

for s odd, while for $s = 2$, we may take every $\chi(i) = 1$, so

$$\begin{aligned}\theta^s &= \sum_{i=1}^{p-1} \chi(i) \alpha^{is} \\ &= \sum_{i=1}^{p-1} \chi(i) \alpha^i = \theta\end{aligned}$$

Therefore, $\theta \in \text{GF}(s)$ (Theorem 7.1 part (ii)).

Examples 8.1

Case (i)

Let $p = 5$. Then

$$\theta = \alpha - \alpha^2 - \alpha^3 + \alpha^4$$

and

$$\begin{aligned}\theta^2 &= \alpha \times \alpha^4 + \alpha^2 \times \alpha^3 + \alpha^3 \times \alpha^2 + \alpha^4 \times \alpha + (\alpha \times \alpha + \alpha^2 \times \alpha^2 + \alpha^3 \times \alpha^3 \\ &\quad + \alpha^4 \times \alpha^4) + \alpha(-\alpha^2 - \alpha^2) - \alpha^2(\alpha + \alpha^4) - \alpha^3(\alpha + \alpha^4) + \alpha^4(-\alpha^2 - \alpha^3) \\ &= 4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4) - [\alpha^3 + \alpha^4 + \alpha^3 + \alpha + \alpha^4 + \alpha^2 + \alpha + \alpha^2] \\ &= 4 - 1 - 2(\alpha + \alpha^2 + \alpha^3 + \alpha^4) \\ &= 4 - 1 + 2 = 5 = p\end{aligned}$$

Case (ii)

Let $p = 7$. Then

$$\theta = \alpha + \alpha^2 - \alpha^3 + \alpha^4 - \alpha^5 - \alpha^6$$

and

$$\begin{aligned}\theta^2 &= - \sum_{i+j=7} \alpha^{i+j} + \sum_{i=1}^6 \alpha^{2i} + \alpha(\alpha^2 - \alpha^3 + \alpha^4 - \alpha^5) + \alpha^2(\alpha - \alpha^3 + \alpha^4 - \alpha^6) \\ &\quad - \alpha^3(\alpha + \alpha^2 - \alpha^5 - \alpha^6) + \alpha^4(\alpha + \alpha^2 - \alpha^5 - \alpha^6) - \alpha^5(\alpha - \alpha^3 + \alpha^4 - \alpha^6) \\ &\quad - \alpha^6(\alpha^2 - \alpha^3 + \alpha^4 - \alpha^5) \\ &= -6 + \sum_{i=1}^6 \alpha^i + [\alpha^3 - \alpha^4 + \alpha^5 - \alpha^6 + \alpha^3 - \alpha^5 + \alpha^6 - \alpha] \\ &\quad + [-\alpha^4 - \alpha^5 + \alpha + \alpha^2 + \alpha^5 + \alpha^6 - \alpha^2 - \alpha^3] \\ &\quad + [-\alpha^6 + \alpha - \alpha^2 + \alpha^4 - \alpha + \alpha^2 - \alpha^3 + \alpha^4] \\ &= -6 - 1 + [2\alpha^3 - \alpha^4 - \alpha] + [\alpha - \alpha^3 - \alpha^4 + \alpha^6] + [-\alpha^3 + 2\alpha^4 - \alpha^6] \\ &= -7 = -p\end{aligned}$$

Case (iii)

Let $p = 13$. Then

$$\theta = \alpha - \alpha^2 + \alpha^3 + \alpha^4 - \alpha^5 - \alpha^6 - \alpha^7 - \alpha^8 + \alpha^9 + \alpha^{10} - \alpha^{11} + \alpha^{12}$$

and

$$\begin{aligned}\theta^2 &= \sum_{i+j=13} \alpha^{i+j} + \sum_{i=1}^{12} \alpha^{2i} + \sum_{k=1}^{12} \left(\sum_{i=1, i \neq k, 2i \neq k}^{12} \chi(i(k-i)) \right) \alpha^k \\ &= 12 - 1 + \sum_{k=1}^{12} \left(\sum_{i=1, i \neq k, 2i \neq k}^{12} (i(k-i)) \right) \alpha^k\end{aligned}$$

