CHAPTER XI

NORM RESIDUE SYMBOL FOR KUMMER EXTENSIONS

Throughout this chapter, p will denote a rational prime number; $\wp$ will denote a prime of $\mathbf{k}$, and $\wp'$ will denote a prime of an extension $\mathbf{K}$ of $\mathbf{k}$. Let m be a positive integer and let $\mathbf{k}$ contain the m-th roots of unity. The general m-power reciprocity law for elements in $\mathbf{k}$ has been found to be

$$\left(\frac{\alpha}{\beta}\right)_m \left(\frac{\beta}{\alpha}\right)_m^{-1} = \prod_{\wp\in E} \left(\frac{\alpha,\beta}{\wp}\right)_m$$

where E contains all primes of $\mathbf{k}$ dividing m and all infinite primes, and elements α and β of $\mathbf{k}$ are relatively prime to each other and to m. Our main objective will be to compute the symbol $\left(\frac{\alpha,\beta}{\wp}\right)_p$ for odd primes p in the case $\mathbf{k} = \mathbf{Q}(\zeta)$ where ζ is a primitive p-th root of unity, obtaining the p-th power reciprocity law in the process.

Lemma 11.1. *Suppose that* $\mathbf{k}$ *contains the* m*-th roots of unity and* $\wp$ *is an infinite prime of* $\mathbf{k}$*. Non-trivial norm residue symbols occur only if* $m = 2$ *and* $\wp$ *is real, in which case we have*

$$\left(\frac{\alpha,\beta}{\wp}\right)_m = \begin{cases} 1 \text{ if } \alpha > 0 \text{ or } \beta > 0, \\ -1 \text{ if } \alpha < 0 \text{ and } \beta < 0. \end{cases}$$

Proof. If $m > 2$ then all infinite primes of $\mathbf{k}$ are complex because $\mathbf{k}$ contains the m-th roots of unity.

Norm residue symbol for composite powers.

Lemma 11.2. *Suppose that* $\mathbf{k}$ *contains the* mn*-th roots of unity,* $\wp$ *is an finite prime of* $\mathbf{k}$ *and* α *and* β *are elements of* $\mathbf{k}_\wp^*$*. Let* m *and* n *be relatively prime. If* $ma + nb = 1$ *then*

$$\left(\frac{\alpha,\beta}{\wp}\right)_{mn} = \left(\frac{\alpha,\beta}{\wp}\right)_m^b \left(\frac{\alpha,\beta}{\wp}\right)_n^a \tag{11.1}$$

Proof. We can choose β_0 in $\mathbf{k}^*$ sufficiently close to β so that $\beta_0 \simeq_{mn} \beta$. Then β may be replaced by β_0 in all norm residue symbol expressions, so we may as well suppose that β is in $\mathbf{k}^*$. For an integer s dividing mn, let σ_s be the norm residue symbol automorphism.

$$\sigma_s = \left(\frac{\alpha, \mathbf{k}\left(\sqrt[s]{\beta}\right)/\mathbf{k}}{\wp}\right)$$

We have $1/mn = a/n + b/m$, so $\sqrt[mn]{\beta} = \left(\sqrt[m]{\beta}\right)^b \left(\sqrt[n]{\beta}\right)^a$. Since σ_m and σ_n are restrictions of σ_{mn} to their respective subfields, then

$$\sigma_{mn}\left(\sqrt[mn]{\beta}\right) = \sigma_{mn}\left(\left(\sqrt[m]{\beta}\right)^b \left(\sqrt[n]{\beta}\right)^a\right) = \left(\sigma_m\left(\sqrt[m]{\beta}\right)\right)^b \left(\sigma_n\left(\sqrt[n]{\beta}\right)\right)^a.$$

Therefore

$$\frac{\sigma_{mn}\left(\sqrt[mn]{\beta}\right)}{\sqrt[mn]{\beta}} = \left(\frac{\sigma_m\left(\sqrt[m]{\beta}\right)}{\sqrt[m]{\beta}}\right)^b \left(\frac{\sigma_n\left(\sqrt[n]{\beta}\right)}{\sqrt[n]{\beta}}\right)^a,$$

so

$$\left(\frac{\alpha, \beta}{\wp}\right)_{mn} = \left(\frac{\alpha, \beta}{\wp}\right)_m^b \left(\frac{\alpha, \beta}{\wp}\right)_n^a.$$

Lemma 11.3. $\mathbf{k}_\wp$ *contains the* $(\mathrm{N}\wp - 1)$*-th roots of unity.*

Proof. Let ζ be a primitive $(\mathrm{N}\wp - 1)$-th root of unity. Then $\mathbf{k}_\wp(\zeta)/\mathbf{k}_\wp$ is unramified since $\wp$ does not divide $\mathrm{N}\wp - 1$. Let $\wp'$ be the prime of $\mathbf{k}_\wp(\zeta)$. In the map $\mathbf{O}_{\wp'} \to \mathbf{O}_{\wp'}/\wp'$, element ζ maps to an element of $\mathbf{o}_\wp/\wp$ since $\mathbf{o}_\wp/\wp$ is the splitting field of $x^{\mathrm{N}\wp-1} - 1$. This shows that $\mathbf{O}_{\wp'}/\wp' = \mathbf{o}_\wp/\wp$. Therefore $f = 1$, so $[\mathbf{k}_\wp(\zeta) : \mathbf{k}_\wp] = ef = 1$, and we have $\mathbf{k}_\wp(\zeta) = \mathbf{k}_\wp$.

Lemma 11.4. *Let V be the group of $(N\wp - 1)$-th roots of unity in $\mathbf{k}_\wp$. Then the image of V in $\mathbf{o}_\wp/\wp$ is all of $(\mathbf{o}_\wp/\wp)^*$.*

Proof. If v is in V and $v \neq 1$, then v is a root of $x^{\mathrm{N}\wp-2} + \cdots + x + x = 0$. If $v = 1 (\mathrm{mod}\ \wp)$ then we would have $\mathrm{N}\wp - 1 = 0 (\mathrm{mod}\ \wp)$, which is impossible. Therefore the kernel of $V \to (\mathbf{o}_\wp/\wp)^*$ is trivial, so the map is an isomorphism since both V and $(\mathbf{o}_\wp/\wp)^*$ have $(\mathrm{N}\wp - 1)$ elements.

Lemma 11.5. *Let π be an element of $\mathbf{k}_\wp^*$ such that $\wp = (\pi)$. For fixed π, every element α of $\mathbf{k}_\wp^*$ has a unique representation as*

$$\alpha = \pi^a v u \qquad \textit{where } v \in V \textit{ and } u \in W_\wp(1).$$

Therefore $\mathbf{k}_\wp^*$ is a direct product $\langle\pi\rangle V W_\wp(1)$.

Proof. Exponent a is determined by $a = \mathrm{ord}_\wp(\alpha)$. Put $\alpha' = \alpha/\pi^a$. Then α' is in $\mathbf{u}_\wp$. By lemma 11.4, there is a unique element v in V so that $\alpha' = v (\mathrm{mod}\ \wp)$. Then $u = \alpha'/v$ is in $W_\wp(1)$. Since α' and v are uniquely determined then so is u.

LEMMA 11.6. *If n is relatively prime to $N\wp - 1$ then $V = V^n$ and the map $x \to x^n$ is an isomorphism of $(\mathbf{o}_\wp/\wp)^*$.*

PROOF. Let a and b be integers such that $na + (\mathrm{N}\wp - 1)b = 1$. Then $y \to y^a$ is inverse to $x \to x^n$, and we have $V \supset V^n \supset V^{na} = V$, so $V = V^n$.

The case of powers relatively prime to $\wp$. Suppose that $n = p^x$ where (p) is the rational prime divisible by $\wp$ and m is relatively prime to p. Lemma 11.2 shows how computation of the norm residue symbol for mn-th powers is reduced to separate computations for m-th powers and p^x-th powers. Lemma 11.7 gives an explicit formula for the former case.

LEMMA 11.7. *Let π be an element of $\mathbf{k}_\wp^*$ such that $\wp = (\pi)$. Suppose that m is relatively prime to $\wp$. If $\alpha = \pi^a vu$ and $\beta = \pi^b v'u'$ as in lemma 11.5, then*

$$\left(\frac{\alpha, \beta}{\wp}\right)_m = \left(\frac{-1}{\wp}\right)_m^{ab} (v)^{-b\frac{\mathrm{N}\wp-1}{m}} (v')^{a\frac{\mathrm{N}\wp-1}{m}}$$

PROOF. Since $\wp$ does not divide m then we can apply lemma 10.9.

$$\left(\frac{\alpha, \beta}{\wp}\right)_m = \left(\frac{-1}{\wp}\right)_m^{ab} \left(\frac{\beta^a/\alpha^b}{\wp}\right)_m = \left(\frac{-1}{\wp}\right)_m^{ab} \left(\frac{(v'u')^a \,/\, (vu)^b}{\wp}\right)_m .$$

We have $u = 1 (\mathrm{mod}\ \wp)$ and $u' = 1 (\mathrm{mod}\ \wp)$, so both $\left(\frac{u}{\wp}\right)_m$ and $\left(\frac{u'}{\wp}\right)_m$ are trivial. $\left(\frac{v}{\wp}\right)_m$ is the unique $(\mathrm{N}\wp-1)$-th root of unity such that $\left(\frac{v}{\wp}\right)_m = v^{\frac{\mathrm{N}\wp-1}{m}} (\mathrm{mod}\ \wp)$. But v is an $(\mathrm{N}\wp-1)$-th root of unity, so $\left(\frac{v}{\wp}\right)_m = (v)^{\frac{\mathrm{N}\wp-1}{m}}$, and likewise $\left(\frac{v'}{\wp}\right)_m = (v')^{\frac{\mathrm{N}\wp-1}{m}}$.

