Make sure you justify all your answers appropriately.

Throughout this assignment:

For the odd prime p, χ is the function on $\mathbb{F}_p$ that is 0 at 0, +1 on nonzero squares, and −1 on nonsquares. The related function χ^+ agrees with χ on the nonzero elements of $\mathbb{F}_p$ but has $\chi^+(0) = +1$.

The associated *Legendre sequence* is the sequence $L^p = (w_0, w_1, \ldots, w_{p-1})$ with $w_i = \chi^+(i)$.

For a sequence $\mathbf{w} = (w_0, \ldots, w_i, \ldots, w_{m-1})$ and a k-tuple $\mathbf{a} = (a_0, \ldots, a_{k-1})$, the function $K^{\mathbf{a}}(\mathbf{w})$ counts the number of times $\mathbf{a}$ occurs cyclically within $\mathbf{w}$. That is, $K^{\mathbf{a}}(\mathbf{w})$ is the number of distinct i with $0 \le i \le m-1$ and

$$(w_i, w_{i+1}, \ldots, w_{i+k-1}) = (a_0, a_1, \ldots, a_{k-1}),$$

where subscripts are read modulo m.

1. (a) Write down the Legendre sequence $\mathbf{w} = L^{11}$.
(b) For each $\mathbf{a} \in \{\pm 1\}^1$ calculate $K^{\mathbf{a}}(\mathbf{w})$.
(c) For each $\mathbf{a} \in \{\pm 1\}^2$ calculate $K^{\mathbf{a}}(\mathbf{w})$.
(d) For each $\mathbf{a} \in \{\pm 1\}^3$ calculate $K^{\mathbf{a}}(\mathbf{w})$.

2. (a) Write down the Legendre sequence $\mathbf{w} = L^{13}$.
(b) For each $\mathbf{a} \in \{\pm 1\}^1$ calculate $K^{\mathbf{a}}(\mathbf{w})$.
(c) For each $\mathbf{a} \in \{\pm 1\}^2$ calculate $K^{\mathbf{a}}(\mathbf{w})$.
(d) For each $\mathbf{a} \in \{\pm 1\}^3$ calculate $K^{\mathbf{a}}(\mathbf{w})$.

3. Based on the previous two problems, what can you say about k-tuple optimality for the Legendre sequences L^p for $p = 11, 13$? What is your guess about the behaviour for arbitrary primes?

4. For the sequence $\mathbf{w} = (w_0, \ldots, w_i, \ldots, w_{m-1})$ the periodic autocorrelation function $C^{\mathbf{w}}(j)$, with $0 \le j \le m-1$, is given by

$$C^{\mathbf{w}}(j) = \sum_{i=0}^{m-1} w_i w_{i+j},$$

where subscripts are read modulo m.

For $\mathbf{w}$ the Legendre sequence L^{13} and each j with $0 \le j \le 12$, calculate $C^{\mathbf{w}}(j)$.

5. Use the squares and nonsquares in $\mathbb{F}_{11}$ to construct a 12×12 Hadamard matrix.

(Continued on other side)

6. (Hadamard matrices of side $2(q+1)$ for $q \equiv 1 \pmod 4$.)
We now consider the case where there is a finite field $\mathbb{F}_q$ containing q elements with $q \equiv 1 \pmod 4$. We know that $\mathbb{F}_p = \mathbb{Z}_p$ is an example for every prime $p = q \equiv 1 \pmod 4$.

Let C be the $q+1 \times q+1$ matrix indexed by $\infty \cup \mathbb{F}_q$ that has

- 0 in position (∞, ∞) ,
- $+1$'s in all nondiagonal positions in column and row ∞, and
- $\chi(c-r)$ in position (r, c) for $r, c \in \mathbb{F}_q$.

For example, with $p = q = 5$, we have

	∞	0	1	2	3	4
∞	0	+1	+1	+1	+1	+1
0	+1	0	+1	−1	−1	+1
1	+1	+1	0	+1	−1	−1
2	+1	−1	+1	0	+1	−1
3	+1	−1	−1	+1	0	+1
4	+1	+1	−1	−1	+1	0

(a) Prove that C is a symmetric matrix with $CC = CC^\top = qI$, where I is the $q+1 \times q+1$ identity matrix. (Recall that we have proven that -1 is a square in $\mathbb{F}_q$ when $q \equiv 1 \pmod 4$.)

(b) Prove that

$$\begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}$$

is a $2(q+1) \times 2(q+1)$ Hadamard matrix.