TOWARDS ANKENY–ARTIN–CHOWLA TYPE CONGRUENCE MODULO p^3

FRANTIŠEK MARKO

Abstract. We formulate and generalize the technique of Jakubec established to derive congruences of Ankeny–Artin–Chowla type for a cyclic subfield K of prime conductor p. Then we concentrate on the case of congruences modulo p^3 and clear a significant technical hurdle which allows us to formulate Ankeny–Artin–Chowla congruences modulo p^3 in a concise way.

Introduction

In a series of papers [J1], [J2], [J3], [J4], [J5], [J6], [JL], Stanislav Jakubec has developed a technique that enabled him to established congruences of Ankeny–Artin–Chowla type modulo p and p^2 for cyclic fields K of prime degree l and of prime conductor p. At the begining of this paper we recall and generalize his results and formulate Jakubec's technique in general.

In order to apply Jakubec's technique in the modulo p^3 case, we analyze properties of a map Φ and in Theorem 1.2 we formulate results in a form that does not use the map Φ. We conjecture that a result analogous to Theorem 1.2 is valid in general.

Finally, Theorem 1.3 gives a simplified formulation of congruences of Ankeny–Artin–Chowla type modulo p^3.

1. The technique of Jakubec

Let p be an odd prime, $\zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ be a primitive p-th root of unity and

Received: 23. 03. 2006. Revised: 21. 06. 2006.
(2000) Mathematics Subject Classification: 11R29.
Key words and phrases: Ankeny–Artin–Chowla congruence, class number, divisibility, units.

$\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field. We will consider various subfields K of $\mathbb{Q}(\zeta_p)$ of degrees $n = [K : \mathbb{Q}]$ dividing $p-1$. Put $k = \frac{p-1}{n}$ and denote by $\beta_K = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$ the Gauss period of the field K.

Fix a positive integer t and choose an integer a that is a primitive root modulo p^t. Then the authomorphism σ, defined by $\sigma(\zeta_p) = \zeta_p^a$, generates the Galois group $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Further, denote $g = a^{p^{t-1}}$ and $g_n = g^k$ so that $g_n^n \equiv 1 \pmod{p^t}$ for each n dividing $p-1$.

The prime p is totally ramified in $\mathbb{Q}(\zeta_p)$ and factors as $p = \mathfrak{p}^{p-1}$, where $\mathfrak{p} = (1-\zeta_p)$. Thus p is totally ramified in each subfield K of $\mathbb{Q}(\zeta_p)$ and $p = \mathfrak{p}_K^n$ for a unique divisor $\mathfrak{p}_K$ of K.

1.1. Generators π_K

A special choice of a generator of divisor $\mathfrak{p}_K$ plays an important role in the works of Jakubec. Since his notation is ambiguous, we provide more details about these generators.

LEMMA 1.1. *For any natural number t and any subfield K of $\mathbb{Q}(\zeta_p)$ there is an element $\pi_{K,t}$ satisfying*

i) $N_{K/\mathbb{Q}}(\pi_{K,t}) = (-1)^n p$,

ii) $\sigma(\pi_{K,t}) \equiv g_n \pi_{K,t} \pmod{\pi_{K,t}^{tn+1}}$,

iii) $\beta_K \equiv \sum_{i=0}^{n} \frac{k}{(ki)!}\pi_{K,t}^i \pmod{\pi_{K,t}^{n+1}}$.

Moreover, the numbers $\pi_{K,t}$ can be chosen in such a way that if $K_1 \subset K_2$ are subfields of $\mathbb{Q}(\zeta_p)$ of degrees n_1 and n_2 respectively, then

$$\pi_{K_1,t} \equiv \pi_{K_2,t}^{\frac{n_2}{n_1}} \pmod{\pi_{K_2,t}^{tn_2+1}}.$$

PROOF. The existence of a number $\pi_{K,1}$ satisfying (i)–(iii) is the statement of Theorem of [J1]. For a general t, choose a number $\pi \in \mathbb{Q}(\zeta_p)$ as on p. 106 of [J2] that satisfies $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi) = p$, $\sigma(\pi) \equiv g\pi \pmod{\pi^{t(p-1)+1}}$ and $\zeta_p \equiv \sum_{i=0}^{p-1} \frac{1}{i!}\pi^i \pmod{\pi^p}$.

Put $\pi_{K,t} = (-1)^{k+1}\mathrm{N}_{\mathbb{Q}(\zeta_p)/K}(\pi) = (-1)^{k+1}\pi\sigma^n(\pi)\ldots\sigma^{(k-1)n}(\pi)$. Conditions (i) and (ii) for $\pi_{K,t}$ follow immediately from the corresponding conditions for π. Taking the trace we obtain

$$\beta_K = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p) \equiv \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}\left(\sum_{i=0}^{p-1} \frac{1}{i!}\pi^i\right) \equiv \sum_{i=0}^{n} \frac{k}{(ki)!}\pi^{ki} \pmod{\mathfrak{p}_K^{n+1}}.$$

This together with the congruence

$$\begin{aligned}\pi_{K,t} &= (-1)^{k+1}\pi\sigma^n(\pi)\ldots\sigma^{(k-1)n}(\pi) \equiv (-1)^{k+1}\pi(g^n\pi)\ldots(g^{(k-1)n}\pi)\\ &= (-1)^{k+1}\pi^k g^{n+\ldots+(k-1)n} \equiv \pi^k \pmod{\mathfrak{p}^{t(p-1)+1}}\end{aligned}$$

implies the remaining assertions. □

From now on we fix t and choose $\pi_K = \pi_{K,t}$ satisfying the conditions of the preceeding Lemma. It follows immediately from the defining properties that $(\pi_K) = \mathfrak{p}_K$ and

(1) $$\pi_K^n \equiv -p \pmod{\pi_K^{tn+1}}.$$

1.2. Polynomials assigned to π_K-expansions of units

Denote by $\mathcal{O}_K$ the ring of integers of K, U_K the multiplicative group of units of K and by $\langle\epsilon\rangle$ a subgroup of U_K generated by all conjugates of $\epsilon \in U_K$. To $\epsilon \in U_K$ one can find integers $a_0, \dots a_{tn-1}$ modulo p^t and $a_0 \not\equiv 0 \pmod p$ such that

$$\epsilon \equiv a_0 + a_1\pi_K + \dots + a_{tn-1}\pi_K^{tn-1} \pmod{\pi_K^{tn}}$$

and assign to ϵ a polynomial $g(X) = a_0 + a_1X + \dots + a_{tn-1}X^{tn-1} = a_0 + \dots + a_dX^d$ of degree $d \le tn-1$. Further, denote by $a(g(X)) = a_0$ the absolute term of $g(X)$.

There are unique ring isomorphisms $f_K : \mathcal{O}_K/(\pi_K^{tn}) \to \mathbb{Z}[X]/(X^n + p, p^t)$ such that $f_K(\pi_K) = X$. The inclusion $\mathcal{O}_{K_1}/(\pi_{K_1}^{tn_1}) \to \mathcal{O}_{K_2}/(\pi_{K_2}^{tn_2})$ for $K_1 \subset K_2$ corresponds under these isomorphisms to a ring morphism that sends X to $X^{\frac{n_2}{n_1}}$, and the automorphism of $\mathcal{O}_K/(\pi_K^{tn})$ induced by σ corresponds to a ring morphism that sends X to g_nX.

If $g(X)$ is assigned to ϵ, then

$$\begin{aligned} f_K(\epsilon) \equiv\ & (a_0 - pa_n + p^2a_{2n} - \dots + (-1)^{t-1}p^{t-1}a_{(t-1)n}) \\ & + (a_1 - pa_{n+1} + p^2a_{2n+1} - \dots + (-1)^{t-1}p^{t-1}a_{(t-1)n+1})X + \dots \\ & + (a_{n-1} - pa_{2n-1} + p^2a_{3n-1} - \dots + (-1)^{t-1}p^{t-1}a_{nt-1})X^{n-1} \pmod{p^t} \end{aligned}$$

is the unique polynomial modulo p^t of degree less than n that is assigned to ϵ.

For $f_K(\epsilon) = b_{n-1} + b_{n-2}X + \dots + b_0X^{n-1}$ denote $b_K(\epsilon) = (b_0, \dots, b_{n-1})$.

Further, denote by $\lambda_1, \dots, \lambda_d$ the roots of the polynomial $g(X) = a_0 + a_1X + \dots + a_dX^d$ with $d \le tn-1$ and $P = \mathbb{Z}[X]/(X^{tn})$. Then each

$$s_j(g(X)) = \frac{1}{\lambda_1^j} + \dots + \frac{1}{\lambda_d^j}$$

for $j = 1, \dots, tn-1$ defines a semigroup homomorphism $(P \setminus (X), .) \to (\mathbb{Q}, +)$.