The case of p^x-th powers where $\wp$ divides (p). Take $n = p^x$ where $\wp$ divides (p). Then n is relatively prime to $\mathrm{N}\wp - 1$. Group V is cyclic of order $\mathrm{N}\wp - 1$, so $V^n = V$, and every element of V is a n-th power. Since every n-th power norm residue symbol involving an element v in V is trivial, we have

$$\left(\frac{\alpha, \beta}{\wp}\right)_n = \left(\frac{\pi^a vu, \pi^b v'u'}{\wp}\right)_n = \left(\frac{\pi^a u, \pi^b u}{\wp}\right)_n \tag{11.2}$$

To compute (11.2), it is only necessary to assume that $\mathbf{k}$ contains the n-th roots of unity.

LEMMA 11.8. *Suppose that $\wp$ is a prime of $\mathbf{k}$ and (p) is the rational prime that $\wp$ divides. Let $n = p^x$, and suppose that $\mathbf{k}$ contains the n-th roots of unity. Then $W_\wp(1)/W_\wp(1)^n$ is the direct sum of $d+1$ cyclic groups of order n, where $d = [\mathbf{k}_\wp : \mathbf{Q}_{(p)}]$.*

PROOF. Every element of $W_\wp(1)/W_\wp(1)^n$ has order dividing n, so the group is the direct product of cyclic subgroups each having order dividing n. Let α map to a generator of any one of these cyclic subgroups having order $n' = p^y$. Then $y \le x$, and $\alpha^{n'}$ is in $W_\wp(1)^n$, so $\alpha^{n'} = \beta^n$ for some element β in $W_\wp(1)$. Suppose that $y < x$. Then $\alpha^{p^y} = (\beta^{p^{x-y}})^{p^y}$, so $\alpha = \beta^{p^{x-y}}\zeta'$, where ζ' is a p^y-th root of unity. Since $\mathbf{k}$ contains the p^x-th roots of unity then $\zeta' = \zeta^{p^{x-y}}$ where ζ is some p^x-th root of unity, and we have $\alpha = (\beta\zeta)^{p^{x-y}}$. But α cannot be a p-th power, so it impossible to have $y < x$. Therefore each cyclic subgroup in the direct product has order exactly p^x. By lemma 11.5, $\mathbf{u}_\wp$ is a direct product $VW_\wp(1)$. Since $\mathrm{N}\wp - 1$ and $n = p^x$ are relatively prime then $V^n = V$. We therefore have

$$\frac{\mathbf{u}_\wp}{\mathbf{u}_\wp^n} = \frac{VW_\wp(1)}{VW_\wp(1)^n} = \frac{W_\wp(1)}{VW_\wp(1)^n \cap W_\wp(1)} = \frac{W_\wp(1)}{W_\wp(1)^n}.$$

Since $[\mathbf{k}_\wp : \mathbf{Q}_{(p)}] = d$ and $n = p^x$, we have $|n|_\wp = \left|\mathbf{N}_{\mathbf{k}_\wp/\mathbf{Q}_{(p)}} n\right|_p = |n^d|_p = n^{-d}$. By lemma 8.11, we have $[\mathbf{u}_\wp : \mathbf{u}_\wp^n] = n|n|_\wp^{-1}$, so

$$[W_\wp(1) : W_\wp(1)^n] = [\mathbf{u}_\wp : \mathbf{u}_\wp^n] = n(n^d) = n^{d+1}.$$

Therefore $W_\wp(1)/W_\wp(1)^n$ must be the product of $d+1$ cyclic groups of order n.

DEFINITION. An element α in $W_\wp(1)$ is n-primary if $\mathbf{k}_\wp(\sqrt[n]{\alpha})/\mathbf{k}_\wp$ is unramified.

LEMMA 11.9. *With the hypothesis of lemma 11.8, the image in $W_\wp(1)/W_\wp(1)^n$ of the set of n-primary elements is a cyclic group of order n.*

PROOF. Since $\mathbf{k}_\wp^*$ is a direct product $\langle\pi\rangle VW_\wp(1)$ and $V = V^n$ we have

$$\frac{\mathbf{k}_\wp^*}{(\mathbf{k}_\wp^*)^n} = \frac{\langle\pi\rangle\ V\ \ W_\wp(1)}{\langle\pi^n\rangle V^n W_\wp(1)^n} = \frac{\langle\pi\rangle}{\langle\pi^n\rangle} \times \frac{W_\wp(1)}{W_\wp(1)^n}.$$

By lemma 11.8, $\mathbf{k}_\wp^*/(\mathbf{k}_\wp^*)^n$ is the direct sum of $d+2$ cyclic groups of order n, where $d = [\mathbf{k}_\wp : \mathbf{Q}(p)]$. Let $\beta_1, \dots \beta_{d+2}$ be a set of generators for $\mathbf{k}_\wp^*/(\mathbf{k}_\wp^*)^n$, and the β_i may be chosen to be elements of $\mathbf{k}^*$. The β_i are independent modulo n, so by lemma 8.5 the extension $\mathbf{k}_\wp\left(\sqrt[n]{\beta_1}, \dots, \sqrt[n]{\beta_{d+2}}\right)$ of $\mathbf{k}_\wp$ has degree n^{d+2}, with Galois group isomorphic to the direct sum of the $d+2$ Galois groups $G(\mathbf{k}_\wp(\sqrt[n]{\beta_i}) : \mathbf{k}_\wp)$, where $1 \le i \le d+2$. Every extension of the form $\mathbf{k}_\wp(\sqrt[n]{\beta})$ where β is in $\mathbf{k}_\wp^*$ is a subfield of $\mathbf{k}_\wp\left(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_{d+2}}\right)$. Put $\mathbf{K} = \mathbf{k}\left(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_{d+2}}\right)$. The kernel of $\alpha \to \left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{\wp}\right)_n$ has index n^{d+2} in $\mathbf{k}_\wp^*$ and contains $(\mathbf{k}_\wp^*)^n$. Since $[\mathbf{k}_\wp^* : (\mathbf{k}_\wp^*)^n] = n^{d+2}$, then the kernel is exactly $(\mathbf{k}_\wp^*)^n$.

Let H be the image in $G = G(\mathbf{k}_\wp\left(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_{d+2}}\right) : \mathbf{k}_\wp)$ of the units $\mathbf{u}_\wp$ of $\mathbf{k}_\wp$. An element β of $\mathbf{k}_\wp^*$ is in the fixed field of H if and only if $\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{\wp}\right)_n \sqrt[n]{\beta} = \sqrt[n]{\beta}$ for every α in $\mathbf{u}_\wp$, which is if and only if $\left(\frac{\alpha, \beta}{\wp}\right)_n = 1$ for every α in $\mathbf{u}_\wp$, which is if and only if $\mathbf{k}_\wp(\sqrt[n]{\beta})/\mathbf{k}_\wp$ is unramified.

The kernel of the homomorphism $\mathbf{k}_\wp^* \to G/H$ is $\mathbf{u}_\wp(\mathbf{k}_\wp^*)^n$, so we have

$$\frac{G}{H} = \frac{\mathbf{k}_\wp^*}{\mathbf{u}_\wp(\mathbf{k}_\wp)^n} = \frac{\langle\pi\rangle V W_\wp(1)}{V W_\wp(1) \langle\pi^n\rangle V^n W_\wp(1)^n} = \frac{\langle\pi\rangle V W_\wp(1)}{\langle\pi^n\rangle V W_\wp(1)} = \frac{\langle\pi\rangle}{\langle\pi^n\rangle}.$$

Therefore the fixed field of H is a cyclic extension of degree n and, by lemma 8.5, is of the form $\mathbf{k}_\wp(\sqrt[n]{\gamma_2})/\mathbf{k}_\wp$ for some element γ_2 of $\mathbf{k}_\wp^*$. By lemma 8.2, n is the smallest positive value of x such that $\gamma_2^x \simeq_n 1$. Let $(\gamma_2) = \wp^c$ where $c = nq + r$ and $0 \le r < n$. Put $\gamma_1 = \gamma_2/\pi^{qn}$. Then $\gamma_2 \simeq_n \gamma_1$, so the fixed field of H is $\mathbf{k}_\wp\left(\sqrt[n]{\gamma_1}\right)$, and $(\gamma_1) = \wp^r$. The map $\alpha \to \left(\frac{\alpha, \gamma_1}{\wp}\right)_n$ is a homomorphism $\mathbf{k}_\wp^* \to G(\mathbf{k}_\wp(\sqrt[n]{\gamma_1}) : \mathbf{k}_\wp)$. The kernel has index n and contains $\mathbf{u}_\wp(\mathbf{k}_\wp^*)^n$, so the kernel is exactly $\mathbf{u}_\wp(\mathbf{k}_\wp^*)^n$. Since -1 is in $\mathbf{u}_\wp$, we have

$$\left(\frac{\gamma_1, \gamma_1}{\wp}\right)_n = \left(\frac{-\gamma_1, \gamma_1}{\wp}\right)_n \left(\frac{-1, \gamma_1}{\wp}\right)_n = 1.$$

Therefore γ_1 is in the kernel, so γ_1 is in $\mathbf{u}_\wp(\mathbf{k}_\wp^*)^n$. This shows that $r = 0$, so γ_1 is in $\mathbf{u}_\wp$. Put $\gamma_1 = \delta\gamma_0$ where δ is in V and γ_0 is in $W_\wp(1)$. Since $V = V^n$, we have $\gamma_1 \simeq_n \gamma_0$. Therefore the fixed field of H is $\mathbf{k}_\wp(\sqrt[n]{\gamma_0})$. Since $\gamma_0 \simeq_n \gamma_1 \simeq_n \gamma_2$ then n is the smallest positive value of x such that $\gamma_0^x \simeq_n 1$.

