QUADRATIC RESIDUES

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

When is an integer a square modulo p? When does a quadratic equation have roots modulo p? These are the questions that will concern us in this handout.

1. The Legendre Symbol

Definition 1. Let $\overline{a} \in \mathbb{F}_p$ where p is an odd prime. We call $\overline{a}$ a *square* if there is an element $\overline{b} \in \mathbb{F}_p$ such that $\overline{a} = \overline{b}^2$. Non-zero squares are also called *quadratic residues*.

The set of quadratic residues is written $(U_p)^2$ or Q_p. We will see later that $(U_p)^2$ is closed under multiplication (in other words, it is a subgroup of U_p).

Remark. Observe that $\overline{a}$ is a quadratic residue if and only if there is a *non-zero* $\overline{b}$ such that $\overline{b}^2 = \overline{a}$.

(One direction is easy: if $\overline{a}$ is a quadratic residue, then by definition it is a non-zero square. So there is a $\overline{b}$ such that $\overline{b}^2 = \overline{a}$. This $\overline{b}$ cannot be zero since $\overline{a}$ is not zero.

The other direction is not too bad: if $\overline{a} = \overline{b}^2$ where $\overline{b}$ is not zero, then $\overline{a}$ is a square. Now $\overline{a}$ is non-zero: otherwise $\overline{b}$ would be a zero divisor, but we know that the field $\mathbb{F}_p$ has no zero divisors. So $\overline{a}$ is a quadratic residue.)

Definition 2. Let $a \in \mathbb{Z}$, and let p be an odd prime. Then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be $0, +1$, or -1.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 0 when $\overline{a} = \overline{0}$ in $\mathbb{F}_p$. In other words, it is 0 if and only if $p \mid a$.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be $+1$ when $\overline{a}$ is a quadratic residue. In other words, it is $+1$ if and only if $\overline{a} \in (U_p)^2$.

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be -1 in any other case. In other words, it is -1 if and only if $\overline{a}$ is in U_p but not in $(U_p)^2$.

Exercise 1. Calculate $\left(\frac{a}{11}\right)$ for all $0 \le a < 11$ directly from the definition (without using the properties below).

Lemma 1. *Let p be an odd prime. If $\left(\frac{a}{p}\right) = +1$ then $(\overline{a})^{(p-1)/2} = \overline{1}$.*

Proof. The hypothesis implies that $\overline{a} = \overline{b}^2$ for some $b \in U_p$. Then

$$\overline{a}^{(p-1)/2} = \left(\overline{b}^2\right)^{(p-1)/2} = \overline{b}^{p-1} = \overline{1}$$

by Fermat's Little Theorem. $\square$

Date: Fall 2005. Version of November 29, 2005.

The contrapositive gives the following:

Corollary 1. *Let p be an odd prime. If $(\overline{a})^{(p-1)/2} \neq \overline{1}$ then $\overline{a} \notin (U_p)^2$.*

Lemma 2. *Let p be an odd prime. Let $\overline{g}$ be a primitive element of U_p. Then $\overline{g}^{(p-1)/2} = -\overline{1}$. (So by the above corollary, $\overline{g}$ is not a quadratic residue).*

Proof. Recall that $\overline{g}$ has order $p-1$ since it is a generator. Let $\overline{a} = \overline{g}^{(p-1)/2}$. So

$$\overline{a}^2 = (\overline{g}^{(p-1)/2})^2 = \overline{g}^{p-1} = \overline{1}.$$

Since $\overline{a}^2 = \overline{1}$, the element $\overline{a}$ is a root of $x^2 - \overline{1}$. From an earlier result, this implies that $\overline{a}$ is $\overline{1}$ or $-\overline{1}$. However, $\overline{a} = \overline{g}^{(p-1)/2}$ is not $\overline{1}$ since the order of $\overline{g}$ is $p-1$ which is greater than $(p-1)/2$. □

Remark. Recall that every element of U_p is a power of a primitive element $\overline{g}$. In fact,

$$U_p = \left\{\overline{g}^0, \overline{g}^1, \dots, \overline{g}^{p-2}\right\}.$$

Thus half of the elements of U_p can be written as $\overline{g}^k$ with $0 \leq k \leq p-2$ even, and the other half can be written as $\overline{g}^k$ with $0 \leq k \leq p-2$ odd.

