(10) + \alpha^6 z^{11} + \alpha^2 z^{12} \\
&+ \alpha^3 z^{13} + \alpha^9 z^{14}.
\end{aligned}
$$

A(z) has four zeros corresponding to the roots α^{-1}, α^{-2}, α^{-4} and α^{-8}, and these are the roots of $1 + x^3 + x^4$. These are also 4 of the 15 roots of $1 + x^{15}$. Factorising $1 + x^{15}$ produces the identity

$$
1 + x^{15} = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4). \tag{4.41}
$$

It can be seen that $1 + x^3 + x^4$ is one of the factors of $1 + x^{15}$.

Another point to notice is that $A(z) = A(z)^2$ and $A(z)$ is an idempotent. The reason for this is that the inverse Mattson–Solomon polynomial of $A(z)$ will produce $a(x)$ a polynomial that has binary coefficients. Let $\cdot$ denote the dot product of polynomials, i.e.

$$
\left(\sum A_i z^i\right) \cdot \left(\sum B_i z^i\right) = \sum A_i B_i z^i.
$$

It follows from the Mattson–Solomon polynomial that with $a(x)b(x) = c(x)$, $\sum C_i z^i = \sum A_i B_i z^i$.

This concept is analogous to multiplication and convolution in the time and frequency domains, where the Fourier and inverse Fourier transforms correspond to the inverse Mattson–Solomon and Mattson–Solomon polynomials, respectively. In the above example, $A(z)$ is an idempotent which leads to the following lemma.

Lemma 4.1 *The Mattson–Solomon polynomial of a polynomial having binary coefficients is an idempotent.*

Proof Let $c(x) = a(x) \cdot b(x)$. The Mattson–Solomon polynomial of $c(x)$ is $C(z) = A(z)B(z)$. Setting $b(x) = a(x)$ then $C(z) = A(z)A(z) = A(z)^2$. If $a(x)$ has binary coefficients, then $c(x) = a(x) \cdot a(x) = a(x)$ and $A(z)^2 = A(z)$. Therefore $A(z)$ is an idempotent.

Of course the reverse is true.

Lemma 4.2 *The Mattson–Solomon polynomial of an idempotent is a polynomial having binary coefficients.*

Proof Let $c(x) = a(x)b(x)$. The Mattson–Solomon polynomial of $c(x)$ is $C(z) = A(z)B(z)$. Setting $b(x) = a(x)$ then $C(z) = A(z) \cdot A(z)$. If $a(x)$ is an idempotent then $c(x) = a(x)^2 = a(x)$ and $A(z) = A(z) \cdot A(z)$. The only values for the coefficients of $A(z)$ that satisfy this constraint are the values 0 and 1. Hence, the Mattson Solomon polynomial, $A(z)$, has binary coefficients.

A polynomial that has binary coefficients and is an idempotent is a binary idempotent, and combining Lemmas 4.1 and 4.2 produces the following lemma.

Lemma 4.3 *The Mattson–Solomon polynomial of a binary idempotent is also a binary idempotent.*

Proof The proof follows immediately from the proofs of Lemmas 4.1 and 4.2. As $a(x)$ is an idempotent, then from Lemma 4.1, $A(z)$ has binary coefficients. As $a(x)$ also has binary coefficients, then from Lemma 4.2, $A(z)$ is an idempotent. Hence, $A(z)$ is a binary idempotent.

As an example consider the binary idempotent $a(x)$ from $GF(16)$ listed in Table 4.1:

$$a(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12}.$$

The Mattson–Solomon polynomial $A(z)$ is

$$A(z) = z^7 + z^{11} + z^{13} + z^{14},$$

which is also a binary idempotent.

Since the Mattson polynomial of $a(x^{-1})$ is the same as the inverse Mattson polynomial of $a(x)$ consider the following example:

$$a(x) = x^{-7} + x^{-11} + x^{-13} + x^{-14} = x + x^2 + x^4 + x^4.$$

The Mattson–Solomon polynomial $A(z)$ is the binary idempotent

$$A(z) = z + z^2 + z^3 + z^4 + z^6 + z^8 + z^9 + z^{12}.$$

This is the reverse of the first example above.

The polynomial $1 + x + x^3$ has no roots of $1 + x^{15}$ and so defining $b(x)$

$$b(x) = (1 + x + x^3)(1 + x^3 + x^4) = 1 + x + x^5 + x^6 + x^7. \tag{4.42}$$

When the Mattson–Solomon polynomial is evaluated, $B(z)$ is given by

$$B(z) = 1 + z + z^5 + z^6 + z^7. \tag{4.43}$$

4.4 Binary Cyclic Codes Derived from Idempotents

In their book, MacWilliams and Sloane [2] describe the Mattson–Solomon polynomial and show that cyclic codes may be constructed straightforwardly from idempotents. An idempotent is a polynomial $\theta(x)$ with coefficients from a base field $GF(p)$ that has the property that $\theta^p(x) = \theta(x)$. The family of Bose–Chaudhuri–Hocquenghem (BCH) cyclic codes may be constructed directly from the Mattson–Solomon polynomial. From the idempotents, other cyclic codes may be constructed which have low-weight dual-code codewords or equivalently sparseness of the parity-check matrix (see Chap. 12).

Definition 4.3 (*Binary Idempotent*) Consider $e(x) \in T(x)$, $e(x)$ is an idempotent if the property of $e(x) = e^2(x) = e(x^2) \bmod (x^n - 1)$ is satisfied.

An (n, k) binary cyclic code may be described by the generator polynomial $g(x) \in T(x)$ of degree $n-k$ and the parity-check polynomial $h(x) \in T(x)$ of degree k, such that $g(x)h(x) = x^n - 1$. According to [2], as an alternative to $g(x)$, an idempotent may also be used to generate cyclic codes. Any binary cyclic code can be described by a unique idempotent $e_g(x) \in T(x)$ which consists of a sum of primitive idempotents. The unique idempotent $e_g(x)$ is known as the *generating idempotent* and as the name implies, $g(x)$ is a divisor of $e_g(x)$, and to be more specific $e_g(x) = m(x)g(x)$, where $m(x) \in T(x)$ contains repeated factors or non-factors of $x^n - 1$.

Lemma 4.4 *If $e(x) \in T(x)$ is an idempotent, $E(z) = MS(e(x)) \in T(z)$.*

Proof Since $e(x) = e(x)^2 \pmod{x^n - 1}$, from (4.37) it follows that $e(\alpha^{-rj}) = e(\alpha^{-rj})^2$ for $j = \{0, 1, \ldots, n-1\}$ and some integer r. Clearly $e(\alpha^{-rj}) \in \{0, 1\}$ implying that $E(z)$ is a binary polynomial.

Definition 4.4 (*Cyclotomic Coset*) Let s be a positive integer, and the $2-$cyclotomic coset of $s \pmod{n}$ is given by

$$C_s = \left\{ 2^i s \pmod{n} \mid 0 \le i \le t \right\},$$

where we shall always assume that the subscript s is the smallest element in the set C_s and t is the smallest positive integer such that $2^{t+1}s \equiv s \pmod{n}$.

For convenience, we will use the term cyclotomic coset to refer to $2-$cyclotomic coset throughout this book. If $\mathcal{N}$ is the set consisting of the smallest elements of all possible cyclotomic cosets, then it follows that

$$C = \bigcup_{s \in \mathcal{N}} C_s = \{0, 1, 2, \ldots, n-1\}.$$

Definition 4.5 (*Binary Cyclotomic Idempotent*) Let the polynomial $e_s(x) \in T(x)$ be given by

$$e_s(x) = \sum_{0 \le i \le |C_s|-1} x^{C_{s,i}}, \tag{4.44}$$

where $|C_s|$ is the number of elements in C_s and $C_{s,i} = 2^i s \pmod{n}$, the $(i+1)$th element of C_s. The polynomial $e_s(x)$ is called a binary cyclotomic idempotent.

Example 4.2 The entire cyclotomic cosets of 63 and their corresponding binary cyclotomic idempotents are as follows:

$$\begin{aligned}
C_0 &= \{0\} & e_0(x) &= 1\\
C_1 &= \{1, 2, 4, 8, 16, 32\} & e_1(x) &= x + x^2 + x^4 + x^8 + x^{16} + x^{32}\\
C_3 &= \{3, 6, 12, 24, 48, 33\} & e_3(x) &= x^3 + x^6 + x^{12} + x^{24} + x^{33} + x^{48}\\
C_5 &= \{5, 10, 20, 40, 17, 34\} & e_5(x) &= x^5 + x^{10} + x^{17} + x^{20} + x^{34} + x^{40}\\
C_7 &= \{7, 14, 28, 56, 49, 35\} & e_7(x) &= x^7 + x^{14} + x^{28} + x^{35} + x^{49} + x^{56}\\
C_9 &= \{9, 18, 36\} & e_9(x) &= x^9 + x^{18} + x^{36}\\
C_{11} &= \{11, 22, 44, 25, 50, 37\} & e_{11}(x) &= x^{11} + x^{22} + x^{25} + x^{37} + x^{44} + x^{50}\\
C_{13} &= \{13, 26, 52, 41, 19, 38\} & e_{13}(x) &= x^{13} + x^{19} + x^{26} + x^{38} + x^{41} + x^{52}\\
C_{15} &= \{15, 30, 60, 57, 51, 39\} & e_{15}(x) &= x^{15} + x^{30} + x^{39} + x^{51} + x^{57} + x^{60}\\
C_{21} &= \{21, 42\} & e_{21}(x) &= x^{21} + x^{42}\\
C_{23} &= \{23, 46, 29, 58, 53, 43\} & e_{23}(x) &= x^{23} + x^{29} + x^{43} + x^{46} + x^{53} + x^{58}\\
C_{27} &= \{27, 54, 45\} & e_{27}(x) &= x^{27} + x^{45} + x^{54}\\
C_{31} &= \{31, 62, 61, 59, 55, 47\} & e_{31}(x) &= x^{31} + x^{47} + x^{55} + x^{59} + x^{61} + x^{62}
\end{aligned}$$

and $\mathscr{N} = \{0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31\}$.

Definition 4.6 (*Binary Parity-Check Idempotent*) Let $\mathscr{M} \subseteq \mathscr{N}$ and let the polynomial $u(x) \in T(x)$ be defined by

$$u(x) = \sum_{s \in \mathscr{M}} e_s(x), \tag{4.45}$$

where $e_s(x)$ is an idempotent. The polynomial $u(x)$ is called a binary parity-check idempotent.

The binary parity-check idempotent $u(x)$ can be used to describe an $[n, k]$ cyclic code. Since $\mathrm{GCD}(u(x), x^n - 1) = h(x)$, the polynomial $\bar{u}(x) = x^{\deg(u(x))} u(x^{-1})$ and its n cyclic shifts $\pmod{x^n - 1}$ can be used to define the parity-check matrix of a binary cyclic code. In general, $\mathrm{wt}_H(\bar{u}(x))$ is much lower than $\mathrm{wt}_H(h(x))$, and therefore a sparse parity-check matrix can be derived from $\bar{u}(x)$. This is important for cyclic codes designed to be used as low-density parity-check (LDPC) codes, see Chap. 12.

