**Construction of BIBD’s Using Quadratic Residues**

Dr. K. Vijayalakshmi,
Loyola Academy, Secunderabad, Telengana

**Definition:** Let v, k, and λ be positive integers such that v > k ≥ 2. A (v, k, λ)-balanced incomplete block design (which we abbreviate to (v, k, λ)-BIBD) is a design (X, A) such that the following properties are satisfied:
1. |X| = v,
2. Each block contains exactly k points, and
3. Every pair of distinct points is contained in exactly λ blocks.

Property 3 in the definition above is the “balance” property. A BIBD is called an incomplete block design because k < v, and hence all its blocks are incomplete blocks.

A BIBD may possibly contain repeated blocks if λ > 1

Example: 1. A (7, 3, 1)-BIBD. X = {1, 2, 3, 4, 5, 6, 7}, and 
A = {123, 145, 167, 246, 257, 347, 356}.
The blocks of the BIBD are the six lines and the circle in this diagram.

2. A (9, 3, 1)-BIBD. X = {1, 2, 3, 4, 5, 6, 7, 8, 9}, and 
A = {123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357}.
The 12 blocks of the BIBD are depicted as eight lines and four triangles. Observe that the blocks can be separated into four sets of three, where each of these four sets covers every point in the BIBD.

3. A (10, 4, 2)-BIBD.
X = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, and A = {0123, 0145, 0246, 0378, 0579, 0689, 1278, 1369, 1479, 1568, 2359, 2489, 2567, 3458, 3467}.

4. A (7, 3, 2)-BIBD containing a repeated block.

In a (v, k, λ)-BIBD, every point occurs in exactly r = λ(v − 1)/ k − 1 blocks.

I. Quadratic Residues

Consider the congruence \( ax^2 + bx + c = 0 \mod p \) …………………(1)
Where p is an odd prime and p does not divide a. i.e. g.c.d (a, p) =1.since p is an odd prime we have
\[(4a,p)=1, \quad 4a(ax^2 + bx + c) = 0 \mod p \text{ using } 4a(ax^2 + bx + c) = \left(2ax + b\right)^2 - \left(b^2 - 4 ac \right)\]
The given congruence can be written as \( \left(2ax + b\right)^2 = \left(b^2 - 4 ac \right) \mod p \)

Put \( X = 2ax + b \) and \( N = b^2 - 4 ac \)
We get \( X^2 = N \mod p \) ………………………..(2)
if \( x = x_0 \mod p \) is a solution of (1) then \( X = 2ax_0 + b \mod p \) satisfies (2).
Conversely if \( y = y_0 \mod p \) is a solution of (2) then \( 2ax = y_0 - b \mod p \) can be solved to obtain a solution of (1). Finding a solution of (1) is equivalent to finding a solution to \( x^2 = a \mod p \).

If the congruence \( x^2 = n \mod p \) where \( p \) is an odd prime and \( p \) does not divide \( n \) then we say that \( n \) is a quadratic residue mod \( p \) and we write \( n \equiv_R p \). If the congruence has no solution then we say that \( n \) is a quadratic non residue mod \( p \) and we write \( n \not\equiv_R p \).

Example: To find quadratic residues mod 11 we square the numbers 1, 2, 3, ….. 10 and reduce to mod 11.

\( 1^2 = 1, \ 2^2=4, \ 3^2=9, \ 4^2=16 = 5, \ 5^2=25=3, \ 6^2=36 = 3, \ 7^2=49 = 5, \ 8^2=64=9, \ 10^2=100=1 \)

Therefore quadratic residues mod 11 are 1, 3, 4, 5, 9 and the quadratic non residues are 2, 6, 7, 8, 10.

**Theorem:** Let \( p \) be an odd prime then every reduced residue system mod \( p \) contains exactly \( \frac{p-1}{2} \) quadratic residues and exactly quadratic non residues mod \( p \). The quadratic residues belong to the residue classes containing the numbers \( 1^2, 2^2, 3^2, ……., \left( \frac{p-1}{2} \right)^2 \).

Proof: the numbers given above are distinct mod \( p \). For \( 1 \leq x \leq \frac{p-1}{2} \), \( 1 \leq y \leq \frac{p-1}{2} \)

if \( x^2 = y^2 \mod p \) \( \Rightarrow \) \( (x + y)(x - y) = 0 \mod p \) \( \Rightarrow \) \( x - y = 0 \mod p \) (since \( 1 < x+y < p \))

hence \( x = y \). Since \( (p-k)^2 = k^2 \mod p \) every quadratic residue is congruent mod \( p \) to exactly one of the numbers.

