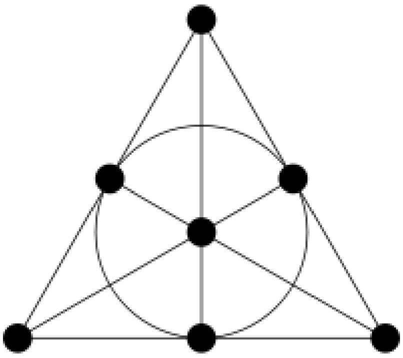
IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 6 Ver. V (Nov. - Dec. 2015), PP 77-82
www.iosrjournals.org

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 iscalled 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.
*X = {0, 1, 2, 3, 4, 5, 6}, and A = [123, 145, 167, 246, 257, 347, 356,*123, 147, 156, 245, 267, 346, 357].
In a (v, k, λ)-BIBD, every point occurs in exactly r = λ(v − 1)/ k − 1 blocks.

I. Quadratic Residues

Consider the congruence $ax^2 + bx + c \equiv 0$ 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, $4a(ax^2 + bx + c) \equiv 0$ mod p using $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$

The given congruence can be written as $(2ax + b)^2 \equiv (b^2 - 4ac)$ mod p

Put $X = 2ax + b$ and N = $b^2 - 4ac$

We get $X^2 \equiv N$ mod p……………………..(2)
if $x \equiv x_0 \pmod{p}$ is a solution of (1) then $X \equiv 2ax_0 + b$ (mod p) satisfies (2).

Conversely if $y \equiv y_0 (\bmod\ p)$ is a solution of (2) then $2ax \equiv y_0 - b(\bmod\ p)$ can be solved to obtain a solution of (1). Finding a solution of (1) is equivalent to finding a solution to $x^2 \equiv a(\bmod\ p)$.

If the congruence $x^2 \equiv n(\bmod\ p)$ 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 R p. If the congruence has no solution then we say that n is a quadratic non residue mod p and we write n $\overline{R}$ p.

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

$1^2 = 1$, $2^2=4$, $3^2 = 9$, $4^2 = 16 \equiv 5$, $5^2 =25\equiv3$, $6^2 =36 \equiv 3$, $7^2 = 49 \equiv 5$, $8^2=64\equiv9$, $10^2= 100 \equiv1$

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 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,…….. $(\frac{p-1}{2})^2$.

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 $x^2 \equiv y^2 (\bmod\ p) \Rightarrow (x+y)(x-y) \equiv 0$ mod p.$\Rightarrow x - y \equiv 0$ mod p (since $1 < x+y < p$)

hence x = y. Since $(p-k)^2 \equiv k^2 (\bmod\ p)$ 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 R p and $(n/p) = -1$ if n $\overline{R}$ p. if $n \equiv 0$ mod p we define $(n/p) = 0$

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

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 $n^{p-1} \equiv 1(\bmod\ p)$ if p does not divide n.

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

Euler's criterion: let p be an odd prime. Then for all n we have $(n/p) \equiv n^{\frac{p-1}{2}} (\bmod\ p)$

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

Suppose (n /p) =1 ⇒∃ an x such that $x^2\equiv$ n (modp) and hence

$n^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 = (n/p)$ modp

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)≡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 $n^{\frac{p-1}{2}}$ is incongruent to 1 mod p is (n/p) =-1. But

$n \frac{p-1}{2} \equiv \pm 1(\bmod\ p)$ so

$$n^{\frac{p-1}{2}} \equiv -1(\bmod\ p) \equiv (n/p) \bmod\ p$$

.

$$\therefore\ (n/p) \equiv n^{\frac{p-1}{2}} (\bmod\ p)$$

Definition: We define a semi-primitive root mod mas 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 asemi-primitive root for mod m whenever m = p^α ,$2p^\alpha$,$2^2.p^\alpha$,2^α, 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 λ(m)called universal exponent of mod m λ(m) is defined as follows:

λ(1) = 1

$\lambda(2^\alpha) = \varphi(2^\alpha) = 2^{\alpha-1}$if α = 1,2

$= \varphi(2^\alpha)/2 = 2^{\alpha-2}$ if α>2.