4.4.1 Non-Primitive Cyclic Codes Derived from Idempotents

The factors of $2^m - 1$ dictate the degrees of the minimal polynomials through the order of the cyclotomic cosets. Some relatively short non-primitive cyclic codes have minimal polynomials of high degree which makes it tedious to derive the generator polynomial or parity-check polynomial using the Mattson–Solomon polynomial. The prime factors of $2^m - 1$ for $m \leq 43$ are tabulated below in Table 4.2.

The Mersenne primes shown in Table 4.2 are $2^3 - 1$, $2^5 - 1$, $2^7 - 1$, $2^{13} - 1$, $2^{17} - 1$, $2^{19} - 1$, $2^{23} - 1$ and $2^{31} - 1$, and cyclic codes of these lengths are primitive cyclic codes. Non-primitive cyclic codes have lengths corresponding to factors of $2^m - 1$ which are not Mersenne primes. Also it may be seen in Table 4.2 that for m even, 3 is a common factor. Where m is congruent to 5, with $m = 5 \times s$, 31 is a common factor and all $M_{j\,5}$ minimal polynomials will be contained in the set, $M_{j\,5\times s}$ of minimal polynomials.

As an example of how useful Table 4.2 can be, consider a code of length 113. Table 4.2 shows that $2^{28} - 1$ contains 113 as a factor. This means that there is a polynomial of degree 28 that has a root β of order 113. In fact, $\beta = \alpha^{2375535}$, where α is a primitive root, because $2^{28} - 1 = 2375535 \times 113$.

The cyclotomic cosets of 113 are as follows:

$$
\begin{aligned}
C_0 &= \{0\} \\
C_1 &= \{1, 2, 4, 8, 16, 32, 64, 15, 30, 60, 7, 14, 28, 56, \\
&\quad 112, 111, 109, 105, 97, 81, 49, 98, 83, 53, 106, 99, 85, 57\} \\
C_3 &= \{3, 6, 12, 24, 48, 96, 79, 45, 90, 67, 21, 42, 84, \\
&\quad 55, 110, 107, 101, 89, 65, 17, 34, 68, 23, 46, 92, 71, 29, 58\} \\
C_5 &= \{5, 10, 20, 40, 80, 47, 94, 75, 37, 74, 35, 70, 27, \\
&\quad 54, 108, 103, 93, 73, 33, 66, 19, 38, 76, 39, 78, 43, 86, 59\} \\
C_7 &= \{9, 18, 36, 72, 31, 62, 11, 22, 44, 88, 63, 13, 26, \\
&\quad 52, 104, 95, 77, 41, 82, 51, 102, 91, 69, 25, 50, 100, 87, 61\}.
\end{aligned}
$$

Each coset apart from C_0 may be used to define 28 roots from a polynomial having binary coefficients and of degree 28. Alternatively, each cyclotomic coset may be used to define the non-zero coefficients of a polynomial, a minimum weight idempotent (see Sect. 4.4). Adding together any combination of the 5 minimum weight idempotents generates a cyclic code of length 113. Consequently, there are only $2^5 - 2 = 30$ non-trivial, different cyclic codes of length 113 and some of these will be equivalent codes. Using Euclid's algorithm, it is easy to find the common factors of each idempotent combination and $x^{113} - 1$. The resulting polynomial may be used as the generator polynomial, or the parity-check polynomial of the cyclic code.

Table 4.2 Prime factors of $2^m - 1$

m	$2^m - 1$	Factors	m	$2^m - 1$	Factors
2	3	3	23	8388607	47×178481
3	7	7	24	16777215	$3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$
4	15	5×3	25	33554431	$31 \times 601 \times 1801$
5	31	31	26	67108863	$3 \times 2731 \times 8191$
6	63	$3 \times 3 \times 7$	27	134217727	$7 \times 73 \times 262657$
7	127	127	28	268435455	$3 \times 5 \times 29 \times 43 \times 113 \times 127$
8	255	$3 \times 5 \times 17$	29	536870911	$233 \times 1103 \times 2089$
9	511	7×73	30	1073741823	$3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$
10	1023	$3 \times 11 \times 31$	31	2147483647	2147483647
11	2047	23×89	32	4294967295	$3 \times 5 \times 17 \times 257 \times 65537$
12	4095	$3 \times 3 \times 5 \times 7 \times 13$	33	8589934591	$7 \times 23 \times 89 \times 599479$
13	8191	8191	34	17179869183	$3 \times 43691 \times 131071$
14	16383	$3 \times 43 \times 127$	35	34359738367	$31 \times 71 \times 127 \times 122921$
15	32767	$7 \times 31 \times 151$	36	68719476735	$3 \times 3 \times 3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73 \times 109$
16	65535	$3 \times 5 \times 17 \times 257$	37	137438953471	223×616318177
17	131071	131071	38	274877906943	$3 \times 174763 \times 524287$
18	262143	$3 \times 3 \times 3 \times 7 \times 19 \times 73$	39	549755813887	$7 \times 79 \times 8191 \times 121369$
19	524287	524287	40	1099511627775	$3 \times 5 \times 5 \times 11 \times 17 \times 31 \times 41 \times 61681$
20	1048575	$3 \times 5 \times 5 \times 11 \times 31 \times 41$	41	2199023255551	13367×164511353
21	2097151	$7 \times 7 \times 127 \times 337$	42	4398046511103	$3 \times 3 \times 7 \times 7 \times 43 \times 127 \times 337 \times 5419$
22	4194303	$3 \times 23 \times 89 \times 683$	43	8796093022207	$431 \times 9719 \times 2099863$

For example, consider the GCD of $C_1 + C_3 = x + x^2 + x^3 + x^4 + x^6 + x^8 + \ldots + x^{109} + x^{110} + x^{111} + x^{112}$ and $x^{113} - 1$. This is the polynomial, $u(x)$, which turns out to have degree 57

$$u(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^{10} + x^{13} \\ \ldots + x^{51} + x^{52} + x^{54} + x^{55} + x^{56} + x^{57}.$$

Using $u(x)$ as the parity-check polynomial of the cyclic code produces a (113, 57, 18) code. This is quite a good code as the very best (113, 57) code has a minimum Hamming distance of 19.

As another example of using this method for non-primitive cyclic code construction, consider the factors of $2^{39} - 1$ in Table 4.2. It will be seen that 79 is a factor and so a cyclic code of length 79 may be constructed from polynomials of degree 39. The cyclotomic cosets of 79 are as follows:

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4, 8, 16, 32, 64, 49, 19, 38, 76, 73, \ldots 20, 40\}$$
$$C_3 = \{3, 6, 12, 24, 48, 17, 34, 68, 57, 35, 70, \ldots 60, 41\}.$$

The GCD of the idempotent sum given by the cyclotomic cosets $C_0 + C_1$ and $x^{79} - 1$ is the polynomial, $u(x)$, of degree 40:

$$u(x) = 1 + x + x^3 + x^5 + x^8 + x^{11} + x^{12} + x^{16} \\ \ldots + x^{28} + x^{29} + x^{34} + x^{36} + x^{37} + x^{40}.$$

Using $u(x)$ as the parity-check polynomial of the cyclic code produces a (79, 40, 15) code. This is the quadratic residue cyclic code for the prime number 79 and is a best-known code.

In a further example Table 4.2 shows that $2^{37} - 1$ has 223 as a factor. The GCD of the idempotent given by the cyclotomic coset $C_3\, x^3 + x^6 + x^{12} + x^{24} + x^{48} + \ldots + x^{198} + x^{204}$ and $x^{223} - 1$ is the polynomial, $u(x)$, of degree 111

$$u(x) = 1 + x^2 + x^3 + x^5 + x^8 + x^9 + x^{10} + x^{12} \\ \ldots + x^{92} + x^{93} + x^{95} + x^{103} + x^{107} + x^{111}.$$

Using $u(x)$ as the parity-check polynomial of the cyclic code produces a (223, 111, 32) cyclic code.

4.5 Binary Cyclic Codes of Odd Lengths from 129 to 189

Since many of the best-known codes are cyclic codes, it is useful to have a table of the best cyclic codes. The literature already contains tables of the best cyclic codes up to length 127 and so the following table starts at 129. All possible binary cyclic codes up to length 189 have been constructed and their minimum Hamming distance has been evaluated.

The highest minimum distance attainable by all binary cyclic codes of odd lengths $129 \leq n \leq 189$ is tabulated in Table 4.3. The column "Roots of $g(x)$" in Table 4.3 denotes the exponents of roots of the generator polynomial $g(x)$, excluding the conjugate roots. All cyclic codes with generator polynomials $1+x$ and $(x^n-1)/(1+x)$, since they are trivial codes, are excluded in Table 4.3 and since primes $n = 8m \pm 3$ contain these trivial cyclic codes only, there is no entry in the table for these primes. The number of permutation inequivalent and non-degenerate cyclic codes, excluding the two trivial codes mentioned earlier, for each odd integer n is given by $N_{\mathscr{C}}$. The primitive polynomial $m(x)$ defining the field is given in octal. Full details describing the derivation of Table 4.3 are provided in Sect. 5.3.

In Table 4.3, there is no cyclic code that improves the lower bound given by Brouwer [1], but there are 134 cyclic codes that meet this lower bound and these codes are printed in bold.

4.6 Summary

The important large family of binary cyclic codes has been explored in this chapter. Starting with cyclotomic cosets, the minimal polynomials were introduced. The Mattson–Solomon polynomial was described and it was shown to be an inverse discrete Fourier transform based on a primitive root of unity. The usefulness of the Mattson–Solomon polynomial in the design of cyclic codes was demonstrated. The relationship between idempotents and the Mattson–Solomon polynomial of a polynomial that has binary coefficients was described with examples given. It was shown how binary cyclic codes may be easily derived from idempotents and the cyclotomic cosets. In particular, a method was described based on cyclotomic cosets for the design of high-degree non-primitive binary cyclic codes. Code examples using the method were presented.

A table listing the complete set of the best binary cyclic codes, having the highest minimum Hamming distance, has been included for all code lengths from 129 to 189 bits.

