§1. As described in Chapter I, we give here a criterion for \( p \) to be an \( \ell \)th power where \( \ell \) is an odd prime.

The criterion is as follows:

**Theorem 15.** Let \( p \equiv 1 (\text{mod } \ell) \) \( (p \text{ a prime).} \text{ Then } \ell \text{ is an } \ell \text{th power modulo } p \text{ iff } a_1 + a_p + \ldots + a_{\ell-1} \equiv 0 (\text{mod } p) \) where \((a_1, a_p, \ldots, a_{\ell-1})\) is one of the exactly \((\ell - 1)\) solutions of the diophantine system

\[
\begin{align*}
(1) & \quad p = \ell - 1 \sum_{i=1}^{\ell-1} a_i^p - \ell - 1 \sum_{i=1}^{\ell-1} a_i a_i + 1 \\
(2) & \quad \sum_{i=1}^{\ell-1} a_i a_i + 1 \equiv \sum_{i=1}^{\ell-1} a_i a_i + p \equiv \ldots \equiv a_i a_i + (\ell - 1) \\
(3) & \quad p + \prod_{i=1}^{\ell-1} (a_i^\lambda)^k \equiv \ldots (6.1)
\end{align*}
\]

(\text{where } \lambda(n) \text{ is the least non-negative residue of } n \text{ modulo } \ell \text{ })

\( \text{(iv)} \quad a_1 + a_p + \ldots + a_{\ell-1} \equiv 0 (\text{mod } \ell) \)

\( \text{(v)} \quad a_1 + 2a_p + \ldots + (\ell - 1)a_{\ell-1} \equiv (\text{mod } \ell) \)
(Note that any one of the $(\ell -1)$ solutions gives the same condition since there are permutations of each other)

Remark: The (i) above can be converted into a positive definite quadratic form by applying the transformation

\[
\begin{align*}
    s_1 &= (\ell -1) a_1 - (a_p + a_{p+1} + \ldots + a_{\ell-1}) \\
    s_2 &= (\ell -2) a_2 - (a_p + a_{p+1} + \ldots + a_{\ell-1}) \\
    \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots \\
    s_p &= (\ell - p) - (a_{p-1} + a_{p-2} + \ldots + a_{\ell-1}) \\
    \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots & \quad \vdots \\
    s_{\ell-p} &= 2a_{\ell-p} - a_{p-1} \\
    s_{\ell-1} &= a_{\ell-1}
\end{align*}
\]

(i) then becomes

\[
(\ell -1)p = \frac{s_1}{(\ell -1)} + \frac{s_2}{(\ell -2)(\ell -1)} + \ldots + \frac{s_{p-2}}{p-3} + \frac{s_{p-1}}{p-2}
\]

which can be checked for solutions in a finite number of steps. Only those solutions $(s_1, s_2, \ldots, s_{\ell-1})$ are to be retained which give integral $a_j$ on substitution. There will be just $(\ell -1)$ such solutions (for a proof of these statements, see (16)). The system (6.2) may be solved for the $a_j$ by inverting the coefficient matrices.
Let $a_{ij} = (a_{ij})$ where $a_{ij} = \begin{cases} 0 & \text{if } i < j, \\ -1 & \text{if } i = j, \\ n-i+1 & \text{if } i > j. \end{cases}$

Then $b_{ij} = (b_{ij})$ where $b_{ij} = \begin{cases} 0 & \text{if } i > j, \\ \frac{1}{(n-j+1)(n-j+2)} & \text{if } i < j, \\ \frac{1}{n-i+1} & \text{if } i = j. \end{cases}$

So $a_{ij} = \lim_{j \to \infty} b_{ij} s_j = \frac{s_1 + s_2 + \cdots + s_{l-1}}{(l-1)(l-1+1)} + \frac{s_l}{(l-1+1)}$

... (6.3)

Our criterion $a_1 + a_2 + \cdots + a_{l-1} \equiv 0 \pmod{2}$ then becomes $z_1 + a_1 \equiv (\mod 2)$ (using the first equation of (6.4)),

i.e. $\frac{z_1 + \frac{s_1 + s_2 + \cdots + s_{l-1}}{l-1}}{l-1} + \frac{s_l}{l} \equiv 0 \pmod{2}$ (by (6.3))

i.e. that the integer $\frac{s_1 + \cdots + s_{l-1}}{l-1}$ is even.