Lemma 3. *Let p be an odd prime, and let $\overline{g} \in U_p$ be a primitive element. If $\overline{a} = \overline{g}^k$ with k even, then $\left(\frac{a}{p}\right) = +1$. If $\overline{a} = \overline{g}^k$ with k odd, then $(\overline{a})^{(p-1)/2} = -\overline{1}$ and $\left(\frac{a}{p}\right) = -1$.*

Proof. If $\overline{a} = \overline{g}^k$ with k even, then $k = 2l$ for some l. Thus $\overline{a} = (\overline{g}^l)^2$. So $\overline{a}$ is a square. It is non-zero since it is a unit (powers of $\overline{g}$ are units). Thus $\left(\frac{a}{p}\right) = +1$.

If $\overline{a} = \overline{g}^k$ with k odd then

$$(\overline{a})^{(p-1)/2} = \left(\overline{g}^k\right)^{(p-1)/2} = \left(\overline{g}^{(p-1)/2}\right)^k = (-\overline{1})^k = -\overline{1}$$

using the fact that k is odd together with Lemma 2. Finally, by Corollary 1 we know that the unit $\overline{a}$ is not a quadratic residue, so $\left(\frac{a}{p}\right) = -1$. □

Corollary 2. *Of the $p-1$ elements of U_p, there are $(p-1)/2$ quadratic residues and there are $(p-1)/2$ that are not quadratic residues.*

Proof. Recall, $U_p = \left\{\overline{g}^0, \overline{g}^1, \dots, \overline{g}^{p-2}\right\}$. In the range $0 \leq k \leq p-2$ there are $(p-1)/2$ even values of k and $(p-1)/2$ odd values of k. □

Theorem 1. *If p is an odd prime and a is an integer, then $\left(\frac{a}{p}\right) = \overline{a}^{(p-1)/2}$.*

Remark. In the above theorem we are considering $\left(\frac{a}{p}\right)$ as taking values $\overline{0}, \overline{1}, -\overline{1} \in U_p$ instead of $0, 1, -1 \in \mathbb{Z}$. So, technically we should put a big bar over $\left(\frac{a}{p}\right)$.

Proof. There are three cases to consider.

First suppose that $\left(\frac{a}{p}\right) = 0$. By definition, $\overline{a} = \overline{0}$. Thus, $\overline{a}^{(p-1)/2} = \overline{0}^{(p-1)/2} = \overline{0}$, and the result follows.

Next suppose that $\left(\frac{a}{p}\right) = +1$. Then $\overline{a}^{(p-1)/2} = \overline{1}$ by Lemma 1.

Finally, suppose that $\left(\frac{a}{p}\right) = -1$. Let $\overline{g}$ be a primitive element of U_p. Since $\overline{g}$ generates U_p, there is a k such that $\overline{g}^k = \overline{a}$. By Lemma 3, this k cannot be even. So k is odd. The result follows from Lemma 3: $\overline{a}^{(p-1)/2} = -\overline{1}$. ☐

Exercise 2. Calculate $\left(\frac{a}{11}\right)$ for all $0 \leq a < 11$ using Theorem 1.

2. Basic properties of the Legendre Symbol

Here are some very useful properties to know in order to calculate $\left(\frac{a}{p}\right)$. Throughout this section, let p be an odd prime.