**Legendre’s Symbol:** Let \( p \) be an odd prime. If \( p \) does not divide \( n \), we define Legendre symbol \( (n/p) \) as follows:

\( (n/p) = 1 \) if \( n \equiv_R p \) and \( (n/p) = -1 \) if \( n \equiv_R p \). if \( n \equiv 0 \mod p \) we define \( (n/p) = 0 \)

For example \( \left( 1/p \right) = 1 \), \( \left( m^2/p \right) = 0 \), \( \left( 7/11 \right) = -1 \), \( \left( 22/11 \right) = 0 \)

Also \( (m/p) = (n/p) \) whenever \( m = n \mod p \). so \( (n/p) \) is a periodic function of \( n \) with period \( p \). From little Fermat’s theorem we have \( n^{p-1} = 1 \mod p \) if \( p \) does not divide \( n \).

\( n^{p-1} - 1 = (n^{\frac{p-1}{2}} - 1)(n^{\frac{p-1}{2}} + 1) \) Therefore \( n^{-1} = \pm 1 \mod p \).

**Euler’s criterion:** let \( p \) be an odd prime. Then for all \( n \) we have \( (n/p) = n^{(p-1)/2} \mod p \)

Proof: clearly the result is true when \( n \equiv 0 \mod p \) since both the numbers are congruent to 0 mod \( p \).

Suppose \( (n/p) = 1 \) \( \Rightarrow \exists \) an \( x \) such that \( x^2 = n \mod p \) and hence

\( n^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1 \mod p \)

Suppose \( (n/p) = -1 \) and consider the polynomial \( f(x) = x^{\frac{p-1}{2}} - 1 \)

Since \( f(x) \) has the degree \( p-1/2 \) \( f(x) \equiv 0 \mod p \) has at most \( \frac{p-1}{2} \) solutions but the \( \frac{p-1}{2} \) quadratic residues mod \( p \) are solutions so the non-residues are not. hence is incongruent to 1 mod \( p \) is \( (n/p) = -1 \). But

\( n^{-1} = \pm 1 \mod p \)

DOI: 10.9790/5728-11657782 www.iojsrjournals.org 78 | Page
\[
\frac{p-1}{n^2} = -1 \pmod{p} = (n/p) \pmod{p} 
\]

\[
\therefore (n/p) = n^2 \pmod{p}
\]

**Definition:** We define a semi-primitive root mod m as follows: Suppose \(a\) is any integer and \(m\) is a positive integer such that \((a, m) = 1\). We say that \(a\) is a semi-primitive root mod \(m\) if \(\exp_m a = \frac{\phi(m)}{2}\).

We know that there exists a semi-primitive root for mod \(m\) whenever \(m = p^\alpha 2^\beta \), for \(\alpha \geq 3\) also for \(m = p_1 p_2\) where \(p_1\) and \(p_2\) are distinct odd primes and at least one prime is of the form \(4n+3\). In these cases it was found to be convenient to define a function \(\lambda(m)\) called the universal exponent of mod \(m\). \(\lambda(m)\) is defined as follows:

\[
\lambda(1) = 1 \\
\lambda(2^\alpha) = \phi(2^\alpha) = 2^{\alpha-1} \text{ if } \alpha = 1,2 \\
= \phi(2^\alpha)/2 = 2^{\alpha-2} \text{ if } \alpha > 2.
\]

\[
\lambda(p^\alpha) = \phi(p^\alpha) \text{ where } p \text{ is an odd prime.}
\]

Where \(p_1, p_2, p_3, \ldots, p_r\) are distinct odd primes and \([\alpha, \beta]\) denotes L.C.M of \(\alpha\) and \(\beta\). An integer, whose exponent mod \(m\) is \(\lambda(m)\), is called a semi-primitive root of \(m\).

**Existence of semi-primitive roots:** Now we establish some results on the existence of semi-primitive roots.

**Theorem:** There exists a semi-primitive root for mod \((p^\alpha)\) and for mod \(2 p^\alpha\) for \(\alpha > 2\).

**Proof:** Let \(m = p^\alpha\) and \(\alpha > 2\).

We know that from the properties of exponents that if \(\exp_m a = t\) then \(\exp_m a^b = t/(n,t)\).

