数理解析研究所講究録
第759巻 1991年 198-209


# Eisenstein の積公式の種数 2 への一般化について

大西良博 (Yoshihiro Ônishi)

東京都立大学理学部
(Department of Mathmatics, Faculty of Science,
Tokyo Metropolitan University)

## 0. はじめに

$p$ を奇素数とするとき公式

$$\prod_{r=1}^{p-1} 2\sqrt{-1}\sin\frac{2\pi r}{p} = p \tag{0.1}$$

はよく知られている. これを楕円函数に一般化する公式は最初は恐らく Eisenstein によって扱われた. その例として以下の様な公式がある. affine な方程式が

$$y^2 = x^3 + \frac{1}{4} \tag{0.2}$$

で与えられるような楕円曲線 $E$ は $\mathbf{Z}[\zeta_3]$, $\zeta_3 = e^{\frac{2\pi\sqrt{-1}}{3}}$ を自己同型環として持ち, 素元

$$\varpi \in \mathbf{Z}[\zeta_3], \equiv 1 \mod (1-\zeta_3)^2$$

について $\varpi$ - 等分点の全体 ${}_{\varpi}E$ は $p = N\varpi$ 個の元から成るが, このとき

$$\prod_{P\in {}_{\varpi}E, \neq O} x(P) = \frac{1}{\varpi^2} \tag{0.3}$$

が成り立つ. ここで $x(P)$ は $P$ の方程式 (0.1) での $x$ - 座標, $O$ は $E$ の群としての単位元である.

これらの公式を扱う動機の一つとして Gauss の和の符号決定問題があることは言うまでもない ([M1], [M2]).

## I. 目的

この講演の目的は David Grant によって発見された積公式, 即ち (1),(2) を種数 2 の曲線に一般化する公式を紹介し, 併せてその積に現れる座標が生成する体の Galois 群についての講演者による数値実験の結果を述べることにある.

## II. 種数 2 の曲線 ( Riemann 面 ) 上の函数論 (H.F. Baker の仕事)

Grant の公式 (3.2) を述べるために超楕円曲線及びそれらの Jacobi 多様体上の Abel 函数論について以下で必要な場合に限ってその概略を述べる. それらは Weierstrass の仕事を元に H. F. Baker が整備したものである. ([B1],[B2]).

**a. Jacobi 多様体の代数的理論.**

いま $C$ を affine な方程式が

$$y^2 = x^5 + \frac{1}{4} \tag{2.1}$$

で表される射影的で smooth な C 上定義された代数曲線とし, $J$ をその Jacobi 多様体とする. $J$ には $C$ の 2 次対称積 $\mathrm{Symm}^2 C$ から $J$ への全射

$$\begin{aligned} \varphi : &\mathrm{Symm}^2 C \to J \\ &(P_1, P_2) \mapsto P_1 + P_2 - 2\infty \end{aligned}$$

があり, これは丁度 $J$ の単位元での blowing up になっている. そこで $J$ 上の函数は $\mathrm{Symm}^2 C$ の点 $((x_1, y_1), (x_2, y_2))$ を用いてその対称式として表すことが多い. また

$$\begin{aligned} \iota : &C \hookrightarrow J \\ &P \mapsto P + \infty \end{aligned}$$

なる埋め込みの像を $\Theta$ で表す. $\zeta := e^{\frac{2\pi\sqrt{-1}}{5}}$ とするとき $C$ には $-\zeta$ が

$$[-\zeta](x, y) = (\zeta x, -y)$$

によって作用しているから $J$ には $\varphi$ を通じて $\mathbf{Z}[\zeta]$ が作用している.

**b. Jacobi 多様体の解析的理論.**

$C$ 上の正則な 1- 形式の層 $\Omega^1_C$ の基を

$$\omega_1 = \frac{dx}{y}, \quad \omega_2 = \frac{x dx}{y}.$$

と取り, 第 3 種微分形式の層の基底

$$\eta_1 = \frac{3x^3}{2y} dx, \quad \eta_2 = \frac{x^2}{2y} dx$$

をとる. 下の図のように $C$ の積分路 $\alpha_1, \alpha_2, \beta_1, \beta_2$ をとり, 周期行列

$$\Omega_1 = \begin{bmatrix} \int_{\alpha_1} \omega_1 & \int_{\alpha_2} \omega_1 \\ \int_{\alpha_1} \omega_2 & \int_{\alpha_2} \omega_2 \end{bmatrix} = \begin{bmatrix} 2K_1(\zeta^3 - \zeta^4) & 2K_1(\zeta - \zeta^2) \\ 2K_2(\zeta - \zeta^3) & 2K_2(\zeta^2 - \zeta^4) \end{bmatrix}$$

$$\Omega_2 = \begin{bmatrix} \int_{\beta_1} \omega_1 & \int_{\beta_2} \omega_1 \\ \int_{\beta_1} \omega_2 & \int_{\beta_2} \omega_2 \end{bmatrix} = \begin{bmatrix} 2K_1(-1 + \zeta - \zeta^2 + \zeta^3) & 2K_1(\zeta - 1) \\ 2K_2(-1 + \zeta^2 - \zeta^4 + \zeta) & 2K_2(\zeta^2 - 1) \end{bmatrix}$$