1.3. Map Φ

Given a monic polynomial $g(X) = X^d + Y_1X^{d-1} + \dots + Y_d$, put $Y_0 = 1$ and define $X_j = S_j(g(X))$ to be the sum of the j-th powers of the roots of $g(X)$.

Assign to a polynomial $g(X) = X^d + Y_1X^{d-1} + \dots + Y_d$ of degree $d \le tn-1$ a $(tn-1)$-tuple $(Y_1, \dots, Y_d, 0, \dots, 0)$ by adding zeroes if $d < tn-1$. Then the $(tn-1)$-tuple $(X_1, \dots, X_{tn-1})$ satisfies the recurrence relation

(2) $$mY_m + \sum_{i=0}^{m-1} X_{m-i}Y_i = 0 \qquad \text{for } m = 1, \dots, tn-1.$$

Conversely, given a set $(X_1, \dots, X_{tn-1})$ of sums of powers of roots of $g(X)$ of degree $d \leq tn-1$, the set $(Y_1, \dots, Y_{tn-1})$ of "extended" coefficients of $g(X)$ is expressed from the equation (2) as

$$(3)\quad Y_m(X_1, \dots, X_m) = -\frac{1}{m}\sum_{i=0}^{m-1} X_{m-i}Y_i(X_1, \dots, X_i) \qquad \text{for } m = 1, \dots, tn-1,$$

where Y_m is defined as the following function of variables $X_1, \dots, X_{m-1}$:

$$Y_m = Y_m(X_1, \dots, X_m) = (-1)^m \frac{1}{m!}\begin{vmatrix} X_1 & 1 & 0 & \dots & 0 \\ X_2 & X_1 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ X_{m-1} & X_{m-2} & X_{m-3} & \dots & m-1 \\ X_m & X_{m-1} & X_{m-2} & \dots & X_1 \end{vmatrix}.$$

and $Y_0 = 1$.

The map $\Phi : \mathbb{C}^{tn-1} \to \mathbb{C}^n$ is defined as follows:

$$\begin{aligned}\Phi(X_1, \dots, X_{tn-1}) = (&1 - pY_n + p^2Y_{2n} - \dots + (-1)^{t-1}p^{t-1}Y_{(t-1)n}, \\ &Y_1 - pY_{n+1} + p^2Y_{2n+1} - \dots + (-1)^{t-1}p^{t-1}Y_{(t-1)n+1}, \dots, \\ &Y_{n-1} - pY_{2n-1} + p^2Y_{3n-1} - \dots + (-1)^{t-1}p^{t-1}Y_{tn-1}).\end{aligned}$$

The main property of the map Φ relates any polynomial $g(X)$ assigned to ϵ, maps s_j and the polynomial $f(\epsilon)$ as follows: If $g(X) = a_0 + a_1X + \dots a_dX^d$, then the reciprocal polynomial $g^{rec}(X) = a_d + \dots + a_1X^{d-1} + a_0X^d$ is a product of a nonzero constant $a_0 = a(g(X))$ and a monic polynomial $h(X)$. Then $s_j(g(X)) = S_j(g^{rec}(X)) = S_j(h(X))$ and

$$a(g(X))\Phi(s_1(g(X)), \dots, s_{tn-1}(g(X))) = b_K(\epsilon).$$

This property of the map Φ allows us to work with different polynomials $g(X)$ assigned to ϵ.

1.4. Congruence of Ankeny–Artin–Chowla type

From now on let K be a subfield of the real cyclotomic field $L = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $C(K)$ be the group of cyclotomic units of K. If $\eta_K = \mathrm{N}_{L/K}(\zeta_p^{\frac{(1-g)}{2}}\frac{1-\zeta_p^g}{1-\zeta_p})$, then $C(K) = \langle\eta_K\rangle$.

By Theorem 4.1 and Theorem 5.3 of [S] the class number h_K of the field K equals $[U_K : C(K)]$. According to Theorem 1 of [M], there is $\delta \in U_K$ such that $[U_K : \langle\delta\rangle] = f$ with f coprime to p. Fix such a unit δ, denote $e = [\langle\delta\rangle : \langle\eta_K^f\rangle]$ and write

$$(4)\qquad \eta_K^f = \delta^{c_0}\sigma(\delta)^{c_1}\dots\sigma^{n-2}(\delta)^{c_{n-2}}.$$

Then $e = [U_K : C(K)]f^{n-2}$ and according to Lemma 1 of [M] the index

$$e = \left| \prod_{r|n;r>1} \mathrm{N}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(c_0 + c_1\zeta_r + \ldots + c_{n-2}\zeta_r^{n-2}) \right|$$

$$= \left| \prod_{i=1}^{n-1} (c_0 + c_1\zeta_n^i + \ldots + c_{n-2}\zeta_n^{(n-2)i}) \right|.$$

The Gauss periods $\beta_0 = \beta_K$, $\beta_1 = \sigma(\beta_K)$, ..., $\beta_{n-1} = \sigma^{n-1}(\beta_K)$ form an integral basis of K. Therefore we can write $\delta = x_0\beta_0 + \ldots + x_{n-1}\beta_{n-1}$.

Assume $f(\zeta_p) = a_0 + a_1X + \ldots + a_{p-2}X^{p-2}$ is given. Remark that in the case $t = 2$ the polynomial $f(\zeta_p)$ was computed in [J6]. Then $f(\beta_K) = k\sum_{i=0}^{n-1} a_{ki}X^i$, $f(\beta_j) = k\sum_{i=0}^{n-1} a_{ki}g_n^{ij}X^i$ for $i = 0, \ldots, n-1$ and

$$f(\delta) = k\sum_{i=0}^{n-1} a_{ki} \left(\sum_{j=0}^{n-1} x_j g_n^{ij} \right) X^i.$$

Moreover, $a(f(\zeta_p)) = -\frac{1}{p-1}$ implies $a(f(\delta)) = -\frac{1}{n}(x_0 + \ldots + x_{n-1})$.

There is a polynomial $l(X)$ assigned to $\delta^{c_0}\sigma(\delta)^{c_1}\ldots\sigma^{n-2}(\delta)^{c_{n-2}}$ such that

$$s_j(l(X)) = c_0 s_j(f(\delta)) + c_1 g_n^j s_j(f(\delta)) + \ldots + c_{n-2}g_n^{j(n-2)} s_j(f(\delta)) = \alpha_j s_j(f(\delta)),$$

where $\alpha_j = c_0 + c_1g_n^j + \ldots + c_{n-2}g_n^{j(n-2)}$ for $j = 1, \ldots, tn-1$ and $a(l(X)) = (-\frac{x_0+\ldots+x_{n-1}}{n})^{c_0+\ldots+c_{n-2}} = (-\frac{x_0+\ldots+x_{n-1}}{n})^{\alpha_0}$.

Observe that $\alpha_i \equiv \alpha_{kn+i} \pmod{p^t}$ for $i = 0, \ldots, n-1$ and $-\alpha_n \equiv g_n\alpha_1 + g_n^2\alpha_2 + \ldots + g_n^{n-1}\alpha_{n-1} \pmod{p^t}$.

Because $p \equiv 1 \pmod n$, p splits completely in $\mathbb{Q}(\zeta_r)$ for each divisor $r > 1$ of n. Since $g_r^r \equiv 1 \pmod{p^t}$, there is a prime divisor $\mathfrak{q}_r$ of p in $\mathbb{Q}(\zeta_r)$ satisfying $\zeta_r \equiv g_r = g_n^{\frac{n}{r}} \pmod{\mathfrak{q}_r^t}$. Consequently

$$c_0 + c_1\zeta_r + \ldots + c_{n-2}\zeta_r^{n-2} \equiv c_0 + c_1g_r + \ldots + c_{n-2}g_r^{n-2} = \alpha_{\frac{n}{r}} \pmod{\mathfrak{q}_r^t}$$

and

$$c_0 + c_1\zeta_r^j + \ldots + c_{n-2}\zeta_r^{j(n-2)} \equiv c_0 + c_1g_r^j + \ldots + c_{n-2}g_r^{j(n-2)} = \alpha_{j\frac{n}{r}} \pmod{\mathfrak{q}_r^t}$$

for $j = 1, \ldots, r-1$. Hence

$$\mathrm{N}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(c_0 + c_1\zeta_r + \ldots + c_{n-2}\zeta_r^{n-2}) = \prod_{s|n;s\geq 1;(s,n)=\frac{n}{r}} \alpha_s \pmod{p^t}$$

and

$$\prod_{r|n;r>1} \mathrm{N}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(c_0 + c_1\zeta_r + \ldots + c_{n-2}\zeta_r^{n-2}) \equiv \prod_{i=1}^{n-1} \alpha_i \pmod{p^t}.$$

On the other hand, in the case $t = 1$, the values of $s_j(\eta_K)$ were determined in Lemma 5 of [J2]. The case $t = 2$ and n prime was considered in [J4], where the values of $s_j(f(\zeta_p + \zeta_p^{-1}))$ were determined. If 2 is not a n-th power modulo p and n is prime, then the conjugates of the unit $\eta_{K,2} = \mathrm{N}_{L/K}(\zeta_p + \zeta_p^{-1})$ generate the group $C(K)$ and we may replace η_K in the above arguments by $\eta_{K,2}$. The advantage of using $\zeta_p + \zeta_p^{-1}$ instead of $\zeta_p^{\frac{(1-g)}{2}} \frac{1-\zeta_p^g}{1-\zeta_p}$ is that $f_L(\zeta_p + \zeta_p^{-1})$ is easily derived from $f(\zeta_p)$; namely using Lemma 1.1 we obtain

$$f_L(\zeta_p + \zeta_p^{-1}) = 2a_0 + 2a_2X + \ldots + 2a_{p-3}X^{\frac{p-3}{2}},$$

where the absolute term $2a_0 = \frac{-2}{p-1} \equiv 2 + 2p + \ldots + 2p^{t-1} \pmod{p^t}$.

