

## Quadratic Residues

### Some algebraic preliminaries

$p$  will always denote an odd prime.

Let  $Z_p^*$  be the multiplicative group of non-zero elements in  $Z_p$ .

Now, the mapping  $\phi: Z_p^* \rightarrow Z_p^*$  by  $\phi(x) = x^2$  is a homomorphism of abelian groups.

An element  $a \in Z_p^*$  is a quadratic residue mod  $p$  if

$a = \phi(x)$  for some  $x \in Z_p^*$ .

Alternately, a non-zero integer  $a$  with  $(a, p) = 1$  is a quadratic residue mod  $p$  if there exists an integer  $x$  with  $x^2 \equiv a \pmod{p}$ .

### Examples

- 1) 3 is a quadratic residue (mod 11) since  $5^2 \equiv 3 \pmod{11}$
- 2) The image of  $\phi$ ,  $\phi(Z_p^*)$ , is the set of quadratic residues (mod  $p$ ). Note that this is a group under multiplication.
- 3)  $\{1, 2, 4\}$  is the set of quadratic residues mod 7.

### Proposition 4

The set of quadratic residues mod  $p$  has order  $\frac{p-1}{2}$ .

i. e. exactly half the elements of  $Z_p^*$  are quadratic residues.

### Proof:

The homomorphism  $\phi$  described above has kernel

$$= \{x \in Z_p^* \mid x^2 = 1\} = \{1, -1\}.$$

Note that  $1 \neq -1$  since  $p > 2$ . Apply the Fundamental theorem of Group Homomorphisms to get

$$|\phi(Z_p^*)| = \frac{|Z_p^*|}{2} = \frac{p-1}{2}.$$

### Remarks

1. An element which is not a quadratic residue is called a quadratic non-residue.
2. Proposition 4 shows that  $H = \phi(Z_p^*)$  is a normal subgroup of  $Z_p^*$  of

index two -- so if  $b$  is a quadratic non-residue then  $Z_p^* = H \cup bH$  gives a coset decomposition of  $Z_p^*$  relative to  $H$ . Further, if  $a$  and  $b$  are non-residues, then  $aH = bH$  and  $abH = (aH)(bH) = (aH)^2 = H$ , the last equality courtesy of the fact that the group  $Z_p^*/H$  has order two. Thus,  $ab \in H$ .

Expressed another way,

$$(\text{non-residue}) \cdot (\text{non-residue}) = \text{residue}$$

Our discussion also shows that

$$(\text{residue}) \cdot (\text{residue}) = \text{residue}$$

$$(\text{residue}) \cdot (\text{non-residue}) = \text{non-residue.}$$

### Example

Notice that the quadratic residues (mod 7)  $\{1, 2, 4\}$  form a difference set since

$$\underline{+}(1 - 2) = 6, 1, \quad \underline{+}(1 - 4) = 4, 3, \quad \underline{+}(2 - 4) = 5, 2.$$

To exhibit a connection between residues and difference sets we need

### Lemma

If  $p \equiv 3 \pmod{4}$ , then  $-1$  is not a quadratic residue mod  $p$ .

### Proof:

Suppose there does exist an integer  $x$  with  $x^2 \equiv -1 \pmod{p}$ .

Let  $g$  be a primitive root (mod  $p$ ) and write  $x \equiv g^t \pmod{p}$ ,

$$\text{Then } -1 \equiv x^2 \equiv g^{2t} \pmod{p}$$

Note that, by hypothesis,  $\frac{p-1}{2}$  is odd.

$$\text{So, } -1 \equiv (-1)^{\frac{p-1}{2}} \equiv g^{(2t)\frac{p-1}{2}} \equiv (g^{p-1})^t \pmod{p}.$$

But,  $g^{p-1} \equiv 1 \pmod{p}$ , since  $g$  has order  $p-1$ .

We then have  $-1 \equiv 1 \pmod{p}$ , which is a contradiction.

Our main result is

### Proposition 5

Let  $p$  be a prime with  $p \equiv 3 \pmod{4}$ .

Write  $p = 4t - 1$  for some  $t$ .