Property 1. *If $a \equiv 0 \bmod p$ then $\left(\frac{a}{p}\right) = 0$. In particular, $\left(\frac{p}{p}\right) = 0$.*

Proof. This follows straight from the definition. ☐

Property 2. *If $a \not\equiv 0 \bmod p$ and $a \in \mathbb{Z}$ is a square, then $\left(\frac{a}{p}\right) = 1$. In particular, $\left(\frac{1}{p}\right) = 1$.*

Proof. If a is a square, then $\overline{a}$ is a square modulo p. So $\left(\frac{a}{p}\right) = 1$ since $\overline{a} \neq \overline{0}$. ☐

Property 3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. *In particular:*

$$\text{If } p \equiv 1 \bmod 4, \quad \text{then } \left(\frac{-1}{p}\right) = 1.$$

$$\text{If } p \equiv 3 \bmod 4, \quad \text{then } \left(\frac{-1}{p}\right) = -1.$$

Proof. The first equation follows from Theorem 1. If $p \equiv 1 \bmod 4$, then $p - 1 = 4k$ for some k. Thus $(p-1)/2 = 2k$. In this case $(-1)^{(p-1)/2} = (-1)^{2k} = 1$.

If $p \equiv 3 \bmod 4$, then $p - 3 = 4k$ for some k. Thus $p - 1 = 4k + 2$, and $(p-1)/2 = 2k + 1$. In this case $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. ☐

Property 4. *For $a, b \in \mathbb{Z}$ we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. This follows from Theorem 1:

$$\left(\frac{ab}{p}\right) = (\overline{ab})^{(p-1)/2} = \overline{a}^{(p-1)/2} \cdot \overline{b}^{(p-1)/2} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

☐

Property 5. *If $a \equiv r \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$.*

Proof. If $a \equiv r \bmod p$ then $\overline{a} = \overline{r}$. By Definition 1, $\overline{a} = \overline{r}$ clearly implies $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$. ☐

Exercise 3. Use Property 4 to show that the product of two quadratic residues is a quadratic residue. Thus the set $(U_p)^2$ of quadratic residues is closed under multiplication. (In fact, it is a subgroup of U_p.)

Exercise 4. Use Property 4 to show that if $\overline{a}, \overline{b} \in U_p$ are units such that one of them is a quadratic residue but the other is not, then $\overline{ab}$ is *not* a quadratic residue.

Exercise 5. Use Property 4 to show that if $\overline{a}, \overline{b} \in U_p$ are units that are both non-quadratic residues, then $\overline{ab}$ is a quadratic residue.

Remark. For those of you who have taken abstract algebra, observe that Property 4 tells us that the map $\overline{a} \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism $U_p \to \{\pm 1\}$. The kernel of this homomorphism is the subgroup $(U_p)^2$ of quadratic residues. The quadratic residues form a subgroup, but the non-quadratic residues only form a coset.

Exercise 6. Give a multiplication table for $(U_{11})^2$. Hint: it should have 5 rows and columns.

3. Advanced properties of the Legendre Symbol

The proofs of the properties of this section will be postponed.

Property 6. *Let p be an odd prime, then $\left(\frac{2}{p}\right)$ is determined by what p is modulo 8.*

$$\text{If } p \equiv 1 \text{ or } p \equiv 7 \mod 8, \quad \text{then } \left(\frac{2}{p}\right) = 1.$$

$$\text{If } p \equiv 3 \text{ or } p \equiv 5 \mod 8, \quad \text{then } \left(\frac{2}{p}\right) = -1.$$

The following is a celebrated theorem of Gauss.

Property 7 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Remark. As we discussed above, $\frac{p-1}{2}$ is even if $p \equiv 1 \bmod 4$, but is odd if $p \equiv 3 \bmod 4$. Similarly, for q. So $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even if either p or q is congruent to 1 modulo 4, but is odd if both are congruent to 3. So

$$\text{If } p \equiv 1 \text{ or } q \equiv 1 \mod 4, \quad \text{then } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

$$\text{If } p \equiv 3 \text{ and } q \equiv 3 \mod 4, \quad \text{then } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

4. Square roots

If $\overline{b}^2 = \overline{a}$ in $\mathbb{F}_p$ then $\overline{b}$ is called a *square root* of $\overline{a}$.

