Triangles and Elliptic Curves. VI

By Takashi ONO

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

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

This is a continuation of the series of papers [1] each of which will be referred to as (I), (II), (III), (IV), (V) in this paper. By a *real* triangle we shall mean an element of the following set:

(0.1) $Tr = \{t = (a, b, c) \in \boldsymbol{R}^3,\ 0 < a < b + c,\ 0 < b < c + a,\ 0 < c < a + b\}.$

For each $t \in Tr$, set $s = s(t) = \frac{1}{2}(a + b + c)$. One sees easily that

(0.2) $Tr = \{t = (a, b, c) \in \boldsymbol{R}^3,\ 0 < a, b, c < s\}.$

As in (I), we associate an elliptic curve E_t to $t \in Tr$:

(0.3) $E_t : y^2 = x^3 + P_t x^2 + Q_t x$

where

(0.4) $P_t = \frac{1}{2}(a^2 + b^2 - c^2),$

(0.5) $Q_t = -s(s-a)(s-b)(s-c) = -(\text{area of } t)^2.$

In this paper, we shall describe isomorphisms (over $\boldsymbol{R}$) among elliptic curves (0.3) in terms of relations among triangles (0.1).

§1. Basic facts. Let k be a field of characteristic not 2. Consider an elliptic curve of the form:

(1.1) $y^2 = x^3 + Px^2 + Qx,\ P, Q \in k.$

Referring to the standard notation of Weierstrass equations ([2], Chapter III, §1), we have

(1.2) $a_1 = a_3 = a_6 = 0,\ a_2 = P,\ a_4 = Q,$

(1.3) $b_2 = 4P,\ b_4 = 2Q,\ b_6 = 0,\ b_8 = -Q^2,$

(1.4) $c_4 = 16(P^2 - 3Q),\ c_6 = -32P(2P^2 - 9Q),$

(1.5) $\Delta = 16Q^2(P^2 - 4Q) \neq 0,$

(1.6) $j = c_4^3/\Delta = 2^8(P^2 - 3Q)^3/(Q^2(P^2 - 4Q)).$

Now let $k = \boldsymbol{R}$. Inspired by (0.5) for triangles, *we shall focus our attention on elliptic curves* (1.1) *with* $Q < 0$. Thus we have, from (1.4), (1.5), (1.6),

(1.7) $c_4 > 0,\ \Delta > 0,\ j > 0$

and

(1.8) $\operatorname{sign}(c_6) = -\operatorname{sign}(P),\quad c_6 = 0 \Leftrightarrow P = 0 \Leftrightarrow j = 1728.$

From now on, for a real number $a > 0$, we assume that $\sqrt{a} > 0$. We put

(1.9) $M = \frac{1}{2}(P + \sqrt{P^2 - 4Q}),\quad N = \frac{1}{2}(P - \sqrt{P^2 - 4Q}).$

Since $M - N = \sqrt{P^2 - 4Q} > 0$ and $MN = Q < 0$, we have

(1.10) $M > 0,\ N < 0.$

From (1.1), (1.9), it follows that

(1.11) $y^2 = x^3 + Px^2 + Qx = x(x + M)(x + N).$

Now, we introduce a quantity

(1.12) $\lambda = N/M < 0.$

Since the elliptic curve (1.11) is isomorphic (over $\boldsymbol{C}$) to the Legendre form $y^2 = x(x-1)(x-\lambda)$, we obtain

(1.13) $j = 2^8(\lambda^2 - \lambda + 1)^3/(\lambda^2(\lambda - 1)^2).$

Next, we put

(1.14) $\rho = -\frac{1}{2}(\lambda + \lambda^{-1}) = 1 - (P^2/2Q) \geq 1.$

Finally, following [3], Chapter V, §2, define a quantity γ:

(1.15) $\gamma = \begin{cases} \operatorname{sign}(c_6), & \text{if } j \neq 1728 \text{ (i.e., if } c_6 \neq 0) \\ \operatorname{sign}(c_4), & \text{if } j = 1728 \text{ (i.e., if } c_6 = 0). \end{cases}$