Suppose \( \alpha \) is a primitive root mod \(m\). Then \(\exp_m a = \phi(m)\), \(\exp_m a^2 = \phi(m)/(2, \phi(m)) = \phi(m)/2\).

Therefore whenever \(a\) is a primitive root, \(a^2\) is a semi-primitive root. As there exists primitive roots for mod \(p^\alpha\) mod and for mod \(2 p^\alpha\) we have, there exists a semi-primitive root for mod \(p^\alpha\) and for mod \(2 p^\alpha\).

**Theorem 2:** There exists a semi-primitive root for mod \(m\) where \(m = 2^2 p^\alpha\).

**Proof:** From the definition of \(\lambda\)-primitive root, there exists a \(\lambda\)-primitive root for mod \(2^2 p^\alpha\).

\[
\phi(m) = \phi(2^2 p^\alpha) = 2 \cdot 2^{\alpha-1}(p-1).
\]

\[
\frac{\phi(p^\alpha)}{2} = 2 \cdot \frac{\phi(p^\alpha)}{2} = \phi(p^\alpha)
\]

\[
\therefore \lambda(m) = \frac{\phi(m)}{2}
\]

\[
\lambda(m) = \lambda(2^2) \cdot \lambda(p^\alpha) = \frac{\phi(2^2) \cdot \phi(p^\alpha)}{(\phi(2^2) \cdot \phi(p^\alpha))}
\]

Hence there exists a semi-primitive root for mod \(2^2 p^\alpha\).

**Theorem 3:** There exists a semi-primitive root for mod \(2^\alpha\) if \(\alpha > 3\).

**Proof:** There exists a \(\lambda\)-primitive root for mod \(2^\alpha\) if \(\alpha > 3\), i.e., for every \( \alpha \) relatively prime to \(2^\alpha\) suppose \(m = 2^\alpha\) we have

\[
\exp_{2^\alpha} a = \lambda(2^\alpha)
\]

\[
\lambda(m) = \lambda(2^\alpha) = \frac{\phi(p^\alpha)}{2} = \frac{\phi(m)}{2}
\]

Hence there exists a semi-primitive root for mod \(2^\alpha\).

**Theorem 4:** There exists a semi-primitive root for mod \(m\) when \(m = p_1 p_2\) where \(p_1\) and \(p_2\)

DOI: 10.9790/5728-11657782
are distinct odd primes and at least one prime is of the form 4n+3.
Proof: Let \( m = p_1p_2 \).

\[
\begin{align*}
\lambda (m) &= \frac{\phi (m)}{2} \text{ if } (p_1-1, p_2-1) = 2 \\
\phi (m) &= \phi (p_1) \phi (p_2) = (p_1-1)(p_2-1) \\
\frac{\phi (m)}{2} &= \frac{(p_1-1)(p_2-1)}{2} \\
\lambda (m) &= \left[ \lambda (p_1), \lambda (p_2) \right] = \left[ \phi (p_1), \phi (p_2) \right] = \frac{\phi (p_1) \phi (p_2)}{(\phi (p_1), \phi (p_2))} \\
&= \frac{\phi (p_1), \phi (p_2)}{(p_1-1, p_2-1)}
\end{align*}
\]

Clearly \((p_1-1, p_2-1) = 2\)

If at least one of \( p_1, p_2 \) is of the form 4n+3. Therefore there exists a semi-primitive root for \( \mod m \) when \( m = p_1p_2 \) where \( p_1 \) and \( p_2 \) are distinct odd primes and at least one prime is of the form 4n+3.

**Theorem:** If \( \alpha \) is semi-primitive root \( \mod p \) then \( \alpha \) is a quadratic residue \( \mod p \).

**Proof:** \( \frac{p-1}{2} \) is a semi primitive root \( \mod p \) \( \Rightarrow \alpha^2 \equiv 1 \pmod{p} \).

Since \( p \) is an odd prime \( p \) has a primitive root say \( g \).

Since \( (a, p) = 1 \) we have \( a = g^k \pmod{p} ; 1 \leq k \leq \phi(p) \).

\[
1 = \alpha^2 = (g^k)^2 \pmod{p}
\]

\( \Rightarrow \) Since \( g \) is a primitive root \( \mod p \) we have \( p-1 \) divides \( k \cdot \frac{p-1}{2} \).

\( \Rightarrow \frac{k}{2} \) is an integer i.e \( \frac{k}{2} = m \).

\( \therefore \ a = (g^m)^2 \pmod{p} \) \( \Rightarrow \ g^m \) is a solution of \( x^2 = a \pmod{p} \).