Lemma 4. *Let p be an odd prime. If $\overline{b}$ is not zero, then $\overline{b} \neq -\overline{b}$.*

Proof. Suppose otherwise, that $\overline{b} = -\overline{b} = (-\overline{1})\overline{b}$. Since $\overline{b}$ is a unit, it has a multiplicative inverse. Multiply both sides of $\overline{b} = (-\overline{1})\overline{b}$ by b^{-1}. This gives $\overline{1} = -\overline{1}$. So $1 \equiv -1 \bmod p$. This means that p divides $1 - (-1) = 2$. However, $p > 2$, a contradiction. $\square$

Proposition 1. *Let p be an odd prime. If $\overline{a}$ has a square root $\overline{b}$, then $-\overline{b}$ is also a square root. Furthermore, $\pm\overline{b}$ are the only square roots of $\overline{a}$.*

Proof. Since $(-\overline{b})^2 = (-\overline{1})^2 \cdot \overline{b}^2 = \overline{b}^2$, if $\overline{b}^2 = \overline{a}$ then $(-\overline{b})^2 = \overline{a}$. So the first statement follows.

Now we must show that $\pm\overline{b}$ are the only square roots of $\overline{a}$. First assume $\overline{b} \neq \overline{0}$. Then by Lemma 4, $\pm\overline{b}$ are two distinct solutions to $x^2 = \overline{a}$. However, the polynomial $x^2 - \overline{a}$ has at most two roots by Lagrange's theorem. Thus $x^2 = \overline{a}$ has no other solutions. In other words, there are no other square roots.

Finally, consider the case where $\overline{b} = \overline{0}$, so $-\overline{b} = \overline{0}$ and $\overline{a} = \overline{0}$ as well. Now if $\overline{c}$ is a non-zero square root of $\overline{a} = \overline{0}$ then it is a zero divisor. Zero divisors do not exist in $\mathbb{F}_p$ since it is a field. So $\overline{b} = \overline{0}$ is the only square root. □

Proposition 2. *Let p be an odd prime. Then the number of square roots of $\overline{a}$ in $\mathbb{F}_p$ is given by the formula $(\frac{a}{p}) + 1$.*

Proof. There are three cases.

Case $(\frac{a}{p}) = 0$. By definition, $\overline{a} = 0$, which has $\overline{0}$ for a square root. By Proposition 1 the square roots are $\pm\overline{0}$. So $\overline{0}$ is the unique square root: there is exactly one square root. Observe that $(\frac{a}{p}) + 1 = 0 + 1 = 1$ gives the correct answer in this case.

Case $(\frac{a}{p}) = 1$. By definition, $\overline{a}$ is a non-zero square, so it has a square root $\overline{b}$ in $\mathbb{F}_p$. Clearly $\overline{b}$ is non-zero (otherwise $\overline{a}$ would be $\overline{0}^2$, but $\overline{a}$ is non-zero). By Proposition 1 and Lemma 4 there is exactly one other square root, namely $-\overline{b}$. So there are two square roots. Observe that $(\frac{a}{p}) + 1 = 1 + 1 = 2$ gives the correct answer in this case.

Case $(\frac{a}{p}) = -1$. By definition, $\overline{a}$ is not a square in $\mathbb{F}_p$. So there are no roots. Observe that $(\frac{a}{p}) + 1 = -1 + 1 = 0$ gives the correct answer in this case. □

Exercise 7. Find all the square roots of all the elements of $\mathbb{F}_{11}$. For more practice try $\mathbb{F}_7$ or $\mathbb{F}_5$.

Exercise 8. For which primes p is it true that $-\overline{1}$ has a square root? Find the first eight primes with this property. For a few of these, find square roots of $-\overline{1}$.

5. Quadratic equations modulo odd primes

The previous section considered the roots of $x^2 - \overline{a} = \overline{0}$ (which are called "square roots"). In this section we consider the general quadratic equation $\overline{a}x^2 + \overline{b}x + \overline{c} = \overline{0}$ in $\mathbb{F}_p$ with p an odd prime.

Lemma 5 (Completing the square)**.** *Let p be an odd prime, and consider the quadratic polynomial $\overline{a}x^2 + \overline{b}x + \overline{c}$ where $\overline{a} \neq 0$. Then $\overline{r}$ is a root of this polynomial if and only if $\overline{2ar} + \overline{b}$ is a square root of $\overline{b}^2 - \overline{4ac}$.*

Proof. Observe that

$$(2ar+b)^2 = 4a^2r^2 + 4abr + b^2 = 4a^2r^2 + 4abr + 4ac - 4ac + b^2 = 4a(ar^2 + br + c) + (b^2 - 4ac).$$

So if $ar^2 + br + c \equiv 0 \bmod p$, then $(2ar + b)^2 \equiv (b^2 - 4ac) \bmod p$.