LEMMA 1.2. *Let $K_1 \subset K_2$ be fields of degree n_1 and n_2, respectively, $z = \frac{n_2}{n_1}$ and $\epsilon \in U_{K_2}$. Then*

$$b_{K_1}(N_{K_2/K_1}(\epsilon)) \equiv a(f_{K_2}(\epsilon))^z \Phi(s_z(f_{K_2}(\epsilon)), \ldots, s_{(tn_1-1)z}(f_{K_2}(\epsilon))) \pmod{p^t}.$$

PROOF. It is enough to show that there is a polynomial $g(X)$ assigned to $\mathrm{N}_{K_2/K_1}(\epsilon)$ treated as an element of K_1 such that $a(g(X)) = a(f_{K_2}(\epsilon))^z \pmod{p^t}$ and $s_i(g(X)) = s_{iz}(f_{K_2}(\epsilon)) \pmod{p^t}$ for $i = 1, \ldots, tn_1 - 1$.

If $f(X) = f_{K_2}(\epsilon) = a_0 + a_1X + \ldots + a_{n_2-1}X^{n_2-1}$, then $\sigma^{jn_1}(\epsilon)$ is assigned a polynomial $f(g_{jz}X) = a_0 + a_1g_{n_2}^{jn_1}X + \ldots + a_{n_2-1}g_{n_2}^{jn_1(n_2-1)}X^{n_2-1}$ for $j = 1, \ldots, z-1$. Also, $s_{iz}(f(g_zX)) = g_z^{iz}s_{iz}(f(X)) \equiv s_{iz}(f(X)) \pmod{p^t}$ for $i = 1, \ldots, tn_1 - 1$. Put $h(X) \equiv f(X)f(g_zX)\ldots f(g_{(n_1-1)z}X) \pmod{X^{tn_2}}$. Then $h(X)$ is assigned to $\mathrm{N}_{K_2/K_1}(\epsilon)$ treated as an element of K_2, $a(h(X)) = a_0^z$ and $s_{iz}(h(X)) = zs_{iz}(f(X))$ for $i = 1, \ldots, tn_1 - 1$.

Using Lemma 1.1 one finds a polynomial $g(X)$ modulo X^{tn_1} that is assigned to $\mathrm{N}_{K_2/K_1}(\epsilon)$ treated as an element of K_1 such that $h(X) = g(X^z)$. Using Newton formulas we establish that $s_{iz}(h(X)) = zs_i(g(X))$ proving the claim of the lemma. $\square$

We have proved the following statement.

THEOREM 1.1. *Let K be a cyclic subfield of the real cyclotomic field L of prime conductor p, l be the degree of K over $\mathbb{Q}$, $k = \frac{p-1}{l}$, $\eta \in U_L$ be such that $N_{L/K}(\eta)$ generates the group $C(K)$ of cyclotomic units of K, and $T_i = s_{\frac{i(p-1)}{2l}}(f_L(\eta))$ for $i = 1, \ldots, tl-1$. Let $\delta = x_0\beta_0 + x_1\beta_2 + \ldots + x_{l-1}\beta_{l-1} \in U_K$ be such that $\delta^{c_0}\sigma(\delta)^{c_1}\ldots\sigma^{l-2}(\delta)^{c_{l-2}} = N_{L/K}(\eta)^f$ where f is not divisible by p. Denote $f(\zeta_p) = a_0 + a_1X + \ldots + a_{p-2}X^{p-2}$ and put $\alpha_m = c_0 + c_1g_l^m + \ldots + c_{l-2}g_l^{m(l-2)}$ for $m = 1, \ldots l$. For $i = 1, \ldots, tl-1$ denote $S_i = s_i(f_K(\delta))$, where $f_K(\delta) = k\sum_{i=0}^{l-1} a_{ki}(\sum_{j=0}^{l-1} x_jg_l^{ij})X^i$.*

Then

$$a(f_L(\eta))^{\frac{p-1}{2l}}\Phi(fT_1, \ldots, fT_{tl-1}) \equiv \left(-\frac{x_0+x_1+\ldots+x_{l-1}}{l}\right)^{\alpha_0}. \tag{5}$$

$$\Phi(\alpha_1S_1, \ldots, \alpha_lS_l, \alpha_1S_{l+1}, \ldots, \alpha_lS_{2l}, \alpha_1S_{2l+1}, \ldots, \alpha_{l-1}S_{tl-1}) \pmod{p^t}$$

and

$$\pm\alpha_1\dots\alpha_{l-1} = h_K f^{l-2} \pmod{p^t}. \tag{6}$$

In order to obtain a congruence of Ankeny-Artin-Chowla type from the above theorem, it is necessary to solve for $\alpha_1,\dots,\alpha_{l-1}$ from (5) and apply the results to (6). In the case $t=2$ this was done in [JL]. The purpose of the remainder of the paper is to solve for $\alpha_1,\dots,\alpha_{l-1}$ from (5) in the case $t=3$.

We will prove the following theorem.

THEOREM 1.2. *Assume $3l<p$ and $P_1,\dots,P_{3l-1};R_1,\dots,R_{3l-1}$ are p-integral rational numbers. If $\Phi(P_1,\dots,P_{3l-1}) \equiv c\Phi(R_1,\dots,R_{3l-1}) \pmod{p^3}$ for some constant $c\in\mathbb{Q}$, then*

$$\frac{P_m-R_m}{m} - p\frac{P_{l+m}-R_{l+m}}{l+m} + p^2\frac{P_{2l+m}-R_{2l+m}}{2l+m} \equiv 0 \pmod{p^3}$$

for each $m=1,\dots,l-1$.

Consequently, under the assumption of Theorem 1.1 we obtain

THEOREM 1.3. *If $3l<p$, then*

$$\alpha_m\left(\frac{S_m}{m} - p\frac{S_{l+m}}{l+m} + p^2\frac{S_{2l+m}}{2l+m}\right) \equiv f\left(\frac{T_m}{m} - p\frac{T_{l+m}}{l+m} + p^2\frac{T_{2l+m}}{2l+m}\right) \pmod{p^3}$$

for $m=1,\dots,l-1$ and

$$\pm\alpha_1\dots\alpha_{l-1} = h_K f^{l-2} \pmod{p^3}.$$

2. Analysis of the asumptions of Theorem 1.2

From now on, write $\Phi(P)$ for $\Phi(P_1,\dots,P_{3l-1})$, $\Phi(R)$ for $\Phi(R_1,\dots,R_{3l-1})$, $Y_m(P)$ for $Y_m(P_1,\dots,P_m)$ and $Y_m(R)$ for $Y_m(R_1,\dots,R_m)$ for each $m=1,\dots,3l-1$.

If $\Phi(P)\equiv c\Phi(R) \pmod{p^3}$, then

$$\frac{\Phi(P)}{1-pY_l(P)+p^2Y_{2l}(P)} \equiv \frac{\Phi(R)}{1-pY_l(R)+p^2Y_{2l}(R)} \pmod{p^3}. \tag{7}$$

From now on assume that $3l<p$, $P_1,\dots,P_{3l-1};R_1,\dots,R_{3l-1}$ are p-integral rational numbers and the above congrunce (7) is valid.