Therefore \( a \) is a quadratic residue \( \mod p \).

However converse is not true as there are \( \phi(p)/2 \) semi-primitive roots and \( \frac{p-1}{2} \) quadratic residues.

**Definition:** Let \( G \) be an additive abelian group of order \( v \). A subset \( S \) of \( G \) of order \( k \) is called a difference set in \( G \) with parameters \( (v, k, \lambda) \).

**Example:** Let \( G = Z_7 \) be the additive group of integers modulo 7. Let \( S = \{1, 2, 4\} \). Show that \( S \) is a difference set in \( G \), and find its parameters.

**Solution:** Writing the non zero differences of all of all ordered pairs of elements in \( S \), we see that each non zero element in \( G \) occurs once as a difference of two elements of \( S \). Hence \( S \) is a difference set in \( G \).

**Theorem:** Let \( S \) be a difference set in a group \( G \) with parameters \( (v, k, \lambda) \), then \( k(k-1) = \lambda(v-1) \).

**Proof:** Because \( S \) has \( k \) elements, the number of ordered pairs \( (x, y) \in S \times S \) such that \( x \neq y \) is equal to \( k(k-1) \). On the other hand, \( G \) has \( v-1 \) non zero elements, and for each non zero element \( a \in G \), there are \( \lambda \) ordered pairs \( (x, y) \in S \times S \) such that \( a = x - y \). Hence \( k(k-1) = \lambda(v-1) \).

Given a subset \( S \) of \( G \) and an element \( g \in G \), we write \( g + S = \{g + s : s \in S\} \).

It is clear that if \( S \) is a \( (v, k, \lambda) \)-difference set, then for every \( g \in G \), \( g + S \) is also a \( (v, k, \lambda) \)-difference set in \( G \). We have \( a = x - y \Leftrightarrow (g + x) - (g + y) \).

Thus \( S \) determines \( v \) difference sets \( g + S \), \( g \in G \).

**Theorem:** Let \( S = \{s_1, s_2, \ldots, s_l\} \) be a difference set in a group \( G = \{g_1, g_2, \ldots, g_v\} \) with parameters \( (v, k, \lambda) \). For each \( i = 1, 2, \ldots, v \), let \( B_i = g_i + S = S = \{g_i + s : s \in S\} \). Then
D = {B₁, B₂, …, Bₙ} is a symmetric BIBD on the set with parameters \((v, k, \lambda)\).

**Example:** We have seen that \(S = \{1, 2, 4\}\) is a \((7, 3, 1)\)-difference set in the additive group \(Z_7\). Now we find the symmetric BIBD with the following blocks as follows:

\[0 + S = \{1, 2, 4\}, 1 + S = \{2, 3, 5\}, 2 + S = \{(3, 4, 6), 3 + S = \{4, 5, 0\}, 4 + S = \{5, 6, 1\}, 5 + S = \{6, 0, 2\}, 6 + S = \{0, 1, 3\}\]

So \(D = \{(1, 2, 4), (2, 3, 5), (3, 4, 6), (4, 5, 0), (5, 6, 1), (6, 0, 2), (0, 1, 3)\}\) is a symmetric BIBD on the set \(Z_7\) with parameters \((7, 3, 1)\). It was proved in [6] that

**Theorem:** Let \(p\) be an odd prime such that \(p \equiv 3\pmod{4}\). Then \(Q_p\) is a difference set in the additive group \(Z_p\) with parameters \(\left(\frac{p - 1}{2}, \frac{p - 3}{4}\right)\).

Proof: We first show that \(-1 \notin Q_p\). If possible suppose \(-1 = x^2\) for some \(x \in Z_p^*\).

Since \(p \equiv 3\pmod{4}\), we have \(\frac{p - 1}{2}\) is an odd integer. Hence working in the field \(Z_{p^2}\), we have

\[-1 - \left(\frac{p - 1}{2}\right)^2 = \left(x^2\right)^{\frac{p - 1}{2}} = x^{p - 1}\]

But \(Z_p^*\) is a group of order \(p - 1\) and hence \(x^{p - 1} = -1\), a contradiction.

Thus \(-1\) cannot be a quadratic residue modulo \(p\).

Let \(a \in Z_p^*\). If \(a \in Q_p\), then \(-a = (1)a \in Q_p\). If, on the contrary, \(a \notin Q_p\) then \(-a = (1)a \in Q_p\). Thus for any \(a\) in \(Z_p^*\) either \(a \in Q_p\) or \(-a \in Q_p\).