The coefficient of α in the above summation is

$$= 2[\chi(2(12)) + \chi(3 \times 11) + \chi(4 \times 10) + \chi(5 \times 9) + \chi(6 \times 8)]$$

Among the pairs (2, 12), (3, 11), (4, 10), (5, 9), (6, 8), the pairs (2, 12), (3, 11), (5, 9) are such that one of the numbers is a quadratic residue mod 13, while the other is a non-residue. Also, the pairs (4, 10) and (6, 8) are pairs in which both the numbers are either residues or non-residues mod 13. Therefore, the coefficient of α is -2 .

$$\text{coeff of } \alpha^2 = 2[\chi(3 \times 12) + \chi(4 \times 11) + \chi(5 \times 10) + \chi(6 \times 9) + \chi(7 \times 8)]$$

Pairs (4, 11), (5, 10), (6, 9) are of numbers one of which is a residue and the other a non-residue while the pairs (3, 12), (7, 8) have both their numbers either residues or non-residues. Therefore

$$\text{coeff of } \alpha^2 = -2$$

$$\text{coeff of } \alpha^3 = 2[\chi(1 \times 2) + \chi(4 \times 12) + \chi(5 \times 11) + \chi(6 \times 10) + \chi(7 \times 9)] = -2$$

$$\text{coeff of } \alpha^4 = 2[\chi(1 \times 3) + \chi(5 \times 12) + \chi(6 \times 11) + \chi(7 \times 10) + \chi(8 \times 9)] = -2$$

$$\text{coeff of } \alpha^5 = 2[\chi(1 \times 4) + \chi(2 \times 3) + \chi(6 \times 12) + \chi(7 \times 11) + \chi(8 \times 10)] = -2$$

$$\text{coeff of } \alpha^6 = 2[\chi(1 \times 5) + \chi(2 \times 4) + \chi(7 \times 12) + \chi(8 \times 11) + \chi(9 \times 10)] = -2$$

$$\text{coeff of } \alpha^7 = 2[\chi(1 \times 6) + \chi(2 \times 5) + \chi(3 \times 4) + \chi(8 \times 12) + \chi(9 \times 11)] = -2$$

$$\text{coeff of } \alpha^8 = 2[\chi(1 \times 7) + \chi(2 \times 6) + \chi(3 \times 5) + \chi(9 \times 12) + \chi(10 \times 11)] = -2$$

$$\text{coeff of } \alpha^9 = 2[\chi(1 \times 8) + \chi(2 \times 7) + \chi(3 \times 6) + \chi(4 \times 5) + \chi(10 \times 12)] = -2$$

$$\text{coeff of } \alpha^{10} = 2[\chi(1 \times 9) + \chi(2 \times 8) + \chi(3 \times 7) + \chi(4 \times 6) + \chi(11 \times 12)] = -2$$

$$\text{coeff of } \alpha^{11} = 2[\chi(1 \times 10) + \chi(2 \times 9) + \chi(3 \times 8) + \chi(4 \times 7) + \chi(5 \times 6)] = -2$$

$$\text{coeff of } \alpha^{12} = 2[\chi(1 \times 11) + \chi(2 \times 10) + \chi(3 \times 9) + \chi(4 \times 8) + \chi(5 \times 7)] = -2$$

therefore

$$\sum_{k=1}^{12} \left(\sum_{i=1, i \neq k, 2i \neq k}^{12} \chi(i(k-i)) \right) \alpha^k = -2 \sum_{k=1}^{12} \alpha^k = -2 \times (-1) = 2$$

Hence

$$\theta^2 = 11 + 2 = 13 = p$$

We now prove a general result about θ^2 , but for that we need a result of Perron about quadratic residues which we state without proof.