を定める．ここに

$$K_1 = \int_{(0,\frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}},0)} \omega_1$$
$$= -0.95015013898843674150305765442105298951\cdots,$$
$$K_2 = \int_{(0,\frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}},0)} \omega_2$$
$$= 0.42261692031717290436050061364858957077\cdots.$$

さらに擬周期行列を

$$\eta = \begin{bmatrix} \int_{\alpha_1}\eta_1 & \int_{\alpha_1}\eta_2 \\ \int_{\alpha_2}\eta_1 & \int_{\alpha_2}\eta_2 \end{bmatrix} = \begin{bmatrix} 2H_1(\zeta^2-\zeta) & 2H_1(\zeta^4-\zeta^3) \\ 2H_2(\zeta^4-\zeta^2) & 2H_2(\zeta^3-\zeta) \end{bmatrix}$$

で定める．ここに

$$H_1 = \int_{(0,\frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}},0)} \omega_1$$
$$= \sqrt{(-1)} \cdot 0.45508926983787695734043475371247514671\cdots,$$
$$H_2 = \int_{(0,\frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}},0)} \omega_2$$
$$= -\sqrt{(-1)} \cdot 0.24153442080024718212596751624538334733\cdots.$$

簡単な計算により $C$ の modulus $\tau$ は

$$\tau = \Omega_1^{-1}\Omega_2 = \begin{bmatrix} 1-\zeta^4 & -\zeta^2-\zeta^4 \\ -\zeta^2-\zeta^4 & \zeta \end{bmatrix}$$

となる．このとき $C$ から定まる超楕円 sigma 関数が

$$\sigma(u) = c\exp(-\frac{1}{2}u\eta\Omega_1^{-1}\,{}^t u)\,\vartheta\begin{bmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \end{bmatrix}(\Omega_1^{-1}\,{}^t u;\ \tau) \tag{2.2}$$

で定義される．ここに

$$u = (u_1,\ u_2),$$
$$u_1 = \int_{(\infty,\infty)}^{(x_1,y_1)} \omega_1 + \int_{(\infty,\infty)}^{(x_2,y_2)} \omega_1,$$
$$u_2 = \int_{(\infty,\infty)}^{(x_1,y_1)} \omega_2 + \int_{(\infty,\infty)}^{(x_2,y_2)} \omega_2$$

は $J$ を 2 次元の複素トーラスとして解析的多様体と考えたときの原点における標準的な局所座標であり定数 $c$ は

$$
\begin{aligned}
c &= 5^{5/8}\frac{\sqrt{\det(\Omega_1)}}{2\pi} \\
&= 5^{5/8}\frac{\sqrt{(K_1K_2(1-\zeta)(1-\zeta^2)^2)}}{\pi} \\
&= 1.13746122339326612848644850415000 4558\cdots,
\end{aligned}
$$

で与えられる ( [G1] 参照). さらに $i,\ j,\ k\in\{1,2\}$ に対して

$$
\begin{aligned}
\wp_{ij}(u) &= \frac{\partial^2}{\partial u_i\partial u_j}\sigma(u), \\
\wp_{ijk}(u) &= \frac{\partial}{\partial u_k}\wp_{ij}(u),
\end{aligned}
\tag{2.3}
$$

$$
\sigma_2(u) = \frac{\partial}{\partial u_2}\sigma(u) \tag{2.4}
$$

とおく. このとき楕円関数の時のように $u,\ v\in J-\Theta$ に対して

$$
-\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \wp_{11}(u)-\wp_{11}(v)+\wp_{12}(u)\wp_{22}(v)-\wp_{22}(u)\wp_{12}(v) \tag{2.5}
$$

なる式が成り立って ([B2]), これより $\wp_{ij}(u)$ らの代数的加法公式が得られる ([B1, G3]).

また $\alpha\in\mathbf{Z}[\zeta]$ に対して $N_{\mathbf{Q}(\zeta)/\mathbf{Q}(\zeta+\zeta^{-1})}(\alpha)=n_\alpha+m_\alpha\varepsilon^2$ とし, $\varepsilon=1+\zeta+\zeta^4$ とするとき

$$
\psi_\alpha(u) = \frac{\sigma(\alpha u)}{\sigma_2(u)^{n_\alpha}(-\sigma(\varepsilon u))^{m_\alpha}}. \tag{2.6}
$$

が Weber の psi 関数の良い一般化になっている ( [G3, §3] 参照). さて [G3] に従って

$$
X(u) = \frac{1}{2}\left(\wp_{11}(u)\wp_{22}(u)-\wp_{12}(u)^2\right) \tag{2.7}
$$

とおくと

$$
X(u) = \frac{\sigma(u+P)\sigma(u+2P)\sigma(u-3P)+\sigma(u-P)\sigma(u-2P)\sigma(u+3P)}{2\sigma(u)^3\sigma_2(P)\sigma(2P)\sigma(-3P)}, \tag{2.8}
$$

と $\sigma$ 函数を使って表される. ここに $P=\iota(0,\frac{1}{2})$ であり, $X$ は

$$
X(-\zeta u) = \zeta^4 X(u) \tag{2.9}
$$

なる性質を持つ.