Table 4.3 The highest attainable minimum distance of binary cyclic codes of odd lengths from 129 to 189

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
$n = 129, m(x) = 77277, N_{\mathscr{C}} = 388$								
127	**2**	**43**	**84**	**14**	**0, 1, 19, 21, 43**	42	30	0, 1, 3, 7, 9, 11, 19, 43
115	3	1	73	15	1, 3, 7, 19	31	32	1, 7, 9, 11, 13, 19, 21
114	**6**	**0, 1**	**72**	**18**	**0, 1, 7, 9, 19**	**30**	**38**	**0, 1, 3, 7, 9, 11, 13, 19**
113	4	3, 43	71	17	1, 3, 7, 19, 43	29	37	1, 3, 7, 11, 13, 19, 21, 43
112	**6**	**0, 1, 43**	70	18	0, 1, 3, 7, 19, 43	28	40	0, 1, 3, 7, 11, 13, 19, 21, 43
101	**8**	**1, 9**	59	22	1, 3, 7, 9, 19	17	43	1, 3, 7, 9, 11, 13, 19, 21
100	**10**	**0, 1, 3**	58	22	0, 1, 3, 7, 9, 19	**16**	**52**	**0, 1, 3, 7, 9, 11, 13, 19, 21**
99	8	1, 9, 43	57	22	1, 3, 7, 9, 19, 43	15	54	1, 3, 7, 9, 11, 13, 19, 21, 43
98	**10**	**0, 1, 3, 43**	**56**	**24**	**0, 1, 5, 9, 19, 21, 43**	14	54	0, 1, 3, 7, 9, 11, 13, 19, 21, 43
87	**13**	**1, 13, 21**	**45**	**29**	**1, 3, 7, 9, 11, 19**	**2**	**86**	**0, 1, 3, 5, 7, 9, 11, 13, 19, 21**
86	**14**	**0, 1, 19, 21**	**44**	**30**	**0, 1, 3, 7, 9, 11, 19**			
85	13	1, 19, 21, 43	43	29	1, 3, 7, 9, 11, 19, 43			
$n = 133, m(x) = 1334325, N_{\mathscr{C}} = 198$								
130	**2**	**57**	91	8	1, 7, 19, 57	43	19	1, 7, 9, 15, 31
129	**2**	**0, 57**	90	10	0, 1, 19, 31, 57	42	28	0, 1, 5, 7, 9, 31
127	**2**	**19, 57**	79	14	1, 7, 31	**40**	**32**	**1, 5, 7, 9, 31, 57**
126	**2**	**0, 19, 57**	78	14	0, 1, 5, 9	**39**	**32**	**0, 1, 5, 7, 9, 31, 57**
115	3	1	76	16	1, 7, 31, 57	37	32	1, 5, 7, 9, 19, 31, 57
114	4	0, 1	75	16	0, 1, 7, 31, 57	36	32	0, 1, 5, 7, 9, 19, 31, 57
112	**6**	**31, 57**	73	16	1, 7, 19, 31, 57	25	19	1, 3, 5, 7, 9, 31
111	6	0, 31, 57	72	16	0, 1, 7, 19, 31, 57	24	38	0, 1, 3, 5, 7, 9, 31
109	6	1, 19, 57	61	19	1, 7, 9, 31	22	44	1, 5, 7, 9, 15, 31, 57
108	6	0, 1, 19, 57	**60**	**24**	**0, 1, 3, 7, 9**	21	44	0, 1, 5, 7, 9, 15, 31, 57

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
97	7	1, 31	**58**	**24**	**1, 7, 9, 31, 57**	19	48	1, 3, 5, 7, 9, 19, 31, 57
96	10	0, 1, 31	**57**	**24**	**0, 1, 7, 9, 31, 57**	18	48	0, 1, 3, 5, 7, 9, 19, 31, 57
94	8	7, 31, 57	55	24	1, 7, 9, 19, 31, 57	4	57	1, 3, 5, 7, 9, 15, 31, 57
93	10	0, 1, 31, 57	54	24	0, 1, 7, 9, 19, 31, 57	**3**	**76**	**0, 1, 3, 5, 7, 9, 15, 31, 57**
$n = 135$, $m(x) = 1000000001001$, $N_{\mathscr{C}} = 982$								
133	**2**	**45**	89	6	1, 15, 63	45	10	1, 7, 21, 45, 63
132	**2**	**0, 45**	88	6	0, 1, 15, 63	44	10	0, 1, 7, 21, 45, 63
131	**2**	**63**	87	6	1, 15, 45, 63	43	10	1, 7, 15, 21, 45
130	**2**	**0, 63**	86	6	0, 1, 15, 45, 63	42	10	0, 1, 7, 15, 21, 45
129	**2**	**45, 63**	85	6	1, 21, 45	41	10	1, 7, 15, 21, 63
128	**2**	**0, 45, 63**	84	6	0, 1, 21, 45	40	10	0, 1, 7, 15, 21, 63
127	2	15, 45	83	6	1, 15, 27, 45, 63	39	10	1, 7, 15, 21, 45, 63
126	2	0, 15, 45	82	6	0, 1, 21, 63	38	10	0, 1, 7, 15, 21, 45, 63
125	2	15, 63	81	6	1, 21, 45, 63	37	10	1, 3, 7, 21, 45
124	2	0, 15, 63	80	6	0, 1, 21, 45, 63	36	10	0, 1, 3, 7, 21, 45
123	2	15, 45, 63	79	6	1, 15, 21, 45	35	12	1, 5, 7, 15, 63
122	2	0, 15, 45, 63	78	6	0, 1, 15, 21, 45	34	12	0, 1, 5, 7, 15, 63
121	2	21, 45	77	6	1, 5, 63	33	12	1, 5, 7, 15, 45, 63
120	2	0, 21, 45	76	6	0, 1, 5, 63	32	12	0, 1, 5, 7, 15, 45, 63
119	2	21, 63	75	6	1, 5, 45, 63	31	12	1, 5, 7, 21, 45
118	2	0, 21, 63	74	6	0, 1, 5, 45, 63	30	12	0, 1, 5, 7, 21, 45
117	2	21, 45, 63	73	6	1, 3, 21, 45	29	15	1, 5, 7, 21, 63
116	2	0, 21, 45, 63	72	6	0, 1, 3, 21, 45	28	18	0, 1, 5, 7, 21, 63
115	2	5, 45	71	8	1, 5, 15, 63	27	18	1, 5, 7, 21, 45, 63
114	2	0, 5, 45	70	8	0, 1, 5, 15, 63	26	18	0, 1, 5, 7, 21, 45, 63

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
113	4	5, 63	69	8	1, 5, 15, 45, 63	25	15	1, 5, 7, 21, 27, 63
112	4	0, 5, 63	68	8	0, 1, 5, 15, 45, 63	24	18	0, 1, 5, 7, 21, 27, 63
111	4	5, 45, 63	67	8	1, 5, 21, 45	23	21	1, 5, 7, 15, 21, 63
110	4	0, 5, 45, 63	66	8	0, 1, 5, 21, 45	22	24	0, 1, 5, 7, 15, 21, 63
109	4	5, 27, 63	65	8	1, 5, 15, 27, 45, 63	21	24	1, 5, 7, 15, 21, 45, 63
108	4	0, 5, 27, 63	64	8	0, 1, 5, 21, 63	20	24	0, 1, 5, 7, 15, 21, 45, 63
107	4	5, 15, 63	63	8	1, 5, 21, 45, 63	19	21	1, 5, 7, 15, 21, 27, 63
106	4	0, 5, 15, 63	62	8	0, 1, 5, 21, 45, 63	18	24	0, 1, 5, 7, 15, 21, 27, 63
105	4	5, 15, 45, 63	61	8	1, 5, 15, 21, 45	17	24	1, 5, 7, 15, 21, 27, 45, 63
104	4	0, 5, 15, 45, 63	60	8	0, 1, 5, 15, 21, 45	16	30	0, 1, 3, 5, 7, 21, 63
103	4	5, 21, 45	59	8	1, 5, 15, 21, 63	15	30	1, 3, 5, 7, 21, 27, 45
102	4	0, 5, 21, 45	58	8	0, 1, 5, 15, 21, 63	14	30	0, 1, 3, 5, 7, 21, 45, 63
101	4	5, 21, 63	57	8	1, 5, 15, 21, 45, 63	13	24	1, 5, 7, 9, 15, 21, 27, 45, 63
100	4	0, 5, 21, 63	56	8	0, 1, 5, 15, 21, 45, 63	12	30	0, 1, 3, 5, 7, 21, 27, 63
99	4	5, 21, 45, 63	55	8	1, 3, 5, 21, 45	11	30	1, 3, 5, 7, 21, 27, 45, 63
98	4	0, 5, 21, 45, 63	54	8	0, 1, 3, 5, 21, 45	10	36	0, 1, 3, 5, 7, 15, 21, 63
97	4	1, 45	53	10	1, 7, 15, 63	9	36	1, 3, 5, 7, 15, 21, 27, 45
96	4	0, 1, 45	52	10	0, 1, 7, 15, 63	8	36	0, 1, 3, 5, 7, 15, 21, 45, 63
95	5	1, 63	51	10	1, 7, 15, 45, 63	7	45	1, 3, 5, 7, 15, 21, 27, 63
94	6	0, 1, 63	50	10	0, 1, 7, 15, 45, 63	6	54	0, 1, 3, 5, 7, 15, 21, 27, 63
93	6	1, 45, 63	49	10	1, 7, 21, 45	5	63	1, 3, 5, 7, 15, 21, 27, 45, 63
92	6	0, 1, 45, 63	48	10	0, 1, 7, 21, 45	**4**	**72**	**0, 1, 3, 5, 7, 15, 21, 27, 45, 63**
91	5	1, 27, 63	47	10	1, 7, 15, 27, 45, 63			
90	6	0, 1, 27, 63	46	10	0, 1, 7, 21, 63			

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
$n = 137, m(x) = 673573303732676066 75673, N_{\mathscr{C}} = 2$								
69	21	1	68	22	0, 1			
$n = 141, m(x) = 2146417666311013, N_{\mathscr{C}} = 30$								
139	**2**	**47**	93	4	3, 15, 47	47	24	1, 3, 15, 47
138	**2**	**0, 47**	92	6	0, 1, 47	46	24	0, 1, 3, 15, 47
118	2	3	72	21	3, 5	26	33	1, 3, 5
117	2	0, 3	**71**	**22**	**0, 3, 5**	25	36	0, 1, 3, 5
116	4	3, 47	70	21	3, 5, 47	24	33	1, 3, 5, 47
115	4	0, 3, 47	**69**	**24**	**0, 3, 5, 47**	23	36	0, 1, 3, 5, 47
95	3	1	49	22	1, 3, 15			
94	6	0, 1	48	22	0, 1, 3, 15			
$n = 143, m(x) = 1452367605473245050 61, N_{\mathscr{C}} = 16$								
133	2	13	83	11	1	61	24	1, 11, 13
132	2	0, 13	82	12	0, 1	60	24	0, 1, 11, 13
131	2	11	73	11	1, 13	23	11	1, 5
130	2	0, 11	72	16	0, 1, 13	22	22	0, 1, 5
121	4	11, 13	71	13	1, 11			
120	4	0, 11, 13	70	18	0, 1, 11			
$n = 145, m(x) = 3572445367, N_{\mathscr{C}} = 40$								
141	**2**	**29**	89	14	1, 5	57	26	1, 5, 11, 29
140	**2**	**0, 29**	88	14	0, 1, 5	56	26	0, 1, 5, 11, 29
117	5	1	85	14	1, 5, 29	33	29	1, 3, 5, 11
116	**8**	**0, 1**	84	14	0, 1, 5, 29	**32**	**44**	**0, 1, 3, 5, 11**
113	5	1, 29	61	24	1, 5, 11	29	46	1, 3, 5, 11, 29
112	**10**	**0, 1, 29**	60	24	0, 1, 5, 11	28	46	0, 1, 3, 5, 11, 29