Theorem 8.3 (Perron)

- (i) Suppose $p = 4k - 1$. Let r_1, \dots, r_{2k} be the $2k$ quadratic residues mod p together with 0, and let a be a number relatively prime to p . Then among the $2k$ numbers $r_i + a$, there are k residues (possibly including 0) and k non-residues.
- (ii) Suppose $p = 4k - 1$. Let $n_1, n_2, \dots, n_{2k-1}$ be the $2k - 1$ non-residues, and let a be prime to p . Then among the $2k - 1$ numbers $n_i + a$, there are k residues (possibly including 0) and $k - 1$ non-residues.
- (iii) Suppose $p = 4k + 1$. Among the $2k + 1$ numbers $r_i + a$ are, if a is itself a residue, $k + 1$ residues (including 0) and k non-residues; and, if a is a non-residue, k residues (not including 0) and $k + 1$ non-residues.
- (iv) Suppose $p = 4k + 1$. Among the $2k$ numbers $n_i + a$ are, if a is itself a residue, k residues (not including 0) and k non-residues; and, if a is a non-residue, $k + 1$ residues (including 0) and $k - 1$ non-residues.

Theorem 8.4

If $p = 4l + 1$, then $\theta^2 = p$.

Proof

$$\theta^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \chi(i)\chi(j)\alpha^{i+j}$$

As $p = 4k + 1$, -1 is a residue mod p and, therefore, i and $p - i$ are either both residues or both non-residues. Therefore, $p - 1$ terms in the sum with $i + j = p$ have coefficient $\chi(i)\chi(j) = 1$ each. Therefore

$$\begin{aligned} \theta^2 &= p - 1 + \sum_{i=1}^{p-1} \chi(i)^2 \alpha^{2i} + \sum_{\substack{i+j=p \\ i \neq j}} \chi(i)\chi(j)\alpha^{i+j} \\ &= p - 1 + \sum_{i=1}^{p-1} \alpha^{2i} + \sum_{k=1}^{p-1} \left(\sum_{\substack{i=1, i \neq k, 2i \neq k}}^{p-1} \chi(i(k-i)) \right) \alpha^k \\ &= p - 1 + \sum_{i=1}^{p-1} \alpha^i + \sum_{k=1}^{p-1} \psi(k) \alpha^k \\ &= p - 2 + \sum_{k=1}^{p-1} \psi(k) \alpha^k \end{aligned}$$

where

$$\psi(k) = \sum_{i=1, i \neq k, 2i \neq k}^{p-1} \chi(i(k-i))$$

Observe that, in the summation for $\psi(k)$, there are $p - 3$ terms. Let

$$M_k = \{t/t = i(k-i) \text{ for some } i, 1 \leq i \leq p-1, i \neq k, 2i \neq k\}$$

Then M_k has $(p-3)/2$ elements. If $i, i \leq i \leq p-1$ is one choice for which $t = i(k-i)$, then $j = k-i$ is another choice with $1 \leq j \leq p-1$ for which the given t arises as

$$j(k-j) = (k-i)i = i(k-i)$$

Therefore

$$\psi(k) = 2 \sum_{t \in M_k} \chi(t)$$

Now, if $t = i(k-i)$, then $i^2 - ki + t = 0$. Therefore,

$$k^2 - 4t = \left(\frac{i^2 + t}{i} \right)^2 - 4t = \left(\frac{i^2 - t}{i} \right)^2$$

which being a square is in Q (as it is non-zero as well). Thus

$$k^2 - 4t \in Q \quad \text{or} \quad -4t = r - k^2$$

for some $r \in Q$. As $0 \notin M_k$, we have $r \neq k^2$. Therefore

$$-4M_k = \{r - k^2/r \in Q, r \neq k^2\}$$

Let $\bar{Q} = Q \cup \{0\}$. As $k^2 \in Q$ and p being of the form $4l+1$, -1 is also a residue mod p , $-k^2$ is a residue mod p . It then follows (from Perron's Theorem 8.3 part (iii)) that among $\{r - k^2/r \in \bar{Q}\}$ there are $k+1$ residues (including 0) and k non-residues. But

$$-4M_k = \{r - k^2/r \in \bar{Q}\} \setminus \{0, -k^2\}$$

and, so, in the set $-4M_k$ there are $k-1$ residues and k non-residues mod p . Again -4 is a residue mod p and hence M_k contains $k-1$ residues and k non-residues mod p . Therefore,

$$\psi(k) = 2(-1) = -2$$

and

$$\theta^2 = p - 2 - 2 \sum_{k=1}^{p-1} \alpha^k = p - 2 + 2 = p$$

Using part (i) of Theorem 8.3 and the fact that -1 is a non-residue mod p when $p \equiv -1 \pmod{4}$, we can prove the following theorem.