Let  $D = \{a_1, \dots, a_k\}$  be the set of  $k = \frac{p-1}{2}$  quadratic residues (mod  $p$ ).

Then  $D$  is a  $(v, k, \lambda)$  difference set in  $Z_p$  with

$$v = p = 4t - 1$$

$$k = \frac{p-1}{2} = 2t - 1$$

$$\lambda = t - 1.$$

Proof:

Note that  $-1$  is a non-residue (mod  $p$ ) and hence given any  $a, b \in Z_p^*$  exactly one of  $a - b$  and  $b - a$  is a residue (mod  $p$ ).

Let  $a_i - a_j = x$ , where  $x$  is a quadratic residue. Then  $x^{-1}a_i - x^{-1}a_j = 1$ .

Conversely, if  $a_i - a_j = 1$  and  $x$  is a quadratic residue then  $(xa_i) - (xa_j) = x$ .

This sets up a 1 - 1 correspondence between the set of all pairs  $(a_i, a_j)$  with  $a_i - a_j = 1$  and pairs  $(a_i', a_j')$  with  $a_i' - a_j' = x$  for any residue  $x$ . So any residue occurs as a difference as often as any other. That each non-residue occurs as a difference  $a_i - a_j$  as often as each residue follows from the fact that

$$a_i - a_j = x \iff a_j - a_i = -x$$

and that  $x$  is a residue if and only if  $-x$  is a non-residue. It follows that  $D$  is a difference set with

$$\begin{aligned} \lambda &= \frac{(2t-1)(2t-2)}{p-1} \\ &= \frac{(2t-1)(2t-2)}{4t-2} = t - 1. \end{aligned}$$

Examples

1. The quadratic residues (mod 11)  $\{1, 4, 9, 5, 3\}$  yield a symmetric block design with  $v = 11$ ,  $k = 5$  and  $\lambda = 2$ .
2. As a sidelight we note that elementary number theory can be used to show that there are infinitely many primes  $p \equiv 3 \pmod{4}$ .
3. The case  $t = 2$  of Proposition 5 produces the symmetric block design

$$\{1, 2, 4\}$$

ratic

{2, 3, 5}

{3, 4, 6}

{4, 5, 0}

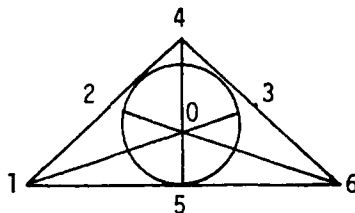
{5, 6, 1}

{6, 0, 2}

{0, 1, 3}

for which the picture

y a, b  $\in Z_p^*$



then

all pairs

$a_j = x$  for any

in as any

$a_j$  as often as

is a nice representation. The blocks are represented by lines (including the circle). In the above any two lines (blocks) intersect in precisely one element. It is a fact that in a symmetric block design any two distinct blocks have exactly  $\lambda$  objects in common (see Exercise 11). Symmetric block designs with  $\lambda = 1$  thus provide examples of finite projective planes. The example here is often referred to as the Fano geometry.

#### Concluding Remarks

e. It follows

The subject of block designs has produced an enormous literature. Many of the initial results dealt with statistical analyses of agricultural experiments [6]. Much current research revolves around the question of determining sufficient conditions for the existence of block designs. Equations (3) and (4) are not enough -- there is, for example, no block design with the parameters  $b = v = 43, k = 7, \lambda = 1$  [3]. Our elementary treatment draws on simplified versions of Bose's "method of symmetrically repeated differences" [1].

ld a symmetric

an be used to 3 (mod 4).

block design

Interest in Steiner triples dates back to 1847 when the Rev. Thomas Kirkman posed and solved what is now known as the Kirkman schoolgirl problem: A teacher takes her class of 15 girls on a daily walk. The girls walk in 5 rows of 3 each. The problem is to arrange the schedule so that in 7 consecutive days every girl will have walked in a group of 3 once with every other girl. A solution would require a block design with  $v = 15, b = 35, r = 7, k = 3$ , and  $\lambda = 1$  with the added condition that the design is resolvable into 7 sets of 5 blocks each, with each girl appearing once in each of the 7 sets. For a solution, see [7].