We now show that \(Q_p\) is a difference set in the additive group \(Z_p\). For any nonzero \(a\) in \(Z_p\), let \(S(a)\) denote the set of ordered pairs \((x, y)\) such that \(x, y \in Q_p, x - y = a\). We claim that there is a one to one correspondence between \(S(1)\) and \(S(a)\).

Consider first the case where \(a \in Q_p\). Let \((x, y) \in S(1)\). Then \(1 = x - y\) and hence \(a = a(x - y) = ax - ay\). Now \(a, x, y \in Q_p\) and hence \(ax, ay \in S(a)\). So \(ax, ay \in S(a)\).

Conversely let \((x', y') \in S(a)\), then \(a = x'^* - y'^*\), and hence \(1 = a^{-1} = a^{-1}(x' - y') = a^{-1}x' - a^{-1}y'\).

Since \(Q_p\) is a subgroup of \(Z_p^*\), \(a^{-1} \in Q_p\). So \((a^{-1}x, a^{-1}y) \in S(1)\). Thus we have a one to one correspondence between \(S(1)\) and \(S(a)\), given by \((x, y) \rightarrow (ax, ay)\).

Now suppose \(a \in Q_p\). Then \(-a \in Q_p\). If \((x, y) \in S(1)\), then \(a = a(x - y) = ax - ay = (-a)y - (-a)x\).

Hence \((-ay, -ax) \in S(a)\). Conversely if \((x', y') \in S(a)\), then \(1 = a^{-1} = a^{-1}(x' - y') = (-a^{-1})y' - (-a^{-1})x'\).

Since \(a \notin Q_p, a^{-1} \notin Q_p\) and hence \(-a^{-1} \in Q_p\). Thus \((-a^{-1})y', -a^{-1}x') \in S(1)\). So there is a one to one correspondence between \(S(1)\) and \(S(a)\), given by \((x, y) \rightarrow (-ax, -ay)\), i.e. for every non zero \(a\) in \(Z_p\), there is one to one correspondence between \(S(1)\) and \(S(a)\).

We write \(\lambda = |S(1)|\). Then \(|S(a)| = \lambda\) for every non zero \(a\) in \(Z_p\).

Hence, for every non zero \(a\) in \(Z_p\), there are exactly \(\lambda\) ordered pairs of elements in \(Z_p\) such that \(a = x - y\). This proves that \(Q_p\) is a difference set in the additive group \(Z_p\).

Now \(|Z_p| = p\) and \(|Q_p| = \frac{p - 1}{2}\).

Therefore we have \(\lambda(p - 1) = \left(\frac{p - 1}{2}\right)\left(\frac{p - 3}{2}\right) \Rightarrow \lambda = \frac{p - 3}{4}\).

Thus \(Q_p\) is a difference set with parameters \(\left(\frac{p - 1}{2}, \frac{p - 3}{4}\right)\).

**II. Result:**

For every positive integer \(t\) such that \(4t + 3\) is a prime, there exists a symmetric BIBD with parameters \((4t + 3, 2t + 1, t)\).

**Example:** Find the set of quadratic residues modulo 11, and construct the symmetric BIBD determined by it.

Solution: The quadratic residues modulo 11 are \(\{1, 4, 9, 5, 3\}\). Since \(11 \equiv 3\pmod{4}\), \(Q_{11}\) is a difference set with parameters \((11, 5, 2)\) in the additive group \(Z_{11}\). The blocks of the symmetric design \(D\) on the set \(Z_{11}\) determined by the difference set \(S = Q_{11}\) are \(i + s, i = 0, 1, \ldots, 10\).

DOI: 10.9790/5728-11657782 www.iosrjournals.org 81 | Page
Construction of BIBD's Using Quadratic Residues

So $D = \{ \{1,3,4,5,9\}, \{2,4,5,6,10\}, \{3,5,6,7,0\}, \{4,6,7,8,1\}, \{5,7,8,9,2\} \}
\{ \{6,8,9,10,3\}, \{7,9,10,0,4\}, \{8,10,0,1,5\}, \{9,0,1,2,6\}, \{10,1,2,3,7\}, \{0,2,3,4,8\} \}$

$D$ is a symmetric BIBD with parameters $(11, 5, 2)$.

References

[2]. Introduction to Number theory, Tom M. Apostol, Springer.