Using the congruence $\frac{1}{1-pa+p^2b} \equiv 1+pa+p^2(a^2-b) \pmod{p^3}$ one can infer that (7) is equivalent to a system of congruences

(8)
$$\begin{aligned} &Y_m(P)+p(Y_l(P)Y_m(P)-Y_{l+m}(P)) \\ &\quad +p^2(Y_l^2(P)Y_m(P)-Y_{2l}(P)Y_m(P)-Y_l(P)Y_{l+m}(P)+Y_{2l+m}(P)) \\ &\equiv Y_m(R)+p(Y_l(R)Y_m(R)-Y_{l+m}(R)) \\ &\quad +p^2(Y_l^2(R)Y_m(R)-Y_{2l}(R)Y_m(R)-Y_l(R)Y_{l+m}(R)+Y_{2l+m}(R)) \pmod{p^3} \end{aligned}$$

for $m=1,\dots,l-1$.

To analyze these congruences, we will strive to obtain formulas that will relate $Y_{2l+m}(P)-Y_{2l+m}(R)$ modulo p, $Y_{l+m}(P)-Y_{l+m}(R)$ modulo p^2 and $Y_m(P)-Y_m(R)$ modulo p^3 to expressions involving P_k-R_k and values of Y_i with smaller indices i. This will enable us to use an induction later.

First observe that by considering the "truncated" map Φ_2 defined by

$$\Phi_2(X_1,\dots,X_{2l-1})=\Phi(X_1,\dots,X_{2l-1},0,\dots,0)$$

we can repeat the proof of Lemma 2 of [JL]. In particular,

Proposition 2.1 ([JL]).

$$P_m \equiv R_m \pmod p, \qquad Y_m(P)\equiv Y_m(R) \pmod p \tag{9}$$

$$\frac{P_m-R_m}{m}-p\frac{P_{l+m}-R_{l+m}}{l+m}\equiv 0 \pmod{p^2} \tag{10}$$

for $m=1,\dots,l-1$ *and*

$$Y_{l+m}(P)-Y_{l+m}(R)\equiv -\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \pmod p \tag{11}$$

for $m=0,\dots,l-1$.

3. $Y_{2l+m}(P)-Y_{2l+m}(R)$ modulo p

Lemma 3.1.

$$\begin{aligned} &Y_{2l+m}(P)-Y_{2l+m}(R) \\ &\qquad \equiv -\sum_{i=0}^{l+m} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ &\qquad\quad +\frac{1}{2}\sum_{i=0}^{m} Y_{m-i}(R)\sum_{j=0}^{i}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \pmod p \end{aligned}$$

for $m=0,\dots,l-1$.

PROOF. By induction on m. For $m=0$ we have

$$\begin{aligned}
&Y_{2l}(P)-Y_{2l}(R)\\
&\quad=-\frac{1}{2l}\sum_{i=0}^{2l-1}P_{2l-i}Y_i(P)-R_{2l-i}Y_i(R)\\
&\quad=-\frac{1}{2l}\sum_{i=0}^{2l-1}P_{2l-i}(Y_i(P)-Y_i(R))-\frac{1}{2l}\sum_{i=0}^{2l-1}Y_i(R)(P_{2l-i}-R_{2l-i})\\
&\quad\equiv-\frac{1}{2l}\sum_{i=0}^{l-1}P_{l-i}(Y_{l+i}(P)-Y_{l+i}(R))-\frac{1}{2l}\sum_{i=0}^{l}Y_i(R)(P_{2l-i}-R_{2l-i})\\
&\quad\equiv\frac{1}{2l}\sum_{i=0}^{l-1}P_{l-i}\sum_{j=0}^{i}Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}-\frac{1}{2l}\sum_{i=0}^{l}Y_i(R)(P_{2l-i}-R_{2l-i})\pmod p
\end{aligned}$$

using (3),(9) and (11). Put $t=i-j$ and change the summation in the double sum to get

$$\begin{aligned}
&\sum_{i=0}^{l-1}P_{l-i}\sum_{j=0}^{i}Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\\
&\quad=\sum_{j=0}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{t=0}^{l-j-1}Y_t(R)P_{l-j-t}\\
&\quad=\sum_{j=0}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{t=0}^{l-j-1}Y_t(R)R_{l-j-t}+\sum_{j=0}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{t=0}^{l-j-1}Y_t(R)(P_{l-j-t}-R_{l-j-t})\\
&\quad\equiv-\sum_{j=0}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}(l-j)Y_{l-j}(R)+\frac{P_l-R_l}{l}(P_l-R_l)\pmod p
\end{aligned}$$

using (3) and (9).

Rewrite

$$\sum_{i=0}^{l}Y_i(R)(P_{2l-i}-R_{2l-i})=\sum_{j=0}^{l}Y_{l-j}(R)(P_{l+j}-R_{l+j})$$

to get

$$\begin{aligned}
&Y_{2l}(P)-Y_{2l}(R)\\
&\qquad\equiv-\frac{1}{2l}\sum_{j=0}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}(l-j)Y_{l-j}(R)-\frac{1}{2l}\sum_{j=0}^{l}Y_{l-j}(R)(P_{l+j}-R_{l+j})\\
&\qquad\quad+\frac{1}{2}\frac{P_l-R_l}{l}\frac{P_l-R_l}{l}\\
&\qquad\equiv-\sum_{j=0}^{l}Y_{l-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}+\frac{1}{2}\frac{P_l-R_l}{l}\frac{P_l-R_l}{l}\pmod p,
\end{aligned}$$

hence the statement is valid for $m=0$.

For the inductive step, write

$$
\begin{aligned}
&Y_{2l+m}(P) - Y_{2l+m}(R) \\
&\quad = -\frac{1}{2l+m} \sum_{i=0}^{2l+m-1} P_{2l+m-i}Y_i(P) - R_{2l+m-i}Y_i(R) \\
&\quad = -\frac{1}{2l+m} \sum_{i=0}^{2l+m-1} P_{2l+m-i}(Y_i(P) - Y_i(R)) \\
&\qquad - \frac{1}{2l+m} \sum_{i=0}^{2l+m-1} Y_i(R)(P_{2l+m-i} - R_{2l+m-i}) \\
&\quad \equiv -\frac{1}{2l+m} \sum_{i=0}^{l-1} P_{l+m-i}(Y_{l+i}(P) - Y_{l+i}(R)) \\
&\qquad - \frac{1}{2l+m} \sum_{i=0}^{m-1} P_{m-i}(Y_{2l+i}(P) - Y_{2l+i}(R)) \\
&\qquad - \frac{1}{2l+m} \sum_{i=0}^{l+m} Y_i(R)(P_{2l+m-i} - R_{2l+m-i}) \pmod p
\end{aligned}
$$

using (3) and (9). Further, using (11) and the inductive assumption we obtain

$$
\begin{aligned}
&Y_{2l+m}(P) - Y_{2l+m}(R) \\
&\quad \equiv \frac{1}{2l+m} \sum_{i=0}^{l-1} P_{l+m-i} \sum_{j=0}^{i} Y_{i-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j} \\
&\qquad + \frac{1}{2l+m} \sum_{i=0}^{m-1} P_{m-i} \sum_{j=0}^{l+i} Y_{l+i-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j} \\
&\qquad - \frac{1}{2}\frac{1}{2l+m} \sum_{i=0}^{m-1} P_{m-i} \sum_{k=0}^{i} Y_{i-k}(R) \sum_{j=0}^{k} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+k-j} - R_{l+k-j}}{l+k-j} \\
&\qquad - \frac{1}{2l+m} \sum_{i=0}^{l+m} Y_i(R)(P_{2l+m-i} - R_{2l+m-i}) \pmod p.
\end{aligned}
$$

Combine the two terms

$$
\sum_{i=0}^{l-1} P_{l+m-i} \sum_{j=0}^{i} Y_{i-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j} + \sum_{i=0}^{m-1} P_{m-i} \sum_{j=0}^{l+i} Y_{l+i-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j}
$$

into

$$\sum_{i=0}^{l+m-1} P_{l+m-i} \sum_{j=0}^{i} Y_{i-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j}$$
$$= \sum_{j=0}^{l+m-1} \frac{P_{l+j} - R_{l+j}}{l+j} \sum_{t=0}^{l+m-j-1} Y_t(R) P_{l+m-j-t}$$
$$= \sum_{j=0}^{l+m-1} \frac{P_{l+j} - R_{l+j}}{l+j} \sum_{t=0}^{l+m-j-1} Y_t(R) R_{l+m-j-t}$$
$$+ \sum_{j=0}^{l+m-1} \frac{P_{l+j} - R_{l+j}}{l+j} \sum_{t=0}^{l+m-j-1} Y_t(R)(P_{l+m-j-t} - R_{l+m-j-t})$$
$$= - \sum_{j=0}^{l+m-1} \frac{P_{l+j} - R_{l+j}}{l+j} (l+m-j) Y_{l+m-j}(R)$$
$$+ \sum_{j=0}^{m} \frac{P_{l+j} - R_{l+j}}{l+j} \sum_{t=0}^{m-j} Y_t(R)(P_{l+m-j-t} - R_{l+m-j-t})$$

by changing the summation using $t = i - j$, and using (3) and (9).