For completeness we give a (new) proof of the following known:
Lemma 4: 2 is an \( l \) th power modulo \( p \) iff the cyclotomic constant \((0,0)\) is odd.

**Proof.** Let 
\[ \lambda_0 = \left\{ x \in \mathbb{F}_p^* \mid x \text{ and } x + 1 \text{ are both } l \text{ th powers} \right\} \]

Then \( 2 \) is an \( l \) th power iff \( l \in \lambda_0 \) \( \ldots \) (6.4)

On the other hand

\[ \lambda_0 = \bigcup_{x \in \lambda_0} \left\{ x, \frac{1}{x} \right\} \]

In this union two sets \( \left\{ x, \frac{1}{x} \right\} \) and \( \left\{ y, \frac{1}{y} \right\} \) are either the same or disjoint. Further \( x = \frac{1}{x} \) iff \( x = 1 \), since \( x \) cannot take the value \(-1\). Thus \( \lambda_0 \) is even unless \( l \in \lambda_0 \), i.e. \( |\lambda_0| \) is odd if \( l \in \lambda_0 \). This together with (6.4) above gives the lemma noting that \((0,0)\) = \( |\lambda_0| \).

**Proof of the theorem:**

\[ \ell \mathbb{P} (0,0) = \sum_{0 \leq i,j \leq \ell - 1} j(1,1) \]

\[ = q^{-\ell} - \mathbb{P} (l,1) + \sum_{0 \leq i,j \leq \ell - 1} j(1,1) \]

(Since \( j(0,0) = q^{-\ell}, j(1,1) = j(0,1) = -1 \ (l \neq 0) \).)

\[ = q^{-\ell} - \mathbb{P} (l,1) + \sum_{j=1}^{\ell-1} \text{tr. } j(1,j) \]
\[
= (q-2)(l-1) + \sum_{j=1}^{(l-3)/2} \text{tr} \left( J(l,j) + J(1, l-1-j) \right) \\
+ \text{tr} \left( J(1, \frac{l-1}{2}) + J(1, l-1) \right) \\
= (q-2)(l-1) + \sum_{j=1}^{(l-3)/2} \text{tr} \left( J(l,j) + J(\frac{l-1}{2}, \frac{l-1}{2}) \right) \\
+ \text{tr} \left( J(1,0) \right)
\]

(since the respective replacements in the \( J \)'s are equal by the Stickelberger relation)

\[
\equiv 1 + \text{tr} \left( J(1,1) \right) \pmod{2}
\]

(since \( J(1,1) \) is a conjugate of \( J(\frac{l-1}{2}, \frac{l-1}{2}) \) and
\[
\text{tr} \left( J(1,0) \right) = \text{tr} \left( -1 \right) = - (l-1) \equiv 0 \pmod{2}.
\]

But now \( \text{tr} \left( J(1,1) \right) \) is even iff \( a_1 + a_2 + \ldots + a_{l-1} \) is even;

since \( J(1,1) = a_1 + a_2 + \ldots + a_{l-1} \); so that
\[
\text{tr} \left( J(1,1) \right) = a_1 + a_2 + \ldots + a_{l-1}.
\]

Thus \((0,0)_l \) is odd iff \( a_1 + a_2 + \ldots + a_{l-1} \) is even;

i.e. \( \varphi \) is an \( l \) th power iff \( a_1 + a_2 + \ldots + a_{l-1} \) is even.

This completes the proof of the theorem.
2. Let \( p \equiv 1 \pmod{7} \). Leonard and Williams [13] proved a criteria for \( 3 \) to be a 7th power. Their proof depends upon a result of Maksatz [18] which in turn depends on a paper of Harken [21], so that a self-contained proof would not be easy to work out and would be rather lengthy.

Our object to give a self contained proof of the result.

We first give a short proof of the following (all congruences are modulo 3).

**Lemma 5**: (Alderson [1]). Let \( p \equiv 1 \pmod{7} \). The following statements are equivalent.

1. \( 3 \) is a 7th power mod \( p \).
2. \( (0,0)^2 + (0,1)^2 + \ldots + (0,6)^2 = 1 - f \pmod{3} \).
3. \( (0,1)^2 + (0,2)^2 + \ldots + (0,6)^2 = 0 \pmod{3} \).
4. \( (0,1) \equiv (0,2) \equiv (0,4) \pmod{3} \).
   and \( (0,3) \equiv (0,5) \equiv (0,6) \pmod{3} \).