Theorem 8.5

If $p = 4k - 1$, then $\theta^2 = -p$.

8.3.1 Extended QR codes

We are now in a position to extend QR codes by adding an overall parity check. For a code \mathcal{C} , let $\hat{\mathcal{C}}$ denote the extended code of \mathcal{C} . We like to extend \mathcal{F} and \mathcal{N} in such a way that dual of $\hat{\mathcal{F}}$ is either $\hat{\mathcal{F}}$ or $\hat{\mathcal{N}}$. Similarly for $\hat{\mathcal{N}}$.

Case (i): $p = 4k - 1$

If $(a_0, a_1, \dots, a_{p-1})$ is a code word in \mathcal{F} (or \mathcal{N}), the extended code $\hat{\mathcal{F}}$ (or $\hat{\mathcal{N}}$) is formed by taking

$$a_p = -y \sum_{i=0}^{p-1} a_i$$

where $1 + y^2p = 0$. Then

$$(yp)^2 = -p = \theta^2$$

so that $y = \pm \theta/p$. As already seen, $\theta \in \text{GF}(s)$. Also s and p being distinct primes, p is invertible in $\text{GF}(s)$ and so $\pm \theta/p \in \text{GF}(s)$. Hence a choice of y in $\text{GF}(s)$ with the above condition is possible.

Case (ii): $p = 4k + 1$

If $(a_0, a_1, \dots, a_{p-1})$ is a code word in \mathcal{F} , the extended code $\hat{\mathcal{F}}$ is formed by taking

$$a_p = y \sum_{i=0}^{p-1} a_i$$

where $1 - y^2p = 0$ and if $a = (a_0, a_1, \dots, a_{p-1})$ is in \mathcal{N} , the extended code $\hat{\mathcal{N}}$ is formed by taking

$$a_p = -y \sum_{i=0}^{p-1} a_i$$

where y , as before, satisfies $1 - y^2p = 0$. Observe that

$$y^2p^2 = p = \theta^2$$

(Theorem 8.4) and, so, $yp = \pm \theta$. The number p is invertible in $\text{GF}(s)$ and, therefore, y satisfying the given condition can be obtained in $\text{GF}(s)$.

Theorem 8.6

If $p = 4k + 1$, the extended QR codes $\hat{\mathcal{F}}$ and $\hat{\mathcal{N}}$ defined above satisfy

$$(\hat{\mathcal{F}})^\perp = \hat{\mathcal{N}}$$

Proof

Let $\bar{\mathbf{G}}$ be a generator matrix for $\hat{\mathcal{F}}$. Then

$$\mathbf{G} = \left(\begin{array}{c|ccc} \bar{\mathbf{G}} & & & \\ \hline 1 & 1 & \dots & 1 \end{array} \right)$$

is a generator matrix for \mathcal{F} . A generator matrix for $\hat{\mathcal{F}}$ is then given by

$$\hat{\mathbf{G}} = \left(\begin{array}{c|ccc} \bar{\mathbf{G}} & & & \\ \hline 1 & 1 & \dots & 1 \end{array} \middle| \begin{array}{c} 0 \\ yp \end{array} \right)$$

Let $\bar{\mathbf{H}}$ be a generator matrix for $\bar{\mathcal{N}}$ so that

$$\mathbf{H} = \left(\begin{array}{c|ccc} \bar{\mathbf{H}} & & & \\ \hline 1 & 1 & \dots & 1 \end{array} \right)$$

is a generator matrix for \mathcal{N} . Generator matrix for $\hat{\mathcal{N}}$ is then given by

$$\hat{\mathbf{H}} = \left(\begin{array}{c|ccc} \bar{\mathbf{H}} & & & \mathbf{0} \\ \hline 1 & 1 & \dots & 1 \end{array} \middle| \begin{array}{c} \\ -yp \end{array} \right)$$