If β is n-primary then β is in $W_\wp(1)$ and $\mathbf{k}_\wp(\sqrt[n]{\beta})/\mathbf{k}_\wp$ is unramified. Therefore β is in the fixed field of H, so β is in $\mathbf{k}_\wp(\sqrt[n]{\gamma_0})$, and therefore $\beta \simeq_n \gamma_0^x$ for some x by lemma 8.3. Put $\beta = \alpha^n \gamma_0^x$. Since γ_0 and β are both in $W_\wp(1)$ then $\alpha^n = 1 (\mathrm{mod}\ \wp)$, so $\alpha = 1 (\mathrm{mod}\ \wp)$ by lemma 11.6. We have shown that the image in $W_\wp(1)/W_\wp(1)^n$ of an n-primary element is a coset $(\gamma_0)^x W_\wp(1)^n$ and that n is the smallest positive value of x such that γ_0^x is in $W_\wp(1)^n$. Therefore the image of the n-primary elements is the cyclic group of order n generated by the image of γ_0. This concludes the proof of lemma 11.9.

LEMMA 11.10. *With the hypothesis of lemma 11.8, choose a fixed element π so that $\wp = (\pi)$. Put*

$$W_\pi = \left\{ \alpha \in W_\wp(1) \;\middle|\; \left(\frac{\pi, \alpha}{\wp}\right)_n = 1 \right\}.$$

Let γ_0 in $W_\wp(1)$ be a generator of group the n-primary elements modulo $W_\wp(1)^n$ and let $\overline{\gamma_0}$ be the coset $\gamma_0 W_\wp(1)^n$. Then $W_\wp(1)/W_\wp(1)^n$ is a direct product

$$\frac{W_\wp(1)}{W_\wp(1)^n} = \frac{W_\pi}{W_\wp(1)^n} \times \langle\overline{\gamma_0}\rangle.$$

PROOF. Suppose that α is n-primary and in W_π. Then $\left(\frac{\beta,\alpha}{\wp}\right)_n = 1$ for every element β of $\mathbf{k}_\wp^*$, and in particular for a set of generators $\beta_1, \ldots, \beta_{d+2}$ generators of $\mathbf{k}_\wp/(\mathbf{k}_\wp^*)^n$. Therefore for $1 \le i \le d+2$, the norm residue symbols $\left(\frac{\alpha, \mathbf{k}_\wp(\sqrt[n]{\beta_i})/\mathbf{k}_\wp}{\wp}\right)_n$ are trivial, so $\left(\frac{\alpha, \mathbf{k}_\wp(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_{d+2}})/\mathbf{k}_\wp}{\wp}\right)_n$ is trivial by lemma 8.5, and therefore α is in $(\mathbf{k}_\wp^*)^n \cap W_\wp(1)$. Then $\alpha = v^n u^n$ with v in V and u in $W_\wp(1)$. We have $v^n = 1 (\mathrm{mod}\ \wp)$, so $v = 1$, and therefore α is in $W_\wp(1)^n$. We have shown that $W_\wp(1)/W_\wp(1)^n \cap \langle\overline{\gamma_0}\rangle$ is a trivial group.

Now suppose that α is an arbitrary element of $W_\wp(1)$. It remains to show that W_π and γ_0 generate $W_\wp(1)$ modulo $W_\wp(1)^n$. Since $\mathbf{k}_\wp(\sqrt[n]{\gamma_0})$ has degree n over $\mathbf{k}_\wp$ then there exists an element β in $\mathbf{k}_\wp^*$ such that $\left(\frac{\beta,\gamma_0}{\wp}\right)_n$ is a primitive n-th root of unity. Let $\beta = \pi^b v u$. Then $\left(\frac{\beta,\gamma_0}{\wp}\right)_n = \left(\frac{\pi,\gamma_0}{\wp}\right)_n^b$, so $\left(\frac{\pi,\gamma_0}{\wp}\right)_n$ must be a primitive n-th root of unity. There exists an a so that $\left(\frac{\pi,\alpha}{\wp}\right)_n = \left(\frac{\pi,\gamma_0}{\wp}\right)_n^a$. We have $\alpha = (\alpha\gamma_0^{-a})\gamma^a$. Then $\alpha\gamma_0^{-a}$ is in W_π because $\left(\frac{\pi,\alpha\gamma_0^{-a}}{\wp}\right)_n = \left(\frac{\pi,\alpha}{\wp}\right)_n \left(\frac{\pi,\gamma_0}{\wp}\right)_n^{-a} = 1$. This completes the proof of the lemma.

The computation of the norm residue symbol for p^x-th powers has been reduced to the following. An element α of $\mathbf{k}_\wp^*$ may be expressed as $x = \pi^a v w$ where v is in V and w is in $W_\wp(1)$. Let $w \simeq_n u\gamma_0^{a'}$ with u in W_π. Likewise, let β in $\mathbf{k}_\wp^*$ be expressed as $\beta = \pi^b v' w'$ where v' is in V and $w' \simeq_n u'\gamma_0^{b'}$ with u' in W_π. Then

$$\left(\frac{x,y}{\wp}\right)_n = \left(\frac{\pi^a v u \gamma_0^{a'}, \pi^b v' u' \gamma_0^{b'}}{\wp}\right)_n = \left(\frac{\pi,\pi}{\wp}\right)_n^{ab} \left(\frac{\pi,\gamma_0}{\wp}\right)_n^{ab'} \left(\frac{u,u'}{\wp}\right)_n \left(\frac{\gamma_0,\pi}{\wp}\right)_n^{ba'}$$

Therefore

$$\left(\frac{x,y}{\wp}\right)_n = \left(\frac{\pi,-1}{\wp}\right)_n^{ab} \left(\frac{\pi,\gamma_0}{\wp}\right)_n^{ab'-ba'} \left(\frac{u,u'}{\wp}\right)_n$$

The problems that remain are essentially two.

(1) Find a generator γ_0 for the n-primary elements and calculate $\left(\frac{\pi,\gamma_0}{\wp}\right)_n$.

(2) Find a basis $v_1,\dots,v_d$ of W_π modulo $W_\wp(1)^n$ and calculate $\left(\frac{v_i,v_j}{\wp}\right)_n$.

The p-primary elements for odd primes. We specialize to the case $n=p$ and $p>2$. Let $\mathbf{k}=\mathbf{Q}(\zeta)$ where ζ is a primitive p-th root of unity. Then $\big[\mathbf{k}:\mathbf{Q}\big]=p-1$. The prime (p) is completely ramified in $\mathbf{k}$; if $\pi=1-\zeta$ then $(p)=\wp^{p-1}$ where $\wp=(\pi)$. We have $\big[\mathbf{k}_\wp:\mathbf{Q}_{(p)}\big]=p-1$ with ramification index $e=p-1$; since $f=1$ then the rational integers $0,1,\dots,p-1$ are a complete residue system for $\mathbf{o}_\wp/\wp$.

Lemma 11.11. $[W_\wp(1):W_\wp(k+1)]=p^k$

Proof. Every element of $W_\wp(1)$ may be uniquely represented modulo π^{k+1} by $1+a_1\pi+a_2\pi^2+\cdots+a_k\pi^k$ with coefficients a_i belonging to a complete residue system for $\mathbf{o}_\wp/\wp$. There are p^k choices for the coefficients $a_1,\dots,a_k$.

Lemma 11.12. $W_\wp(1)^p=W_\wp(p+1)$

Proof. Let $b=\mathrm{ord}_\wp(p)$. By lemma 4.13, every element x of $\mathbf{k}_\wp$ such that $\mathrm{ord}_\wp(x)>b/(p-1)+\mathrm{ord}_\wp(p)$ is the p-th power of some element y in $\mathbf{k}_\wp$ such that $\mathrm{ord}_\wp(y)>b/(p-1)$. Since $\mathrm{ord}_\wp(p)=p-1$, then every x such that $\mathrm{ord}_\wp(x)>p$ is the p-th power of some y such that $\mathrm{ord}_\wp(y)>1$, that is $W_\wp(p+1)\subset W_\wp(2)^p$. Let $V_p=\langle\zeta\rangle$ be the group of p-power roots of unity. Since $\zeta=1(\mathrm{mod}\ \wp)$ then

$$W_\wp(p+1)\subset W_\wp(2)^p\subset \big(W_\wp(2)V_p\big)^p\subset W_\wp(1)^p\subset W_\wp(1)$$

By lemma 11.8 and lemma 11.11, subgroups $W_\wp(p+1)$ and $W_\wp(1)^p$ both have index p^p in $W_\wp(1)$, so the two must coincide.

Lemma 11.13. *If element α of $\mathbf{k}_\wp$ is in $W_\wp(p)$ then $\frac{\sqrt[p]{\alpha}-1}{\pi}$ is integral over $\mathbf{o}_\wp$.*

Proof. The element in question is a root of polynomial $(p\pi)^{-1}\big((\pi x+1)^p-\alpha\big)$ having coefficients in $\mathbf{k}_\wp$, and

$$\frac{(\pi x+1)^p-\alpha}{p\pi}=\frac{\pi^p}{p\pi}x^p+\frac{\binom{p}{1}\pi^{p-1}}{p\pi}x^{p-1}+\cdots+\frac{\binom{p}{p-1}\pi}{p\pi}x+\frac{1-\alpha}{p\pi}.$$

The leading coefficient is a unit and the other coefficients except possibly the constant term are elements of $\mathbf{o}_\wp$. If $\alpha=1(\mathrm{mod}\ \wp^p)$ then the constant term is also in $\mathbf{o}_\wp$.

LEMMA 11.14. *Let* α *of* $\mathbf{k}_\wp$ *be in* $W_\wp(1)$. *Then* α *is* p*-primary if and only if* α *is in* $W_\wp(p)$.