In view of (1.8), we have

(1.16) $\gamma = \begin{cases} 1, & \text{if } P \leq 0 \\ -1, & \text{if } P > 0. \end{cases}$

(1.17) **Proposition.** *Let* E, E' *be elliptic curves over* $\boldsymbol{R}$ *of the form* $E : y^2 = x^3 + Px^2 + Qx$, $E' : y^2 = x^3 + P'x^2 + Q'x$ *with* $Q, Q' < 0$. *Let* j, λ, ρ, γ (*resp.* $j', \lambda', \rho', \gamma'$) *be quantities* (1.6), (1.12), (1.14), (1.15) *for* E (*resp.* E'). *Then we have*

$$E \cong E' \text{ over } \boldsymbol{R} \Leftrightarrow \rho = \rho' \text{ and } \operatorname{sign} P = \operatorname{sign} P'.$$

Proof. First of all, we know ([3], Chapter V, §2) that

(1.18) $E \cong E'$ *over* $\boldsymbol{R} \Leftrightarrow j = j'$ *and* $\gamma = \gamma'$.

Now since λ, λ' are both < 0, we have

$$j' = j \Leftrightarrow \lambda' \in \{\lambda, 1/\lambda, 1 - \lambda, 1/(1-\lambda), \lambda/(\lambda - 1), (\lambda - 1)/\lambda\}$$
$$\Leftrightarrow \lambda' \in \{\lambda, 1/\lambda\} \Leftrightarrow \rho' = \rho.$$

Our assertion then follows from these equivalences and (1.16), (1.18). Q.E.D.

(1.19) **Corollary.** *Elliptic curves* $y^2 = x^3 + Qx$, $Q < 0$, *are all isomorphic over* $\boldsymbol{R}$.

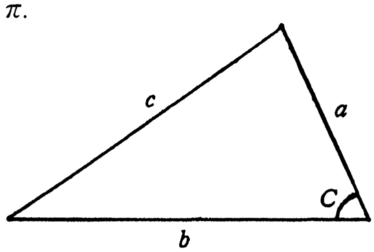
In fact, for $P=0$, $\rho=1$ for all $Q<0$.

Q.E.D.

§2. Real triangles. Let $t=(a, b, c)$ be an element of the set Tr in (0.1), (0.2). Since $Q_t = -(\text{area } t)^2 < 0$ by the definition (0.5), we can apply results of §1 to all elliptic curves E_t, $t \in Tr$. The meaning of P_t in (0.4) is obvious:

$$(2.1)\qquad P_t = \frac{1}{2}(a^2+b^2-c^2) = ab\cos C \begin{cases} >0, & \text{if } C<\pi/2, \\ =0, & \text{if } C=\pi/2, \\ <0, & \text{if } C>\pi/2, \end{cases}$$

where C is the angle between sides a and b, $0<C<\pi$.



From the defining equations:

$$(2.2)\qquad P = P_t = \frac{1}{2}(a^2+b^2-c^2) = ab\cos C,\quad t=(a, b, c),$$
$$Q = Q_t = -s(s-a)(s-b)(s-c),\quad s=\frac{1}{2}(a+b+c),$$

it follows that

$$(2.3)\qquad P^2-4Q=(ab)^2.$$

Substituting (2.3) into (1.5), (1.6), (1.9), (1.12), (1.14), we obtain

$$(2.4)\qquad \Delta = (4abQ)^2,$$
$$(2.5)\qquad j = 2^8(a^2b^2+Q)^3/(abQ)^2,$$
$$(2.6)\qquad M = s(s-c) = \frac{1}{2}(P+ab),\quad N = -(s-a)(s-b) = \frac{1}{2}(P-ab).$$
$$(2.7)\qquad \lambda = (P-ab)/(P+ab),$$
$$(2.8)\qquad \rho = (a^2b^2+P^2)/(a^2b^2-P^2) = (1+\cos^2 C)/(1-\cos^2 C).$$

Note that

$$(2.9)\qquad \rho \geq 1, \text{ and } \rho=1 \Leftrightarrow P=0 \Leftrightarrow C=\pi/2.$$