## III. GRANT の公式

いま

$$G(\beta) = \{Q = \iota(x, y);\ \mathrm{Im}y > 0,\ Q \in \Theta \cap \left[\beta\beta^{\sigma^{-1}}\right]^* (X)_0,\ 2Q \neq O\} \tag{3.1}$$

とおく. ここで $(X)_0$ は函数 $X$ の零点因子であり, $O$ は $J$ の単位元である. 因子 $\Theta$ の自己交点数は 2 であり $(X)_0$ は $3\Theta$ と線形同値であるから $\sharp G(\beta) = 3(p-1)$ ([G3, Remark]. 以上の準備のもとに Grant の公式は次のように述べられる:

**定理 3.2.**

$$\prod_{Q \in G(\beta)} x(\iota^{-1}(Q)) = \frac{1}{\beta\beta^{\sigma}}.$$

**注意.**
$G(\beta)$ に属する点はすべて $J$ の群構造に関して捻れが無い事がわかる *([G3] 参照)*. しかし同様の定義を楕円曲線の場合に行えば従来の等分点に一致する.

## IV. $G(\beta)$ が生成する GALOIS 群に付いて

さて $\{x(Q); Q \in G(\beta)\}$ が $\mathbf{Q}(\zeta)$ 上に生成する体拡大について調べるために

$$\Phi(\beta; T) = \prod_{Q \in G(\beta)} (T - \frac{1}{x(Q)}) \in \mathbf{Q}[\zeta][T], \tag{4.1}$$

とおく. このとき [G3, §4] により,

$$x(u)^{3(p-1)}\Phi(\beta; \frac{1}{x(u)}) = \frac{(-1)^{N\beta-1}X(\beta\beta^{\sigma^{-1}}u)\left(\psi_{\beta\beta^{\sigma^{-1}}}(u)\right)^3}{y(u)} \tag{4.2}$$

が成り立つ. ここで $T$ は不定元である. $\mathbf{Z}[\zeta]$ の作用から, 多項式 $\Psi(\beta; S) \in \mathbf{Q}[\zeta][S]$ (ここで $S$ も不定元) が存在して

$$\Phi(\beta; T) = \Psi(\beta; T^5) \tag{4.3}$$

をみたす. そこで $\Phi(\beta; T)$ 及び $\Psi(\beta; S)$ の $\mathbf{Q}(\zeta)$ 上のそれぞれの分解体を $L_\beta = \mathbf{Q}(x(Q); P \in G(\beta))$ 及び $K_\beta = \mathbf{Q}(x(Q)^5; Q \in G(\beta))$ とし,

$$\{\zeta^\nu \alpha_j\} \quad (\nu = 0, \cdots, 4; j = 1, \cdots, \frac{3(p-1)}{5}) \tag{4.4}$$

を $\Phi(\beta; T) = 0$ の根の全体とする. このとき $\mathrm{Gal}(L_\beta/\mathbf{Q}(\zeta))$ は上の根の置換群 ( $\mathcal{G}_\beta$ と名付ける) の部分群と考えられる. $\mathcal{G}_\beta$ は次の 2 種類の置換から生成される. すなわち

$$\langle i_1, i_2, \cdots, i_{\frac{3(p-1)}{5}} \rangle : \alpha_\nu \mapsto \zeta^{i_\nu}\alpha_\nu \text{ for all } \nu, \tag{4.5}$$

と互換

$$(ij) : \zeta^\nu\alpha_i \leftrightarrow \zeta^\nu\alpha_j,\ \zeta^\nu\ \alpha_k \mapsto \zeta^\nu\alpha_k \quad (\nu = 0, 1, \cdots, 4;\ k \neq i, j) \tag{4.6}$$

からである. 講演者は $G(\beta)$ にはその Galois 群を統制するような構造 (楕円曲線の場合の $\mathbf{F}_p$ 加群の構造などに対応するもの) が無いと思われることから次のような予想を立ててみた.

予 想 4.7.
任意の素元 $\beta \equiv \pm 1 \mod (1-\zeta)^2$ について $N\beta = p$ と書く. 体 $L_\beta$ 及び群 $\mathcal{G}_\beta$ は上のとおりとする. このとき

$$Gal(L_\beta/\mathbf{Q}(\zeta)) = \mathcal{G}_\beta$$

となっているであろう.