Rewrite

$$\sum_{i=0}^{l+m} Y_i(R)(P_{2l+m-i} - R_{2l+m-i}) = \sum_{j=0}^{l+m} Y_{l+m-j}(R)(P_{l+j} - R_{l+j})$$

and obtain

$$Y_{2l+m}(P) - Y_{2l+m}(R)$$
$$\equiv -\frac{1}{2l+m} \sum_{j=0}^{l+m-1} \frac{P_{l+j} - R_{l+j}}{l+j} (l+m-j) Y_{l+m-j}(R)$$
$$- \frac{1}{2l+m} \sum_{j=0}^{l+m} Y_{l+m-j}(R)(P_{l+j} - R_{l+j})$$
$$- \frac{1}{2} \frac{1}{2l+m} \sum_{i=0}^{m-1} P_{m-i} \sum_{k=0}^{i} Y_{i-k}(R) \sum_{j=0}^{k} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+k-j} - R_{l+k-j}}{l+k-j}$$
$$+ \frac{1}{2l+m} \sum_{j=0}^{m} \frac{P_{l+j} - R_{l+j}}{l+j} \sum_{t=0}^{m-j} Y_t(R)(P_{l+m-j-t} - R_{l+m-j-t}) \pmod{p}.$$

The first two terms combine to

$$- \sum_{j=0}^{l+m} Y_{l+m-j}(R) \frac{P_{l+j} - R_{l+j}}{l+j}.$$

Change the order of summations in the remaining two terms and set $t = i - k$ and $k = m - t$, respectively, to rewrite these terms as follows:

$$
\begin{aligned}
&-\frac{1}{2}\frac{1}{2l+m}\sum_{k=0}^{m-1}\sum_{t=0}^{m-k-1} P_{m-k-t}Y_t(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+k-j}-R_{l+k-j}}{l+k-j}\\
&+\frac{1}{2l+m}\sum_{k=0}^{m}Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}(P_{l+k-j}-R_{l+k-j})\\
\equiv{}&\frac{1}{2}\frac{1}{2l+m}\sum_{k=0}^{m-1}(m-k)Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+k-j}-R_{l+k-j}}{l+k-j}\\
&+\frac{1}{2l+m}\sum_{k=0}^{m}Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}(P_{l+k-j}-R_{l+k-j}) \pmod p
\end{aligned}
$$

using (3) and (9).

The coefficients at $Y_{m-k}(R)(P_{l+j} - R_{l+j})(P_{l+k-j} - R_{l+k-j})$ in the previous expression and in the expression

$$
\frac{1}{2}\sum_{k=0}^{m}Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+k-j}-R_{l+k-j}}{l+k-j}
$$

are the same. Namely, if $j \neq \frac{k}{2}$, then the coefficient at

$$
Y_{m-k}(R)(P_{l+j} - R_{l+j})(P_{l+k-j} - R_{l+k-j})
$$

in the former expression equals

$$
\frac{1}{2l+m}\left(\frac{1}{2}\frac{2(m-k)}{(l+k-j)(l+j)}+\frac{1}{l+j}+\frac{1}{l+k-j}\right)=\frac{1}{(l+k-j)(l+j)};
$$

if $j = \frac{k}{2}$, then it equals

$$
\frac{1}{2l+m}\left(\frac{m-2j}{2(l+j)^2}+\frac{1}{l+j}\right)=\frac{1}{2(l+j)^2}.
$$

Therefore

$$
\begin{aligned}
&\frac{1}{2}\frac{1}{2l+m}\sum_{k=0}^{m-1}(m-k)Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+k-j}-R_{l+k-j}}{l+k-j}\\
&+\frac{1}{2l+m}\sum_{k=0}^{m}Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}(P_{l+k-j}-R_{l+k-j})\\
={}&\frac{1}{2}\sum_{k=0}^{m}Y_{m-k}(R)\sum_{j=0}^{k}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+k-j}-R_{l+k-j}}{l+k-j},
\end{aligned}
$$

which concludes the proof of the lemma. □

It is possible to start with a different starting setup, namely, instead of

$$Y_{2l+m}(P) - Y_{2l+m}(R) = -\frac{1}{2l+m}\sum_{i=0}^{2l+m-1} P_{2l+m-i}(Y_i(P) - Y_i(R)) - \frac{1}{2l+m}\sum_{i=0}^{2l+m-1} Y_i(R)(P_{2l+m-i} - R_{2l+m-i})$$

one can write

$$Y_{2l+m}(P) - Y_{2l+m}(R) = -\frac{1}{2l+m}\sum_{i=0}^{2l+m-1} R_{2l+m-i}(Y_i(P) - Y_i(R)) - \frac{1}{2l+m}\sum_{i=0}^{2l+m-1} Y_i(P)(P_{2l+m-i} - R_{2l+m-i}).$$

We will apply this approach in the next sections.

4. $Y_{l+m}(P) - Y_{l+m}(R)$ modulo p^2

LEMMA 4.1.

$$Y_m(P) - Y_m(R) \equiv -p\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} \pmod{p^2}$$

for $m = 1, \ldots, l-1$.

PROOF. Consider (8) modulo p^2 and use (9) and (11) to write

$$\begin{aligned} Y_m(P) - Y_m(R) &\equiv p(Y_{l+m}(P) - Y_{l+m}(R)) - pY_m(R)(Y_l(P) - Y_l(R)) \\ &\equiv -p\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} + pY_m(R)\frac{P_l - R_l}{l} \\ &= -p\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} \pmod{p^2}. \end{aligned}$$

□

LEMMA 4.2.

$$\begin{aligned} Y_{l+m}(P) - Y_{l+m}(R) \equiv & -\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} - p\sum_{i=1}^{l-1} Y_{l+m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} \\ & + p\sum_{i=1}^{m} Y_{m-i}(R)\sum_{j=1}^{i}\frac{P_{l+j} - R_{l+j}}{l+j}\,\frac{P_{l+i-j} - R_{l+i-j}}{l+i-j} \pmod{p^2} \end{aligned}$$

for each $m = 0, \ldots, l-1$.

PROOF. By induction on m. For the basic step $m=0$, first use (3), Lemma 4.1 and (10) to derive

$$\begin{aligned} Y_l(P)-Y_l(R) &= -\frac{P_l-R_l}{l} - \frac{1}{l}\sum_{i=1}^{l-1} R_{l-i}(Y_i(P)-Y_i(R)) \\ &\quad - \frac{1}{l}\sum_{i=1}^{l-1} Y_i(P)(P_{l-i}-R_{l-i}) \\ &\equiv -\frac{P_l-R_l}{l} + p\frac{1}{l}\sum_{i=1}^{l-1} R_{l-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\ &\quad - p\frac{1}{l}\sum_{i=1}^{l-1} Y_i(P)(l-i)\frac{P_{2l-i}-R_{2l-i}}{2l-i} \pmod{p^2}. \end{aligned}$$

Changing the order of summation, using (9), putting $j=l-i$, and rearranging, we obtain that

$$\begin{aligned} Y_l(P)-Y_l(R) &\equiv -\frac{P_l-R_l}{l} + p\frac{1}{l}\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{i=j}^{l-1} R_{l-i}Y_{i-j}(R) \\ &\quad - p\frac{1}{l}\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j} jY_{l-j}(R) \pmod{p^2}. \end{aligned}$$

Since

$$\sum_{i=j}^{l-1} R_{l-i}Y_{i-j}(R) = \sum_{k=0}^{l-j-1} R_{l-j-k}Y_k(R) = -(l-j)Y_{l-j}(R)$$

by (3), we conclude that

$$Y_l(P)-Y_l(R) \equiv -\frac{P_l-R_l}{l} - p\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}Y_{l-j}(R) \pmod{p^2}.$$

For the inductive step, assume that the congruence is valid for all nonnegative integers smaller than m and consider

$$\begin{aligned} &Y_{l+m}(P)-Y_{l+m}(R) \\ &\quad = -\frac{P_{l+m}-R_{l+m}}{l+m} - \frac{1}{l+m}\sum_{i=1}^{l+m-1} R_{l+m-i}(Y_i(P)-Y_i(R)) \\ &\quad\quad - \frac{1}{l+m}\sum_{i=1}^{l+m-1} Y_i(P)(P_{l+m-i}-R_{l+m-i}) \end{aligned}$$

$$
\begin{aligned}
&= -\frac{P_{l+m}-R_{l+m}}{l+m} - \frac{1}{l+m}\sum_{i=1}^{l-1} R_{l+m-i}(Y_i(P)-Y_i(R)) \\
&\quad - \frac{1}{l+m}\sum_{i=l}^{l+m-1} R_{l+m-i}(Y_i(P)-Y_i(R)) \\
&\quad - \frac{1}{l+m}\sum_{i=1}^{l+m-1} Y_i(R)(P_{l+m-i}-R_{l+m-i}) \\
&\quad - \frac{1}{l+m}\sum_{i=1}^{l+m-1} (Y_i(P)-Y_i(R))(P_{l+m-i}-R_{l+m-i}).
\end{aligned}
$$

