Some Properties of the Elementary Symmetric Functions of the Roots of the Congruence \( x^n \equiv 1 \pmod{p} \) in \( K(\sqrt[n]{m}) \),

by

Hiroshi HATTORI, Taihoku.

In my former paper(1) I have stated some properties of the elementary symmetric functions of the roots of the congruence

\[ x^n \equiv A \pmod{p}. \]

The same method is applicable to obtain the corresponding results, when the modulus is a prime ideal \( p \) of the corpus \( K(\sqrt[n]{m}) \).

In this paper we take \( n \) as a rational integer, \( p \) as a rational prime number, \( p \) as a prime ideal of \( K(\sqrt[n]{m}) \), and \([1, \omega]\) as the canonical basis of \( K(\sqrt[n]{m}) \).

**Theorem.** Let \( n \) be a divisor of \( \varphi(p) \), and \( s_1, s_2, \ldots, s_n \) be incongruent roots of the congruence

\[ x^n \equiv 1 \pmod{p}; \]

then

\[ A_1 \equiv A_2 \equiv \ldots \equiv A_{n-1} \equiv 0 \pmod{p}, \]

\[ A_n \equiv (-1)^{n+1} \pmod{p}, \]

where \( A_1, A_2, \ldots, A_n \) are given by

\[ (x-s_1)(x-s_2)\ldots(x-s_n)=x^n-A_1x^{n-1}+\ldots+(-1)^nA_n. \]

**Proof.** It is evident that the congruence

\[ x^n \equiv 1 \pmod{p} \]

has just \( n \) incongruent roots, mod. \( p \), as \( n \) is a divisor of \( \varphi(p) \). Hence we have the identical congruence

\[ x^n-1 \equiv (x-s_1)(x-s_2)\ldots(x-s_n) \equiv x^n-A_1x^{n-1}+\ldots+(-1)^nA_n \pmod{p}, \]

as \( p \) is a prime ideal, hence we get

\[ A_1 \equiv A_2 \equiv \ldots \equiv A_{n-1} \equiv 0 \pmod{p}, \]

\[ A_n \equiv (-1)^{n+1} \pmod{p}. \]

Here, putting \( n=\varphi(p) \), we have Lagrange's theorem for ideals, and especially

\[ A_{\varphi(p)} \equiv -1 \pmod{p}. \]

---

is Wilson’s theorem for ideals.

Now, we will make use of the well known facts that the set of $p$ numbers
\[ \rho_{ab} = a \quad (a = 0, 1, 2, \ldots, p-1) \]
forms a complete system of residues, mod. $p$, when $N(p) = p$, and the set of $p^2$ numbers
\[ \rho_{a} = a + b \omega \quad (a = 0, 1, 2, \ldots, p-1), \quad (b = 0, 1, 2, \ldots, p-1) \]
forms a complete system of residues, mod. $p$, when $N(p) = p^2$.

**Theorem.** If $n(\geq 4)$ be an even number and a divisor of $\varphi(p)$, and $s_1, s_2, \ldots, s_n$, each one of these is equal to some one of those $\rho_{ab}$, be the set of incongruent roots of the congruence
\[ x^n \equiv 1 \pmod{p}, \]
then
\[ A_3 = A_5 = \ldots = A_{n-1} \equiv 0 \pmod{2p}, \]
where $A_3, A_5, \ldots, A_n$ are given by
\[ (x-s_1)(x-s_2)\ldots(x-s_n) = x^n - A_1x^{n-1} + A_2x^{n-2} - A_3x^{n-3} + \ldots - A_{n-1}x + A_n, \]
and
\[ N(p) = p^f \quad (f = 1 \text{ or } 2). \]

**Proof.** It is clear that
\[ (n-s)^n \equiv s^n \pmod{p}, \quad \begin{cases} n = p, & \text{when } f = 1 \smallskip \cr n = p + p \omega, & \text{when } f = 2 \end{cases} \]
as $n$ is an even number, hence $n-s_1, n-s_2, \ldots, n-s_n$ are also a set of incongruent roots of the congruence
\[ x^n \equiv 1 \pmod{p}, \]
and each one of them is equal to some one of those $\rho_{ab}$, therefore they coincide with $s_1, s_2, \ldots, s_n$ as a whole.