PROOF. Let P be the group of p-primary elements in $W_\wp(1)$. Then we have $[W_\wp(1) : W_\wp(1)^p] = p^p$ and $[P : W_\wp(1)^p] = p$ by lemma 11.8 and lemma 11.9, so $[W_\wp(1) : P] = p^{p-1}$. Also we have $[W_\wp(1) : W_\wp(p)] = p^{p-1}$ by lemma 11.11, so it will be enough to show that $W_\wp(p)$ is contained in P, *i.e.* $\mathbf{k}_\wp(\sqrt[p]{\alpha})/\mathbf{k}_\wp$ is unramified if $\alpha = 1 (\text{mod } \wp^p)$. Let τ be an automorphism in the inertial subgroup of $G(\mathbf{k}_\wp(\sqrt[p]{\alpha}) : \mathbf{k}_\wp)$, and let $\tau(\sqrt[p]{\alpha}) = \zeta' \sqrt[p]{\alpha}$ where ζ' is a p-th root of unity. (We need to show that ζ' must be 1.) Let $\wp'$ be the prime of $\mathbf{k}_\wp(\sqrt[p]{\alpha})$ dividing $\wp$. Then $\tau(\gamma) = \gamma (\text{mod } \wp')$ for every γ that is integral over $\mathbf{o}_\wp$. The element $(\sqrt[p]{\alpha} - 1)/\pi$ is integral over $\mathbf{o}_\wp$ by lemma 11.13, so we have

$$\frac{\zeta' \sqrt[p]{\alpha} - 1}{\pi} = \frac{\sqrt[p]{\alpha} - 1}{\pi} (\text{mod } \wp').$$

Therefore

$$\frac{(\zeta' - 1) \sqrt[p]{\alpha}}{\pi} = 0 (\text{mod } \wp').$$

If $\zeta' \neq 1$ then $(\zeta' - 1)/\pi$ is a unit, but that is impossible since $\sqrt[p]{\alpha}$ is also a unit. This shows that $\zeta' = 1$, the inertial group is trivial, and $\mathbf{k}_\wp(\sqrt[p]{\alpha})/\mathbf{k}_\wp$ is unramified, which concludes the proof.

LEMMA 11.15. *With* $\pi = 1 - \zeta$ *we have*

$$\zeta^i = 1 - i\pi (\text{mod } \wp^2) \quad \text{and} \quad \frac{\pi^{p-1}}{p} = -1 (\text{mod } \wp).$$

PROOF. Since $\zeta = 1 (\text{mod } \wp)$ then, for $1 \leq i < p$, we have

$$\frac{1 - \zeta^i}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{i-1} = i (\text{mod } \wp),$$

so $1 - \zeta^i = i\pi (\text{mod } \wp^2)$, which establishes the first conclusion. For the second, substitute $x = 1$ in $x^{p-1} + \cdots + x + 1 = (x - \zeta)(x - \zeta^2) \ldots (x - \zeta^{p-1})$ to obtain

$$p = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{p-1}). \tag{11.3}$$

Therefore

$$\frac{\pi^{p-1}}{p} = \frac{(1 - \zeta)(1 - \zeta) \ \ldots (1 - \zeta)}{(1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{p-1})} = \frac{1}{(p-1)!} (\text{mod } \wp).$$

Since $(p - 1)! = -1 (\text{mod } p)$ then the second conclusion follows.

LEMMA 11.16. *If α in $\mathbf{k}_\wp$ is a p-primary element, there is a rational integer a such that $0 \le a < p$ and $\alpha = 1 + ap\pi \left(\text{mod } \wp^{p+1}\right)$. With $\pi = 1 - \zeta$, we have*

$$\left(\frac{\pi, \alpha}{\wp}\right)_p = \zeta^a.$$

PROOF. Let α be p-primary. There is an integer a so that $\alpha = 1 + ap\pi$ modulo $\wp^{p+1}$ since the integers $0, 1, \ldots, p-1$ are a complete residue system for $\mathbf{o}_\wp/\wp$. We can choose an element α' in $\mathbf{k}$ that is sufficiently close to α so that $\alpha' \simeq_p \alpha$ and $\alpha' = \alpha\left(\text{mod } \wp^{p+1}\right)$, so we may assume that α is in $\mathbf{k}$. In that case, put $\mathbf{K} = \mathbf{k}\left(\sqrt[p]{\alpha}\right)$ and let $\wp'$ be a prime of $\mathbf{K}$ dividing $\wp$. If α is p-primary then $\wp$ is unramified in $\mathbf{K}$ so in the completion we have $\wp' = \wp\mathbf{O}_{\wp'}$ and therefore $\wp' = (\pi)$. Put

$$\sqrt[p]{\alpha} = 1 + b\pi \qquad \text{where } b \in \mathbf{O}_{\wp'}.$$

Then

$$\alpha = (1 + b\pi)^p = 1 + pb\pi + b^p\pi^p \left(\text{mod } {\wp'}^{p+1}\right).$$

By lemma 11.15, $\pi^p = -p\pi\left(\text{mod } \wp^{p+1}\right)$, so $\pi^p = -p\pi\left(\text{mod } {\wp'}^{p+1}\right)$, and

$$\alpha = 1 + pb\pi - b^p p\pi \left(\text{mod } {\wp'}^{p+1}\right).$$

Therefore we have

$$a = b - b^p (\text{mod } \wp'). \tag{11.4}$$

Let $\left(\frac{\pi,\alpha}{\wp}\right)_p \sqrt[p]{\alpha} = \zeta^{a'} \sqrt[p]{\alpha}$. Since $\mathbf{K}/\mathbf{k}$ is unramified then we have

$$\left(\frac{\pi, \mathbf{K}/\mathbf{k}}{\wp}\right) = \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{i}(\pi, \wp, \mathbf{k})\big) = \left(\frac{\mathbf{K}/\mathbf{k}}{\wp}\right).$$

and therefore for any β in $\mathbf{O}_{\wp'}$ we have

$$\left(\frac{\pi, \mathbf{K}/\mathbf{k}}{\wp}\right)\beta = \beta^{\mathrm{N}\wp} = \beta^p (\text{mod } \wp').$$

Choose $\beta = (\sqrt[p]{\alpha} - 1)/\pi$, which is in $\mathbf{O}_{\wp'}$ by lemma 11.13. Then

$$\left(\frac{\pi, \mathbf{K}/\mathbf{k}}{\wp}\right)\beta = \frac{\zeta^{a'}\sqrt[p]{\alpha} - 1}{\pi},$$

so

$$\frac{\zeta^{a'}\sqrt[p]{\alpha}-1}{\pi}=\left(\frac{\sqrt[p]{\alpha}-1}{\pi}\right)^p=b^p(\text{mod }\wp').$$

We have $\zeta^{a'}=1-a'\pi(\text{mod }\wp^2)$ by lemma 11.15, so

$$\frac{(1-a'\pi)(1+b\pi)-1}{\pi}=b^p(\text{mod }\wp').$$

This shows that $-a'+b=b^p(\text{mod }\wp')$, or $a'=b-b^p(\text{mod }\wp')$. Comparison with (11.4) shows $a=a'(\text{mod }\wp')$. Both a and a' are rational integers, so have

$$a=a'(\text{mod }p),$$

which completes the proof of the lemma.

We have solved the first basic problem for prime p. The generator of the p-primary elements modulo $W_\wp(1)^p=W_\wp(p+1)$ is $\gamma_0=1+p\pi$, and

$$\left(\frac{\pi,\gamma_0}{\wp}\right)_p=\zeta \qquad \text{where } \pi=1-\zeta.$$

Generators of $W_\pi/W(1)^p$ and the p-th power reciprocity law. If we can find a set of generators $u_1,\dots u_{p-1}$ for $W_\wp(1)/W_\wp(p)$, then every element α of $W_\wp(1)$ will be expressible as $\alpha=u_1^{t_1}\dots u_{p-1}^{t_{p-1}}\gamma_0^{t_0}(\text{mod }\wp^{p+1})$, so if $\left(\frac{\pi,u_i}{\wp}\right)=\zeta^{c_i}$ then we will have

$$W_\pi=\left\{\alpha\in W_\wp(1)\quad|\quad c_1t_1+\dots c_{p-1}t_{p-1}+t_0=0(\text{mod }p)\right\}.$$

The constants c_i will be determined in the last section.