By Theorem 8.2

$$\mathcal{F}^\perp = \mathcal{N}$$

Therefore, every row of $\bar{\mathbf{H}}$ is orthogonal to every row of \mathbf{G} and, then, every row of $(\bar{\mathbf{H}} \ \mathbf{0})$ is orthogonal to every row of $(\mathbf{G} \ \mathbf{0})$ and, hence, every row of $(\bar{\mathbf{H}} \ \mathbf{0})$ is orthogonal to every row of $\hat{\mathbf{G}}$. Now the last row of $\hat{\mathbf{H}}$ is orthogonal to the last row of $\hat{\mathbf{G}}$ iff

$$p - y^2 p^2 = 0 \quad \text{or} \quad (yp)^2 = \theta^2$$

Since y has been chosen to satisfy this condition, every row of $\hat{\mathbf{H}}$ is orthogonal to every row of $\hat{\mathbf{G}}$. Hence

$$\hat{\mathcal{N}} \leq (\hat{\mathcal{F}})^\perp \tag{8.3}$$

Now $\hat{\mathcal{N}}$ is a code of length $p+1$ and dimension $(p+1)/2$. Also

$$\dim(\hat{\mathcal{F}})^\perp = p+1 - \dim \hat{\mathcal{F}} = p+1 - \frac{p+1}{2} = \frac{p+1}{2}$$

It, therefore, follows from relation (8.3) that

$$(\hat{\mathcal{F}})^\perp = \hat{\mathcal{N}}$$

Using the case $p = 4k - 1$ of Theorem 8.2, we can similarly prove the following theorem.

Theorem 8.7

The extended QR codes $\hat{\mathcal{F}}$ and $\hat{\mathcal{N}}$ defined as above are self dual in the case $p = 4k - 1$.

Corollary

The extended (i) binary Golay code $\mathcal{G}_{24} = \hat{\mathcal{G}}_{23}$ and (iii) ternary Golay code $\mathcal{G}_{12} = \hat{\mathcal{G}}_{11}$ are self dual.

Corollary

If $p = 4k - 1$, the weight of every non-zero code word in the extended QR codes $\hat{\mathcal{F}}$ and $\hat{\mathcal{N}}$ is divisible by s while the weight of every non-zero code word in the QR codes \mathcal{F} and \mathcal{N} is congruent to 0 or $s - 1$ modulo s .

We now come to the main theorem of this section.

Theorem 8.8

If d is the minimum distance between code words of the augmented QR code \mathcal{F} (or \mathcal{N}) neither of which is in the expurgated QR code $\bar{\mathcal{F}}$ (respectively $\bar{\mathcal{N}}$) except the 0 word, then $d^2 \geq p$. If $p = 4k - 1$, this minimum distance satisfies

$$d^2 - d + 1 \geq p$$

Proof

Observe that this minimum distance d equals the weight of a non-zero code word $a(x)$ in \mathcal{F} which is not in $\bar{\mathcal{F}}$. Then

$$x - 1 \nmid a(x)$$

Let n be a quadratic non-residue mod p . Set

$$\bar{a}(x) = a(x^n)$$

As α^r , $r \in Q$, are among the roots of $a(x)$, $\alpha^{r/n}$ are among the roots of $\bar{a}(x)$. Moreover, n is a non-residue implies $1/n$ is a non-residue. Therefore, α^m , $m \in N$ are among the roots of $\bar{a}(x)$. Thus $\bar{a}(x)$ is divisible by $n(x)$. As 1 is not a root of $a(x)$, $1^{1/n} = 1$ is not a root of $\bar{a}(x)$. Hence $\bar{a}(x) \in \mathcal{N}$ but is not in the expurgated code $\bar{\mathcal{N}}$. The number of non-zero terms in $\bar{a}(x)$ is precisely equal to the number of non-zero terms of $a(x)$, i.e.

$$\text{wt}(\bar{a}(x)) = d$$

Therefore, the number of non-zero terms in $a(x)\bar{a}(x)$ is at most d^2 . Also $a(x)\bar{a}(x)$ is divisible by

$$q(x)n(x) = \sum_{i=0}^{p-1} x^i$$

so that $a(x)\bar{a}(x)$ is non-zero constant multiple of

$$\sum_{i=0}^{p-1} x^i$$

and

$$\text{wt}(a(x)\bar{a}(x)) = p$$

Hence $d^2 \geq p$.