$\lambda(p^\alpha) = \varphi(p^\alpha)$ where p is an odd prime.

$$\lambda(2^\alpha.p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots p_r^{\alpha_r}) = [\lambda(2^\alpha), \lambda(p_1^{\alpha_1}),\ldots\ldots \lambda(p_r^{\alpha r})]$$

Where $p_{1,}\ p_{2\ ,}\ p_{3,}$ ----- p_r are distinct odd primes and [α ,β]denotes L.C.M of α and β.An integer, whose exponent mod m is λ(m), is called λ- primitive root of m.

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

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

Proof: let m = p^α and α>2.

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

Suppose 'a' is primitive root mod m. Then $\exp_m a = \varphi(m).\exp_m a^2 = \varphi(m)/(2, \varphi(m)) = \varphi(m)/2$

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

Theorem2*:* There exists a semi-primitive root for mod m where m = $2^2.p^\alpha$

Proof: From the definition of λ- primitive root, there exists a λ- primitive root for mod $2^2.p^\alpha$.

$\varphi(m) = \varphi(2^2.p^\alpha) = 2.p^{\alpha-1}(p-1)$.

$$\frac{\phi(m)}{2} = 2.\frac{\phi(p^\alpha)}{2} = \varphi(p^\alpha)$$

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

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

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

Theorem 3:There exists a semi-primitive root for mod 2^αif α>3.

Proof: There exists a λ-primitive root for mod 2^αif α>3.i.e for every 'a' relatively primeto 2^αsuppose m = 2^α 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^α.

Theorem 4: 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.
Proof: Let m = p_1p_2.Then

$$Now\ \lambda(m) = \frac{\phi(m)}{2} if\ (p_1 - 1, p_2 - 1) = 2$$

$$\phi(m) = \phi(p_1).\phi(p_2) = (p_1 - 1).(p_2 - 1)$$

$$\frac{\phi(m)}{2} = \frac{(p_1 - 1).(p_2 - 1)}{2}$$

$$\lambda(m) = [\lambda(p_1), \lambda(p_2)] = [\phi(p_1), \phi(p_2)] = \frac{\phi(p_1).\phi(p_2)}{(\phi(p_1), \phi(p_2))}$$

$$= \frac{\phi(p_1), \phi(p_2)}{(p_1 - 1, p_2 - 1)}$$

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 'a' is semi-primitive root mod p then 'a' is a quadratic residue mod p.

Proof: a is a semi primitive root mod p $\Rightarrow a^{\frac{p-1}{2}} \equiv 1(\text{mod}\ \ p)$
Since p is an odd prime p has a primitive root say g.

Since (a. p) = 1 we have $a \equiv g^k (\text{mod}\ \ p); 1 \le k \le \phi(p)$

$$1 \equiv a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} (\text{mod}\ \ p)$$

⇒Since g is a primitive root mod p we have p -1 divides k. $\frac{p-1}{2}$

$$\Rightarrow \frac{k}{2} \text{ is an integer i.e } \frac{k}{2} = m$$

$$\therefore a \equiv (g^m)^2 (\text{mod}\ \ p) \Rightarrow g^m \text{ is a solution of } x^2 \equiv a(\text{mod}\ \ p)$$

Therefore a is a quadratic residue mod p.

However converse is not true as there are ϕ(ϕ(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,λ) if for each non zero a∈ G, there are exactly λ ordered pairs (x, y) of elements in S such that *a = x - y*.

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 have
1 - 2 = 6, 1- 4 = 4, 2 - 1=1, 2 – 4 = 5, 4 - 1= 3, 4 - 2 = 2. Thus we see that each non zero element in G Occurs exactly once as a difference of two elements of S. Hence S is a difference set in with parameters (7, 3, 1).

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

Proof: Because S has k elements, the number of ordered pairs (x, y)∈ S×S such that x≠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∈ G, there are λ ordered pairs (x, y)∈ S×S such that a = x – y. Hence k(k-1) =λ(v-1).