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
$n = 147, m(x) = 100002000040201, N_{\mathscr{C}} = 488$								
145	**2**	**49**	96	4	0, 1, 35, 49	48	8	1, 3, 7, 9, 21, 35
144	**2**	**0, 49**	95	4	0, 1, 21, 35	47	8	0, 1, 3, 7, 9, 21, 35
143	**2**	**0, 21**	94	4	1, 21, 35, 49	46	8	1, 3, 7, 9, 21, 35, 49
142	**2**	**21, 49**	93	4	0, 1, 21, 35, 49	45	8	0, 1, 3, 7, 9, 21, 35, 49
141	**2**	**35**	92	4	0, 1, 7, 35	44	8	0, 1, 3, 7, 9, 21, 35, 63
140	**2**	**0, 35**	91	4	1, 21, 35, 49, 63	43	8	1, 3, 7, 9, 21, 35, 49, 63
139	2	35, 49	90	4	1, 7, 21, 35	42	8	0, 1, 3, 7, 9, 21, 35, 49, 63
138	2	0, 35, 49	89	4	0, 1, 7, 21, 35	40	9	1, 5, 9, 49
137	2	0, 7, 21	88	4	1, 7, 21, 35, 49	39	12	0, 1, 5, 9, 49
136	2	21, 35, 49	87	4	0, 1, 7, 21, 35, 49	38	10	0, 1, 5, 9, 21
135	2	7, 35	86	4	0, 1, 7, 21, 35, 63	37	12	1, 5, 9, 21, 49
134	2	0, 7, 35	85	4	1, 7, 21, 35, 49, 63	36	12	0, 1, 5, 9, 21, 49
133	2	21, 35, 49, 63	84	4	0, 1, 7, 21, 35, 49, 63	35	12	0, 1, 5, 9, 35
132	2	7, 21, 35	82	5	5, 9, 49	34	12	1, 5, 9, 21, 49, 63
131	2	0, 7, 21, 35	81	8	0, 5, 9, 49	33	12	0, 1, 5, 9, 35, 49
130	2	7, 21, 35, 49	80	6	0, 5, 9, 21	32	12	0, 1, 5, 9, 21, 35
129	2	0, 7, 21, 35, 49	79	8	5, 9, 21, 49	31	12	1, 5, 9, 21, 35, 49
127	2	7, 21, 35, 49, 63	78	8	0, 5, 9, 21, 49	30	12	0, 1, 5, 9, 21, 35, 49
126	2	0, 7, 21, 35, 49, 63	77	8	0, 5, 9, 35	29	12	0, 1, 5, 7, 9, 35
124	3	9, 49	76	8	5, 9, 21, 49, 63	28	12	1, 5, 9, 21, 35, 49, 63
123	4	0, 9, 49	75	8	0, 5, 9, 35, 49	27	12	1, 5, 7, 9, 21, 35
122	2	0, 9, 21	74	8	0, 5, 9, 21, 35	26	12	0, 1, 5, 7, 9, 21, 35
121	4	9, 21, 49	73	8	5, 9, 21, 35, 49	25	12	1, 5, 7, 9, 21, 35, 49
120	4	0, 9, 21, 49	72	8	0, 5, 9, 21, 35, 49	24	12	0, 1, 5, 7, 9, 21, 35, 49

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
119	4	0, 9, 35	71	8	0, 5, 7, 9, 35	23	12	0, 1, 5, 7, 9, 21, 35, 63
118	4	9, 21, 49, 63	70	8	5, 9, 21, 35, 49, 63	22	12	1, 5, 7, 9, 21, 35, 49, 63
117	4	0, 9, 35, 49	69	8	5, 7, 9, 21, 35	21	12	0, 1, 5, 7, 9, 21, 35, 49, 63
116	4	0, 9, 21, 35	68	8	0, 5, 7, 9, 21, 35	19	14	1, 3, 5, 9, 49
115	4	9, 21, 35, 49	67	8	5, 7, 9, 21, 35, 49	18	14	0, 1, 3, 5, 9, 49
114	4	0, 9, 21, 35, 49	66	8	0, 5, 7, 9, 21, 35, 49	17	14	0, 1, 3, 5, 9, 21
113	4	0, 7, 9, 35	65	8	0, 5, 7, 9, 21, 35, 63	16	21	1, 3, 5, 9, 21, 49
112	4	9, 21, 35, 49, 63	64	8	5, 7, 9, 21, 35, 49, 63	15	28	0, 1, 3, 5, 9, 21, 49
111	4	7, 9, 21, 35	63	8	0, 5, 7, 9, 21, 35, 49, 63	14	28	0, 1, 3, 5, 9, 35
110	4	0, 7, 9, 21, 35	61	8	1, 3, 9, 49	13	28	1, 3, 5, 9, 21, 49, 63
109	4	7, 9, 21, 35, 49	60	8	0, 1, 3, 9, 49	12	35	1, 3, 5, 7, 9, 21
108	4	0, 7, 9, 21, 35, 49	59	6	0, 1, 5, 21	11	42	0, 1, 3, 5, 7, 9, 21
107	4	0, 7, 9, 21, 35, 63	58	8	1, 3, 9, 21, 49	10	35	1, 3, 5, 7, 9, 21, 49
106	4	7, 9, 21, 35, 49, 63	57	8	1, 3, 9, 35	9	56	0, 1, 3, 5, 7, 9, 21, 49
105	4	0, 7, 9, 21, 35, 49, 63	56	8	0, 1, 3, 9, 35	8	42	0, 1, 3, 5, 7, 9, 35
103	4	3, 9, 49	55	8	1, 3, 9, 35, 49	7	56	1, 3, 5, 9, 21, 35, 49, 63
102	4	0, 1, 49	54	8	0, 1, 3, 9, 35, 49	6	56	0, 1, 3, 5, 9, 21, 35, 49, 63
101	4	0, 1, 21	53	8	0, 1, 3, 9, 21, 35	5	70	0, 1, 3, 5, 7, 9, 21, 35
100	4	1, 21, 49	52	8	1, 3, 9, 21, 35, 49	4	63	1, 3, 5, 7, 9, 21, 35, 49
99	4	0, 1, 21, 49	51	8	1, 3, 7, 9, 35	**3**	**84**	**0, 1, 3, 5, 7, 9, 21, 35, 49**
98	4	0, 1, 35	50	8	0, 1, 3, 7, 9, 35			
97	4	1, 21, 49, 63	49	8	1, 3, 9, 21, 35, 49, 63			
$n = 151, m(x) = 166761, N_{\mathscr{C}} = 212$								
136	**5**	**1**	**91**	**17**	**1, 5, 15, 37**	46	31	1, 5, 7, 11, 15, 23, 37

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
135	**6**	**0, 1**	**90**	**18**	**0, 1, 5, 15, 37**	**45**	**36**	**0, 1, 5, 7, 11, 15, 23, 37**
121	**8**	**1, 5**	**76**	**23**	**1, 5, 15, 35, 37**	**31**	**47**	**1, 5, 7, 11, 15, 17, 23, 37**
120	8	0, 1, 5	**75**	**24**	**0, 1, 5, 15, 35, 37**	**30**	**48**	**0, 1, 5, 7, 11, 15, 17, 23, 37**
106	**13**	**1, 3, 5**	**61**	**31**	**1, 3, 5, 11, 15, 37**	16	60	1, 5, 7, 11, 15, 17, 23, 35, 37
105	**14**	**0, 1, 3, 5**	**60**	**32**	**0, 1, 3, 5, 11, 15, 37**	15	60	0, 1, 5, 7, 11, 15, 17, 23, 35, 37
$n = 153, m(x) = 110110001, N_{\mathscr{C}} = 2114$								
151	**2**	**51**	99	8	1, 9, 15, 17, 27	51	19	1, 5, 9, 11, 15, 17, 27
150	**2**	**0, 51**	98	8	0, 1, 9, 15, 17, 27	50	24	0, 1, 5, 9, 11, 15, 17, 27
145	2	9	97	9	1, 5, 15	49	24	1, 5, 9, 11, 15, 17, 27, 51
144	2	0, 9	96	10	0, 1, 5, 15	48	24	0, 1, 5, 9, 11, 15, 17, 27, 51
143	2	9, 51	95	10	1, 5, 9, 51	47	18	1, 5, 9, 11, 15, 27, 33, 51
142	2	0, 9, 51	94	10	0, 1, 5, 9, 51	46	18	0, 1, 5, 9, 11, 15, 27, 33, 51
139	**4**	**9, 17**	91	9	1, 5, 15, 17	43	19	1, 5, 9, 11, 15, 17, 27, 33
138	**4**	**0, 9, 17**	90	10	0, 1, 5, 15, 17	42	24	0, 1, 5, 9, 11, 15, 17, 27, 33
137	4	9, 17, 51	89	13	1, 5, 9, 57	41	24	1, 5, 9, 11, 15, 17, 27, 33, 51
136	4	0, 9, 17, 51	88	14	0, 1, 5, 9, 57	40	24	0, 1, 5, 9, 11, 15, 17, 27, 33, 51
135	2	9, 27, 51	87	14	1, 5, 9, 51, 57	39	18	1, 5, 9, 11, 15, 19, 51
134	2	0, 9, 27, 51	86	14	0, 1, 5, 9, 51, 57	38	18	0, 1, 5, 9, 11, 15, 19, 51
131	4	9, 17, 27	83	15	1, 5, 9, 17, 57	35	19	1, 5, 9, 11, 15, 17, 27, 33, 57
130	4	0, 9, 17, 27	82	16	0, 1, 5, 9, 17, 57	34	24	0, 1, 5, 9, 11, 15, 17, 27, 33, 57
129	4	9, 17, 27, 51	81	16	1, 5, 9, 17, 51, 57	33	24	1, 5, 9, 11, 15, 17, 27, 33, 51, 57
128	4	0, 9, 17, 27, 51	80	16	0, 1, 5, 9, 17, 51, 57	32	30	0, 1, 5, 9, 11, 15, 19, 57
127	4	1, 51	79	14	1, 5, 9, 15, 27, 51	31	30	1, 5, 9, 11, 15, 19, 51, 57
126	4	0, 1, 51	78	14	0, 1, 5, 9, 15, 27, 51	30	30	0, 1, 5, 9, 11, 15, 19, 51, 57