This expression is congruent to

$$
\begin{aligned}
&-\frac{P_{l+m}-R_{l+m}}{l+m} + p\frac{1}{l+m}\sum_{i=1}^{l-1} R_{l+m-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
&+\frac{1}{l+m}\sum_{i=0}^{m-1} R_{m-i}\sum_{j=0}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
&+p\frac{1}{l+m}\sum_{i=l}^{l+m-1} R_{l+m-i}\sum_{j=1}^{l-1} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
&-p\frac{1}{l+m}\sum_{i=1}^{m-1} R_{m-i}\sum_{t=1}^{i} Y_{i-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \\
&-\frac{1}{l+m}\sum_{i=m+1}^{l+m-1} Y_i(R)(P_{l+m-i}-R_{l+m-i}) \\
&-\frac{1}{l+m}\sum_{i=1}^{m} Y_i(R)(P_{l+m-i}-R_{l+m-i}) \\
&-\frac{1}{l+m}\sum_{i=1}^{m}(Y_i(P)-Y_i(R))(P_{l+m-i}-R_{l+m-i}) \\
&-\frac{1}{l+m}\sum_{i=0}^{m-1}(Y_{l+i}(P)-Y_{l+i}(R))(P_{m-i}-R_{m-i}) \pmod{p^2}
\end{aligned}
$$

by (3), Lemma 4.1, the inductive assumption and (9).

Next, we will group like terms and simplify.

Change the order of summation, substitute $j = m - i$ and apply (3) to get

$$
\begin{aligned}
&-\frac{P_{l+m}-R_{l+m}}{l+m}+\frac{1}{l+m}\sum_{i=0}^{m-1}R_{m-i}\sum_{j=0}^{i}Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\\
&-\frac{1}{l+m}\sum_{i=1}^{m}Y_i(R)(P_{l+m-i}-R_{l+m-i})\\
\equiv\ &-\frac{P_{l+m}-R_{l+m}}{l+m}+\frac{1}{l+m}\sum_{j=0}^{m-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{i=j}^{m-1}R_{m-i}Y_{i-j}(R)\\
&-\frac{1}{l+m}\sum_{j=0}^{m-1}Y_{m-j}(R)(P_{l+j}-R_{l+j})\\
\equiv\ &-\frac{P_{l+m}-R_{l+m}}{l+m}-\frac{1}{l+m}\sum_{j=0}^{m-1}\frac{P_{l+j}-R_{l+j}}{l+j}(m-j)Y_{m-j}(R)\\
&-\frac{1}{l+m}\sum_{j=0}^{m-1}(P_{l+j}-R_{l+j})Y_{m-j}(R)\\
=\ &-\sum_{j=0}^{m}Y_{m-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\pmod{p^2}.
\end{aligned}
$$

Change the order of summation twice, apply (10) and (3) to infer

$$
\begin{aligned}
&p\frac{1}{l+m}\sum_{i=1}^{l-1}R_{l+m-i}\sum_{j=1}^{i}Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\\
&+p\frac{1}{l+m}\sum_{i=l}^{l+m-1}R_{l+m-i}\sum_{j=1}^{l-1}Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\\
&-\frac{1}{l+m}\sum_{i=m+1}^{l+m-1}Y_i(R)(P_{l+m-i}-R_{l+m-i})\\
\equiv\ &p\frac{1}{l+m}\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{i=j}^{l-1}R_{l+m-i}Y_{i-j}(R)\\
&+p\frac{1}{l+m}\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{i=l}^{l+m-1}R_{l+m-i}Y_{i-j}(R)\\
&-p\frac{1}{l+m}\sum_{i=1}^{l-1}Y_{m+i}(R)(l-i)\frac{P_{2l-i}-R_{2l-i}}{2l-i}\pmod{p^2}.
\end{aligned}
$$

The right hand side equals

$$
\begin{aligned}
& p\frac{1}{l+m}\sum_{j=1}^{l-1}\frac{P_{l+j}-R_{l+j}}{l+j}\sum_{i=j}^{l+m-1} R_{l+m-i}Y_{i-j}(R) \\
& -p\frac{1}{l+m}\sum_{j=1}^{l-1} jY_{l+m-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
= & -p\frac{1}{l+m}\sum_{j=1}^{l-1}(l+m-j)Y_{l+m-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
& -p\frac{1}{l+m}\sum_{j=1}^{l-1} jY_{l+m-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j} \\
= & -p\sum_{j=1}^{l-1} Y_{l+m-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}.
\end{aligned}
$$

Put $s = m - i$, change the summation and use (3) to get

$$
\begin{aligned}
& -p\frac{1}{l+m}\sum_{i=1}^{m-1} R_{m-i}\sum_{t=1}^{i} Y_{i-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \\
= & -p\frac{1}{l+m}\sum_{t=1}^{m-1}\Big(\sum_{s=1}^{m-t} Y_{m-s-t}(R)R_s\Big)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \\
= & \, p\frac{1}{l+m}\sum_{t=1}^{m-1}(m-t)Y_{m-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j}.
\end{aligned}
$$

Use Lemma 4.1, put $t = m - i + j$ and change the summation to obtain

$$
\begin{aligned}
& -\frac{1}{l+m}\sum_{i=1}^{m}(Y_i(P)-Y_i(R))(P_{l+m-i}-R_{l+m-i}) \\
\equiv & \, p\frac{1}{l+m}\sum_{i=1}^{m}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}(P_{l+m-i}-R_{l+m-i}) \\
\equiv & \, p\frac{1}{l+m}\sum_{t=1}^{m} Y_{m-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}(P_{l+t-j}-R_{l+t-j}) \pmod{p^2}.
\end{aligned}
$$

Use (10), (11), put $t = m - i + j$ and change the summation to infer

$$\begin{aligned}
&-\frac{1}{l+m}\sum_{i=0}^{m-1}(Y_{l+i}(P) - Y_{l+i}(R))(P_{m-i} - R_{m-i})\\
&\equiv p\frac{1}{l+m}\sum_{i=0}^{m-1}\sum_{j=0}^{i}(m-i)Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+m-i}-R_{l+m-i}}{l+m-i}\\
&\equiv p\frac{1}{l+m}\sum_{t=1}^{m}Y_{m-t}(R)\sum_{j=0}^{t-1}(t-j)\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j}\\
&\equiv p\frac{1}{l+m}\sum_{t=1}^{m}Y_{m-t}(R)\sum_{j=1}^{t}j\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \pmod{p^2}.
\end{aligned}$$

Therefore

$$\begin{aligned}
&-p\frac{1}{l+m}\sum_{i=1}^{m-1}R_{m-i}\sum_{t=1}^{i}Y_{i-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j}\\
&-\frac{1}{l+m}\sum_{i=1}^{m}(Y_i(P) - Y_i(R))(P_{l+m-i} - R_{l+m-i})\\
&-\frac{1}{l+m}\sum_{i=0}^{m-1}(Y_{l+i}(P) - Y_{l+i}(R))(P_{m-i} - R_{m-i})\\
&\equiv p\frac{1}{l+m}\sum_{t=1}^{m}Y_{m-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j}((m-t)+(l+t-j)+j)\\
&= p\sum_{t=1}^{m}Y_{m-t}(R)\sum_{j=1}^{t}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \pmod{p^2}.
\end{aligned}$$

Put all terms together to finish the proof. □

5. $Y_m(P) - Y_m(R)$ modulo p^3

LEMMA 5.1.

$$\begin{aligned}
Y_m(P) - Y_m(R) \equiv\ & -p\sum_{i=1}^{m}Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} + p^2\sum_{i=1}^{m}Y_{m-i}(R)\frac{P_{2l+i}-R_{2l+i}}{2l+i}\\
&+\frac{1}{2}p^2\sum_{i=2}^{m}Y_{m-i}(R)\sum_{j=1}^{i-1}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \pmod{p^3}
\end{aligned}$$

for each $m = 1, \ldots, l-1$.