Given a subset S of G and an element g in G, we writeg + S = {g +s : s∈S}

It is clear that if S is a (v, k,λ)- difference set , then for every g ∈ G, g + S is also a (v, k,λ)- difference set in G. we have a = x – y ⇔ (g + x) – (g + y)

Thus S determines v difference sets g + S, g ∈ G

Theorem: Let S = {s_1,s_2,……s_k}be a difference set in a group G = {g_1,g_2,…….g_v}with parameters (v, k, λ). For each I = 1,2,……v. let B_i = g_i+ S = S=g_i+s :s∈S}. Then

D = {B_1,B_2,……B_v} is a symmetric BIBDonthe set withparameters(v, k, λ).

Example: We have seen that S = {1, 2, 4} is a (7, 3, 1)-difference set in the additive group Z_7 = {0, 1, 2, 3, 4, 5, 6}. 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 ≡ 3(mod4).Then Q_p is a difference set in the additive group Z_p with parameters $\left(p, \frac{p-1}{2}, \frac{p-3}{4} \right)$.

Proof: we first show that -1∉ Qp. If possible suppose -1=x^2 for some x∈Z_p*.

Since p ≡ 3(mod4), we have $\frac{p-1}{2}$ is an odd integer. Hence working in the field Z_p, we have

$-1 = (-1)^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1}$ ButZ_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∈Z_p*.If a ∈Q_p, then –a=(-1)a ∉ Q_p. If , on the contrary , a∉ Q_p, then –a = (-1)a ∈Q_p. Thus for any a in Z_p* either a ∈Q_p or -a∈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 ∈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∈Q_p. Let (x, y) ∈ S(1).Then 1= x- y and hence a = a(x- y) = ax-ay. Now a, x, y ∈Q_p and hence ax, ay∈ Q_p. So ax, ay ∈ S(a).

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

Since Qp is a sub group of Z_p*, a^{-1}∈ Q_p, So ($a^{-1}x' - a^{-1}y'$)∈S(1).Thus we have a one to one correspondence between S(1) and S(a), given by (x, y)→ (ax, ay).

Now suppose a∉ Q_p . Then –a ∈ Q_p. If (x, y)∈ S(1)., Then $a = a(x - y) = ax - ay = (-a)y - (-a)x$.

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

Since a ∉ Q_p,a^{-1}∉ Q_p and hence -a^{-1}∈ 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)→ (-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 λ 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 $\lambda(p-1) = (\frac{p-1}{2})(\frac{p-1}{2} - 1) \Rightarrow \lambda = \frac{p-3}{4}$

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

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≡3 (mod 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, ……10.

$$\text{So } D = \left\{ \begin{array}{l} \{1,3,4,5,9\}, \{2,4,5,6,10\}, \{3,5,6,7,0\}, \{4,6,7,8,1\}, \{5,7,8,9,2\} \\ \{6,8,9,10,3\}, \{7,9,10,0,4\}, \{8,10,0,1,5\}, \{9,0,1,2,6\}, \{10,1,2,3,7\}, \{0,2,3,4,8\} \end{array} \right\}$$

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

References

[1]. Discrete and Combinatorial Mathematics "An Applied Introduction" 5th Edition, Ralph P. Grimaldi, B. V. Ramana.

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

[3]. A course in Combinatorics second edition, J.H.Van Lint and R.M. Wilson.

[4]. "Existence of Semi Primitive root Mod p$^{\alpha}$" in IOSR Journal of Mathematics p-ISSN2319-765X, Vol.11, Issue2, ver. II (March- April 2015), PP14-17. By Dr.K.Vijayalakshmi

[5]. "Properties of Semi primitive roots" in IOSR Journal of Mathematics Vol.No.5, Issue 4, Jan - Feb 2013.By Dr.K.Vijayalakshmi.

[6]. Topics in Applied Abstract Algebra by S. R. Nagpaul and S.K.Jain American mathematical society.