4. POWER CONGRUENCES

§4.1. p-Order and p-Inertia

If \( p \) is prime and is coprime with \( m \), the \textbf{p-order} of \( m \) is the order of \( p \) in \( \mathbb{Z}_m \). It is denoted by \( u(p, m) \). By Euler’s theorem \( u(p, m) \) divides \( \varphi(m) \). If \( p, q \) are distinct primes the \textbf{p-inertia} of \( q \) is the largest \( y \) such that \( p^{u(p, q)} \equiv 1 \pmod{q^y} \). It will be denoted by \( v(p, q) \).

Example:

\[
u(2, 17) = 8 \quad \text{because} \quad 2^n \text{ is not congruent to } 1 \pmod{17} \text{ for } 0 < n < 8 \text{ and } 2^8 \equiv 1 \pmod{17}.
\]

\[
v(2, 17) = 1 \quad \text{because} \quad 2^n \text{ is not congruent to } 1 \pmod{17} \text{ for } 0 < n < 8 \text{ and } 2^8 \equiv 1 \pmod{17}.
\]

\[
u(2, 1093) = 364 \quad \text{because} \quad 2^n \text{ is not congruent to } 1 \pmod{17} \text{ for } 0 < n < 8 \text{ and } 2^{364} \equiv 1 \pmod{1093}.
\]

\[
v(2, 1093) = 2 \quad \text{because} \quad 2^{364} \equiv 1 \pmod{1093^2} \text{ but not } \pmod{1093^3}.
\]

\[
u(3, 11) = 5 \quad \text{because} \quad 3^n \text{ is not congruent to } 1 \pmod{11} \text{ for } 0 < n < 5 \text{ and } 3^5 \equiv 1 \pmod{11}.
\]

\[
v(3, 17) = 2 \quad \text{because} \quad 3^5 \text{ is congruent to } 1 \pmod{11^2} \text{ but not } \pmod{11^3}.
\]

\[
\text{Theorem 1:} \quad \text{If } q \text{ is prime and } t \geq 1 \text{ and } s \geq 0 \text{ then } (1 + kq^t)^q^s \equiv 1 + kq^{t+s} \pmod{q^{t+s+1}}, \text{ unless } t = 1 \text{ and } q = 2.
\]

\[
\text{Proof:} \quad (1 + kq^t)^q^s \equiv 1 + kq^{t+s} \pmod{q^{t+s+1}} \quad \text{by Theorem 1 unless } q = 2 \text{ and } v = 1.
\]

\[
\text{Hence } k \equiv k \pmod{q^t}. \quad \text{By induction } (1 + kq^t)^q^s \equiv 1 + kq^{t+s} \pmod{q^{t+s+1}}.
\]

\[
\text{Theorem 2:} \quad \text{If } u = u(p, q) \text{ and } v = v(p, q) \text{ and } p^u \equiv 1 \pmod{q^{v+1}} \text{ for some } s \geq 1 \text{ then } q = 2 \text{ and } v = 1.
\]

\[
\text{Proof:} \quad \text{We have } p^1 = 1 + kq^t \text{ for some } k \text{ where } GCD(q, k) = 1.
\]

\[
\text{Then } p^u = (1 + kq^t)^v \equiv 1 + kq^{v+s} \pmod{q^{v+s+1}} \text{ by Theorem 1 unless } q = 2 \text{ and } v = 1.
\]

\[
\text{But } 1 + kq^{v+s} \text{ is not congruent to } 1 \pmod{q^{v+s+1}} \text{ since } GCD(q, k) = 1.
\]

\[
\text{Hence } q = 2 \text{ and } v = 1.
\]

\[
\text{Theorem 3:} \quad \text{Unless } q = 2 \text{ and } v(p, q) = 1,
\]

\[
u(p, q^t) = \left\{ \begin{array}{ll} u(p, q^t) & \text{if } 0 < t \leq v(p, q^t) \\ u(p, q^t) q^{t-v(p, q^t)} & \text{if } t > v(p, q^t) \end{array} \right.
\]

\[
\text{Proof:} \quad \text{Let } u = u(p, q), v = v(p, q) \text{ and } R = u(p, q^t).
\]

\[
\text{If } 0 < t \leq v \text{ then clearly } R = u.
\]

\[
\text{Suppose that } t > v.
\]

\[
\text{Since } p^u = kq^v + 1 \text{ we have by Theorem 1 that}
\]
\[ p^{uq^{t-v-1}} = 1 + kq^{t-1}(\text{mod } q^t) \] for some \( k \) and
\[ p^{uq^{t-v}} = 1 + kq^t(\text{mod } q^{t+1}). \]

Thus \( p^{uq^{t-v}} \equiv 1(\text{mod } q^t) \) and so \( R \) divides \( uq^{t-v} \).

As \( p^R \equiv 1(\text{mod } q) \), \( u \) divides \( R \) and since \( p^{uq^{t-1}} \equiv 1(\text{mod } q) \), \( u \) divides \( q-1 \) and so \( \text{GCD}(q, u) = 1 \).

Thus \( R = uq^{t-v-d} \) for some \( d \geq 0 \).

Since \( p^{uq^{t-v-1}} \) is not congruent to 1 mod \( q^t \) it follows that \( d = 0 \).

**Theorem 4:** If \( v(p, 2) = 1 \) then \( p = 2^s w - 1 \) for some odd \( w \), and some \( s \geq 2 \).

Also \( u(p, 2^t) = \begin{cases} 1 & \text{if } t = 1 \\ 2 & \text{if } 2 \leq t \leq s + 1 \\ 2^{t-s} & \text{if } t > s + 1 \end{cases} \)

**Proof:** For any odd \( p \) we have \( p = 2^s w - 1 \) where \( w \) is odd and \( s \geq 1 \).

If \( s = 1 \) then \( p = 2w - 1 = 2(w - 1) + 1 = 2^2 \left( \frac{w-1}{2} \right) + 1 \) where \( \frac{w-1}{2} \) is an integer.

Consequently \( p \equiv 1(\text{mod } 2^2) \) contrary to the fact that \( v(p, 2) = 1 \).

(i) Obviously \( u(p, 2) = 1 \).

(ii) \( p^2 = (2^s w - 1)^2 = 2^{2s} w^2 - 2^{s+1} w + 1 \equiv 1(\text{mod } 2^{s+1}) \) which proves the theorem for \( 2 \leq t \leq s + 1 \).

(iii) By (ii) \( p^2 = 1 + k2^{s+1} \) for some \( k \) with \( 0 < k < 2^{s+1} \).

Applying Theorem 1, if \( t \geq s + 1 \),
\[ (p^2)^{2^{t-s-1}} = (1 + k2^{s+1})^{2^{t-s-1}} \quad \text{and so} \]
\[ p^{2^{t-s}} = 1 + k2^t(\text{mod } 2^{t+1}). \]

Similarly \( p^{2^{t-s}} \equiv 1(\text{mod } 2^t) \). But \( p^{2^{t-s-1}} \) is not congruent to 1 mod \( 2^t \).

Clearly \( u(p, 2^t) \) divides \( 2^{t-s} \) and hence must be a power of 2 greater than \( 2^{t-s-1} \).

Consequently \( u(p, 2^t) = 2^{t-s} \).

Having \( v(p, 2) \) bigger than 1 is not very common. The smallest prime \( p \) for which this is the case is \( p = 1093 \), for which \( u(p, 1) = 364 \).