PROOF. According to (8) we have

$$\begin{aligned}
&Y_m(P) - Y_m(R)\\
&\equiv -p(Y_l(P)Y_m(P) - Y_l(R)Y_m(R)) + p(Y_{l+m}(P) - Y_{l+m}(R))\\
&\quad - p^2(Y_l^2(P)Y_m(P) - Y_l^2(R)Y_m(R)) + p^2(Y_{2l}(P)Y_m(P) - Y_{2l}(R)Y_m(R))\\
&\quad + p^2(Y_l(P)Y_{l+m}(P) - Y_l(R)Y_{l+m}(R)) - p^2(Y_{2l+m}(P) - Y_{2l+m}(R)) \pmod{p^3}.
\end{aligned}$$

Using (9) we rearrange

$$\begin{aligned}
&Y_m(P) - Y_m(R)\\
&\quad\equiv -pY_m(P)(Y_l(P) - Y_l(R)) - pY_l(R)(Y_m(P) - Y_m(R))\\
&\quad\quad + p(Y_{l+m}(P) - Y_{l+m}(R)) - p^2Y_l^2(P)(Y_m(P) - Y_m(R))\\
&\quad\quad - p^2Y_l(P)Y_m(R)(Y_l(P) - Y_l(R)) - p^2Y_l(R)Y_m(R)(Y_l(P) - Y_l(R))\\
&\quad\quad + p^2Y_m(P)(Y_{2l}(P) - Y_{2l}(R)) + p^2Y_{2l}(R)(Y_m(P) - Y_m(R))\\
&\quad\quad + p^2Y_{l+m}(P)(Y_l(P) - Y_l(R)) + p^2Y_l(R)(Y_{l+m}(P) - Y_{l+m}(R))\\
&\quad\quad - p^2(Y_{2l+m}(P) - Y_{2l+m}(R))\\
&\quad\equiv -pY_m(R)(Y_l(P) - Y_l(R)) - p(Y_m(P) - Y_m(R))(Y_l(P) - Y_l(R))\\
&\quad\quad - pY_l(R)(Y_m(P) - Y_m(R)) + p(Y_{l+m}(P) - Y_{l+m}(R))\\
&\quad\quad - 2p^2Y_l(R)Y_m(R)(Y_l(P) - Y_l(R)) - p^2Y_m(R)(Y_l(P) - Y_l(R))^2\\
&\quad\quad + p^2Y_m(R)(Y_{2l}(P) - Y_{2l}(R)) + p^2Y_{l+m}(R)(Y_l(P) - Y_l(R))\\
&\quad\quad + p^2(Y_{l+m}(P) - Y_{l+m}(R))(Y_l(P) - Y_l(R))\\
&\quad\quad + p^2Y_l(R)(Y_{l+m}(P) - Y_{l+m}(R)) - p^2(Y_{2l+m}(P) - Y_{2l+m}(R)) \pmod{p^3}.
\end{aligned}$$

Next, we expand the summands of the last expression:

$$\begin{aligned}
-pY_m(R)(Y_l(P) - Y_l(R)) &\equiv pY_m(R)\frac{P_l - R_l}{l}\\
&\quad + p^2Y_m(R)\sum_{i=1}^{l-1} Y_{l-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} \pmod{p^3}
\end{aligned}$$

by Lemma 4.2;

$$-p(Y_m(P)-Y_m(R))(Y_l(P)-Y_l(R)) \equiv -p^2\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}\,\frac{P_l-R_l}{l} \pmod{p^3}$$

by Lemma 4.1 and (11);

$$-pY_l(R)(Y_m(P) - Y_m(R)) \equiv p^2Y_l(R)\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} \pmod{p^3}$$

by Lemma 4.1;

$$\begin{aligned} p(Y_{l+m}(P) - Y_{l+m}(R)) \\ \equiv -p\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} - p^2\sum_{i=1}^{l-1} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ + p^2\sum_{i=1}^{m} Y_{m-i}(R)\sum_{j=1}^{i}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \pmod{p^3} \end{aligned}$$

by Lemma 4.2;

$$\begin{aligned} -2p^2Y_l(R)Y_m(R)(Y_l(P)-Y_l(R)) - p^2Y_m(R)(Y_l(P)-Y_l(R))^2 \\ \equiv 2p^2Y_l(R)Y_m(R)\frac{P_l-R_l}{l} - p^2Y_m(R)\left(\frac{P_l-R_l}{l}\right)^2 \pmod{p^3} \end{aligned}$$

by (11);

$$\begin{aligned} p^2Y_m(R)(Y_{2l}(P)-Y_{2l}(R)) \\ \equiv -p^2Y_m(R)\sum_{i=0}^{l} Y_{l-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} + \frac{1}{2}p^2Y_m(R)\left(\frac{P_l-R_l}{l}\right)^2 \pmod{p^3} \end{aligned}$$

by Lemma 3.1;

$$p^2Y_{l+m}(R)(Y_l(P)-Y_l(R)) \equiv -p^2Y_{l+m}(R)\frac{P_l-R_l}{l} \pmod{p^3}$$

by (11);

$$\begin{aligned} p^2(Y_{l+m}(P)-Y_{l+m}(R))(Y_l(P)-Y_l(R)) \\ \equiv p^2\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}\frac{P_l-R_l}{l} \pmod{p^3} \end{aligned}$$

by (11);

$$p^2Y_l(R)(Y_{l+m}(P)-Y_{l+m}(R)) \equiv -p^2Y_l(R)\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \pmod{p^3}$$

by (11);

$$\begin{aligned} -p^2(Y_{2l+m}(P)-Y_{2l+m}(R)) \\ \equiv p^2\sum_{i=0}^{l+m} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ -\frac{1}{2}p^2\sum_{i=0}^{m} Y_{m-i}(R)\sum_{j=0}^{i}\frac{P_{l+j}-R_{l+j}}{l+j}\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \pmod{p^3} \end{aligned}$$

by Lemma 3.1.

Further, we collect like terms and simplify

$$pY_m(R)\frac{P_l-R_l}{l} - p\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} = -p\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i};$$

$$\begin{aligned} p^2Y_m(R)\sum_{i=1}^{l-1} Y_{l-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} &- p^2Y_m(R)\sum_{i=0}^{l} Y_{l-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ &= -p^2Y_m(R)Y_l(R)\frac{P_l-R_l}{l} - p^2Y_m(R)\frac{P_{2l}-R_{2l}}{2l}; \end{aligned}$$

$$\begin{aligned} & p^2Y_l(R)\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} + 2p^2Y_l(R)Y_m(R)\frac{P_l-R_l}{l} \\ & - p^2Y_l(R)\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ &= p^2Y_l(R)Y_m(R)\frac{P_l-R_l}{l}; \end{aligned}$$

$$\begin{aligned} -p^2\sum_{i=1}^{l-1} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} &- p^2Y_{l+m}(R)\frac{P_l-R_l}{l} + p^2\sum_{i=0}^{l+m} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ &= p^2Y_{l+m}(R)\frac{P_l-R_l}{l} - p^2Y_{l+m}(R)\frac{P_l-R_l}{l} + p^2\sum_{i=l}^{l+m} Y_{l+m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i} \\ &\equiv p^2\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{2l+i}-R_{2l+i}}{2l+i} \pmod{p^3} \end{aligned}$$

and

$$\begin{aligned} & -p^2\sum_{i=1}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}\,\frac{P_l-R_l}{l} \\ & + p^2\sum_{i=1}^{m} Y_{m-i}(R)\sum_{j=1}^{i} \frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \\ & - p^2Y_m(R)(\frac{P_l-R_l}{l})^2 + \frac{1}{2}p^2Y_m(R)\left(\frac{P_l-R_l}{l}\right)^2 \\ & + p^2\sum_{i=0}^{m} Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}\,\frac{P_l-R_l}{l} \\ & - \frac{1}{2}p^2\sum_{i=0}^{m} Y_{m-i}(R)\sum_{j=0}^{i} \frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \end{aligned}$$

$$= p^2 \sum_{i=1}^{m} Y_{m-i}(R) \sum_{j=1}^{i} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}$$
$$- \frac{1}{2}p^2 \sum_{i=1}^{m} Y_{m-i}(R) \sum_{j=0}^{i} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}$$
$$= p^2 \sum_{i=1}^{m} Y_{m-i}(R) \sum_{j=1}^{i-1} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}$$
$$+ p^2 \sum_{i=1}^{m} Y_{m-i}(R) \frac{P_{l+i} - R_{l+i}}{l+i} \frac{P_l - R_l}{l}$$
$$- \frac{1}{2}p^2 \sum_{i=1}^{m} Y_{m-i}(R) \sum_{j=1}^{i-1} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}$$
$$- p^2 \sum_{i=1}^{m} Y_{m-i}(R) \frac{P_{l+i} - R_{l+i}}{l+i} \frac{P_l - R_l}{l}$$
$$= \frac{1}{2}p^2 \sum_{i=2}^{m} Y_{m-i}(R) \sum_{j=1}^{i-1} \frac{P_{l+j} - R_{l+j}}{l+j} \frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}.$$

Putting all terms together concludes the proof. □

6. Proof of Theorem 1.2

PROOF. We proceed by induction on m. Lemma 5.1 applied to $m = 1$ states that

$$Y_1(P) - Y_1(R) = -(P_1 - R_1) \equiv -p\frac{P_{l+1} - R_{l+1}}{l+1} + p^2 \frac{P_{2l+1} - R_{2l+1}}{2l+1} \pmod{p^3}$$

which proves the statement of the theorem for $m = 1$.