Put
\[ f(x) = (x-s_1)(x-s_2)\ldots(x-s_n), \]
then
\[ f(n) = (n-s_1)(n-s_2)\ldots(n-s_n) = s_1s_2\ldots s_n = A_n, \]
that is,
\[ A_n = n^n - A_1n^{n-1} + \ldots + A_{n-1}n^{2} - A_{n-2}n + A_n, \]
hence

\[ (1) \text{ I owe Mr. Tannaka much for his obliging advice on this proof.} \]
\( \omega^n-A_1\omega^{n-1}+\ldots+A_{n-2}\omega^2=A_{n-1}\omega, \)

hence
\( \omega^{n-1}-A_1\omega^{n-2}+\ldots+A_{n-2}\omega=A_{n-1}, \)

in which
\( \omega^{n-1}-A_1\omega^{n-2}+\ldots+A_{n-2}\omega\equiv 0 \text{ (mod. } p^3), \)
as \( n \geq 4 \) and \( A_{n-2}\equiv 0 \text{ (mod. } p) \), hence
\( A_{n-1}\equiv 0 \text{ (mod. } pp). \)

Next, we have on one hand
\[
f^{(k)}(\omega) = k! \left\{ \sum (\omega-s_1)(\omega-s_2)\ldots(\omega-s_{n-k}) \right\}
= k! \sum s_1s_2\ldots s_{n-k} = k! A_{n-k},
\]
and on the other hand
\[
f^{(k)}(\omega) = \frac{n!}{(n-k)!} \omega^{n-k} - \frac{(n-1)!}{(n-k-1)!} A_1\omega^{n-k-1} + \ldots
+ (-1)^{k+1} \frac{(k+2)!}{2!} A_{n-k-2}\omega^2
+ (-1)^{k+1}(k+1)! A_{n-k-1}\omega \equiv (-1)^{k} k! A_{n-k}.
\]

Therefore, when \( k \) is even, we have
\[
\frac{n!}{(n-k)!} \omega^{n-k} - \frac{(n-1)!}{(n-k-1)!} A_1\omega^{n-k-1} + \ldots
+ \frac{(k+2)!}{2!} A_{n-k-2}\omega^2 - (k+1)! A_{n-k-1}\omega = 0,
\]
hence
\[
\binom{n}{k} \omega^{n-k} - \binom{n-1}{k} A_1\omega^{n-k-1} + \ldots
+ \binom{k+2}{k} A_{n-k-2}\omega - (k+1) A_{n-k-1} = 0.
\]

Let \( k < n-3 \), then
\[
\binom{n}{k} \omega^{n-k} - \binom{n-1}{k} A_1\omega^{n-k-2} + \ldots + \binom{k+2}{k} A_{n-k-3}\omega \equiv 0 \text{ (mod. } pp),
\]
hence
\( (k+1) A_{n-k-3} \equiv 0 \text{ (mod. } pp), \)

and
\( A_{n-k-1} \equiv 0 \text{ (mod. } pp), \)

if \( k+1 \equiv 0 \text{ (mod. } p) \). On the contrary, if \( k+1 \equiv tp \), which may well be only when \( N(p) = p^2 \), we have
\[
\binom{k+2}{k} \equiv 0 \text{ (mod. } p),
\]
because \( t < p - 1, p > 2 \) and
\[
\left[ \frac{k+2}{p} \right] - \left[ \frac{k}{p} \right] - \left[ \frac{2}{p} \right] = t - (t - 1) - 0 = 1,
\]
hence
\[
\left( \frac{n}{k} \right) w^{n-k-1} - \left( \frac{n-1}{k} \right) A_1 w^{n-k-2} + \ldots + \left( \frac{k+2}{k} \right) A_{n-k-2} w \equiv 0 \pmod{p^2p},
\]
hence
\[
(n+1) A_{n-k-1} \equiv 0 \pmod{p^2p},
\]
and
\[
A_{n-k-1} \equiv 0 \pmod{pp},
\]
as
\[
k + 1 \equiv 0 \pmod{pp}, \quad \neq 0 \pmod{pp}.
\]
Therefore we get
\[
A_3 \equiv A_5 \equiv \ldots \equiv A_{n-1} \equiv 0 \pmod{pp}.
\]

Put \( n = \varphi(p) \), then the theorem is for ideals the exact analogue of the theorem due to Wolstenholme\(^1\), Nielsen\(^2\) and Mason\(^3\) for rational integers.

December 1932.

---

\(^1\) Quarterly J., 5 (1862).
\(^2\) Nyt Tidsskrift, 4 (1893).
\(^3\) Tohoku Math. J., 5 (1914).