Triangles and Elliptic Curves. V

By Takashi ONO

Department of Mathematics, The Johns Hopkins University, U.S.A.

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1995)

This is a continuation of my series of papers [4] each of which will be referred to as (I), (II), (III), (IV) in this paper. Let k be a field of characteristic not 2. We shall fix once for all a complete set $\mathcal{M}$ of representatives of $k^\times/(k^\times)^2$. For $M \in \mathcal{M}$ and an element $\lambda \neq 0,1$ of k, consider the set of k-rational points

(0.1) $E(M, \lambda M)(k) = \{p = [x_0, x_1, x_2, x_3];$
$x_0^2 + Mx_1^2 = x_2^2,\ x_0^2 + \lambda M x_1^2 = x_3^2\}$

of the elliptic curve $E(M, \lambda M)$ and the bunch of (0.1) taken over $\mathcal{M}$:

(0.2) $\boldsymbol{E}(\lambda; k) = \bigcup_{M \in \mathcal{M}} E(M, \lambda M)(k)$.[1)]

Denote by D the set of four points $[1,0, \pm 1, \pm 1]$ in P^3. For each λ, M, the set D is a subgroup of $E(M, \lambda M)(k)$ consisting of points P such that $2P = \mathcal{O} = [1,0,1,1]$; $D \approx \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$. From the definition of $\mathcal{M}$ we find that

(0.3) $E(M, \lambda M)(k) \cap E(M', \lambda M')(k) = D, \quad M \neq M'$.

In other words, the union in (0.2) is "disjoint" up to elements of D.

In this paper, we shall introduce a *surjective* map

(0.4) $c : \boldsymbol{E}(\lambda; k) \to P^1(k)$

which is an analogue of the branched covering of Riemann surfaces. We shall also examine this map for special fields k including some local and global fields in number theory.

§1. Map c. For $P = [x_0, x_1, x_2, x_3] \in \boldsymbol{E}(\lambda; k)$ in (0.2), put

(1.1) $\pi(P) = [x_2, x_3, x_0]$.

Since each $M \in \mathcal{M}$ is $\neq 0$, $\pi(P)$ is a point in $P^2(k)$. For $\lambda \neq 0,1$ of k, let $C(\lambda)$ be the conic defined by

(1.2) $C(\lambda) = \{[x, y, z] \in P^2(\bar{k}); y^2 - z^2 = \lambda(x^2 - z^2)\}$.

Clearly π induces a map, written again by π:

(1.3) $\pi : \boldsymbol{E}(\lambda; k) \to C(\lambda)(k)$.

Furthermore,

(1.4) π is surjective.

In fact, take any point $Q = [x, y, z] \in C(\lambda)(k)$. If $x^2 = z^2$ then $y^2 = z^2$, so $Q = [\pm 1, \pm 1, 1]$. Therefore there is a point $P = [1,0, \pm 1, \pm 1]$ in D such that $\pi(P) = Q$. If $x^2 \neq z^2$, then there is a unique $M \in \mathcal{M}$ and an element $W \in k^\times$ such that $x^2 - z^2 = w^2 M$ and hence $y^2 - z^2 = w^2 \lambda M$. In other words, we have $\pi(P) = Q$ with $P = [z, w, x, y] \in E(M, \lambda M)(k)$. Q.E.D.

We can verify easily that, for $P, P' \in \boldsymbol{E}(\lambda; k)$,

(1.5) $\pi(P) = \pi(P') \Leftrightarrow P' = P$ or $-P$,

where $-P = [x_0, -x_1, x_2, x_3]$ is the inverse in the abelian group $E(M, \lambda M)(k)$ to which P belongs. Hence the fibre of π consists of two points $P, -P$ except for the case where $2P = \mathcal{O}$, i.e., $P \in D$. In the latter case, π induces on D a bijection: $[1,0, \pm 1, \pm 1] \leftrightarrow [\pm 1, \pm 1, 1] \in C(\lambda)(k)$.

Now consider the point $[1,1,1]$ on $C(\lambda)$ and the line L_∞ defined dy $Z = 0$. Let $[t] = [x, y, z]$ be a point on $C(\lambda)$ and $\sigma[t]$ the intersection of L_∞ and the line joining $[1,1,1]$ and $[t]$ (stereographic projection). When $[t] = [1,1,1]$ we understand by $\sigma[t]$ the point of intersection of L_∞ and the tangent at $[t]$ to $C(\lambda)$. The equation of the line is

(1.6) $(y - z)X + (z - x)Y + (x - y)Z = 0$.