さらに N$\beta$=11, 31, 41, 61 なる $\beta$ について本稿の最後にある Table 1 のように $\Phi(\beta;T)$ を UBASIC を用いて計算してみたが, その結果この予想がこれらについてはに成り立つことがわかった. 以下その計算方法に付いて略述し, 若干の注意を述べる.

## V. $\Phi(\beta;T)$ は $\mathbf{Z}[\zeta]$ に属するか?

命 題 5.1.
$\Phi(\beta;T) \in \mathbf{Z}[\frac{1}{2}][\zeta]$.

証明. ([G3, Remark (1) in the introduction]). いま $\mathfrak{p}$ の上にある $L_\beta$ の素イデアル $\mathfrak{P}$ に対して $x(Q) \equiv 0 \mod \mathfrak{P}$ であるとする. これは例えば non-Weierstrass 点が Weierstrass 点に degenerate することを意味するから, $\mathfrak{P}$ は bad reduction prime である. 従って $\mathfrak{p}$ は 10 を割る. 一方, もし $x(Q)^{-1} \equiv \ \mod \mathfrak{P}$ とすると,

$$t_2(Q)^2 = \frac{y(Q)^2}{x(Q)^6} = \frac{1}{x(Q)} + \frac{1}{2x(Q)^6},$$

であることによって $\mathfrak{P}$ は $2\beta\beta^\sigma$ を割る. よって $x(Q)^{-1}$ $(Q \in G(\beta))$ は 2 を割らない任意の素点において整である. ∎

一般に $\Phi(\beta;T)$ が $\mathbf{Z}[\zeta]_{(2)}$ 上でも定義されるか否かはわかっていないが, いくつかの $\beta$ についてはそうなることが以下のようにしてわかる. すなわち, まず Weber が Argebra III で用いた方法 ([T, p.145], [F, p.184]) に基付き, 前に定義した $\phi_\alpha(u)$ の $\alpha$ に関する漸化式が (2.5) から導かれる

$$(5.2)\quad -\frac{\psi_{\alpha+\beta}(u)\psi_{\alpha-\beta}(u)}{\psi_\alpha(u)^2\psi_\beta(u)^2} + \wp_{11}(\beta u) = -\wp_{11}(\alpha u) + \wp_{12}(\alpha u)\wp_{22}(\beta u) - \wp_{22}(\alpha u)\wp_{12}(\beta u).$$

により得られる. 漸化式から $\phi_\alpha(u)$ が $\mathbf{Z}_{(2)}[\zeta]$ 上整であることがわかる. 一方 $\sigma(u)$ の, $C$ の座標でいえば $(\infty,\infty)$ 及び $(0, \pm\frac{1}{2})$ に於ける Taylor 展開から $\phi_{\beta\beta^{-1}}(u)$ の最高次係数と定数項がわかる. そこで $\Theta$ 上 $x(u)$ の多項式として $\mathbf{Z}[\zeta]_{(2)}$ 上原始的であることがその 2 係数からわかる場合は $X(\beta\beta^{\sigma^{-1}}u)$ の分母としての (see [O]) $\Phi(\beta;T)$ が $\mathbf{Z}[\zeta]_{(2)}$ 上整であることが次のことからわかる.

$$(5.3)\quad \begin{aligned} & y(u)x(u)^{3(p-1)}\Phi(\beta; x(Q)^{-1})\psi_\alpha(u) \\ &= \psi_\alpha(u)^4 X(\alpha u) \\ &= \frac{1}{2}\left\{\wp_{11}(\alpha u)\psi_\alpha(u)^2\wp_{22}(\alpha u)\psi_\alpha(u)^2 - (\wp_{12}(\alpha u)\psi_\alpha(u)^2)^2\right\} \\ &\in \mathbf{Z}[\zeta]_{(2)}[x(Q)]. \end{aligned}$$

特に Table 1 にある $N\beta = 11, 31, 41, 61$ の場合は $\Phi(\beta;T)$ は $\mathbf{Z}[\zeta]$ 上整である.

## VI. $\Phi(\beta;T)$ の近似計算

$\psi_\alpha(u)$, $X(u)$ の定義と(5.3)式からわかるように $\Phi(\beta, x(Q)^{-1})$ は $\sigma(u)$ や $\sigma_2(u)$ の特殊値で書けるが, フーリエ級数であるそれらは収束が早く非常に精密な近似値が得られる. よって次数が小さいとき, つまり $N\beta-1$ が小さいときは補間法により $\Phi(\beta,T)$ が求められる.

## VII. Galois 群の計算

適当な素イデアルで reduction (Table 2) して, 次の補題を用いれば, これら 4 つの場合についてはさきの予想が正しいことがわかる. (2つの

命題 7.1.
$H$ を $n$ 次対称群 $\mathfrak{S}_n$ の部分群とする. もし $H$ が互換と長さ $n$ 及び $n-1$ の巡回置換を含むならば $H$ は $\mathfrak{S}_n$ に一致する.