Lemma 11.17. *If r is a primitive root modulo p then*

$$r^i\prod_{\substack{k=1\\k\neq i}}^{p-1}(r^i-r^k)=-1(\text{mod }p).$$

Proof. Since $r,r^2,\dots,r^{p-1}$ form a reduced residue system modulo p, then

$$\prod_{k=1}^{p-1}(x-r^k)=x^{p-1}-1(\text{mod }p).$$

Then

$$\frac{d}{dx}\prod_{k=1}^{p-1}(x-r^k)=\frac{d}{dx}\left(x^{p-1}-1\right)(\text{mod } p),$$

or

$$\sum_{\ell=1}^{p-1}\prod_{\substack{k=1\\k\neq\ell}}^{p-1}(x-r^k)=(p-1)x^{p-2}(\text{mod } p).$$

Set $x=r^i$ and multiply both sides by r^i to obtain the desired result.

$$r^i\prod_{\substack{k=1\\k\neq i}}^{p-1}(r^i-r^k)=(p-1)r^{i(p-1)}=-1(\text{mod } p).$$

LEMMA 11.18. *Let σ be a generator of $G(\mathbf{k}_\wp:\mathbf{Q}_{(p)})$ and let $\zeta^\sigma=\zeta^r$. Then r is a primitive root modulo p. For $i=1,\ldots,p-1$, set*

$$u_i=(1-\pi^i)^{-r^i(\sigma-r)(\sigma-r^2)\ldots(\sigma-r^{i-1})(\sigma-r^{i+1})\ldots(\sigma-r^{p-1})}$$

Then

$$u_i^\sigma\simeq_p u_i^{r_i}\quad \textit{and}\quad u_i=1-\pi^i(\textit{mod } \wp^{i+1}).$$

PROOF. If $f(x)$ and $g(x)$ are polynomials in $\mathbf{Z}[x]$ and $f(x)=g(x)(\text{mod } p)$ then $\alpha^{f(\sigma)}\simeq_p\alpha^{g(\sigma)}$ for α in $\mathbf{k}^*$. Since $f(x)=(x-r)(x-r^2)\ldots(x-r^{p-1})$ is a polynomial of degree $p-1$ having roots $1,2,\ldots,p-1$, modulo p, then $f(x)=x^{p-1}-1(\text{mod } p)$. Therefore $\alpha^{f(\sigma)}\simeq_p 1$. We have $u_i^{\sigma-r^i}=(1-\pi^i)^{-r^if(\sigma)}\simeq_p 1$, so $u_i^\sigma\simeq_p u^{r^i}$, which is the first part of the lemma. For the second part, we have $\pi=1-\zeta$, so

$$\pi^\sigma=1-\zeta^\sigma=1-\zeta^r=\left(1-(1-\pi)^r\right)=r\pi(\text{mod } \wp^2).$$

Put $\pi^\sigma=r\pi+\beta\pi^2$. Then $(\pi^\sigma)^i=(r\pi+\beta\pi^2)^i=r^i\pi^i(\text{mod } \wp^{i+1})$, so

$$(\pi^i)^\sigma=r^i\pi^i(\text{mod } \wp^{i+1}).$$

Before proceeding further, we make the following observation. If $j_1,\ldots,j_{s+1}$ are any given integers, then we have

$$\begin{aligned}&\left(1+r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})\pi^i\right)^{\sigma-r^{j_{s+1}}}\\&=\left(1+r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})\pi^i\right)^\sigma\left(1+r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})\pi^i\right)^{-r^{j_{s+1}}}\\&=\left(1+r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})r^i\pi^i\right)\\&\qquad\left(1-r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})r^{j_{s+1}}\pi^i\right)^{-1}(\text{mod } \wp^{i+1})\\&=\left(1+r^i(r^i-r^{j_1})\ldots(r^i-r^{j_s})(r^i-r^{j_{s+1}})\pi^i\right)(\text{mod } \wp^{i+1})\end{aligned}$$

To compute u_i, we start from $(1-\pi^i)^{-r^i} = 1 + r^i\pi^i (\text{mod } \wp^{i+1})$, then successively apply $\sigma - r$, $\sigma - r^2$, up to $\sigma - r^{p-1}$, but omit $\sigma - r^i$. By applying the above observation at each step, we arrive at

$$u_i = \big(1 + r^i(r^i - r)\dots(r^i - r^{i-1})(r^i - r^{i+1})\dots(r^i - r^{p-1})\pi^i\big)(\text{mod } \wp^{i+1}).$$

By lemma 11.17, we obtain $u_i = 1 - \pi^i (\text{mod } \wp^{i+1})$, which completes the proof.

LEMMA 11.19. *For $1 \le i \le p-1$ and $1 \le j \le p-1$, we have*

$$\left(\frac{u_i, u_j}{\wp}\right)_p = \begin{cases} \zeta^{-i} & \text{if } i + j = p \\ 0 & \text{if } i + j \neq p \end{cases}$$

PROOF. We apply automorphisms on the left in this proof, so we have $\sigma\zeta = \zeta^r$ and $\sigma u_i \simeq_p u_i^{r^i}$. First, we have

$$\left(\frac{\sigma u_i, \sigma u_j}{\wp}\right)_p = \left(\frac{u_i^{r^i}, u_j^{r^j}}{\wp}\right)_p = \left(\frac{u_i, u_j}{\wp}\right)_p^{r^{i+j}}. \tag{11.5}$$

We also have

$$\left(\frac{\sigma u_i, \sigma u_j}{\wp}\right)_p \sqrt[p]{\sigma u_j} = \left(\frac{\sigma u_i, \mathbf{k}\left(\sqrt[p]{\sigma u_j}\right)/\mathbf{k}}{\wp}\right)_p \sqrt[p]{\sigma u_j}.$$

Automorphism $\sigma : \mathbf{k} \to \mathbf{k}$ may be extended to an isomorphism $\sigma : \mathbf{k}\left(\sqrt[p]{u_j}\right) \to \mathbf{k}\left(\sqrt[p]{\sigma u_j}\right)$. (In the notation of lemma 10.43, we have $\mathbf{K} = \mathbf{k}\left(\sqrt[p]{u_j}\right)$, $\mathbf{K}' = \mathbf{k}\left(\sqrt[p]{\sigma u_j}\right)$, $\mathbf{k}' = \mathbf{k}$, and $\wp' = \wp$.) Since $\left(\sigma \sqrt[p]{u_j}\right)^p = \sigma u_j$, then $\sigma \sqrt[p]{u_j}$ is a root of $x^p - \sigma u_j$, and we may write $\sigma \sqrt[p]{u_j} = \sqrt[p]{\sigma u_j}$. (The particular choice of $\sqrt[p]{\sigma u_j}$ determines the extension of σ.) Using the notation of lemma 10.43, we have

$$\begin{aligned}\left(\frac{\sigma u_i, \mathbf{k}\left(\sqrt[p]{\sigma u_j}\right)/\mathbf{k}}{\wp}\right) &= \left(\frac{u_i', \mathbf{K}'/\mathbf{k}'}{\wp'}\right) \\ &= \sigma\left(\frac{u_i, \mathbf{K}/\mathbf{k}}{\wp}\right)\sigma^{-1} = \sigma\left(\frac{u_i, \mathbf{k}\left(\sqrt[p]{u_j}\right)/\mathbf{k}}{\wp}\right)\sigma^{-1}\end{aligned}$$

Therefore

$$\begin{aligned}\left(\frac{\sigma u_i, \mathbf{k}\left(\sqrt[p]{\sigma u_j}\right)/\mathbf{k}}{\wp}\right)\sqrt[p]{\sigma u_j} &= \sigma\left(\frac{u_i, \mathbf{k}\left(\sqrt[p]{u_j}\right)/\mathbf{k}}{\wp}\right)\sigma^{-1}\left(\sigma \sqrt[p]{u_j}\right) \\ &= \sigma\left(\left(\frac{u_i, u_j}{\wp}\right)\sqrt[p]{u_j}\right) = \left(\frac{u_i, u_j}{\wp}\right)_p^r \sqrt[p]{\sigma u_j}\end{aligned}$$

or

$$\left(\frac{\sigma u_i, \sigma u_j}{\wp}\right)_p = \left(\frac{u_i, u_j}{\wp}\right)_p^r$$

Comparison with (11.5) shows that

$$\left(\frac{u_i, u_j}{\wp}\right)_p^r = \left(\frac{u_i, u_j}{\wp}\right)_p^{r^{i+j}}$$

If $\left(\frac{u_i,u_j}{\wp}\right) \neq 1$, then we must have $r = r^{i+j} (\text{mod } p)$, so $1 = i + j (\text{mod } p - 1)$. For i and j in the range $1 \leq i \leq p - 1$ and $1 \leq j \leq p - 1$, the only value of $i + j$ which satisfies the condition $1 = i + j (\text{mod } p - 1)$ is $i + j = p$. So far, we have established that

$$\left(\frac{u_i, u_j}{\wp}\right)_p = 0 \qquad \text{if } i + j \neq p.$$

We need to compute $\left(\frac{u_i,u_{p-i}}{\wp}\right)_p$. Since $u_k = 1 - \pi^k (\text{mod } \wp^{k+1})$ for $1 \leq k < p$, and $\gamma_0 = 1 + p\pi$, then we can find integers a_k for $i + 1 \leq k \leq p$ such that $0 \leq a_k < p$ and

$$1 - \pi^i = u_i u_{i+1}^{a_{i+1}} \dots u_{p-1}^{a_{p-1}} \gamma_0^{a_p} (\text{mod } \wp^{p+1}).$$

Likewise, we can find integers b_ℓ for $p - i + 1 \leq \ell \leq p$ such that $0 \leq b_\ell < p$ and

$$1 - \pi^{p-i} = u_{p-i} u_{p-i+1}^{b_{p-i+1}} \dots u_{p-1}^{b_{p-1}} \gamma_0^{b_p} (\text{mod } \wp^{p+1}).$$

Since $\left(\frac{u_i,u_j}{\wp}\right)_p = 0$ unless $i + j = p$, and since γ_0 is p-primary, we have

$$\text{(11.6)} \quad \left(\frac{1 - \pi^i, 1 - \pi^{p-i}}{\wp}\right)_p$$
$$= \left(\frac{u_i u_{i+1}^{a_{i+1}} \dots u_{p-1}^{a_{p-1}} \gamma_0^{a_p}, u_{p-i} u_{p-i+1}^{b_{p-i+1}} \dots u_{p-1}^{b_{p-1}} \gamma_0^{b_p}}{\wp}\right)_p = \left(\frac{u_i, u_{p-i}}{\wp}\right)_p.$$

The problem now is to compute $\left(\frac{1-\pi^i,1-\pi^{p-i}}{\wp}\right)_p$. Suppose that $\alpha + \beta = \gamma$, and put $\mu = \alpha/\gamma$. Then $1 - \mu = \beta/\gamma$. By lemma 10.6(f), we have

$$1 = \left(\frac{1 - \mu, \mu}{\wp}\right)_p = \left(\frac{\frac{\beta}{\gamma}, \frac{\alpha}{\gamma}}{\wp}\right)_p = \left(\frac{\beta, \alpha}{\wp}\right)_p \left(\frac{\beta, \gamma}{\wp}\right)_p^{-1} \left(\frac{\gamma, \alpha}{\wp}\right)_p^{-1} \left(\frac{\gamma, \gamma}{\wp}\right)_p$$