Putting $Z = 0$ in (1.6), we use $[X, Y]$ as the homogeneous coordinates on L_∞ and identify $[X, Y]$ with the non-homogeneous coordinate $u = Y/X$ on $L_\infty = \boldsymbol{P}^1$. Consequently, we have

(1.7) $\sigma[t] = \dfrac{y - z}{x - z} = \lambda \dfrac{x + z}{y + z}$,
$[t] = [x, y, z] \in C(\lambda)$.

Notice that

(1.8) $\sigma[1,1,-1] = 1,\ \sigma[1,-1,1] = \infty,$
$\sigma[-1,1,1] = 0,\ \sigma[1,1,1] = \lambda$.

On the other hand, let u be a point of L_∞. Then the equation of the line joining u and $[1,1,1]$ is

(1.9) $uX - Y + (1 - u)Z = 0$.

[1)] As usual, we write $X(k)$ or X_k for the k-rational subset of a set X of geometric objects. We also use X for $X(\bar{k})$ occasionally where $\bar{k}$ denotes the algebraic closure of k. E.g., $X = E(M, \lambda M)$ is an elliptic curve in $P^3 = P^3(\bar{k})$ and (0.1) is the subset of k-rational points of X. On the other hand, since the set $\mathcal{M}$ is not necessarily finite, the set $\boldsymbol{E}(\lambda; k)$ in (0.2) is merely the union in the sense of sets.

Call $\psi(u)$ the intersection of $C(\lambda)$ and the line (1.9). From (1.2), (1.9), it follows that

(1.10) $\psi(u) = [u^2 - 2u + \lambda, -u^2 + 2u\lambda - \lambda, u^2 - \lambda]$

and

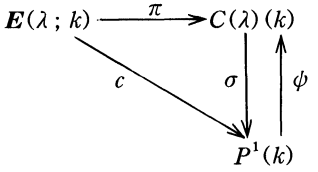
(1.11) $\sigma\varphi(u) = u$, $u \in L_\infty$, i.e., ψ is the inverse of σ.

Consequently, from (1.11), we obtain a bijection:

(1.12) $\sigma : C(\lambda)(k) \tilde{\to} P^1(k)$.

Combining (1.3) and (1.12), we obtain a map c:

(1.13)



In view of (1.4), (1.5), (1.8), c is a surjective map such that the fibre $c^{-1}(u)$ consists of two points $P, -P$ for $u \in P^1(k) - \{0,1,\infty,\lambda\}$ and of a single point in D for $u \in \{0,1,\infty,\lambda\}$. From (1.1), (1.7), (1.8) we obtain the values of the map c as follows:

(1.14) $$c(P) = \frac{x_3 - x_0}{x_2 - x_0} = \lambda \frac{x_2 + x_0}{x_3 + x_0}, \qquad P = [x_0, x_1, x_2, x_3]$$

and, in particular,

(1.15) $c[1,0,1,1] = \lambda$, $c[1,0,-1,1] = 0$, $c[1,0,1,-1] = \infty$, $c[1,0,-1,-1] = 1$,

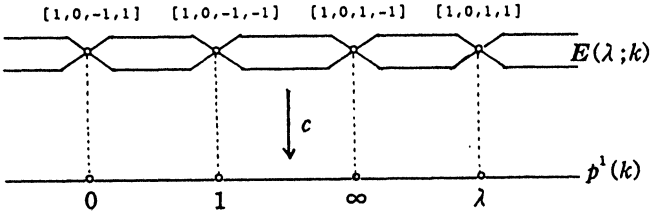


Fig. 1

§2. Map c_M. According to our convention in earlier papers (e.g., (IV)), set

(2.1) $E_0(M, \lambda M)(k) = \{t = (x, y, z) \in k^3 ; z^2 + M = x^2, z^2 + \lambda M = y^2\}$,

Since we have $E_0(M, \lambda M)(k) = E(M, \lambda M)(k) - D$ after the identification:

(2.2) $t = (x, y, z) \leftrightarrow P = [z, 1, x, y]$,

the union

(2.3) $$\boldsymbol{E}_0(\lambda ; k) = \bigcup_{M \in \mathcal{M}} E_0(M, \lambda M)(k)$$

is disjoint. The "branched" covering c induces an "unramified" covering c_0

(2.4) $c_0 : \boldsymbol{E}_0(\lambda ; k) \to k - \{0, 1, \lambda\}$. (See Figure 1)

Call c_M the restriction of c on the M-part $E(M, \lambda M)(k)$. For any $u \in k - \{0,1,\lambda\}$, there is a unique $M \in \mathcal{M}$ and $t \in E_0(M, \lambda M)(k)$ such that $u = c_M(t)$ where t is determined up to ± 1. (Note that the double use of the minus sign in the elliptic curve and the vector space is compatible with the identification (2.2).) The next theorem and its proof provide us with an explicit way to find M and t.

(2.5) **Theorem.** *For a point $u \in k - \{0,1,\lambda\}$, we have*

$$u \in \operatorname{Im} c_M \Leftrightarrow -u(u-1)(u-\lambda) \equiv M \mod (k^\times)^2.$$

Proof. ($\Rightarrow$) Assume that $u = c_M(t)$, $t = (x, y, z) \in E_0(M, \lambda M)(k)$. Since $u = c_M(t) = \sigma\pi(t)$ by (1.13), we have $\psi(u) = \pi(t)$ from (1.7) and, using (1.10), $\rho x = u^2 - 2u + \lambda$, $\rho z = u^2 - \lambda$, $\rho \in k^\times$. Since $x^2 - z^2 = M$ by (0.1), we have $\rho^2 M = \rho^2(x^2 - z^2) = (\rho x + \rho z)(\rho x - \rho z) = -4u(u-1)(u-\lambda)$, or

(2.6) $-u(u-1)(u-\lambda) \equiv M \mod (k^\times)^2$.

($\Leftarrow$) Assume (2.6). Put $(x_0, y_0, z_0) = (u^2 - 2u + \lambda, -u^2 + 2u\lambda - \lambda, u^2 - \lambda)$. Then we have $x_0^2 - z_0^2 = -4u(u-1)(u-\lambda) = \rho^2 M$, $y_0^2 - z_0^2 = \rho^2 M$. Hence, setting $t = (x, y, z) = (x_0/\rho, y_0/\rho, z_0/\rho)$, we find $t \in E_0(M, \lambda M)(k)$ and $\psi(u) = \pi(t)$, i.e., $u = c_M(t)$, q.e.d.

Example (cf. [2]Ch. XIV, p 422). Let $k = \boldsymbol{Q}$, $M = \{\pm 1, \pm 2, \pm 3, \pm 5, \ldots\} = \{$squarefree integers$\}$, $\lambda = 3$ and $u = 25/9$. Then we have $-u(u-1)(u-\lambda) = -(25/9)(16/9)(-2/9) \equiv 2 \bmod (\boldsymbol{Q}^\times)^2$. Hence $M = 2$, $N = \lambda M = 2 \cdot 3 = 6$. To find $t \in E_0(2,6)(\boldsymbol{Q})$ such that $u = c_2(t)$, we first compute $t_0 = (x_0, y_0, z_0) = (u^2 - 2u + \lambda, -u^2 + 2u\lambda - \lambda, u^2 - \lambda) = (2 \cdot 209/3^4, 2 \cdot 241/3^4, 2 \cdot 191/3^4)$. Then $x_0^2 - z_0^2 = -4u(u-1)(u-3) = 2\rho^2$ with $\rho = 2^3 \cdot 5/3^3$. Finally, the point $t = (x, y, z) = t_0/\rho = (209/60, 241/60, 191/60) \in E_0(2,6)(\boldsymbol{Q})$ is what we want.

(2.7) **Definition.** Points u, u' in $k - \{0,1,\lambda\}$ are equivalent, written $u \sim u'$, if there exists $M \in \mathcal{M}$ such that $u, u' \in \operatorname{Im} c_M$.

In this situation, we obtain from (2.5)

(2.8) **Theorem.** $u \sim u' \Leftrightarrow u(u-1)(u-\lambda) \equiv u'(u'-1)(u'-\lambda) \bmod (k^\times)^2$.