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
123	4	9, 15, 17, 27	75	16	1, 5, 9, 15, 17, 27	27	27	1, 5, 9, 11, 15, 17, 19, 57
122	4	0, 9, 15, 17, 27	74	16	0, 1, 5, 9, 15, 17, 27	26	30	0, 1, 5, 9, 11, 15, 17, 19, 57
121	5	1, 9	73	16	1, 5, 9, 15, 17, 27, 51	25	30	1, 5, 9, 11, 15, 17, 19, 51, 57
120	6	0, 1, 9	72	16	0, 1, 5, 9, 15, 17, 27, 51	24	34	0, 1, 5, 9, 11, 15, 19, 27, 57
119	6	1, 9, 51	71	14	1, 5, 9, 15, 27, 33, 51	23	34	1, 5, 9, 11, 15, 19, 27, 33, 51
118	6	0, 1, 9, 51	70	14	0, 1, 5, 9, 15, 27, 33, 51	22	34	0, 1, 5, 9, 11, 15, 19, 27, 33, 51
115	6	1, 9, 17	67	16	1, 5, 9, 15, 17, 27, 33	19	42	1, 5, 9, 11, 15, 17, 19, 27, 57
114	6	0, 1, 9, 17	66	16	0, 1, 5, 9, 15, 17, 27, 33	18	42	0, 1, 5, 9, 11, 15, 17, 19, 27, 57
113	8	1, 9, 57	65	16	1, 5, 9, 15, 17, 27, 33, 51	17	48	1, 5, 9, 11, 15, 17, 19, 27, 51, 57
112	8	0, 1, 9, 57	64	18	0, 1, 5, 9, 11, 57	16	48	0, 1, 5, 9, 11, 15, 17, 19, 27, 51, 57
111	8	1, 9, 27, 51	63	18	1, 5, 9, 19, 51, 57	15	34	1, 5, 9, 11, 15, 19, 27, 33, 51, 57
110	8	0, 1, 9, 27, 51	62	18	0, 1, 5, 9, 11, 51, 57	14	34	0, 1, 5, 9, 11, 15, 19, 27, 33, 51, 57
107	8	1, 9, 17, 57	59	16	1, 5, 9, 15, 17, 27, 33, 57	11	51	1, 5, 9, 11, 15, 17, 19, 27, 33, 57
106	8	0, 1, 9, 17, 57	58	18	0, 1, 5, 9, 11, 17, 57	10	54	0, 1, 5, 9, 11, 15, 17, 19, 27, 33, 57
105	8	1, 9, 15, 27	57	18	1, 5, 9, 11, 17, 51, 57	9	57	1, 5, 9, 11, 15, 17, 19, 27, 33, 51, 57
104	8	0, 1, 9, 15, 27	56	18	0, 1, 5, 9, 11, 15, 27	8	72	0, 1, 5, 9, 11, 15, 17, 19, 27, 33, 51, 57
103	8	1, 9, 15, 27, 51	55	18	1, 5, 9, 11, 15, 27, 51	7	34	1, 3, 5, 9, 11, 15, 19, 27, 33, 51, 57
102	8	0, 1, 9, 15, 27, 51	54	18	0, 1, 5, 9, 11, 15, 27, 51	6	34	0, 1, 3, 5, 9, 11, 15, 19, 27, 33, 51, 57
$n = 155, m(x) = 7154113, N_{\mathscr{C}} = 2768$								
151	**2**	**31**	101	12	1, 3, 25, 31, 75	51	24	1, 3, 9, 23, 25, 31, 35, 55, 75
150	**2**	**0, 31**	100	12	0, 1, 9, 25, 31, 75	50	24	0, 1, 3, 9, 23, 25, 31, 35, 55, 75
149	**2**	**0, 25**	99	10	0, 1, 9, 25, 35, 75	49	22	0, 1, 3, 5, 11, 23, 25, 35, 55, 75
146	**4**	**25, 31**	96	12	1, 9, 25, 31, 35, 75	46	24	1, 3, 5, 11, 23, 25, 31, 35, 55, 75
145	**4**	**0, 25, 31**	95	12	0, 1, 9, 25, 31, 35, 75	45	25	1, 3, 9, 11, 23, 25, 75
144	2	0, 25, 75	94	10	0, 1, 11, 25, 35, 55, 75	44	28	0, 1, 3, 9, 11, 23, 25, 75

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
141	**4**	**25, 31, 75**	91	12	1, 11, 25, 31, 35, 55, 75	41	25	1, 3, 9, 11, 23, 25, 31, 75
140	**4**	**0, 25, 31, 75**	90	12	0, 1, 11, 25, 31, 35, 55, 75	40	30	0, 1, 3, 9, 11, 23, 25, 31, 75
139	2	0, 25, 35, 75	89	12	0, 1, 3, 11, 25	39	30	0, 1, 3, 9, 11, 23, 25, 35, 75
136	4	25, 31, 35, 75	86	12	9, 11, 23, 25, 31	36	31	1, 3, 9, 11, 23, 25, 31, 35, 75
135	4	0, 25, 31, 35, 75	85	14	1, 3, 9, 25, 75	35	32	0, 1, 3, 9, 11, 23, 25, 31, 35, 75
134	4	0, 1	84	14	0, 1, 3, 9, 25, 75	34	30	0, 1, 3, 9, 11, 23, 25, 35, 55, 75
131	4	1, 31	81	16	1, 3, 9, 25, 31, 75	31	32	1, 3, 9, 11, 23, 25, 31, 35, 55, 75
130	5	1, 25	80	16	0, 1, 3, 9, 25, 31, 75	30	32	0, 1, 3, 9, 11, 23, 25, 31, 35, 55, 75
129	6	0, 1, 25	79	14	0, 1, 3, 9, 25, 35, 75	29	30	0, 1, 3, 5, 9, 11, 23, 25, 35, 55, 75
126	6	1, 25, 31	76	16	1, 3, 9, 25, 31, 35, 75	26	32	1, 3, 5, 9, 11, 23, 25, 31, 35, 55, 75
125	6	0, 1, 25, 31	75	16	0, 1, 3, 9, 25, 31, 35, 75	25	32	0, 1, 3, 5, 9, 11, 23, 25, 31, 35, 55, 75
124	6	0, 1, 25, 75	74	14	0, 1, 3, 9, 25, 35, 55, 75	24	30	0, 1, 3, 7, 9, 11, 23, 25, 75
121	8	1, 25, 31, 75	71	16	1, 9, 11, 25, 31, 35, 55, 75	21	32	1, 3, 5, 9, 11, 15, 23, 25, 31, 35, 55, 75
120	8	0, 1, 25, 31, 75	70	16	0, 1, 9, 11, 25, 31, 35, 55, 75	20	32	0, 1, 3, 5, 9, 11, 15, 23, 25, 31, 35, 55, 75
119	6	0, 1, 25, 35, 75	69	16	0, 1, 9, 11, 23, 25	19	40	0, 1, 3, 7, 9, 11, 23, 25, 35, 75
116	8	1, 25, 31, 35, 75	66	16	1, 5, 9, 11, 25, 31, 35, 55, 75	16	35	1, 3, 7, 9, 11, 23, 25, 31, 35, 75
115	8	0, 1, 25, 31, 35, 75	65	16	0, 1, 3, 9, 11, 25, 31	15	40	0, 1, 3, 7, 9, 11, 23, 25, 31, 35, 75
114	6	0, 1, 11	64	20	0, 1, 9, 11, 23, 25, 55	14	60	0, 1, 3, 7, 9, 11, 23, 25, 35, 55, 75
111	8	1, 25, 31, 35, 55, 75	61	20	1, 3, 9, 23, 25, 31, 75	11	55	1, 3, 7, 9, 11, 23, 25, 31, 35, 55, 75
110	8	0, 1, 25, 31, 35, 55, 75	60	22	1, 3, 9, 23, 25, 35, 75	10	60	0, 1, 3, 7, 9, 11, 23, 25, 31, 35, 55, 75
109	8	0, 1, 11, 25	59	22	0, 1, 3, 9, 23, 25, 35, 75	9	62	0, 1, 3, 5, 7, 9, 11, 23, 25, 35, 55, 75
106	8	1, 11, 25, 31	56	24	1, 3, 9, 23, 25, 31, 35, 75	6	75	1, 3, 5, 7, 9, 11, 23, 25, 31, 35, 55, 75
105	10	1, 3, 25, 75	55	24	0, 1, 3, 9, 23, 25, 31, 35, 75	**5**	**80**	**0, 1, 3, 5, 7, 9, 11, 23, 25, 31, 35, 55, 75**
104	10	0, 1, 9, 25, 75	54	22	0, 1, 3, 9, 23, 25, 35, 55, 75			

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
$n = 157, m(x) = 352125723713652127, N_{\mathscr{C}} = 4$								
105	13	1	53	26	1, 3			
104	**14**	**0, 1**	52	26	0, 1, 3			
$n = 159, m(x) = 303667410520550411, N_{\mathscr{C}} = 16$								
157	**2**	**53**	105	4	3, 53	53	32	1, 3, 53
156	**2**	**0, 53**	104	6	0, 1, 53	52	32	0, 1, 3, 53
107	3	1	55	30	1, 3			
106	6	0, 1	54	30	0, 1, 3			
$n = 161, m(x) = 150536353761, N_{\mathscr{C}} = 156$								
158	**2**	**23**	106	4	1, 7, 35	56	7	1, 3, 5, 23, 69
157	**2**	**0, 23**	105	4	0, 1, 7, 35	55	14	0, 1, 3, 5, 23, 69
155	**2**	**23, 69**	103	8	5, 7, 23, 35	51	23	1, 5, 11, 35
154	**2**	**0, 23, 69**	102	8	0, 5, 7, 23, 35	50	28	0, 1, 5, 11, 35
150	2	35	100	8	1, 7, 23, 35, 69	48	32	3, 5, 11, 23, 35
149	2	0, 35	99	8	0, 1, 7, 23, 35, 69	47	32	0, 3, 5, 11, 23, 35
147	**4**	**23, 35**	95	7	1, 5	45	32	1, 5, 11, 23, 35, 69
146	**4**	**0, 23, 35**	94	14	0, 1, 5	44	32	0, 1, 5, 11, 23, 35, 69
144	4	23, 35, 69	92	7	1, 3, 23	40	23	1, 3, 5, 7, 35
143	4	0, 23, 35, 69	91	14	0, 1, 5, 23	39	28	0, 1, 3, 5, 7, 35
139	2	7, 35	89	7	1, 5, 23, 69	37	32	1, 3, 5, 7, 23, 35
138	2	0, 7, 35	88	14	0, 1, 5, 23, 69	36	32	0, 1, 3, 5, 7, 23, 35
136	4	7, 23, 35	84	14	1, 5, 35	34	32	1, 3, 5, 7, 23, 35, 69
135	4	0, 7, 23, 35	83	14	0, 1, 5, 35	33	32	0, 1, 3, 5, 7, 23, 35, 69
133	4	7, 23, 35, 69	81	16	5, 11, 23, 35	29	7	1, 3, 5, 11
132	4	0, 7, 23, 35, 69	80	18	0, 3, 11, 23, 35	28	14	0, 1, 3, 5, 11

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
128	3	1	78	18	1, 5, 23, 35, 69	26	7	1, 3, 5, 11, 23
127	4	0, 1	77	18	0, 1, 5, 23, 35, 69	25	14	0, 1, 3, 5, 11, 23
125	6	5, 23	73	23	1, 5, 7, 35	18	23	1, 3, 5, 11, 35
124	6	0, 5, 23	72	24	0, 1, 5, 7, 35	17	46	0, 1, 3, 5, 11, 35
122	6	1, 23, 69	70	24	1, 5, 7, 23, 35	15	49	1, 3, 5, 11, 23, 35
121	6	0, 1, 23, 69	69	24	0, 1, 5, 7, 23, 35	14	56	0, 1, 3, 5, 11, 23, 35
117	4	1, 35	**67**	**28**	**1, 5, 7, 23, 35, 69**	12	49	1, 3, 5, 11, 23, 35, 69
116	4	0, 1, 35	66	28	0, 1, 5, 7, 23, 35, 69	11	56	0, 1, 3, 5, 11, 23, 35, 69
114	8	5, 23, 35	62	7	1, 3, 5	4	69	1, 3, 5, 7, 11, 23, 35
113	8	0, 5, 23, 35	61	14	0, 1, 3, 5	**3**	**92**	**0, 1, 3, 5, 7, 11, 23, 35**
111	8	1, 23, 35, 69	59	7	1, 3, 5, 23			
110	8	0, 1, 23, 35, 69	58	14	0, 1, 3, 5, 23			
$n = 165, m(x) = 6223427, N_{\mathscr{C}} = 4800$								
163	**2**	**55**	109	12	5, 9, 29, 55, 77	55	32	1, 5, 7, 9, 15, 29, 33, 55, 77
162	**2**	**0, 55**	108	12	0, 5, 9, 29, 55, 77	54	32	0, 1, 5, 7, 9, 15, 29, 33, 55, 77
161	**2**	**77**	107	12	5, 9, 29, 33, 77	53	32	1, 5, 7, 9, 11, 15, 29, 33, 77
160	**2**	**0, 77**	106	12	0, 5, 9, 29, 33, 77	52	32	0, 1, 5, 7, 9, 11, 15, 29, 33, 77
159	**2**	**55, 77**	105	12	5, 9, 29, 33, 55, 77	51	32	1, 5, 7, 9, 11, 15, 29, 33, 55, 77
158	**2**	**0, 55, 77**	104	12	0, 5, 9, 29, 33, 55, 77	50	32	0, 1, 5, 7, 9, 11, 15, 29, 33, 55, 77
157	2	33, 77	103	12	1, 5, 9, 11, 33, 77	49	28	1, 5, 7, 9, 15, 25, 29, 55, 77
156	2	0, 33, 77	102	12	0, 1, 9, 29, 55	48	30	0, 1, 3, 5, 7, 9, 29, 55, 77
155	2	5	101	12	5, 9, 15, 29, 77	47	32	1, 5, 7, 9, 15, 25, 29, 33, 77
154	2	0, 5	100	12	0, 1, 9, 29, 77	46	32	0, 1, 5, 7, 9, 15, 25, 29, 33, 77
153	2	5, 55	99	12	1, 9, 29, 33, 55	45	32	1, 5, 7, 9, 15, 25, 29, 33, 55, 77
152	2	0, 5, 55	98	12	0, 5, 9, 15, 29, 55, 77	44	32	0, 1, 5, 7, 9, 15, 25, 29, 33, 55, 77