**Proof.** (1) \( \iff \) (2). Let \( p \equiv 1 + 7f \). Let \( \gamma \) be a generator of the cyclic group \( F_p^* \). Consider the congruence

\[ \gamma^{7x} + \gamma^{7y} + \gamma^{7z} \equiv 1 \pmod{p} \quad (0 \leq x, y, z \leq f-1) \ldots \quad (6.5) \]

First we determine the number of solutions of this congruence.

Let \( z \) be fixed where \( 0 \leq z \leq f-1 \), we shall determine the number of solutions for each fixed \( z \).
If \( z = 0 \) then (6.5) reduces to
\[
\gamma^x + \gamma^y = 1 \pmod{p}
\]
which has \( f \) solutions. ... (6.6)

If \( z \neq 0 \) then there exists unique integers \( h, k \) such that
\[
0 \leq k \leq r - 1, \quad 0 \leq h \leq 6
\]
and
\[
\gamma^z = 1 + \gamma^{7h}
\]
... (6.7)

Moreover, a given integer \( h \) occurs in (6.7) just \((h, 0)\) times as \( z \) runs over \( \{0, 1, \ldots, r - 1\} \).

(6.7) reduces (6.5) into
\[
\gamma^x + \gamma^y + \gamma^z = \gamma^x + \gamma^y + 1 + \gamma^{7h} = 1 \pmod{p}
\]
i.e. \( \gamma^x + \gamma^y + \gamma^{7h} = 0 \pmod{p} \)
i.e. \( \gamma^{7(x-k)-h} + \gamma^{7(y-k)-h} + 1 = 0 \pmod{p} \)
i.e. \( 1 + \gamma^{7(x-h)-h} = -\gamma^{7(y-k)-h} \pmod{p} \)
i.e. \( 1 + \gamma^{7(x-h)-h} = \gamma^{7(y-k)-h + \frac{7f}{2}} \)
\[
= \gamma^{7(y-k + \frac{f}{2})-h} \pmod{p}
\]
(since \( f \) is even).
This has just \((-h, -h)\) solutions i.e. it has just \((h, 0)\) solutions (since \((i, j) = (-i, -i)\) if \(f\) is even) so, for fixed \(h \neq 0\) we get \((h, 0)^2\) solutions.

So the number of solutions of the congruence (6.5) is
\[
\sum_{h=0}^{6} (h, 0) (h, 0) + f = \sum_{h=0}^{6} (0, h)^2 + f = N \text{ (say)}.
\]

Now we prove that 3 is a 7th power iff \(N\) is congruent to 1 (mod 3).

Since 3 is prime, the number of distinct permutations of \((x, y, z)\) is a multiple of 3 unless \(x, y, z\) are all equal. But (6.5) has a solution with \(x = y = z\) iff
\[
\gamma^7x + \gamma^7x + \gamma^7x \equiv 1 \text{ (mod 3)} \quad \text{i.e. iff } 3 \gamma^x \equiv 1 \text{ (mod 3)}
\]
i.e. iff \(3 \equiv \gamma^{-7x} \text{ (mod 3)} \quad \text{i.e. iff } 3\text{ is a 7th power (mod p)}

and in that case there is just one solution.

It follows that
\[
3 \text{ is a 7th power (mod } p\text{) iff } N \equiv 1 \text{ (mod 3)} \quad \text{i.e.}
\]
\[
6
\]
\[
\text{iff } h \in (0, h)^2 + f \equiv 1 \text{ (mod 3)}.
\]

This shows that (1) and (2) are equivalent. We prove it by using Lemmas (1) and (3) of [ 1 ].
(ii) and (iii) are trivially equivalent, since the cyclotomic constant \((0,0)\) equals

\[ 3 \left[ \left( \frac{1}{1} \right) + \left( \frac{1}{1} \right) + \left( \frac{1}{1} \right) + \left( \frac{1}{1} \right) + \left( \frac{1}{1} \right) \right] - (2f + 1) \]

(This follows from the known relations

\[(0,0) + (1,1) + (1,2) + (1,3) + (1,4) + (1,5) + (1,6) = f - 1,\]
\[(1,0) + (1,1) + (1,2) + (1,3) + (1,4) + (1,5) + (1,6) = f,\]
\[(2,0) + (2,1) + (2,2) + (2,3) + (2,4) + (2,5) + (2,6) = f,\]
\[(3,0) + (3,1) + (3,2) + (3,3) + (3,4) + (3,5) + (3,6) = f\]

by adding the last three and subtracting the result from the first one.)