For a global field k of characteristic not 2, let k_v be the local field at a prime v of k. For $\lambda \in k$, $\lambda \neq 0,1$, the set $k - \{0,1,\lambda\}$ is contained in $k_v - \{0,1,\lambda\}$ for all v. We shall denote by $\tilde{}_v$ the equivalence in $k_v - \{0,1,\lambda\}$. Then, by the Hasse principle for quadratic forms[2] and (2.5), we obtain a Hasse principle for our equiva-

lence $u \sim u'$ in $k - \{0,1,\lambda\}$:

(2.6) **Theorem.** *For* $u, u' \in k - \{0,1,\lambda\}$ *we have* $u \sim u'$ *if and only if* $u \underset{v}{\sim} u'$ *for all* v.

§3. Case $k = C$. Since C is algebraically closed $\mathcal{M}$ consists of a single element. In view of classical theory of elliptic functions, it is convenient to choose -1 as such.[3] As λ we use $\lambda = k^2 = k^2(\tau)$, values of *the* modular function for the group $\Gamma(2)$. Then we have

$$(3.1)\quad \boldsymbol{E}(\lambda; \boldsymbol{C}) = E(-1, -\lambda) = \{P \in P^3(\boldsymbol{C}) ; x_0^2 - x_1^2 = x_2^2,\ x_0^2 - \lambda x_1^2 = x_3^2\}.$$

For $\tau \in \mathcal{H}$, let

$$(3.2)\quad \Lambda_\tau = 4K(\boldsymbol{Z} + \boldsymbol{Z}\tau) \text{ with}$$

$$K = K(\tau) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

and

$$(3.3)\quad E_\tau = \boldsymbol{C}/\Lambda_\tau,\ \tau \in \Gamma(2) \backslash \mathcal{H}.$$

In this situation, there is an analytic isomorphism

$$(3.4)\quad \Theta_\tau : E_\tau \xrightarrow{\sim} \boldsymbol{E}(\lambda; \boldsymbol{C}).$$ ([5] Theorem 4.2)

From (1.13) and (3.4), we obtain a covering

$$(3.5)\quad c\Theta_\tau : E_\tau \to P^1(\boldsymbol{C}).$$

It turns out that

$$(3.6)\quad c\Theta_\tau(u) = \frac{dn(u,k) - 1}{cn(u,k) - 1} = \lambda \frac{cn(u,k) + 1}{dn(u,k) + 1}.$$

The four branch points of (3.6) over $0, 1, \infty, \lambda$ are $2K, 2K\tau, 2(K + K\tau), 0$, respectively.

References

[1] Cassels, J. W. S. and Fröhlich (eds.): Algebraic Number Theory. Academic Press, New York (1967).

[2] Euler, L.: Elements of Algebra (Translation of "Vollständige Anleitung zur Algebra"). Springer, New York (1984).

[3] Hurwitz, A. und Courant, R.: Vorlesungen über Allgemeine Funktionentheorie und Elliptische Funktionen. Springer, New York (1964).

[4] Ono. T.: Triangles and elliptic curves. I, II, III, IV. Proc. Japan Acad., **70A**, 106–108 (1994); **70A**, 223–225 (1994); **70A**, 311–314 (1994); **71A**, 104–106 (1995).

[5] Ono, T.: Variations on a Theme of Euler. Plenum, New York (1994).

[6] Tannery, J. et Molk, J.: Éléments de la Théorie des Fonctions Elliptiques. tomes I-IV, Chelsea, New York (1972).

[2] See [1] pp. 357–360.

[3] See [3] and/or [6] for standard notation. I take this opportunity to make corrections to my paper (III). First of all, at the bottom of p. 313, I put carelessly $P_\tau^* = P_\tau - \{0\}$ instead of $P_\tau^* = P_\tau - \{0, 2K, 2K\tau, 2(K + K\tau)\}$. Next, all lower case k's in "$4k$" on p. 312 line 11, line 12 and on p. 313 line 3 should be capitalized. Insert "$-$" (minus) in front of $\alpha/2$ on p. 314 formula (4.4). Finally, in view of the first correction, "$4K$" on p. 313 line 3 and line 14 from the bottom should read "$2K$".