命題 7.2.
$f(T) \in \mathbf{Z}[\zeta][T]$ をモニックな $n$ 次分離的多項式とする. $\varpi$ *of* $\mathbf{Z}[\zeta]$ の素元 $\varpi$ を一つとって固定する. もし $f(T) \mod \varpi$ が $\mathbf{Z}[\zeta][T]/(\varpi)$ 上で次数 $r_1, r_2, \cdots, r_s$ の多項式の積に分解するならば, $f(T)$ の *Galois* 群は $(r_1, r_2, \cdots, r_s)$ 型の置換を含む.

## References


[B1] H.F. Baker, "An Introduction to the Theory of Multiply Periodic Functions," Cambridge, 1907.

[B2] H.F. Baker, *On the hyperelliptic sigma functions*, Amer. J. of Math. XX (1898), 301–384.

[F] R. Fricke, "Die elliptishen Functionen und ihre Anwendungen, II,", 1922.

[G1] D. Grant, *On a generalization of Jacobi's derivative formula to dimension two*, J. reine angew. Math. 392 (1988), 125–136.

[G2] D. Grant, *Formal groups in genus two*, J. reine angew. Math. 411 (1990), 96–121.

[G3] D. Grant, *A generalization of a formula of Eisenstein*, J. London Math. Soc. (1991) (to appear).

[M1] C. R. Matthews, *Gauss sums and elliptic functions : I. The kummer Sum*, Invent. math. 52 (1979), 163–185.

[M2] C. R. Matthews, *Gauss sums and elliptic functions : II. The Quartic Sum*, Invent. Math. 54 (1979), 23–52.

[O] Y. Ônishi, *Some examples of the formula of Grant.*

[T] 竹内端三, "楕圓函數論," 岩波全書, 1936.

Table. 1

<u>$p=11,\ \beta=1-\sqrt{(5)}\,\zeta$</u>

$$
\begin{aligned}
&\Phi(1-\sqrt{5}\,\zeta;T^{-1})T^{30}\\
&=(\ 2\zeta + 0\zeta^2 - 2\zeta^3 + 1\zeta^4)T^{30}\\
&+(\ 481\zeta + 606\zeta^2 + 81\zeta^3 + 31\zeta^4)T^{25}\\
&+(\ 755\zeta + 8850\zeta^2 + 1545\zeta^3 + 790\zeta^4)T^{20}\\
&+(-1045\zeta + 6190\zeta^2 - 850\zeta^3 - 440\zeta^4)T^{15}\\
&+(-235\zeta - 105\zeta^2 - 750\zeta^3 - 370\zeta^4)T^{10}\\
&+(\ 43\zeta + 85\zeta^2 - 23\zeta^3 - 11\zeta^4)T^{5}\\
&+\ 1
\end{aligned}
$$

<u>$p=31,\ \beta=2\zeta-\zeta^2$</u>

$$
\begin{aligned}
&\Phi(2\zeta-\zeta^2;T^{-1})T^{90}\\
&=(\ 3\zeta + 2\zeta^2 + 6\zeta^3 + 0\zeta^4)T^{90}\\
&+(\ 49130\zeta + 63127\zeta^2 + 52114\zeta^3 + 72021\zeta^4)T^{85}\\
&+(\ 72513886\zeta - 95597055\zeta^2 - 32596266\zeta^3 - 180457587\zeta^4)T^{80}\\
&+(\ 5336335946\zeta + 2959913601\zeta^2 - 1703408144\zeta^3 + 1687367536\zeta^4)T^{75}\\
&+(-14754715590\zeta - 7740236770\zeta^2 - 56603191800\zeta^3 - 56429761880\zeta^4)T^{70}\\
&+(-23652059209\zeta + 82699543704\zeta^2 + 25939829052\zeta^3 - 129958364345\zeta^4)T^{65}\\
&+(-1101355052300\zeta - 887460640566\zeta^2 - 895659713302\zeta^3 - 912140700173\zeta^4)T^{60}\\
&+(-1077203581153\zeta - 1518111474740\zeta^2 - 1110674416717\zeta^3 - 1353475398839\zeta^4)T^{55}\\
&+(-896583135093\zeta - 1059408992478\zeta^2 - 936337020063\zeta^3 - 713174075123\zeta^4)T^{50}\\
&+(-502120589520\zeta - 381550846985\zeta^2 - 622101740750\zeta^3 - 444344021415\zeta^4)T^{45}\\
&+(-173127443291\zeta - 51718893939\zeta^2 - 197074499722\zeta^3 - 176927865610\zeta^4)T^{40}\\
&+(-31260272990\zeta + 5439329351\zeta^2 - 21680088963\zeta^3 - 29969845017\zeta^4)T^{35}\\
&+(-926085302\zeta + 424750620\zeta^2 + 582306632\zeta^3 - 186588361\zeta^4)T^{30}\\
&+(\ 769436648\zeta - 104755497\zeta^2 + 579468833\zeta^3 + 384254463\zeta^4)T^{25}\\
&+(\ 103268235\zeta - 26994995\zeta^2 + 66571300\zeta^3 + 18930170\zeta^4)T^{20}\\
&+(\ 4044997\zeta - 2352267\zeta^2 + 1248164\zeta^3 - 856295\zeta^4)T^{15}\\
&+(\ 19910\zeta - 80662\zeta^2 - 66724\zeta^3 + 43169\zeta^4)T^{10}\\
&+(\ 69\zeta - 75\zeta^2 + 726\zeta^3 + 1662\zeta^4)T^{5}\\
&+1
\end{aligned}
$$