So eliminating \((0,0)\) from (ii) gives

\[(0,1)^2 + (0,2)^2 + \ldots + (0,6)^2 = 1 - f - (2f + 1)^2\]

\[= -f(f - 1) \equiv 0 \pmod{3}\]

(Since \(p = 1 - 7f\) and so \(f \equiv 2 \pmod{3}\)).

To show that (iii) and (iv) are equivalent, it is enough to prove that (iii) implies (iv), since (iv) trivially implies (iii).
Now note that

\[(0,1) \star (0,2) \star (0,3) \star (0,4) \star (0,5) \star (0,6) = f_1(0,0) \equiv 0 \pmod{3}.\]

From this we see that the \((0,1)\) \((1 \leq 1 \leq 6)\) are congruent modulo 3 in sets of 3. Choose an integer \(u\) which is congruent to 3 modulo 7 and prime to \(p-1\). Then \(\gamma^u\) is a primitive root \((\text{mod } p)\) if \(\gamma\) is one and replacing \(\gamma\) by \(\gamma^u\) permutes the \((0,1)\) by sending \((0,1)\) to \((0,5i)\) and leaves (iii) invariant.

On repeatedly applying this permutation to the \((0,1)\), we see that all possible ways of taking the \((0,1)\) congruent mod 3 in sets of 3 are essentially the following ones:

1. \((0,1) \equiv (0,2) \equiv (0,4), \quad (0,3) \equiv (0,5) \equiv (0,6).\)
2. \((0,1) \equiv (0,2) \equiv (0,6) \neq (0,3) \equiv (0,4) \equiv (0,5)\)
3. \((0,1) \equiv (0,2) \equiv (0,3) \neq (0,4) \equiv (0,5) \equiv (0,6) \quad (\text{all } \mod 3)\)

We show that (2) and (3) above leads to contradictions. We see that (2) implies

\[(a) \quad x_2 + x_5 \equiv 2 x_4 \quad ((0,1) \equiv (0,2))\]
\[(b) \quad u - x_2 - x_3 \equiv 0 \quad ((0,1) \equiv (0,6))\]
\[(c) \quad u - x_5 + x_4 \equiv 0 \quad ((0,3) \equiv (0,4))\]
\[(d) \quad x_2 - x_6 - x_3 \equiv 0 \quad ((0,3) \equiv (0,5))\]
\[(e) \quad x_3 + x_4 - x_6 \neq 0 \quad ((0,6) \neq (0,3)).\]
These follow by substituting the values of \((0,1)\) in terms of the solutions \((x_1, x_2, \ldots, x_9)\) of the diophantine system of Leonard and Williams given on p. 299 of [11]).

Then (b) and (c) imply

\[ x_3 + x_4 \equiv 0 \pmod{3} \quad \text{and so (e) gives } x_5 \neq 0. \]

While (a) implies \(x_2 + x_4 \equiv 2x_8\).

Now since \((x_1, -x_2, -x_3, -x_4, x_5, x_6)\) is also a solution,

\( -x_2 - x_4 \equiv 2x_8 \) giving \( x_5 = 0 \) — a contradiction.

So (\(c\)) is impossible.

Next we see that (3) implies

\[
\begin{align*}
(a) & \quad x_2 + x_5 \equiv 2x_4 \quad ((0,1) \equiv (0,3)) \\
(b) & \quad u + x_2 + x_3 + x_4 + x_5 \equiv 0 \quad ((0,0) \equiv (0,3)) \\
(c) & \quad u + x_2 + x_3 + x_4 + 2x_6 \equiv 0 \quad ((0,4) \equiv (0,3)) \\
(d) & \quad x_2 + x_4 - x_6 \equiv 0 \quad ((0,5) \equiv (0,3)) \\
(e) & \quad u + x_4 \not\equiv x_2 \quad ((0,5) \not\equiv (0,3))
\end{align*}
\]

Then (b) and (c) give \( x_5 = 0 \), so (\(a\)) and (d) become

\( x_2 \not\equiv 2x_4 \). Hence (e) gives \( x_2 \not\equiv x_3 \). Now \( x_2 \not\equiv 2x_4 \) and

\((x_1, -x_2, x_3, x_4, x_5, \frac{1}{2}(x_6 + 3x_8), \frac{1}{2}(x_6 - x_8))\) is also a solution,

\( -x_3 \equiv 2x_2 \) i.e. \( x_5 \equiv x_2 \) — a contradiction again. Thus (3) too is impossible.
It follows that (1) holds and that completes the proof of the Lemma.