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
151	**4**	**15, 77**	97	16	5, 9, 15, 29, 33, 77	43	32	1, 5, 7, 9, 11, 15, 25, 29, 33, 77
150	**4**	**0, 5, 77**	96	16	0, 5, 9, 15, 29, 33, 77	42	32	0, 1, 5, 7, 9, 11, 15, 25, 29, 33, 77
149	4	15, 55, 77	95	16	5, 9, 15, 29, 33, 55, 77	41	33	1, 3, 5, 7, 9, 15, 29, 77
148	4	0, 5, 55, 77	94	16	0, 5, 9, 15, 29, 33, 55, 77	40	38	0, 1, 3, 5, 7, 9, 15, 29, 77
147	4	5, 33, 77	93	16	1, 3, 5, 7, 55	39	39	1, 5, 7, 9, 15, 19, 29, 33, 55
146	4	0, 5, 33, 77	92	16	0, 1, 5, 9, 29, 55	**38**	**44**	**0, 1, 3, 5, 7, 9, 15, 29, 55, 77**
145	4	5, 33, 55, 77	91	16	5, 9, 19, 29, 77	37	40	1, 3, 5, 7, 9, 15, 29, 33, 77
144	4	0, 1	90	18	0, 1, 5, 9, 29, 33	36	44	0, 1, 5, 7, 9, 15, 19, 29, 33, 77
143	4	9, 55	89	19	1, 3, 7, 15, 55, 77	35	44	1, 3, 5, 7, 9, 15, 29, 33, 55, 77
142	4	0, 1, 55	88	20	0, 1, 5, 9, 29, 55, 77	34	44	0, 1, 3, 5, 7, 9, 15, 29, 33, 55, 77
141	5	1, 33	87	16	5, 9, 15, 25, 29, 33, 77	33	44	1, 3, 5, 7, 9, 11, 15, 29, 33, 77
140	6	0, 29, 77	86	20	0, 1, 5, 9, 29, 33, 77	32	44	0, 1, 3, 5, 7, 9, 11, 15, 29, 33, 77
139	6	1, 33, 55	85	20	1, 3, 7, 15, 33, 55, 77	31	44	1, 3, 5, 7, 9, 11, 15, 29, 33, 55, 77
138	6	0, 29, 55, 77	84	20	0, 1, 5, 9, 29, 33, 55, 77	30	44	0, 1, 3, 5, 7, 9, 15, 25, 29, 77
137	5	29, 33, 77	83	17	1, 5, 9, 15, 29, 55	29	44	1, 5, 7, 9, 15, 19, 25, 29, 33, 55
136	6	0, 1, 33, 77	82	20	0, 1, 5, 9, 15, 29, 55	28	44	0, 1, 3, 5, 7, 9, 15, 25, 29, 55, 77
135	6	1, 33, 55, 77	81	21	1, 5, 9, 15, 29, 77	27	48	1, 3, 5, 7, 9, 15, 25, 29, 33, 77
134	6	0, 1, 33, 55, 77	**80**	**24**	**0, 1, 3, 5, 7, 15, 77**	26	48	0, 1, 3, 5, 7, 9, 15, 25, 29, 33, 77
133	5	1, 11, 33, 77	79	23	1, 3, 5, 7, 15, 55, 77	25	48	1, 3, 5, 7, 9, 15, 25, 29, 33, 55, 77
132	6	0, 1, 11, 33, 77	78	24	0, 1, 3, 5, 7, 15, 55, 77	24	48	0, 1, 3, 5, 7, 9, 15, 25, 29, 33, 55, 77
131	7	3, 5, 77	77	24	1, 5, 9, 15, 29, 33, 77	23	48	1, 3, 5, 7, 9, 11, 15, 25, 29, 33, 77
130	8	0, 5, 9, 77	76	24	0, 1, 5, 9, 15, 29, 33, 77	22	48	0, 1, 3, 5, 7, 9, 11, 15, 25, 29, 33, 77
129	8	1, 15, 33, 55	75	24	1, 5, 9, 15, 29, 33, 55, 77	21	48	1, 3, 5, 7, 9, 11, 15, 25, 29, 33, 55, 77
128	8	0, 5, 9, 55, 77	74	24	0, 1, 5, 9, 15, 29, 33, 55, 77	20	48	0, 1, 3, 5, 7, 9, 11, 15, 25, 29, 33, 55, 77

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
127	8	5, 29, 33, 77	73	24	1, 5, 9, 11, 15, 29, 33, 77	19	44	1, 3, 5, 7, 9, 15, 19, 29, 33, 55
126	8	0, 1, 5, 33, 77	72	24	0, 1, 5, 9, 11, 15, 29, 33, 77	18	44	0, 1, 3, 5, 7, 9, 15, 19, 29, 55, 77
125	8	5, 29, 33, 55, 77	71	24	1, 3, 5, 7, 15, 25, 77	17	50	1, 3, 5, 7, 9, 15, 19, 29, 33, 77
124	8	0, 1, 5, 33, 55, 77	70	24	0, 3, 5, 7, 19, 29, 77	16	50	0, 1, 3, 5, 7, 9, 15, 19, 29, 33, 77
123	8	1, 9, 55	69	24	1, 7, 9, 15, 29, 55, 77	15	55	1, 3, 5, 7, 9, 15, 19, 29, 33, 55, 77
122	8	0, 1, 9, 55	68	24	0, 1, 5, 7, 9, 29, 55, 77	14	60	0, 1, 3, 5, 7, 9, 15, 19, 29, 33, 55, 77
121	8	5, 9, 15, 77	67	24	1, 5, 9, 15, 25, 29, 33, 77	13	50	1, 3, 5, 7, 9, 11, 15, 19, 29, 33, 77
120	10	0, 7, 9, 77	66	26	0, 1, 5, 9, 19, 29, 33, 77	12	50	0, 1, 3, 5, 7, 9, 11, 15, 19, 29, 33, 77
119	10	7, 9, 55, 77	65	24	1, 5, 9, 15, 25, 29, 33, 55, 77	11	55	1, 3, 5, 7, 9, 11, 15, 19, 29, 33, 55, 77
118	10	0, 7, 9, 55, 77	64	28	0, 1, 5, 9, 19, 29, 33, 55, 77	10	60	0, 1, 3, 5, 7, 9, 11, 15, 19, 29, 33, 55, 77
117	8	1, 5, 15, 33, 77	63	24	1, 5, 7, 9, 15, 29, 55	9	44	1, 3, 5, 7, 9, 15, 19, 25, 29, 33, 55
116	10	0, 9, 29, 33, 77	62	28	0, 1, 5, 9, 11, 19, 29, 33, 77	8	44	0, 1, 3, 5, 7, 9, 15, 19, 25, 29, 55, 77
115	10	9, 29, 33, 55, 77	61	27	1, 5, 7, 9, 15, 29, 77	7	55	1, 3, 5, 7, 9, 15, 19, 25, 29, 33, 77
114	10	0, 9, 29, 33, 55, 77	60	28	0, 1, 5, 7, 9, 15, 29, 77	6	66	0, 1, 3, 5, 7, 9, 15, 19, 25, 29, 33, 77
113	8	1, 9, 15, 55	59	28	1, 5, 7, 9, 15, 29, 55, 77	5	77	1, 3, 5, 7, 9, 15, 19, 25, 29, 33, 55, 77
112	10	0, 1, 9, 11, 33, 77	58	28	0, 1, 5, 7, 9, 15, 29, 55, 77	**4**	**88**	**0, 1, 3, 5, 7, 9, 15, 19, 25, 29, 33, 55, 77**
111	11	5, 7, 9, 77	57	32	1, 5, 7, 9, 15, 29, 33, 77			
110	12	0, 5, 7, 9, 77	56	32	0, 1, 5, 7, 9, 15, 29, 33, 77			
$n = 167, m(x) = 5122622544667121565742432523, N_{\mathscr{C}} = 2$								
84	23	1	**83**	**24**	**0, 1**			
$n = 169, m(x) = 10000400020001000040002000100004000200010000400020001, N_{\mathscr{C}} = 2$								
157	2	13	12	26	0, 1			
$n = 171, m(x) = 1167671, N_{\mathscr{C}} = 802$								
169	**2**	**57**	111	12	1, 3, 9, 19	57	35	1, 3, 5, 7, 9, 13, 19