From (1.17), (1.19), (2.9), we obtain

(2.10) **Theorem.** *Let E_t, $E_{t'}$ be elliptic curves over $\boldsymbol{R}$ associated with real triangles $t=(a, b, c)$, $t'=(a', b', c')$. Let C be the angle between sides a, b with $0<C<\pi$ and C' be the one for t'. Then*

$$E_t \cong E_{t'} \text{ over } \boldsymbol{R} \Leftrightarrow C=C'.$$

§3. A triple of elliptic curves associated with a triangle. The statement (2.10) suggests that one should associate not only one elliptic curve E_t but an ordered triple $\boldsymbol{E}_t = \{E_{t,a}, E_{t,b}, E_{t,c}\}$ to a triangle $t=(a, b, c) \in Tr$. The definition of $\boldsymbol{E}_t$ is obvious: $E_{t,c}=E_t$ in the sense of (0.3) and $E_{t,a}$, $E_{t,b}$ are the results of cyclic permutations $(a, b, c) \mapsto (b, c, a)$, (c, a, b) applied to the definition of $E_{t,c}$, respectively. In other words, we have

$$(3.1)\qquad E_{t,a}: y^2 = x^3+P_{t,a}x^2+Q_tx \text{ where } P_{t,a} = \frac{1}{2}(b^2+c^2-a^2),$$
$$(3.2)\qquad E_{t,b}: y^2 = x^3+P_{t,b}x^2+Q_tx \text{ where } P_{t,b} = \frac{1}{2}(c^2+a^2-b^2),$$
$$(3.3)\qquad E_{t,c}: y^2 = x^3+P_{t,c}x^2+Q_tx \text{ where } P_{t,c} = \frac{1}{2}(a^2+b^2-c^2),$$

and

$$(3.4)\qquad Q_t = -s(s-a)(s-b)(s-c) = -(\text{ area of } t)^2,$$

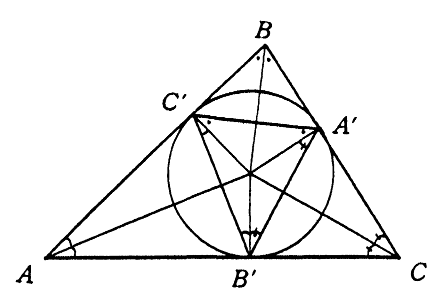
this being invariant under the cyclic permutations.

For $t=(a, b, c)$, $t'=(a', b', c') \in Tr$, triples $\boldsymbol{E}_t$, $\boldsymbol{E}_{t'}$ are said to be isomorphic over $\boldsymbol{R}$ if $E_{t,a}$, $E_{t,b}$, $E_{t,c}$ are isomorphic over $\boldsymbol{R}$ to $E_{t',a'}$, $E_{t',b'}$, $E_{t',c'}$, respectively. When that is so, we shall write $\boldsymbol{E}_t \cong \boldsymbol{E}_{t'}$. Now the following is an immediate consequence of (2.10):

(3.5) **Theorem.** *Let $\boldsymbol{E}_t$, $\boldsymbol{E}_{t'}$ be elliptic curves over $\boldsymbol{R}$ associated with real triangles $t=(a, b, c)$, $t'=(a', b', c')$, respectively. Then*

$$\boldsymbol{E}_t \cong \boldsymbol{E}_{t'} \text{ over } \boldsymbol{R} \Leftrightarrow t \text{ and } t' \text{ are similar.}$$

§4. Sequence of triangles. When a sequence $\{t_i=(a_i, b_i, c_i), i \geq 1\}$ of triangles is given, we obtain a sequence $\{\boldsymbol{E}_{t_i}\}$ of triples of elliptic curves. By way of illustration, let us consider an example where a sequence $\{t_i\}$ is formed inductively from a triangle by a simple geometric construction as seen in the following figure:



Let ABC be any triangle with sides $a = BC$, $b = CA$, $c = AB$. By abuse of notation, we use the same letter a for the length of BC, etc. Let A', B', C' be points on a, b, c at which the inscribed circle of the triangle ABC is tangent to sides a, b, c, respectively. Write $t = (a, b, c)$, $t' = (a', b', c')$. By a simple geometric thinking, we have

(4.1) $C' = \frac{1}{2}(A+B) = \frac{1}{2}(\pi - C) = \frac{1}{2}\pi - \frac{1}{2}C$,

(4.2) $\cos C = 1 - 2\sin^2(C/2) = 1 - 2\cos^2 C'$.