The proof of our main result now follows immediately for the relation (1) gives:

(a) \( x_2 + x_5 = 2x_4 \)  \((0,1) \equiv (0,2)\)
(b) \( x_3 = 2x_4 + x_5 \)  \((0,1) \equiv (0,4)\)
(c) \( x_2 + x_6 = x_3 \)  \((0,3) \equiv (0,5)\)
(d) \( x_4 + x_5 = 2x_3 \)  \((0,3) \equiv (0,6)\)

Then (b) and (d) give \( x_5 = 0 \) and so by (a) and (b), we find

\( x_2 = x_3 = x_4 \).

Now the relation

\[ 7p = x_1^2 + 4x_2^2 + x_3^2 + x_4^2 + 3x_5^2 + 3x_6^2 \]  \( \cdots (6.8) \)

of the Leonard-Williams diophantine system takes modulo 3 gives \( x_1 = 0 \) and so the same relation modulo 9 gives \( x_5 = 0 \).

Thus \( x_5 = 0 \) and \( x_6 \equiv 0 \) as required.

Remark. By Alderson's results (p. 484 of [1]) 3 is 7th power iff modulo p iff \((0,0)^2 + \cdots + (0,6)^2 \equiv 1-f (\text{mod } 3)\) and on substituting for \((0,1)\) the values modulo 3 given on p. 299 of [11], this condition boils down to
\[ u(x_2 + x_3 - x_4) + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_5 x_6 + px_2 x_4 + px_3 x_4 = 0 \pmod{3} \]

\[ \ldots \quad (6.9) \]

Now take the solution \((x_1, x_2, x_3, x_4, x_5, x_6)\) instead of \((x_1, x_2, x_3, x_4, x_5, x_6)\) so that \((6.9)\) becomes

\[-u(x_2 + x_3 - x_4) + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_5 x_6 + px_2 x_4 + px_3 x_4 = 0 \pmod{3}\]

It follows that \(u(x_2 + x_3 - x_4) = 0 \pmod{3}\).

If now \(u \not\equiv 0 \pmod{3}\) then \(x_2 + x_3 - x_4 = 0 \pmod{3}\) and \((6.8)\) gives

\[ x_5^2 + 2px_5 + px_4 + x_3 x_4 = 0 \pmod{3} \]

i.e. \(x_5^2 + 2px_5 + x_4 = 0 \pmod{3}\), since \(x_2 + x_3 = 0 \pmod{3}\)

i.e. \(x_5^2 + x_4^2 + x_4^2 - x_2^2 - x_3^2 \equiv 0 \pmod{3}\), since \((x_2 x_3)^2 \equiv x_4^2 \pmod{3}\)

i.e. \(x_2^2 + x_3^2 + x_4^2 \equiv x_5^2 \pmod{3}\).

If \(3 + x_6\) then \(x_5 \equiv 1 \pmod{3}\)

i.e. \(x_5 \equiv 1 \pmod{3}\)

i.e. \(x_2^2 + x_3^2 + x_4^2 \equiv 1 \pmod{3}\).
Hence two of \( x_2, x_3, x_4 \) are \( \equiv 0 (\text{mod } 3) \) and therefore so is the third, since
\[
x_2 + x_3 - x_4 \equiv 0 (\text{mod } 3)
\]
so
\[
x_2^2 + x_3^2 + x_4^2 \equiv 0 (\text{mod } 3)
\]
which is a contradiction.

It follows that \( 3 \mid x_2 \) and then the relation (6.9) gives \( 3 \mid x_6 \).

This proof does not work in case \( u \equiv 0 (\text{mod } 3) \). It would be nice to find some way out in this case too.

Now we give a criterion for \( 11 \) to be a fifth power.

Let \( r \) be an odd prime. Let \( p \) be a prime \( \equiv 1 (\text{mod } r) \).