Since $\left(\frac{\gamma,\gamma}{\wp}\right)_p = 1$ for $p > 2$, we have

$$\left(\frac{\beta,\alpha}{\wp}\right)_p = \left(\frac{\beta,\gamma}{\wp}\right)_p \left(\frac{\gamma,\alpha}{\wp}\right)_p.$$

Choose $\alpha = \pi^{p-i}(1-\pi^i)$ and $\beta = 1-\pi^{p-i}$. Then $\gamma = 1-\pi^p$, and we have

$$\left(\frac{1-\pi^{p-i},\pi^{p-i}(1-\pi^i)}{\wp}\right)_p = \left(\frac{1-\pi^{p-i},1-\pi^p}{\wp}\right)_p \left(\frac{1-\pi^p,\pi^{p-i}(1-\pi^i)}{\wp}\right)_p.$$

Apply lemma 10.6(f) to the left side, and apply the fact that $1-\pi^p$ is p-primary (annihilates units) to the right to obtain

$$\left(\frac{1-\pi^{p-i},1-\pi^i}{\wp}\right)_p = \left(\frac{1-\pi^p,\pi^{p-i}}{\wp}\right)_p.$$

We have $1-\pi^p = 1+p\pi (\bmod \wp^{p+1})$ by lemma 11.15, so

$$\left(\frac{1-\pi^i,1-\pi^{p-i}}{\wp}\right)_p = \left(\frac{\pi^{p-i},1+p\pi}{\wp}\right)_p.$$

Apply (11.6) on the left side, and apply lemma 11.16 on the right to obtain

$$\left(\frac{u_i,u_{p-i}}{\wp}\right)_p = \zeta^{p-i} = \zeta^{-i}.$$

The completes the proof of lemma 11.19.

Theorem 11.20 - reciprocity law for odd prime powers. *If α and β are elements of $W_\wp(1)$, then let a_i and b_i $(1 \le i < p)$ be integers such that $0 \le a_i < p$ and $0 \le b_i < p$ and*

$$\alpha = u_1^{a_1}\dots u_{p-1}^{a_{p-1}} (\textit{mod } \wp^p) \quad \textit{and} \quad \beta = u_1^{b_1}\dots u_{p-1}^{b_{p-1}} (\textit{mod } \wp^p).$$

Then

$$\left(\frac{\alpha}{\beta}\right)_p \left(\frac{\beta}{\alpha}\right)_p^{-1} = \zeta^{-\sum_{i=1}^{p-1} i a_i b_{p-i}}.$$

Proof. Since α and $u_1^{a_1}\dots u_{p-1}^{a_{p-1}}$ differ only by a factor that is p-primary, and likewise for β and $u_1^{b_1}\dots u_{p-1}^{b_{p-1}}$, then we have

$$\left(\frac{\alpha}{\beta}\right)_p \left(\frac{\beta}{\alpha}\right)_p^{-1} = \left(\frac{\alpha,\beta}{\wp}\right)_p = \prod_{i=1}^{p-1}\prod_{j=1}^{p-1}\left(\frac{u_i,u_j}{\wp}\right)_p^{a_i b_j}$$

$$= \prod_{i=1}^{p-1}\left(\frac{u_i,u_{p-i}}{\wp}\right)_p^{a_i b_{p-i}} = \prod_{i=1}^{p-1}\zeta^{-i a_i b_{p-i}} = \zeta^{-\sum_{i=1}^{p-1} i a_i b_{p-i}}$$

Computation of symbols $\left(\frac{\pi,u_i}{\wp}\right)_p$.

Lemma 11.21.

$$\left(\frac{p,u_i}{\wp}\right)_p = 1 \quad \textit{for } i = 1,\dots,p-1$$

Proof. By lemma 11.18, we have

$$\left(\frac{p,\sigma u_i}{\wp}\right)_p = \left(\frac{p,u_i^{r^i}}{\wp}\right)_p = \left(\frac{p,u_i}{\wp}\right)_p^{r^i}. \tag{10.7}$$

We can compute $\left(\frac{p,\sigma u_i}{\wp}\right)_p$ in another way using lemma 10.43. Proceeding as in the proof of lemma 11.19, we have $\sqrt[p]{\sigma u_i} = \sigma\sqrt[p]{u_i}$ and

$$\left(\frac{p,\mathbf{k}(\sqrt[p]{\sigma u_i})/\mathbf{k}}{\wp}\right)_p = \sigma\left(\frac{p,\mathbf{k}(\sqrt[p]{u_i})/\mathbf{k}}{\wp}\right)_p\sigma^{-1},$$

so

$$\left(\frac{p,\mathbf{k}(\sqrt[p]{\sigma u_i})/\mathbf{k}}{\wp}\right)_p\sqrt[p]{\sigma u_i} = \sigma\left(\frac{p,\mathbf{k}(\sqrt[p]{u_i})/\mathbf{k}}{\wp}\right)_p\sqrt[p]{u_i}.$$

Therefore

$$\left(\frac{p,\sigma u_i}{\wp}\right)_p\sqrt[p]{\sigma u_i} = \sigma\left(\left(\frac{p,u_i}{\wp}\right)_p\sqrt[p]{u_i}\right) = \left(\frac{p,u_i}{\wp}\right)_p^r\sqrt[p]{\sigma u_i}.$$

Comparison with (10.7) shows that $\left(\frac{p,u_i}{\wp}\right)_p^r = \left(\frac{p,u_i}{\wp}\right)_p^{r^i}$. If $\left(\frac{p,u_i}{\wp}\right)_p \neq 1$ then we must have $r = r^i (\bmod p)$, or $i = 1$.

It remains to prove the lemma in the case $i = 1$. We have $1 - \pi = \zeta$, and by lemma 11.17 with $i = 1$ we have $r(r-r^2)\dots(r-r^{p-1}) = -1(\bmod p)$, so

$$u_1 = \zeta^{-r(\sigma-r^2)\dots(\sigma-r^{p-1})} = \zeta^{-r(r-r^2)\dots(r-r^{p-1})} = \zeta. \tag{10.8}$$

We have $p = (1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1})$, so the lemma is proved if $\left(\frac{1-\zeta^j,\zeta}{\wp}\right)_p = 1$ for $1 \le j < p$. For each j there is a j' so that $jj' = 1(\bmod p)$, and

$$\left(\frac{1-\zeta^j,\zeta}{\wp}\right)_p = \left(\frac{1-\zeta^j,\zeta^{jj'}}{\wp}\right)_p = \left(\frac{1-\zeta^j,\zeta^j}{\wp}\right)_p^{j'} = 1.$$

This completes the proof of the lemma.

LEMMA 11.22. *Put* $\xi = -\frac{\pi^{p-1}}{p}$. *Then*

$$\left(\frac{\pi, u_i}{\wp}\right)_p = \left(\frac{\xi, u_i}{\wp}\right)_p \quad \text{for } 1 \leq i < p.$$

PROOF. Since p is odd then $-1 = (-1)^p$, so by lemma 11.21 we have

$$\left(\frac{\pi, u_i}{\wp}\right)_p = \left(\frac{\pi^{p-1}, u_i}{\wp}\right)_p^{-1} = \left(\frac{-\pi^{p-1}/p, u_i}{\wp}\right)_p^{-1} = \left(\frac{\xi, u_i}{\wp}\right)_p^{-1},$$

which proves the lemma.

For any α in $W_\pi(1)$, let $t_1(\alpha), \ldots, t_{p-1}(\alpha)$ be the unique integers satisfying

$$\alpha = u_1^{t_1(\alpha)} \ldots u_{p-1}^{t_{p-1}\alpha} (\text{mod } \wp^p) \quad \text{and } 0 \leq t_i(\alpha) < p \tag{11.9}$$

Then

$$\left(\frac{\xi, u_i}{\wp}\right)_p = \left(\frac{u_{p-i}^{t_{p-i}(\xi)}, u_i}{\wp}\right)_p = \zeta^{i t_{p-i}(\xi)}. \tag{11.10}$$

The problem is to compute $t_1(\xi), \ldots, t_{p-1}(\xi)$ for $1 \leq i \leq p-2$, since the next lemma shows that $t_{p-1}(\xi) = 1$.

LEMMA 11.23.

$$\left(\frac{\xi, u_1}{\wp}\right)_p = 1, \quad \text{or } \; t_{p-1}(\xi) = 0.$$

PROOF. By (11.3) and (11.8) we have

$$\left(\frac{\xi, u_i}{\wp}\right)_p = \left(\frac{-\pi^{p-1}p^{-1}, u_i}{\wp}\right)_p = \left(\frac{-1, \zeta}{\wp}\right)_p \left(\frac{1-\zeta, \zeta}{\wp}\right)_p^{p-1} \prod_{j=1}^{p-1} \left(\frac{1-\zeta^j, \zeta}{\wp}\right)_p$$

We have $-1 = (-1)^p$, and $\left(\frac{1-\zeta^j, \zeta}{\wp}\right)_p = 1$ was shown in the proof of lemma 11.21.