Conversely, suppose $(2ar + b)^2 \equiv (b^2 - 4ac) \bmod p$. So

$$4a(ar^2 + br + c) = (2ar + b)^2 - (b^2 - 4ac) \equiv 0 \bmod p.$$

But a is a unit modulo p by assumption, and $p \nmid 4$ so 4 is also a unit modulo p. Thus we can cancel the $4a$ factor in the above equation leaving us with $ar^2 + br + c \equiv 0 \bmod p$. $\square$

Remark. We call $\overline{b}^2 - \overline{4ac}$ the *discriminant* of $\overline{a}x^2 + \overline{b}x + \overline{c}$.

Corollary 3. *Let p be an odd prime, and consider the polynomial $\overline{a}x^2 + \overline{b}x + \overline{c}$ where $\overline{a} \neq 0$. If this polynomial has a root in $\mathbb{F}_p$ then the discriminant has a square root in $\mathbb{F}_p$.*

Remark. You might have seen something like the above lemma in the context of deriving the classical quadratic formula for $F = \mathbb{R}$ or $F = \mathbb{C}$. In fact, the above lemma is valid in any field F such that $1 + 1 \neq 0$. However, it it fails in $F = \mathbb{F}_2$.

Theorem 2. *Let p be an odd prime, and consider the polynomial $\overline{a}x^2 + \overline{b}x + \overline{c}$ where $\overline{a} \neq 0$.*

If this polynomial has at least one root in $\mathbb{F}_p$ and if $\overline{\delta} \in \mathbb{F}_p$ is a square root of the discriminant $\overline{b}^2 - \overline{4ac}$ (which exists by the previous corollary), then the roots are given by the formula $(-\overline{b} \pm \overline{\delta})(\overline{2a})^{-1}$. This formula is traditionally written as

$$\frac{-\overline{b} \pm \sqrt{\overline{b}^2 - \overline{4ac}}}{\overline{2a}}.$$

Finally, if the discriminant is a square in $\mathbb{F}_p$ then the polynomial has at least one root.

Proof. According to Lemma 5, if $\overline{r}$ is a root of $\overline{a}x^2 + \overline{b}x + \overline{c}$, then $\overline{2ar} + \overline{b}$ is a square root of the discriminant. By Proposition 1 the only square roots of the discriminant are $\overline{\delta}$ and $-\overline{\delta}$. So either $\overline{2ar} + \overline{b} = \overline{\delta}$ or $\overline{2ar} + \overline{b} = -\overline{\delta}$. Now solve for $\overline{r}$.

Now suppose the discriminant is a square with square root $\overline{\delta}$. Let $\overline{r}$ be $(-\overline{b} + \overline{\delta})(\overline{2a})^{-1}$. This implies that $\overline{2ar} + \overline{b} = \overline{\delta}$. So $\overline{r}$ is a root by Lemma 5. $\square$

Proposition 3. *Let p be an odd prime, and consider the polynomial $\overline{a}x^2 + \overline{b}x + \overline{c}$ where $\overline{a} \neq 0$. Then the number of roots in $\mathbb{F}_p$ is given by the following (Legendre Symbol based) formula:*

$$\left(\frac{b^2 - 4ac}{p}\right) + 1.$$

Proof. There are three cases.

Case $\left(\frac{b^2-4ac}{p}\right) = 0$. In other words, discriminant is $\overline{0}$, which is obviously a square. So by Theorem 2, the polynomial has at least one root. Observe that $\overline{\delta} = \overline{0}$ is a square root of the discriminant in this case. So by Theorem 2, the roots are $(-\overline{b} \pm \overline{\delta})(\overline{2a})^{-1}$. Since $\overline{\delta} = 0$, both possibilities give the same answer: there is exactly one root and it is $-\overline{b}(\overline{2a})^{-1}$.