Let \( \chi_p \) be a primitive \( r \)th power multiplicative character (mod \( p \)). Let
\[
\mathcal{C}(\chi_p) = \prod_{n=1}^{p-1} \chi_p(n)^n
\]
\( \mathcal{C}(\chi_p) \) is called a Gauss sum. Let \( q \) be a prime distinct from \( p \) and \( r \). Ankeny [Theorem 2] proved that if \( \mathcal{O} \) is any one of the prime divisors of \( (q) \), then
\[
q \text{ is an } r \text{th power (mod } p) \text{ iff } \mathcal{C}(\chi_p)^{p-1} \equiv 1 (\text{mod } \mathcal{O}) \quad (6.10)
\]
for some \( i \in \{ 1, \ldots, r \} \).
Further H. Lavenport and H. Hasse [p.152] prove that $r$th power Gaussian sums $\zeta(\chi_p)^r$ can be evaluated in terms of Jacobian functions using the formula

$$\zeta(\chi_p)^r = p \cdot \prod_{j=1}^{r-2} J(1,i) \quad \ldots \quad (6.11)$$

(6.10) and (6.11) give that

$q$ is an $r$th power mod $p$ iff $p \prod_{j=1}^{r-1} J(1,i) \equiv r \pmod{\varphi} \quad \ldots \quad (6.12)$

We apply (6.12) to determine a criterion for $11$ to be a 5th power.

Taking $q = 11$, $r = 5$ and $p = 1 \pmod{5}$, (6.12) implies

$$11 \text{ is a 5th power mod } p \text{ iff } p \prod_{j=1}^{3} J(1,i) \equiv 1 \pmod{11}$$

(since by Euler's criterion, $5^{10} = 1$ and hence $5^5 = 1$)

i.e. iff $p \cdot J(1,1) J(1,2) J(1,3) \equiv 1 \pmod{11}$

i.e. iff $p \cdot J(1,1)^2 (J(1,2)^2) \equiv 1 \pmod{11}$

(since $1 + 1 + 3 = 0$, so $J(1,3) = J(1,1)$ by Stickelberger's relation).

i.e. iff $p \left( a_2^2 + a_3^3 + a_4^4 \right)^2 \left( a_3^3 + a_4^4 \right)^2 \left( a_5^5 + a_6^6 \right)^4 \equiv 1 \pmod{11}$
where $J(1,1) = a_1^2 + a_2^3 + a_3^3 + a_4^3$, $(\gamma = e^{i1/5})$.

is determined by the main theorem of $[15]$ if $l = 5$.

Further, Ankeny [Theorem B; 2] proves that if
\[ q \equiv 1 \pmod{r} \text{ and } h \text{ is any integer such that } h^5 \text{ is the least power of } h \text{ which is } \equiv 1 \pmod{q}, \]
then we can replace $\gamma$ by $h$ in the above formula.

Since here $q = 11 = 1 \pmod{r = 5}$ and since $4^5$ is the least power of 4 which is $\equiv 1 \pmod{11}$.

It follows that

11 is a fifth power mod $p$ iff
\[ \pm (4a_1 + 5a_2 + 9a_3 + 3a_4)^2 \cdot (4a_2 + 5a_1 + 9a_4 + 3a_3) = \mp 1 \pmod{11}. \]

In [16] Parmami, Agrewal and Rajwade prove that

\[ 4a_1 = -x + 6u + 4v + w, \]
\[ 4a_2 = -x + 6u - 2v - w, \]
\[ 4a_3 = -x - 6u + 4v - w, \]
\[ 4a_4 = -x - 6u - 4v + w \]

where $x, u, v, w$ satisfy the diophantine system of Dickson for the case $l = 5$. 
Multiplying by both sides of these equations by \( 3 \), i.e. \( 4^{-1} \) modulo 11, we get

\[
\begin{align*}
a_1 &= -3x + 6U + V + 3W \\
a_2 &= -3x + U - 6V + 3W \\
a_3 &= -3x + U + 6V - 3W \\
a_4 &= -3x - 6U - V + 3W
\end{align*}
\]

so \((4a_1 + 5a_2 + 9a_3 + 3a_4) = (-x + 2U + 4V + W) + (-4x + 5U + 3V - 6W) + (6x + 8U - V + 6W) + (2x + 4U - 3V - 2W) = 3x + 9U + 3V + W.\)

Similarly \((5a_1 + 3a_2 + 3a_3 + 9a_4) = 3x - 5U + 2V - W.\)

(Both of the above relations are taken modulo 11)

It follows that

11 is a 5th power \( \text{mod } p \) if and only if

\[
\left\lfloor \frac{(3x + 5U + 3V + W)^2}{(3x - 5U + 2V - W)} \right\rfloor \equiv 1 \pmod{11}.
\]

(See \( \S \).)