Kummer's logarithmic differential quotient for $p > 2$. Every element α in $\mathbf{o}_\wp$ is a linear combination of $1, \zeta, \ldots, \zeta^{p-2}$ with coefficients in $\mathbf{Z}_(p)$. Suppose that $\phi(x)$ and $\psi(x)$ are polynomials over $\mathbf{Z}_(p)$ such that $\alpha = \phi(\zeta) = \psi(\zeta)$. Then ζ is a root of $\phi(x) - \psi(x)$, so $\phi(x) - \psi(x)$ is divisible by the minimal polynomial of ζ over $\mathbf{Z}_{(p)}$, which is $f_0(x) = x^{p-1} + \cdots + x + 1$ because $[\mathbf{Q}_{(2)}(\zeta) : \mathbf{Q}_{(2)}] = p - 1$. Let $\eta(x)$ be a polynomial with coefficients in $\mathbf{Z}_{(p)}$ such that

$$\phi(x) - \psi(x) = f_0(x)\eta(x).$$

Applying formal differentiation, we obtain

$$\phi^{(n)}(x) - \psi^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f_0^{(k)}(x)\eta^{(n-k)}(x) \quad \text{for } 0 \le n \le p-1 \tag{11.11}$$

as an identity of polynomials over $\mathbf{Z}_{(p)}$.

Lemma 11.24. *Let $f_0(x) = x^{p-1} + \cdots + x + 1$. Then*

$$f_0^{(k)}(1) = 0(mod\ p) \quad \textit{for } 0 \le k \le p-2$$

and

$$f_0^{(p-1)}(1) = -1(mod\ p).$$

Proof. Both sides of the identity

$$(p-1)!f_0(x) = \sum_{k=0}^{p-1} f_0^{(k)}(1)\frac{(p-1)!}{k!}(x-1)^k$$

are polynomials with integer coefficients, and $f_0^{(k)}(1)$ and $(p-1)!/k!$ are integers. We have $(x-1)f_0(x) = x^p - 1 = (x-1)^p (\text{mod } p)$, so $f_0(x) = (x-1)^{p-1} (\text{mod } p)$. Therefore

$$(p-1)!(x-1)^{p-1} = \sum_{k=0}^{p-1} f_0^{(k)}(1)\frac{(p-1)!}{k!}(x-1)^k (\text{mod } p)$$

The coefficients of $(x-1)^k$ for $0 \le k \le p-1$ must be identical on both sides, so

$$f_0^{(k)}(1) = 0(\text{mod } p) \quad \text{for } 0 \le k \le p-2,$$

and

$$f_0^{(p-1)}(1) = (p-1)! = -1(\text{mod } p).$$

LEMMA 11.25. *If α is an element of $\mathbf{Q}_{(p)}(\zeta)$ and $\alpha = \phi(\zeta) = \psi(\zeta)$ where $\phi(x)$ and $\psi(x)$ are polynomials with coefficients in $\mathbf{Z}_{(p)}$, then*

$$\phi^{(n)}(1) - \psi^{(n)}(1) = 0(mod\ p) \quad for\ 0 \leq n \leq p-2$$

and

$$\phi^{(p-1)}(1) - \psi^{(p-1)}(1) = -\frac{\phi(1)-\psi(1)}{p}(mod\ p)$$

PROOF. The result for $0 \leq n \leq p-2$ is obtained by setting $x = 1$ in (11.11) and applying lemma 11.24. For $n = p-1$ we have

$$\phi^{(p-1)}(1) - \psi^{(p-1)}(1) = f_0^{(p-1)}(1)\eta(1) = -\eta(1)(\text{mod } p).$$

We have $\phi(1) - \psi(1) = f_0(1)\eta(1)$. Since $f_0(1) = p$ then $\phi(1) - \psi(1)$ is divisible by p and $\eta(1) = \big(\phi(1) - \psi(1)\big)/p$, which gives the desired result for $n = p-1$.

LEMMA 11.26. *Suppose that α is in $W_\wp(1)$ and $\alpha = \phi(\zeta) = \psi(\zeta)$. Then we have $1 = \phi(1) = \psi(1)(mod\ 0)$, and*

$$\phi^{(n)}(1) = \psi^{(n)}(1)(mod\ p) \quad for\ 0 \leq n < p-1$$

and

$$\phi^{(p-1)}(1) + \frac{\phi(1)-1}{p} = \psi^{(p-1)}(1) + \frac{\psi(1)-1}{p}(mod\ p)$$

PROOF. Since $\alpha = 1(\text{mod } \wp)$ and $\zeta = 1(\text{mod } \wp)$ then we have $1 = \phi(1) = \psi(1)(\text{mod } \wp)$. Therefore $1 = \phi(1) = \psi(1)(\text{mod } p)$, so $\phi(1) - 1$ and $\psi(1) - 1$ are divisible by p. The results now follow immediately from lemma 11.25.

We consider the formal power series $F(z) = \log\big(\phi(e^z)\big)$.

$$F(z) = \log\big(\phi(1)\big) + \frac{\phi'(1)}{\phi(1)}z + \frac{\big(\phi''(1) + \phi'(1)\big)\phi(1) - \phi'(1)^2}{\phi(1)^2}z^2 + \dots$$

If $\phi(1)$ is in $W_\wp(1)$ then $\log\big(\phi(1)\big)$ is defined, but we are actually interested only in coefficients of z^n for $1 \leq n \leq p-1$.

LEMMA 11.27.
$$\frac{d^n}{dz^n}F(z) = \frac{\phi^{(n)}(e^z)e^{nz}}{\phi(e^z)} + R_n(z)$$

where $R_n(z)$ is a rational expression in $e^z, \phi(e^z)$, $\phi'(e^z), \ldots, \phi^{(n-1)}(e^z)$. The numerator of $R_n(z)$ is a sum of terms each of which is divisible by at least one of $\phi'(e^z), \ldots, \phi^{(n-1)}(e^z)$, and the denominator is a power of $\phi(e^z)$.

PROOF. Put $w = e^z$, $u_0 = \phi(e^z)$, and $u_i = \phi^{(i)}(e^z)$ for $i \geq 0$. Then $w' = w$ and $u_i' = u_{i+1}w$ for $i \geq 0$. We have $F(z) = \log(u_0)$, so $dF(z)/dz = u_1 w/u_0$. Therefore $R_1(z) = 0$, so the conclusion holds for $n = 1$. For $n = 2$, we have

$$\frac{d^2}{dz^2}F(z) \quad = \quad \frac{u_2 w^2}{u_0} + \frac{u_1 w}{u_0} - \frac{u_1^2 w^2}{u_0^2} \quad = \quad \frac{u_2 w^2}{u_0} + \frac{u_1 u_0 w - u_2 u_1 w^2}{u_0^2}$$

so every term of the numerator of $R_2(z)$ is divisible by u_1.

Assume that the lemma is true for n. Then

$$\frac{d^n}{dz^n}F(z) = \frac{u_n w^n}{u_0} + R_n(z)$$

and

$$R_n(z) = \frac{S_1 u_1 + \cdots + S_{n-1}u_{n-1}}{u_0^{k_n}}$$

where $S_1(z), \ldots S_{n-1}(z)$ are polynomials in $w, u_0, \ldots, u_{n-1}$. We have

$$\frac{d}{dz}R_n(z) = \frac{\sum_{j=1}^{n-1}\left(\left(S_j' u_j + S_j u_{j+1} w\right) u_0^{k_n} - k_n S_j u_j u_0^{k_n - 1} u_1 w\right)}{u_0^{2k_n}}$$

and every term of the numerator is divisible by at least one of $u_1, \ldots, u_n$. Then

$$\frac{d^{n+1}}{dz^{n+1}}F(z) =$$
$$= \frac{u_{n+1}w^{n+1}}{u_0} + \frac{n u_n w^n}{u_0} - \frac{u_n u_1 w^{n+1}}{u_0^2} + \frac{d}{dz}R_n(z) = \frac{u_{n+1}w^{n+1}}{u_0} + R_{n+1}(z)$$

We see that $R_{n+1}(z)$ is a rational expression in $w, u_0, u_1 \ldots, u_n$ with denominator $u_0^{2k_n}$, and every term of the numerator contains at least one factor from the list $u_1, \ldots, u_n$, and the conclusion therefore follows.

LEMMA 11.28. *If $\alpha = \phi(\zeta)$ is in $W_\wp(1)$, define $\ell_n(\alpha)$ by*

$$\ell_n(\alpha) = \begin{cases} \dfrac{d^n}{dz^n} F(0) & \text{for } 1 \leq n \leq p-2 \\ \dfrac{d^{(p-1)}}{dz^{(p-1)}} F(0) + \dfrac{\phi(1)-1}{p} & \text{for } n = p-1. \end{cases}$$

Then $\ell_n(\alpha)$ depends only on α and not on $\phi(x)$ for $1 \leq n \leq p-1$.

PROOF. By lemma 11.27, $\frac{d^n}{dz^n}F(0) = \frac{\phi^{(n)}(1)}{\phi(1)} + R_n(0)$, where $R_n(0)$ is a rational expression in $1, \phi(1), \ldots, \phi^{n-1}(1)$ with denominator a power of $\phi(1)$. By lemma 11.26, $\phi(1) = 1(\text{mod } p)$ and $\ell_1(\alpha), \ldots, \ell_{p-2}(\alpha)$ depend modulo p only on α and not on $\phi(x)$. For $n = p-1$, we have

$$\ell_{p-1}(\alpha) = \phi^{(p-1)}(1) + \frac{\phi(1)-1}{p} + R_{p-1}(0)(\text{mod } p).$$

By lemma 11.26, this expression depends modulo p only on α and not on $\phi(x)$.