$p=41,\ \ \beta=\zeta^2+2\zeta^3+3\zeta^4$

$$\Phi(\zeta^2+2^3+3\zeta^4;T^{-1})T^{120}$$

$$
\begin{aligned}
={}& (-2\zeta + 2\zeta^2 - 4\zeta^3 - 5\zeta^4)T^{120}\\
&+(24807\zeta - 68475\zeta^2 - 154652\zeta^3 - 22369\zeta^4)T^{115}\\
&+(-1035129149\zeta + 4250240268\zeta^2 + 1256418780\zeta^3 + 1766313157\zeta^4)T^{110}\\
&+(364381706505\zeta + 224046286056\zeta^2 + 221479332942\zeta^3 + 81727059798\zeta^4)T^{105}\\
&+(10822902349869\zeta - 17336069896736\zeta^2 - 752514987516\zeta^3 - 16248580066396\zeta^4)T^{100}\\
&+(55420294345053\zeta + 45974992436357\zeta^2 - 139934783318974\zeta^3 - 25874298892050\zeta^4)T^{95}\\
&+(962680198843117\zeta + 1312717533007740\zeta^2 + 859558673820393\zeta^3 + 566842474863106\zeta^4)T^{90}\\
&+(6414290801515241\zeta + 5242565955772993\zeta^2 + 4500468875603315\zeta^3 + 2196172741942577\zeta^4)T^{85}\\
&+(7050363148188925\zeta - 1763240405962434\zeta^2 + 1269991312395817\zeta^3 - 1508959999031162\zeta^4)T^{80}\\
&+(14467648987103144\zeta - 4866798896025541\zeta^2 - 3424006173521701\zeta^3 - 2019299766848561\zeta^4)T^{75}\\
&+(17237482028292603\zeta - 2322168805999833\zeta^2 - 1095116726199179\zeta^3 - 1789095616693445\zeta^4)T^{70}\\
&+(9411820041030182\zeta + 709299803466255\zeta^2 - 1495144619378142\zeta^3 + 39532042053396\zeta^4)T^{65}\\
&+(3011692630603171\zeta + 615305832612413\zeta^2 - 1076718879003750\zeta^3 + 255271885050577\zeta^4)T^{60}\\
&+(780416588154445\zeta + 631202072478341\zeta^2 + 195831864131897\zeta^3 + 521395954860073\zeta^4)T^{55}\\
&+(165732471606604\zeta + 337884308703789\zeta^2 + 312420131959074\zeta^3 + 320333682043184\zeta^4)T^{50}\\
&+(28117625910893\zeta + 70909058240587\zeta^2 + 84635622002171\zeta^3 + 84654838681810\zeta^4)T^{45}\\
&+(6596859551682\zeta + 3608103383795\zeta^2 + 8000311210588\zeta^3 + 15347056749616\zeta^4)T^{40}\\
&+(1164234227031\zeta - 160939539252\zeta^2 + 446105663060\zeta^3 + 1844506446612\zeta^4)T^{35}\\
&+(47587057690\zeta + 12774161396\zeta^2 + 90855113862\zeta^3 + 51760084148\zeta^4)T^{30}\\
&+(-13827072116\zeta - 3470278386\zeta^2 + 6777725144\zeta^3 - 15009421976\zeta^4)T^{25}\\
&+(-1125729797\zeta - 142964613\zeta^2 + 408778486\zeta^3 - 1151049435\zeta^4)T^{20}\\
&+(-17315413\zeta - 304940\zeta^2 + 21867438\zeta^3 - 14365624\zeta^4)T^{15}\\
&+(124331\zeta + 247953\zeta^2 + 537345\zeta^3 + 240827\zeta^4)T^{10}\\
&+(1810\zeta + 2266\zeta^2 + 3607\zeta^3 + 2143\zeta^4)T^{5}\\
&+1
\end{aligned}
$$