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
168	**2**	**0, 57**	**110**	**16**	**0, 1, 3, 5, 19**	**56**	**36**	**0, 1, 3, 5, 7, 9, 13, 19**
163	2	19, 57	109	12	1, 3, 9, 19, 57	55	36	1, 3, 5, 7, 9, 13, 19, 57
162	2	0, 19, 57	108	16	0, 1, 3, 5, 19, 57	54	36	0, 1, 3, 5, 7, 9, 13, 19, 57
153	3	1	99	18	1, 3, 9, 13	45	19	1, 3, 5, 7, 9, 15, 17
152	**6**	**0, 1**	98	18	0, 1, 3, 9, 13	44	38	0, 1, 3, 5, 7, 9, 15, 17
151	5	1, 57	97	18	1, 3, 9, 13, 57	43	38	1, 3, 5, 7, 9, 15, 17, 57
150	**6**	**0, 1, 57**	96	18	0, 1, 3, 5, 7, 57	42	38	0, 1, 3, 5, 7, 9, 13, 17, 57
147	4	9, 19	93	20	1, 3, 5, 9, 19	39	45	1, 3, 5, 7, 9, 15, 17, 19
146	6	0, 1, 19	92	20	0, 1, 3, 5, 9, 19	**38**	**48**	**0, 1, 3, 5, 7, 9, 15, 17, 19**
145	6	1, 19, 57	91	21	1, 3, 5, 9, 19, 57	**37**	**48**	**1, 3, 5, 7, 9, 15, 17, 19, 57**
144	6	0, 1, 19, 57	**90**	**22**	**0, 1, 3, 5, 9, 19, 57**	36	48	0, 1, 3, 5, 7, 9, 15, 17, 19, 57
135	9	1, 3	81	19	1, 3, 5, 7, 9	27	19	1, 3, 5, 7, 9, 13, 15, 17
134	**10**	**0, 1, 3**	**80**	**26**	**0, 1, 3, 5, 7, 9**	26	38	0, 1, 3, 5, 7, 9, 13, 15, 17
133	9	1, 3, 57	79	23	1, 3, 5, 9, 17, 57	25	38	1, 3, 5, 7, 9, 13, 15, 17, 57
132	10	0, 1, 3, 57	78	26	0, 1, 3, 5, 7, 9, 57	24	38	0, 1, 3, 5, 7, 9, 13, 15, 17, 57
129	9	1, 3, 19	75	27	1, 3, 5, 9, 17, 19	21	55	1, 3, 5, 7, 9, 13, 15, 17, 19
128	10	0, 1, 3, 19	**74**	**28**	**0, 1, 3, 5, 9, 17, 19**	20	64	0, 1, 3, 5, 7, 9, 13, 15, 17, 19
127	10	1, 9, 19, 57	73	28	1, 3, 5, 9, 17, 19, 57	**19**	**68**	**1, 3, 5, 7, 9, 13, 15, 17, 19, 57**
126	**12**	**0, 1, 15, 19, 57**	72	28	0, 1, 3, 5, 9, 17, 19, 57	**18**	**68**	**0, 1, 3, 5, 7, 9, 13, 15, 17, 19, 57**
117	10	1, 3, 9	63	19	1, 3, 5, 7, 9, 25	7	38	1, 3, 5, 7, 9, 13, 15, 17, 25, 57
116	14	0, 1, 3, 5	62	32	0, 1, 3, 5, 9, 17, 25	6	38	0, 1, 3, 5, 7, 9, 13, 15, 17, 25, 57
115	12	1, 7, 9, 57	61	32	1, 3, 5, 9, 17, 25, 57			
114	14	0, 1, 7, 9, 57	60	32	0, 1, 3, 5, 9, 17, 25, 57			
$n = 175, m(x) = 10004102040000400204 1, N_{\mathscr{C}} = 242$								

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
172	**2**	**25**	112	6	3, 25	60	8	0, 1, 5, 7, 15, 25, 35, 75
171	**2**	**0, 25**	111	6	0, 3, 25	52	7	1, 3, 25
170	**2**	**0, 35**	110	4	0, 1, 35	51	10	0, 1, 3, 25
169	**2**	**25, 75**	109	6	1, 25, 75	50	10	0, 1, 3, 35
168	**2**	**0, 25, 75**	108	6	0, 1, 25, 75	49	7	1, 3, 25, 75
167	2	0, 25, 35	107	6	0, 3, 25, 35	48	14	1, 3, 25, 35
165	2	25, 35, 75	105	6	1, 25, 35, 75	47	14	0, 1, 3, 25, 35
164	2	0, 25, 35, 75	104	6	0, 1, 25, 35, 75	45	14	1, 3, 25, 35, 75
163	2	5	103	6	1, 5	44	14	0, 1, 3, 25, 35, 75
162	2	0, 5	102	6	0, 1, 5	43	7	1, 3, 5
160	2	5, 25	100	6	1, 5, 25	42	14	0, 1, 3, 5
159	2	0, 5, 25	99	6	0, 1, 5, 25	40	7	1, 3, 5, 25
158	2	0, 5, 35	98	6	0, 1, 5, 35	39	14	0, 1, 3, 5, 25
157	2	5, 25, 75	97	6	1, 5, 25, 75	38	14	0, 1, 3, 5, 35
156	2	0, 5, 25, 75	96	6	0, 1, 5, 25, 75	37	7	1, 3, 5, 25, 75
155	2	0, 5, 25, 35	95	6	0, 1, 5, 25, 35	36	14	0, 1, 3, 5, 25, 75
153	2	5, 25, 35, 75	93	6	1, 5, 25, 35, 75	35	14	0, 1, 3, 5, 25, 35
152	4	7, 25	92	7	3, 7, 25	33	14	1, 3, 5, 25, 35, 75
151	4	0, 7, 25	91	8	0, 3, 7, 25	32	14	0, 1, 3, 5, 25, 35, 75
150	2	0, 7, 35	90	6	0, 1, 5, 15	31	10	0, 1, 3, 7, 25
149	4	7, 25, 75	89	8	1, 7, 25, 75	30	14	0, 1, 3, 5, 15
148	4	0, 7, 25, 75	88	8	0, 1, 7, 25, 75	29	10	1, 3, 7, 25, 75
147	4	0, 7, 25, 35	87	8	0, 3, 7, 25, 35	28	20	1, 3, 7, 25, 35
145	4	7, 25, 35, 75	86	6	0, 1, 5, 15, 35	27	20	0, 1, 3, 7, 25, 35
144	4	0, 7, 25, 35, 75	85	8	1, 7, 25, 35, 75	26	14	0, 1, 3, 5, 15, 35

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
143	4	5, 7	84	8	0, 1, 7, 25, 35, 75	25	20	1, 3, 7, 25, 35, 75
142	4	0, 5, 7	83	7	1, 5, 7	24	20	0, 1, 3, 7, 25, 35, 75
141	2	5, 15, 25, 35, 75	82	8	0, 1, 5, 7	23	15	1, 3, 5, 7
140	4	5, 7, 25	81	6	1, 5, 15, 25, 35, 75	22	20	0, 1, 3, 5, 7
139	4	0, 5, 7, 25	80	8	1, 5, 7, 25	21	14	1, 3, 5, 15, 25, 35, 75
138	4	0, 5, 7, 35	79	8	0, 1, 5, 7, 25	20	30	1, 3, 5, 7, 25
137	4	5, 7, 25, 75	78	8	0, 1, 5, 7, 35	19	30	0, 1, 3, 5, 7, 25
136	4	0, 5, 7, 25, 75	77	8	1, 5, 7, 25, 75	18	20	0, 1, 3, 5, 7, 35
135	4	0, 5, 7, 25, 35	76	8	0, 1, 5, 7, 25, 75	17	30	1, 3, 5, 7, 25, 75
133	4	5, 7, 25, 35, 75	75	8	0, 1, 5, 7, 25, 35	16	35	1, 3, 5, 7, 25, 35
132	4	0, 5, 7, 25, 35, 75	73	8	1, 5, 7, 25, 35, 75	15	40	0, 1, 3, 5, 7, 25, 35
131	4	5, 7, 15	72	8	0, 1, 5, 7, 25, 35, 75	13	40	1, 3, 5, 7, 25, 35, 75
130	4	0, 5, 7, 15	71	8	1, 5, 7, 15	12	40	0, 1, 3, 5, 7, 25, 35, 75
128	4	5, 7, 15, 25	70	8	0, 1, 5, 7, 15	11	25	1, 3, 5, 7, 15
127	4	0, 5, 7, 15, 25	68	8	1, 5, 7, 15, 25	10	50	0, 1, 3, 5, 7, 15
126	4	0, 5, 7, 15, 35	67	8	0, 1, 5, 7, 15, 25	8	35	1, 3, 5, 7, 15, 25
124	4	5, 7, 15, 25, 35	66	8	0, 1, 5, 7, 15, 35	7	70	0, 1, 3, 5, 7, 15, 25
123	4	0, 5, 7, 15, 25, 35	64	8	1, 5, 7, 15, 25, 35	4	75	1, 3, 5, 7, 15, 25, 35
121	4	5, 7, 15, 25, 35, 75	63	8	0, 1, 5, 7, 15, 25, 35	**3**	**100**	**0, 1, 3, 5, 7, 15, 25, 35**
120	4	0, 5, 7, 15, 25, 35, 75	61	8	1, 5, 7, 15, 25, 35, 75			
$n = 177, m(x) = 23563311065422331671, N_{\mathscr{C}} = 16$								
175	**2**	**59**	117	4	3, 59	59	30	1, 3, 59
174	**2**	**0, 59**	116	6	0, 1, 59	58	30	0, 1, 3, 59
119	3	1	61	28	1, 3			
118	6	0, 1	60	28	0, 1, 3			

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
$n = 183, m(x) = 131010354441637571637, N_{\mathscr{C}} = 16$								
181	**2**	**61**	121	4	3, 61	61	36	1, 3, 61
180	**2**	**0, 61**	120	6	0, 1, 61	60	36	0, 1, 3, 61
123	3	1	63	34	1, 3			
122	6	0, 1	62	34	0, 1, 3			
$n = 185, m(x) = 1761557733077, N_{\mathscr{C}} = 40$								
181	**2**	**37**	113	14	1, 5	73	32	1, 3, 5, 37
180	**2**	**0, 37**	112	14	0, 1, 5	72	32	0, 1, 3, 5, 37
149	5	1	109	16	1, 5, 37	41	37	1, 3, 5, 19
148	8	0, 1	108	16	0, 1, 5, 37	40	48	0, 1, 3, 5, 19
145	5	1, 37	77	28	1, 3, 5	37	37	1, 3, 5, 19, 37
144	8	0, 1, 37	76	28	0, 1, 3, 5	36	54	0, 1, 3, 5, 19, 37
$n = 187, m(x) = 36000132706473, N_{\mathscr{C}} = 78$								
179	2	33	129	12	3, 17, 33	59	17	1, 3, 9, 33
178	2	0, 33	128	12	0, 3, 17, 33	58	30	0, 1, 3, 23, 33
177	2	17	121	12	1, 11, 17, 33	57	11	1, 3, 9, 17
176	2	0, 17	120	12	0, 1, 11, 17, 33	56	22	0, 1, 3, 9, 17
171	2	11, 33	107	11	1, 3	51	17	1, 3, 9, 11, 33
170	2	0, 11, 33	106	14	0, 1, 3	50	34	0, 1, 3, 9, 11, 33
169	4	17, 33	99	17	1, 3, 33	49	38	1, 3, 9, 17, 33
168	4	0, 17, 33	98	22	0, 1, 3, 33	48	38	0, 1, 3, 9, 17, 33
161	4	11, 17, 33	97	11	1, 3, 17	41	48	1, 3, 9, 11, 17, 33
160	4	0, 11, 17, 33	96	16	0, 1, 3, 17	40	48	0, 1, 3, 9, 11, 17, 33
147	5	1	91	17	1, 3, 11, 33	27	11	1, 3, 9, 23