Assume that the theorem is valid for every positive integer smaller than m and consider $Y_m(P) - Y_m(R) \pmod{p^3}$. Using (3), the inductive assumption and Lemma 5.1 we obtain

$$Y_m(P) - Y_m(R)$$
$$= -\frac{P_m - R_m}{m} - \frac{1}{m}\sum_{i=1}^{m-1} Y_i(P)(P_{m-i} - R_{m-i}) - \frac{1}{m}\sum_{i=1}^{m-1} R_{m-i}(Y_i(P) - Y_i(R))$$
$$= -\frac{P_m - R_m}{m} - \frac{1}{m}\sum_{i=1}^{m-1} Y_{m-i}(P)(P_i - R_i) - \frac{1}{m}\sum_{i=1}^{m-1} R_{m-i}(Y_i(P) - Y_i(R))$$

$$\equiv -\frac{P_m-R_m}{m}-\frac{1}{m}p\sum_{i=1}^{m-1} iY_{m-i}(P)\frac{P_{l+i}-R_{l+i}}{l+i}+\frac{1}{m}p^2\sum_{i=1}^{m-1} iY_{m-i}(P)\frac{P_{2l+i}-R_{2l+i}}{2l+i}$$
$$+\frac{1}{m}p\sum_{i=1}^{m-1} R_{m-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}$$
$$-\frac{1}{m}p^2\sum_{i=1}^{m-1} R_{m-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{2l+j}-R_{2l+j}}{2l+j}$$
$$-\frac{1}{2m}p^2\sum_{i=2}^{m-1} R_{m-i}\sum_{t=2}^{i} Y_{i-t}(R)\sum_{j=1}^{t-1}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j} \pmod{p^3}.$$

Switch the summation in the last three terms and use (3) to obtain

$$\frac{1}{m}p\sum_{i=1}^{m-1} R_{m-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}$$
$$-\frac{1}{m}p^2\sum_{i=1}^{m-1} R_{m-i}\sum_{j=1}^{i} Y_{i-j}(R)\frac{P_{2l+j}-R_{2l+j}}{2l+j}$$
$$-\frac{1}{2m}p^2\sum_{i=2}^{m-1} R_{m-i}\sum_{t=2}^{i} Y_{i-t}(R)\sum_{j=1}^{t-1}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+t-j}-R_{l+t-j}}{l+t-j}$$
$$\equiv -\frac{1}{m}p\sum_{i=1}^{m-1}(m-i)Y_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}+\frac{1}{m}p^2\sum_{i=1}^{m-1}(m-i)Y_{m-i}(R)\frac{P_{2l+i}-R_{2l+i}}{2l+i}$$
$$+\frac{1}{2m}p^2\sum_{i=2}^{m-1}(m-i)Y_{m-i}(R)\sum_{j=1}^{i-1}\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+i-j}-R_{l+i-j}}{l+i-j} \pmod{p^3}.$$

Further, use Lemma 4.1 to infer

$$-\frac{1}{m}p\sum_{i=1}^{m-1} iY_{m-i}(P)\frac{P_{l+i}-R_{l+i}}{l+i}$$
$$= -\frac{1}{m}p\sum_{i=1}^{m-1} iY_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}$$
$$-\frac{1}{m}p\sum_{i=1}^{m-1} i(Y_{m-i}(P)-Y_{m-i}(R))\frac{P_{l+i}-R_{l+i}}{l+i}$$
$$\equiv -\frac{1}{m}p\sum_{i=1}^{m-1} iY_{m-i}(R)\frac{P_{l+i}-R_{l+i}}{l+i}$$
$$+\frac{1}{m}p^2\sum_{i=1}^{m-1} i\sum_{j=1}^{m-i} Y_{m-i-j}(R)\frac{P_{l+j}-R_{l+j}}{l+j}\,\frac{P_{l+i}-R_{l+i}}{l+i} \pmod{p^3}.$$

Therefore using (9) we get

$$
\begin{aligned}
&Y_m(P) - Y_m(R) \\
&\equiv -\frac{P_m - R_m}{m} - p\sum_{i=1}^{m-1} Y_{m-i}(R)\frac{P_{l+i} - R_{l+i}}{l+i} + p^2 \sum_{i=1}^{m-1} Y_{m-i}(R)\frac{P_{2l+i} - R_{2l+i}}{2l+i} \\
&+ \frac{1}{m}p^2 \sum_{i=1}^{m-1} i \sum_{j=1}^{m-i} Y_{m-i-j}(R)\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i} - R_{l+i}}{l+i} \\
&+ \frac{1}{2m}p^2 \sum_{i=2}^{m}(m-i)Y_{m-i}(R)\sum_{j=1}^{i-1}\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i-j} - R_{l+i-j}}{l+i-j} \pmod{p^3}.
\end{aligned}
$$

Applying Lemma 5.1 we obtain

$$
\begin{aligned}
&Y_m(P) - Y_m(R) \\
&\equiv Y_m(P) - Y_m(R) - \frac{P_m - R_m}{m} + p\frac{P_{l+m} - R_{l+m}}{l+m} - p^2\frac{P_{2l+m} - R_{2l+m}}{2l+m} \\
&+ \frac{1}{m}p^2 \sum_{i=1}^{m-1} i \sum_{j=1}^{m-i} Y_{m-i-j}(R)\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i} - R_{l+i}}{l+i} \\
&- \frac{1}{2m}p^2 \sum_{i=2}^{m} iY_{m-i}(R)\sum_{j=1}^{i-1}\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i-j} - R_{l+i-j}}{l+i-j} \pmod{p^3}.
\end{aligned}
$$

The theorem will be proved if we show that

$$
\begin{aligned}
&2\sum_{i=1}^{m-1} i \sum_{j=1}^{m-i} Y_{m-i-j}(R)\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i} - R_{l+i}}{l+i} \\
&\qquad = \sum_{i=2}^{m} iY_{m-i}(R)\sum_{j=1}^{i-1}\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i-j} - R_{l+i-j}}{l+i-j}.
\end{aligned}
$$

To verify this, change the summation in the first sum and put $t = i + j$ to get

$$
\begin{aligned}
&2\sum_{i=1}^{m-1} i \sum_{j=1}^{m-i} Y_{m-i-j}(R)\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+i} - R_{l+i}}{l+i} \\
&\qquad = \sum_{t=2}^{m} Y_{m-t}(R)\sum_{j=1}^{t-1}(t-j)\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+t-j} - R_{l+t-j}}{l+t-j} \\
&\qquad + \sum_{t=2}^{m} Y_{m-t}(R)\sum_{j=1}^{t-1} j\frac{P_{l+t-j} - R_{l+t-j}}{l+t-j}\frac{P_{l+j} - R_{l+j}}{l+j} \\
&\qquad = \sum_{t=2}^{m} tY_{m-t}(R)\sum_{j=1}^{t-1}\frac{P_{l+j} - R_{l+j}}{l+j}\frac{P_{l+t-j} - R_{l+t-j}}{l+t-j}.
\end{aligned}
$$

□

Acknowledgement. I would like to thank the referee for valuable suggestions that helped me to improve the first section of this paper.

References

[J1] Jakubec S., *The congruence for Gauss period*, Journal of Number Theory **48** (1994), 36–45.

[J2] Jakubec S., *On the Vandiver's conjecture*, Abh. Math. Sem. Univ. Hamburg **64** (1994), 105–124.

[J3] Jakubec S., *Congruence of Ankeny–Artin–Chowla type for cyclic fields of prime degree l*, Math. Proc. Cambridge. Philos. Soc. **119** (1996), 17–22.

[J4] Jakubec S., *Congruence of Ankeny–Artin–Chowla type modulo p^2 for cyclic fields of prime degree l*, Acta Arithmetica **74** (1996), 293–310.

[J5] Jakubec S., *Congruence of Ankeny–Artin–Chowla type for cyclic fields*, Math. Slovaca **48** (1998), 323–326.

[J6] Jakubec S., *Note on the congruence of Ankeny–Artin–Chowla type modulo p^2*, Acta Arithmetica **85** (1998), 377–388.

[JL] Jakubec S., Laššák M., *Congruence of Ankeny–Artin–Chowla type modulo p^2*, Annales Mathematicae Silesianae **12** (1998), 75–92.

[M] Marko F., *On the existence of p-units and Minkowski units in totally real cyclic fields*, Abh. Math. Sem. Univ. Hamburg **66** (1996), 89–111.

[S] Sinnott W., *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

Pennsylvania State University
76 University Drive
Hazleton, PA 18202
USA
e-mail: fxm13@psu.edu