Case $\left(\frac{b^2-4ac}{p}\right) = 1$. In other words, the discriminant is a non-zero square. So by Theorem 2, the polynomial has at least one root. Let $\overline{\delta}$ be a square root of the discriminant. Since the discriminant is non-zero, $\overline{\delta} \neq 0$. So $\overline{\delta}$ and $-\overline{\delta}$ are distinct by Lemma 4. By Theorem 2, the roots are $(-\overline{b} \pm \overline{\delta})(\overline{2a})^{-1}$. Claim: these roots are distinct. To see this suppose $(-\overline{b} + \overline{\delta})(\overline{2a})^{-1} = (-\overline{b} - \overline{\delta})(\overline{2a})^{-1}$. From this equation it is easy to derive $\overline{\delta} = -\overline{\delta}$, a contradiction. Thus there are exactly two roots.

Case $\left(\frac{b^2-4ac}{p}\right) = -1$. In other words, the discriminant does not have a square root in $\mathbb{F}_p$. So by Corollary 3 (contrapositive), there are zero roots. $\square$

6. Additional Practice Problems

Exercise 9. Compute $\left(\frac{5}{71}\right)$ using the above properties. Likewise, compute $\left(\frac{3}{71}\right)$.

Exercise 10. Use the Legendre symbol to decide if 14 is a square in $\mathbb{F}_{101}$.

Exercise 11. How many roots does $\overline{2}x^2 + \overline{3}x + \overline{4}$ have in $\mathbb{F}_{239}$?

Exercise 12. When is 5 a square modulo p where p is an odd prime? List the first eight primes where this happens. Check a few of these to see if you can find square roots of 5. (Hint: the answer depends on what p is modulo 5.)

Exercise 13. When is 7 a square modulo p where p is an odd prime? List the first eight primes where this happens. Check a few of these to see if you can find square roots of 7. (Hint: the answer depends on what p is modulo 28. Divide into two cases: $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. Use the Chinese Remainder Theorem.)

Exercise 14. Show that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ for all odd primes p. (Hint: divide into three cases. (i) $p = 3$, (ii) $p \equiv 1 \bmod 4$, and (iii) $p \equiv 3 \bmod 4$ with $p \neq 3$.)

Exercise 15. For what odd primes p are there elements $\overline{a}$ and $\overline{a} + \overline{1}$ that are multiplicative inverses to each other? List the first eight primes where this happens. Check a few of these to see if you can find $\overline{a}$. (Hint: show this happens if and only if $x^2 + x - \overline{1} = 0$ has roots.)

Exercise 16. For what odd primes p are there elements $\overline{a}$ and $\overline{b}$ in $\mathbb{F}_p$ that are both additive and multiplicative inverses to each other? List the first eight primes where this happens. Check a few of these to see if you can find $\overline{a}$ and $\overline{b}$. (Hint: show this happens if and only if $-x^2 = \overline{1}$ has solutions.)

Exercise 17. For what odd primes p are there elements $\overline{a}$ and $\overline{b}$ in $\mathbb{F}_p$ that add to $\overline{3}$ but multiply to $\overline{2}$?

Exercise 18. For what odd primes p are there elements $\overline{a}$ and $\overline{b}$ in $\mathbb{F}_p$ that add to $\overline{2}$ but multiply to $\overline{3}$? List the first eight primes where this happens. Check a few of these to see if you can find $\overline{a}$ and $\overline{b}$. (Hint: the answer depends on whether -2 is a square modulo p. Compute the Legendre symbol for each possible value of p modulo 8. Observe that knowing p modulo 8 gives you knowledge of p modulo 4.)

Exercise 19. For what odd primes p is there a non-zero element in $\mathbb{F}_p$ whose cube is equal to $\overline{3}$ times itself? List the first eight primes where this happens. Check a few of these primes to see if you can find the desired element in $\mathbb{F}_p$. (Hint: show this happens if and only if $x^2 = \overline{3}$ has a solution. Split into three cases: $p = 3$ and $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$.)

Dr. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA
E-mail address: `waitken@csusm.edu`