If $p = 4k - 1$, then -1 is a quadratic non-residue mod p and we may take

$$\bar{a}(x) = a(x^{-1})$$

Then d terms in $a(x)\bar{a}(x)$ are each equal to 1 and so the number of terms in $a(x)\bar{a}(x)$ is at most $d^2 - d + 1$. Hence, in this case

$$d^2 - d + 1 \geq p$$

Example 8.2

Consider the case $p = 17$. As

$$6^2 \equiv 2 \pmod{17}$$

we can take $s = 2$. The cyclotomic cosets relative to 2 modulo 17 are:

$$C_0 = \{0\}$$

$$C_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}$$

$$C_3 = \{3, 6, 12, 7, 14, 11, 5, 10\}$$

To factorize $x^{17} - 1$ as a product of irreducible polynomials, we find the HCF of

$$x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x + 1$$

and

$$\sum_{i=0}^{16} x^i$$

$$\begin{array}{r} x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x + 1 \overline{) x^{16} + x^{15} + \cdots + x^4 + x^3 + x^2 + x + 1} \\ \underline{x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x + 1} \\ x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3 \end{array}$$

$$\begin{array}{r} x^{14} + x^{12} + x^{11}x^{10} + x^7 + x^6 + x^5 + x^3 \overline{) x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x + 1} \\ \underline{x^{16} + x^{14} + x^{13} + x^{12} + x^9 + x^8 + x^7 + x^5} \\ x^{15} + x^{14} + x^{12} + x^7 + x^5 + x^4 + x^2 + x + 1 \\ \underline{x^{15} + x^{13} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x^4} \\ x^{14} + x^{13} + x^{11} + x^8 + x^6 + x^5 + x^2 + x + 1 \\ \underline{x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3} \\ x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1 \end{array}$$

$$\begin{array}{r} x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1 \overline{) x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3} \\ \underline{x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + x} \\ x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 \\ \phantom{x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4} + x^2 + x \\ \underline{x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1} \\ \hline \end{array}$$

$$\begin{array}{r}
 x^9 + x^6 + x^5 + x^4 + x^3 + 1 \overline{) x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1} \\
 \underline{x^{13} \phantom{+ x^{12} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1}} \\
 x^{10} + x^8 + x^7 + x^4 + x^9 \\
 \underline{x^{12} + x^9 + x^4 + x^3 + x^2 + x + 1} \\
 x^{12} + x^9 + x^8 + x^3 + x^7 + x^6 \\
 \underline{\phantom{x^{12} + x^9 + x^8 + x^3 + x^7 + x^6}} \\
 x^8 + x^7 + x^6 + x^4 + x^2 + x + 1 \\
 \\
 x^8 + x^7 + x^6 + x^4 + x^2 + x + 1 \overline{) x^9 + x^6 + x^5 + x^4 + x^3 + 1} \\
 \underline{x^9 + x^8 + x^5 + x^7 + x^3 + x^2 + x} \\
 x^8 + x^7 + x^6 + x^4 + x^2 + x + 1 \\
 \underline{x^8 + x^7 + x^6 + x^4 + x^2 + x + 1} \\
 0
 \end{array}$$

Thus the required HCF is

$$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$$

Dividing

$$\sum_{i=0}^{16} x^i$$

by the HCF obtained we get the other factor as

$$x^8 + x^5 + x^4 + x^3 + 1$$

Thus

$$x^{17} - 1 = (x - 1)(x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)$$

Let

$$F = \mathbb{B}[x]/I \quad \text{and} \quad \alpha = x + I$$

where I is the ideal of $\mathbb{B}[x]$ generated by

$$x^8 + x^5 + x^4 + x^3 + 1$$

The elements of C_1 being quadratic residues modulo 17 and those of C_3 being non-residues,

$$q(x) = x^8 + x^5 + x^4 + x^3 + 1$$

and

$$n(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$$