Similarly

(4.3) $\cos A = 1 - 2\cos^2 A'$, $\cos B = 1 - 2\cos^2 B'$.

Now let $t_i = (a_i, b_i, c_i)$, $i \geq 1$, be a sequence of triangles $A_iB_iC_i$ formed inductively from t_1 by the geometric construction $t \to t'$ described above. If we put $u_i = \cos A_i$, $v_i = \cos B_i$, $w_i = \cos C_i$, then (4.2), (4.3) become

(4.4) $u_i = 1 - 2u_{i+1}^2$, $v_i = 1 - 2v_{i+1}^2$, $w_i = 1 - 2w_{i+1}^2$, $i \geq 1$.

One finds that

(4.5) $\lim u_i = \lim v_i = \lim w_i = \frac{1}{2} \quad (i \to \infty)$.

Hence all angles A_i, B_i, C_i approach $\pi/3$ and so all elliptic curves in the triples $\{E_{t_i}\}$ eventually become isomorphic to the single elliptic curve of the form

(4.6) $y^2 = x^3 + 4x^2 - 3x$

which corresponds to the equilateral triangle $t = (2,2,2)$.

Here are some numerical data for the right triangle $t = (2, 2\sqrt{3}, 4)$. Then $s = 3 + \sqrt{3}$, $s - a = 1 + \sqrt{3}$, $s - b = 3 - \sqrt{3}$, $s - c = \sqrt{3} - 1$, $P_{t,a} = 12$, $P_{t,b} = 4$, $P_{t,c} = 0$, $Q = -12$, $E_t = \{y^2 = x^3 + 12x^2 - 12x,\ y^2 = x^3 + 4x^2 - 12x,\ y^2 = x^3 - 12x\}$.

As for other quantities such as Δ, j, M, N, λ, ρ ((2.4)-(2.8)), let us write, e.g., j_a for $j(E_{t,a})$, etc. Thus we have, for $t = (2, 2\sqrt{3}, 4)$,

(4.7) $\Delta_a = 2^{14}3^3$, $\Delta_b = 2^{14}3^2$, $\Delta_c = 2^{12}3^3$,

(4.8) $j_a = 2^4 3^3 5^3$, $j_b = 2^4 3^{-2} 13^3$, $j_c = 2^6 3^3$,

(4.9) $M_a = 6 + 4\sqrt{3}$, $M_b = 6$, $M_c = 2\sqrt{3}$,

(4.10) $N_a = -(4\sqrt{3} - 6)$, $N_b = -2$, $N_c = -2\sqrt{3}$,

(4.11) $\lambda_a = -(7 - 4\sqrt{3})$, $\lambda_b = -1/3$, $\lambda_c = -1$,

(4.12) $\rho_a = 7$, $\rho_b = 5/3$, $\rho_c = 1$.

§5. $A + B + C = \pi$. Let $t = (a, b, c)$ be a triangle with angles A, B, C as before. The three elliptic curves $E_{t,a}$, $E_{t,b}$, $E_{t,c}$ can not be independent because of the relation $A + B + C = \pi$. In fact, using the relations

(5.1) $P_a = P_{t,a} = bc\cos A$, $P_b = ca\cos B$, $P_c = ab\cos C$,

we find

(5.2) $a^2P_a^2 + b^2P_b^2 + c^2P_c^2 = -2P_aP_bP_c + a^2b^2c^2$

which is an algebraic relation among middle coefficients (P_a's) of three elliptic curves.

References

[1] Ono, T.: Triangles and elliptic curves. I ~ V. Proc. Japan Acad., **70A**, 106–108 (1994); **70A**, 223–225 (1994); **70A**, 311–314 (1994); **71A**, 104–106 (1995); **71A**, 137–139 (1995).

[2] Silverman, J. H.: The Arithmetic of Elliptic Curves. Springer, New York (1986).

[3] Silverman, J. H.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer, New York (1994).