=61, $\beta=3\zeta^{2}+\zeta^{4}$

$\Phi(3\zeta^{2}+\zeta^{4};T^{-1})T^{180}$

$=(\ 6\zeta - 2\zeta^{2} + 0\zeta^{3} - 3\zeta^{4})T^{180}$

$+(\ 2049676\zeta + 983466\zeta^{2} - 904194\zeta^{3} + 278071\zeta^{4})T^{175}$

$+(\ 181304340245\zeta + 52262734570\zeta^{2} - 189570157255\zeta^{3} + 65417648445\zeta^{4})T^{170}$

$+(-\ 57568214192215\zeta - 16033404398520\zeta^{2} - 152992856122000\zeta^{3} - 97593828395880\zeta^{4})T^{165}$

$+(\ 14716157389618050\zeta - 5598589439456770\zeta^{2} + 18810382591544660\zeta^{3} - 22226814611875585\zeta^{4})T^{160}$

$+(-\ 261501150548488347\zeta + 2115001826030741919\zeta^{2} + 1131970596131071140\zeta^{3} + 2242211081414930646\zeta^{4})T^{155}$

$+(\ 10794602065997152893\zeta - 12516924209465268619 7\zeta^{2} + 5572271617029639788\zeta^{3} - 3578221829410897277\zeta^{4})T^{150}$

$+(-\ 1092489892026193240595\zeta - 190456946803615321 95\zeta^{2} - 824934910686987420 20\zeta^{3} + 105475443709962414 8380\zeta^{4})T^{145}$

$+(-\ 5264940377372806644860\zeta + 7617655486050966135945\zeta^{2} - 2208810719148956967200\zeta^{3} + 5919675578839593861180\zeta^{4})T^{140}$

$+(\ 3523112680202290692 3700\zeta + 7699109678429651126 7395\zeta^{2} - 2844591922704368405660\zeta^{3} + 5764940940374394738 9085\zeta^{4})T^{135}$

$+(-\ 4707855537698870807 5719\zeta + 200899198924234951562728\zeta^{2} - 178949929296735577625890\zeta^{3} + 10036925041345017004512\zeta^{4})T^{130}$

$+(-\ 31983449855840321598354\zeta + 136172420618496196359621\zeta^{2} - 466246706226228978432904\zeta^{3} - 346553448466428222999679\zeta^{4})T^{125}$

$+(\ 118019206764616274873305 0\zeta + 205455482183199912333675\zeta^{2} - 163763655100212872238575\zeta^{3} - 83100189407529085012325\zeta^{4})T^{120}$

$+(\ 305996345458635819612627 5\zeta + 244936329158456058499950\zeta^{2} + 545838422257132671466625\zeta^{3} + 512501234059197317441050\zeta^{4})T^{115}$

$+(\ 397925773293766348643950 0\zeta + 79225077814751555461450\zeta^{2} + 889574660231725659904650\zeta^{3} + 254529912494647967765225\zeta^{4})T^{110}$

$+(\ 346756229781877286800484 0\zeta - 85725012712521041603605\zeta^{2} + 281055925018219463672975\zeta^{3} + 156956932897177155 6605\zeta^{4})T^{105}$

$+(\ 214417350100411610839596 5\zeta - 266875875221026877505210\zeta^{2} - 289731939484927671235510\zeta^{3} + 58416643569308765785065\zeta^{4})T^{100}$

$+(\ 76227321529123525615010 0\zeta - 283528664040523758804150\zeta^{2} - 358301031221634135630400\zeta^{3} - 61886872356522918697150\zeta^{4})T^{95}$

$+(\ 92450484250738213940925\zeta - 176818574494659617988850\zeta^{2} - 176689224147872014607625\zeta^{3} - 174206681963141408783400\zeta^{4})T^{90}$

$+(-\ 40044111178252450781000\zeta - 85737155869841603328100\zeta^{2} - 52967312889452485105200\zeta^{3} - 142803548699047746983800\zeta^{4})T^{85}$

$+(-\ 28320121922644518564190\zeta - 36329555220583241551170\zeta^{2} - 15370939070056432208925\zeta^{3} - 67300961560912082340605\zeta^{4})T^{80}$

$+(-\ 11317157764194631449965\zeta - 12443611579843256032115\zeta^{2} - 6162480797122406437265\zeta^{3} - 20813206535815428571040\zeta^{4})T^{75}$

$+(-\ 3417219276505031827575\zeta - 3168643887326249676825\zeta^{2} - 2433483906393330335825\zeta^{3} - 4388906591501280154450\zeta^{4})T^{70}$

$+(-\ 658421946396854279850\zeta - 528616430424494946050\zeta^{2} - 650737039623651709250\zeta^{3} - 615885744328630532200\zeta^{4})T^{65}$

$+(-\ 38907578100685411125\zeta - 18883362013022544300\zeta^{2} - 80698153065160491225\zeta^{3} - 25644018052789803275\zeta^{4})T^{60}$