LEMMA 11.29. *For α_1 and α_2 in $W_\wp(1)$, we have*

$$\ell_j(\alpha_1\alpha_2) = \ell_j(\alpha_1) + \ell_j(\alpha_2)(\text{mod } p), \tag{1}$$

$$\ell_j(\alpha_1\alpha_2^{-1}) = \ell_j(\alpha_1) - \ell_j(\alpha_2)(\text{mod } p). \tag{2}$$

If $\alpha_1 = \alpha_2(\text{mod } \wp^{p-1})$ then

$$\ell_j(\alpha_1) = \ell_j(\alpha_2)(\text{mod } p) \quad \text{for } 1 \leq j \leq p-2. \tag{3}$$

If $\alpha_1 = \alpha_2(\text{mod } \wp^p)$ then

$$\ell_{p-1}(\alpha_1) = \ell_{p-1}(\alpha_2)(\text{mod } p). \tag{4}$$

If σ generates $G(\mathbf{Q}_{(p)}(\zeta) : \mathbf{Q}_{(p)})$ and $\zeta^\sigma = \zeta^r$ then

$$\ell_j(\alpha^\sigma) = r^j \ell_j(\alpha)(\text{mod } p) \quad \text{for } 1 \leq j \leq p-1 \tag{5}$$

PROOF. If $\alpha_1 = \phi_1(\zeta)$ and $\alpha_2 = \phi_2(\zeta)$ then $\alpha_1\alpha_2 = \phi_1(\zeta)\phi_2(\zeta)$, and (1) follows from the identity of formal power series

$$\log\big(\phi_1(e^z)\phi_2(e^z)\big) = \log\big(\phi_1(e^z)\big) + \log\big(\phi_2(e^z)\big).$$

Then (2) follows from

$$\ell_j\big((\alpha_1\alpha_2^{-1})\alpha_2\big) = \ell_j(\alpha_1\alpha_2^{-1}) + \ell_j(\alpha_2)(\text{mod } p).$$

As to (3), it is enough to show that if $\alpha = 1(\text{mod } \wp^{p-1})$ then $\ell_j(\alpha) = 0(\text{mod } p)$ for $1 \leq j \leq p-2$. Put

$$\alpha = a_0 + \sum_{k=0}^{p-2} a_k \pi^k.$$

Then $a_0 = 1(\text{mod } p)$, and $a_k = 0(\text{mod } p)$ for $1 \leq k \leq p-2$. We have $\alpha = a_0 + \sum_{k=0}^{p-2} a_k(1-\zeta)^k$, so $\alpha = \phi(\zeta)$ with

$$\phi(x) = a_0 + \sum_{k=0}^{p-2} a_k(1-x)^k$$

We have $\phi(x) = 1(\text{mod } p)$, and $\phi^{(n)}(x) = 0(\text{mod } p)$ for $n \geq 1$. By lemma 11.27 we have

$$\ell_1(\alpha) = \cdots = \ell_{p-2}(\alpha) = 0(\text{mod } p).$$

As to (4), since all derivatives of $\phi(x)$ vanish modulo p then all derivatives of $\log\big(\phi(e^z)\big)$ vanish modulo p at $z = 0$. If $\alpha = 1(\text{mod } \wp^p)$ then $a_0 = 1(\text{mod } p^2)$, so we have

$$\ell_{p-1}(\alpha) = \frac{\phi(1) - 1}{p} = \frac{a_0 - 1}{p} = 0(\text{mod } p).$$

As to (5), if $\alpha = \sum_{k=0}^{p-2} b_k\zeta^k = \phi(\zeta)$ and $\zeta^\sigma = \zeta^r$ then $\alpha^\sigma = \sum_{k=0}^{p-2} b_k\zeta^{rk} = \phi(\zeta^r) = \psi(\zeta)$ where $\psi(x) = \phi(x^r)$. If $\log\big(\phi(e^z)\big) = \sum_{n=0}^{\infty} c_n z^n$, then $\log\big(\psi(e^z)\big) = \log\big(\phi(e^{rz})\big) = \sum_{n=0}^{\infty} c_n r^n z^n$. Therefore

$$\ell_j(\alpha^\sigma) = r^j \ell_j(\alpha) \quad \text{for } 1 \leq j \leq p-2.$$

For $j = p-1$, we have $r^{p-1} = 1(\text{mod } p)$ so we are claiming that $\ell_{p-1}(\alpha^\sigma) = \ell_{p-1}(\alpha)(\text{mod } p)$. Since all derivatives of $\log\big(\phi(e^z)\big)$ vanish modulo p at $z = 0$, this reduces to

$$\left.\frac{\phi(x) - 1}{p}\right|_{x=1} = \left.\frac{\phi(x^r) - 1}{p}\right|_{x=1} (\text{mod } p).$$

This completes the proof of lemma 11.29.

LEMMA 11.30. *If α is in $W_\wp(1)$ and $t_1(\alpha), \ldots t_{p-1}(\alpha)$ are as in (11.9), then*

$$t_j(\alpha) = \frac{(-1)^{j-1}}{j!}\ell_j(\alpha)(mod\ p) \quad for\ 1 \leq j \leq p-1.$$

PROOF. We have $\ell_j(u_i^\sigma) = r^j \ell_j(u_i)(\text{mod } p)$ for $1 \leq j \leq p-1$ by lemma 11.29(5). Also, we have $u_i^\sigma = u_i^{r^i}(\text{mod } \wp^p)$ by lemma 11.18, so $\ell_j(u_i^\sigma) = \ell_j(u_i^{r^i})(\text{mod } p)$ for $1 \leq j \leq p-2$ by lemma 11.29(3) and for $j = p-1$ by lemma 11.29(4). Therefore, if $\ell_j(u_i) \neq 0(\text{mod } p)$ then $r^i = r^j(\text{mod } p)$, or $i = j$. Since $u_i = 1 - \pi^i(\text{mod } \wp^{i+1})$ by lemma 11.18, we have

$$u_j = (1-\pi^j)u_{j+1}^{a_{j+1}} \ldots u_{p-1}^{a_{p-1}}(\text{mod } p),$$

so $\ell_j(u_j) = \ell_j(1-\pi^j)(\text{mod } p)$. Since $1 - \pi^j = 1 - (1-\zeta)^j$, then we take $\phi(x) = 1 - (1-x)^j$. Then

$$\phi(e^z) = 1 - (1-e^z)^j = 1 + (-1)^{j-1}z^j + \ldots$$

so

$$\log\big(\phi(e^z)\big) = (-1)^j z^j + \ldots$$

In this case we have $\phi(1) = 1$, so $\big(\phi(1) - 1\big)/p = 0$, and therefore

$$\ell_j(u_j) = \ell_j(1-\pi^j) = \frac{d^j}{dz^j}\log\big(\phi(e_z)\big)\bigg|_{z=0} = (-1)^j j!(\text{mod } p).$$

Putting $\alpha = u_1^{t_1(\alpha)} \ldots u_{p-1}^{t_{p-1}(\alpha)}(\text{mod } \wp^p)$, we have

$$\ell_j(\alpha) = t_j(\alpha)\ell_j(u_j) = (-1)^j j! t_j(\alpha)(\text{mod } p),$$

which proves the lemma.

We will be completely finished if we can compute $\ell_j(\xi)$ for $1 \leq j \leq p-2$, since we have already established that $t_{p-1}(\xi) = 0$ (lemma 11.23). The Bernoulli numbers B_a are defined by

$$\log\left(\frac{e^z - 1}{z}\right) = \sum_{a=1}^{\infty} \frac{B_a}{a}\frac{z^a}{a!}$$

The denominators of $B_1, \ldots, B_{p-2}$ cannot be divisible by p.

LEMMA 11.31. *For* $1 \le j \le p-2$ *we have*

$$\ell_j(\xi) = -\frac{B_j}{j}(mod\ p)$$

PROOF. We have

$$\xi^{-1} = -\frac{p}{\pi^{p-1}} = -\prod_{k=1}^{p-1}\frac{1-\zeta^k}{1-\zeta} = -(p-1)!\prod_{k=1}^{p-1}\frac{1}{k}\frac{1-\zeta^k}{1-\zeta} = -(p-1)!\prod_{k=1}^{p-1}\gamma_k$$

where $\gamma_k = (1+\zeta+\cdots+\zeta^{k-1})/k$ is in $W_\wp(1)$. Since $-(p-1)! = 1(\text{mod } \wp^{p-1})$, then by lemma 11.29(3) we have $\ell_j\big(-(p-1)!\big) = \ell_j(1) = 0$, so

$$\ell_j(\xi^{-1}) = \sum_{k=1}^{p-1}\ell_j(\gamma_k) \quad \text{for } 1 \le j \le p-2.$$

To compute $\ell_j(\gamma_k)$, we use $\phi_k(x) = (1+x+\cdots+x^{k-1})/k = \frac{x^k-1}{k(x-1)}$.

$$\begin{aligned}\log\big(\phi_k(e^z)\big) \quad &= \quad \log\left(\frac{e^{kz}-1}{kz}\frac{z}{e^z-1}\right)\\ &= \log\frac{e^{kz}-1}{kz} - \log\frac{e^z-1}{z} \quad = \quad \sum_{a=1}^{\infty}\frac{B_a}{a}(k^a-1)\frac{z^a}{a!}\end{aligned}$$

Therefore for $1 \le j \le p-2$ we have

$$\ell_j(\gamma_k) = \frac{d^j}{dz^j}\log\big(\phi_k(e^z)\big)\Big|_{z=0} = \frac{B_j}{j}(k^j-1) \qquad \text{for } 1 \le j \le p-2,$$

so

$$\ell_j(\xi^{-1}) = \sum_{k=1}^{p-1}\frac{B_j}{j}(k^j-1).$$

If r is a primitive root modulo p and $1 \le j \le p-2$, then

$$\sum_{\nu=1}^{p-1}k^j = \sum_{\nu=1}^{p-1}r^{\nu j} = \frac{r^{pj}-1}{r^j-1} = 0(\text{mod } p),$$

so

$$\ell_j(\xi^{-1}) = -(p-1)\frac{B_j}{j} = \frac{B_j}{j}(\text{mod } p),$$

which proves the lemma.