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
146	6	0, 1	90	22	0, 1, 3, 11, 33	26	22	0, 1, 3, 9, 23
139	9	3, 33	89	24	1, 3, 17, 33	19	17	1, 3, 9, 23, 33
138	10	0, 3, 33	88	24	0, 1, 3, 17, 33	18	34	0, 1, 3, 9, 23, 33
137	6	1, 17	81	24	1, 3, 11, 17, 33	9	55	1, 3, 9, 17, 23, 33
136	6	0, 1, 17	80	24	0, 1, 3, 11, 17, 33	8	66	0, 1, 3, 9, 17, 23, 33
131	10	1, 11, 33	67	11	1, 3, 9			
130	10	0, 1, 11, 33	66	22	0, 1, 3, 9			
$n = 189, m(x) = 1100111, N_{\mathscr{C}} = 175286$								
187	**2**	**63**	125	12	0, 1, 3, 5, 31, 81	63	24	0, 1, 3, 5, 7, 11, 13, 31, 39, 63, 81
186	**2**	**0, 63**	124	12	1, 3, 5, 7, 63, 81	62	24	0, 1, 3, 5, 7, 9, 11, 13, 15, 31
185	**2**	**0, 81**	123	12	0, 1, 3, 5, 7, 63, 81	61	24	1, 3, 5, 7, 11, 13, 21, 23, 27, 63, 81
184	**2**	**63, 81**	122	12	0, 1, 3, 5, 7, 9	60	24	0, 1, 3, 5, 7, 9, 11, 13, 31, 39, 63
183	**2**	**3**	121	12	1, 3, 5, 7, 9, 63	59	24	0, 1, 3, 5, 7, 9, 11, 13, 15, 31, 81
182	**2**	**0, 3**	120	12	0, 1, 3, 5, 7, 9, 63	58	24	1, 3, 5, 7, 11, 13, 21, 31, 63, 69, 81
181	2	3, 63	119	12	0, 1, 3, 5, 7, 69, 81	57	27	1, 3, 5, 7, 9, 11, 13, 15, 21, 23
180	2	0, 3, 63	118	14	1, 3, 5, 31, 39, 63, 81	56	28	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23
179	2	0, 3, 81	117	14	0, 1, 3, 5, 31, 39, 63, 81	55	27	1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 63
178	2	3, 63, 81	116	14	0, 1, 3, 5, 9, 31, 39	54	31	1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 81
177	2	3, 69	115	14	1, 3, 5, 9, 31, 39, 63	53	32	0, 1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 81
176	2	0, 3, 69	114	14	0, 1, 3, 5, 9, 31, 39, 63	52	32	1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 63, 81
175	2	3, 63, 69	113	14	0, 1, 3, 5, 31, 39, 69, 81	51	32	0, 1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 63, 81
174	2	0, 3, 63, 69	112	14	1, 3, 5, 31, 39, 63, 69, 81	50	32	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 81
173	2	0, 3, 69, 81	111	14	0, 1, 3, 5, 31, 39, 63, 69, 81	49	32	1, 3, 5, 7, 11, 13, 21, 23, 27, 39, 63, 69, 81

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
172	2	3, 63, 69, 81	110	14	0, 1, 3, 5, 9, 31, 39, 69	48	32	0, 1, 3, 5, 7, 11, 13, 21, 23, 27, 39, 63, 69, 81
171	2	3, 21, 69	109	14	1, 3, 5, 9, 31, 39, 63, 69	47	32	0, 1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 69, 81
170	2	0, 3, 21, 69	108	14	0, 1, 3, 5, 9, 31, 39, 63, 69	46	32	1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 63, 69, 81
169	4	1, 63	107	14	0, 1, 3, 11, 13, 21, 39, 69, 81	45	32	0, 1, 3, 5, 7, 11, 13, 21, 23, 39, 45, 63, 69, 81
168	4	0, 1, 63	106	14	1, 3, 11, 13, 21, 39, 63, 69, 81	44	32	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 45, 69
167	4	0, 1, 81	105	14	1, 3, 9, 11, 13, 21, 39, 45	43	32	1, 3, 5, 7, 9, 11, 13, 21, 23, 27, 39, 63, 69, 81
166	4	1, 63, 81	104	14	0, 1, 3, 5, 7, 9, 11	42	32	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 45, 63, 69
165	5	1, 3	103	14	1, 3, 5, 7, 9, 11, 63	41	32	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 45, 69, 81
164	6	0, 1, 3	102	15	1, 3, 5, 7, 11, 21, 81	40	32	1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 45, 63, 69, 81
163	6	1, 3, 63	101	16	0, 1, 3, 5, 7, 11, 21, 81	39	32	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 39, 45, 63, 69, 81
162	6	0, 1, 3, 63	100	16	1, 3, 5, 7, 11, 21, 63, 81	38	32	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 39, 45, 69
161	6	0, 1, 3, 81	99	17	1, 3, 7, 11, 27, 31, 39, 81	37	32	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 39, 63, 69, 81
160	6	1, 3, 63, 81	98	18	0, 1, 3, 7, 11, 27, 31, 39, 81	36	33	1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 81
159	6	3, 9, 13	97	18	1, 3, 7, 11, 27, 31, 39, 63, 81	35	36	0, 1, 3, 5, 7, 11, 13, 23, 31, 45, 69, 81, 93
158	6	0, 1, 3, 69	96	18	0, 1, 3, 7, 11, 27, 31, 39, 63, 81	34	33	1, 3, 5, 7, 11, 13, 23, 31, 39, 45, 63, 69, 81
157	6	1, 3, 63, 69	95	18	0, 1, 3, 7, 11, 21, 31, 39, 81	33	36	0, 1, 3, 5, 7, 11, 13, 23, 31, 39, 45, 63, 69, 81
156	6	0, 1, 3, 63, 69	94	18	1, 3, 7, 11, 21, 31, 39, 63, 81	32	36	0, 1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 69
155	6	0, 1, 3, 69, 81	93	18	3, 5, 7, 9, 11, 13, 39, 45	31	36	1, 3, 5, 7, 11, 13, 21, 23, 27, 31, 39, 63, 69, 81
154	6	1, 3, 63, 69, 81	92	18	0, 1, 3, 7, 9, 11, 21, 31, 39	30	39	1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 69, 81
153	6	3, 9, 13, 69	91	18	1, 3, 7, 9, 11, 21, 31, 39, 63	29	42	0, 1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 69, 81
152	6	0, 1, 3, 21, 69	90	18	0, 1, 3, 7, 9, 11, 21, 31, 39, 63	28	45	1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 63, 69, 81
151	6	1, 31, 63	89	18	0, 1, 3, 7, 11, 21, 31, 39, 69, 81	27	48	0, 1, 3, 5, 7, 11, 13, 21, 23, 31, 39, 45, 63, 69, 81
150	6	0, 1, 31, 63	88	18	1, 3, 7, 11, 21, 31, 39, 63, 69, 81	26	42	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 31, 39, 45, 69
149	6	0, 1, 5, 81	87	18	1, 3, 7, 9, 11, 21, 31, 39, 45	25	45	1, 3, 5, 7, 9, 11, 13, 21, 23, 27, 31, 39, 63, 69, 81
148	6	1, 5, 63, 81	86	18	0, 1, 3, 7, 11, 13, 31, 93	24	48	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 27, 31, 39, 63, 69, 81

(continued)

Table 4.3 (continued)

k	d	Roots of $g(x)$	k	d	Roots of $g(x)$	k	d	Roots of $g(x)$
147	7	1, 3, 5	85	18	1, 3, 7, 9, 11, 21, 31, 39, 63, 69	23	48	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 31, 39, 45, 69, 81
146	8	0, 1, 3, 5	84	18	0, 1, 3, 7, 11, 13, 31, 39, 63	22	48	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 45, 63, 69, 81
145	8	1, 3, 5, 63	83	18	0, 1, 3, 5, 11, 13, 21, 31, 81	21	54	0, 1, 3, 5, 7, 9, 11, 13, 21, 23, 31, 39, 45, 63, 81, 93
144	8	0, 1, 3, 5, 63	82	20	1, 3, 5, 7, 11, 13, 39, 63, 81	20	54	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 45, 69, 93
143	8	0, 1, 3, 5, 81	81	21	1, 3, 5, 7, 9, 11, 13, 15	19	57	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 63, 69, 81, 93
142	8	1, 3, 5, 63, 81	80	22	0, 1, 3, 5, 7, 9, 11, 13, 15	18	63	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 39, 45, 69, 81
141	8	1, 3, 7, 39	79	21	1, 3, 5, 7, 9, 11, 13, 39, 63	17	66	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 39, 45, 69, 81
140	10	0, 1, 3, 7, 39	78	22	0, 1, 3, 5, 7, 9, 11, 13, 39, 63	16	69	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 39, 45, 63, 69, 81
139	10	1, 3, 7, 39, 63	77	22	0, 1, 3, 5, 7, 9, 11, 13, 15, 81	15	72	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 39, 45, 63, 69, 81
138	10	0, 1, 3, 7, 39, 63	76	24	1, 3, 5, 7, 11, 13, 21, 39, 63, 81	14	66	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 39, 45, 69, 81
137	10	0, 1, 3, 7, 39, 81	75	24	0, 1, 3, 5, 7, 11, 13, 21, 39, 63, 81	13	72	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 39, 63, 69, 81, 93
136	10	1, 3, 7, 39, 63, 81	74	24	0, 1, 3, 5, 7, 9, 11, 13, 15, 21	12	72	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 33, 39, 63, 69, 81
135	10	1, 3, 9, 31, 39	73	24	1, 3, 5, 7, 9, 11, 13, 21, 39, 63	11	78	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 33, 39, 45, 69, 81
134	10	0, 1, 3, 31, 39, 69	72	24	0, 1, 3, 5, 7, 9, 11, 13, 21, 39, 63	10	81	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 39, 45, 63, 69, 81, 93
133	10	1, 3, 31, 39, 63, 69	71	24	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 81	9	84	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 33, 39, 45, 63, 69, 81
132	10	0, 1, 3, 31, 39, 63, 69	70	24	1, 3, 5, 7, 11, 13, 21, 39, 63, 69, 81	8	78	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 33, 39, 45, 69, 81
131	10	0, 1, 3, 31, 39, 69, 81	69	24	1, 3, 7, 9, 11, 13, 21, 31, 39, 45	7	93	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 33, 39, 45, 63, 69, 81
130	10	1, 3, 31, 39, 63, 69, 81	68	24	0, 1, 3, 5, 7, 9, 11, 13, 21, 39, 69	**6**	**96**	**0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 31, 33, 39, 45, 63, 69, 81**
129	10	1, 3, 9, 21, 31, 45	67	24	1, 3, 5, 7, 9, 11, 13, 21, 39, 63, 69	5	90	0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 33, 39, 45, 69, 81, 93
128	10	0, 1, 3, 5, 7	66	24	0, 1, 3, 5, 7, 9, 11, 13, 21, 39, 63, 69	4	81	1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 33, 39, 45, 63, 69, 81, 93
127	10	1, 3, 5, 7, 63	65	24	0, 1, 3, 5, 7, 9, 11, 13, 21, 39, 69, 81	**3**	**108**	**0, 1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 31, 33, 39, 45, 63, 69, 81, 93**
126	10	0, 1, 3, 5, 7, 63	64	24	1, 3, 5, 7, 9, 11, 13, 21, 39, 63, 69, 81			

References

1. Brouwer, A.E.: Bounds on the size of linear codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 295–461. Elsevier, North Holland (1998)
2. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
3. Mattson, H.F., Solomon, G.: A new treatment of Bose-Chaudhuri codes. J. Soc. Ind. Appl. Math. **9**(4), 654–669 (1961). doi:10.1137/0109055
4. Peterson, W.W.: Error-Correcting Codes. MIT Press, Cambridge (1961)
5. Prange, E.: Cyclic error-correcting codes in two symbols. Technical Report TN-58–103, Air Force Cambridge Research Labs, Bedford, Massachusetts, USA (1957)