$+(\ 12672276508303245799\zeta + 15176377615902722242\zeta^{2} + 4789997165491124475\zeta^{3} + 14234235783867177438\zeta^{4})T^{55}$

$+(\ 3203254527174167929\zeta + 3797253764271593439\zeta^{2} + 3055155956145585774\zeta^{3} + 3885314532490306684\zeta^{4})T^{50}$

$+(\ 291949745622074780\zeta + 433081185270028705\zeta^{2} + 427937400402498905\zeta^{3} + 437184792279348330\zeta^{4})T^{45}$

$+(\ 8015095785609415\zeta + 29250162314242120\zeta^{2} + 28785572362552250\zeta^{3} + 22607038185282280\zeta^{4})T^{40}$

$+(-\ 667090421851 75\zeta + 1396760616130745\zeta^{2} + 1151266328971040\zeta^{3} + 418607393258260\zeta^{4})T^{35}$

$+(\ 8195468724622\zeta + 39045235623931\zeta^{2} + 32870511466660\zeta^{3} + 4474269099729\zeta^{4})T^{30}$

$+(\ 1019179484982\zeta + 252468849497\zeta^{2} - 459131887563\zeta^{3} + 363520052\zeta^{4})T^{25}$

$+(\ 35724629370\zeta + 10212806845\zeta^{2} - 16496176080\zeta^{3} - 11902515605\zeta^{4})T^{20}$

$+(\ 73971560\zeta + 282361655\zeta^{2} + 4762200\zeta^{3} - 339029280\zeta^{4})T^{15}$

$+(\ 3599175\zeta + 1610205\zeta^{2} + 1159860\zeta^{3} + 796965\zeta^{4})T^{10}$

$+(-\ 3261\zeta + 3957\zeta^{2} - 435\zeta^{3} - 6447\zeta^{4})T^{5}$

$+1$

**Table 2.**

$\beta = 1 - 5\zeta, \mathrm{N}\beta = 11$

| The norm of the prime $\mathfrak{l}$ | The minimum in N $\equiv \zeta \mod \mathfrak{l}$ | The type of the factors of $\Psi$ and $\Phi$ |
|---|---|---|
| 41 | 16 | *irred.* |
| 131 | 61 | $(1^5)(25)$ |
| 191 | 184 | $(5)(5^5)$ |
| 191 | 49 | $(10)(41^5)$ |
| 281 | 90 | $(5)^4(10)$ |
| 761 | 684 | $(5)(1^5)(4^5)$ |

$\beta = 2\zeta - \zeta^2, \mathrm{N}\beta = 31$

| The norm of the prime $\mathfrak{l}$ | The minimum in N $\equiv \zeta \mod \mathfrak{l}$ | The type of the factors of $\Psi$ and $\Phi$ |
|---|---|---|
| 41 | 37 | $(1^5)(85)$ |
| 71 | 54 | $(1^5)(5)(80)$ |
| 271 | 187 | $(5)^2(10)(35)^2$ |
| 281 | 90 | *irred.* |
| 311 | 6 | $(5)(17^5)$ |

$\beta = \zeta^2 + 2\zeta^3 + 3\zeta^4, \mathrm{N}\beta = 41$

| The norm of the prime $\mathfrak{l}$ | The minimum in N $\equiv \zeta \mod \mathfrak{l}$ | The type of the factors of $\Psi$ and $\Phi$ |
|---|---|---|
| 61 | 3 | $(24^5)$ |
| 271 | 10 | $(5)(10)(105)$ |
| 281 | 232 | $(5)(115)$ |
| 971 | 803 | $(10)(22^5)$ |
| 1811 | 956 | $(5)(4^5)(19^5)$ |

$\beta = -3\zeta^2 - \zeta^4, \mathrm{N}\beta = 61$

| The norm of the prime $\mathfrak{l}$ | The minimum in N $\equiv \zeta \mod \mathfrak{l}$ | The type of the factors of $\Psi$ and $\Phi$ |
|---|---|---|
| 211 | 188 | $(10)(7^5)(135)$ |
| 1231 | 190 | $(5)^2(34^5)$ |
| 1291 | 319 | *irred.* |
| 1831 | 655 | $(1^5)(5)(10)(4^5)(28^5)$ |
| 2311 | 2006 | $(1^5)(175)$ |

1) All the cases, the reduced polynomials are separable.

2) In the third column, for instance, $(1^5)(5)(10)(4^5)(28^5)$ indicates
(a) $\Psi(\beta; S)$ modulo$\mathfrak{l}$ factors the product of 2 polynomials of degree 1, 1 polynomial of degree 2, 1 polynomial of degree 4 and 1 polynomial of degree 28; furthermore
(b) if we substitute $T^5$ as $S$, then each factor decomposes respectively the product of 5 polynomials of degree 1, of 1 polynomial of degree 10, of 5 polynomials of degree 4 and of 5 polynomials of degree 28.