Torsion points on elliptic curves and modular polynomial symmetries

Semjon Adlaj

CCRAS, Moscow, Russia

The joined MSU-CCRAS Computer Algebra Seminar

September 24, 2014

"A mysterious equality" E

Let γ_4 be a root of

$$r(x) := x^4 + 4\,\alpha\,x^3 + 2\,x^2 - \frac{1}{3},\ \alpha \in \mathbb{C} \setminus \left\{\pm\frac{2}{3}\right\},$$

and put

$$t(x) := x^3 + \left(\frac{1}{\gamma_4^2} - 4\right) x + 2\,\gamma_4.$$

One might, then, verify that for any given root ξ of t, thus $t(\xi) = 0$, and any given root $\gamma \neq \gamma_4$ of r, thus $r(\gamma) = 0$, the equality

$$E:\ \xi^9 \left(\frac{r(1/\xi)}{r(\xi)}\right)^2 = -2\gamma_4 \left(\frac{\gamma^3\,t(1/\gamma)}{t(\gamma)}\right)^2$$

holds, and so all three value pairs (on both sides of the equation) coincide with one and the same invariant, which lies, in fact, in the field of rational functions in the variable γ_4.

The equality E as an exception to Vavilov rule

Nikolai Vavilov (PDMI, St. Petersburg) notes that (any!) formula, taken from contemporary source on Number Theory (such as Introduction to Modern Number Theory Fundamental Problems by Manin Ju. & Panchishkin A.), which length exceeds 2.5 inches is wrong! He does not exclude that the critical length might be up to 3.5 inches for some other disciplines, such as analysis. He further comments that formulas derived and correctly written in an original source (from nineteenth century, say) are too often transferred to said contemporary books with multiple errors. The remedy to this problem was known to Bartel Leendert van der Waerden: “Het is niet alleen veel leerrijker, het geeft ook veel meer genot de klassieke schrijvers zelf te lezen.” He goes on to say “Daarom zeg ik mijn lezers met nadruk: geloof niets op mijn woord, maar kijk alles na!”

The equality E on the preceding slide was presented on April 16, 2014 at the 7^{th} PCA conference in St. Petersburg. It (being correct) is, thus, an exception to Vavilov's rule.

Towards proving the equality E

Ivan Kozhevnikov (CC RAS, Moscow) tested (by hand!) several special cases, including the case when the expressions (on both sides) coincide with (complex) infinity.

Mikhail Malykh (FNM MSU, Moscow) applied further numerical (computer) tests, and employed Sage and Maple packages to simplify the difference between the left-hand and the right-hand sides with negative result!

Sergei Meshveliani (PSI RAS, Pereslavl-Zalessky) repoted a machine-proof (employing Grobner basis techniques) which he presented on May 21, 2014 at the $17^{\rm th}$ Workshop on Computer Algebra (Dubna, Russia).

Helmut Ruhland, in recent communication, presented an elementary (no machine requiring) constructive proof, which I (given his permission) shall present at this talk.

$$\left(\frac{\gamma^4 p_4(\frac{1}{\gamma})}{p_4(\gamma)}\right)^2 = -2\gamma_4\left(\frac{\gamma^3 p_3(\frac{1}{\gamma})}{p_3(\gamma)}\right)^2$$

$\gamma \to p_4(x) = x^4 + 4\alpha x^3 + 2x^2 - \frac{1}{3}$

$\zeta \to p_3(x) = x^3 + \left(\frac{1}{\gamma_4^2} - 4\right)x + 2\gamma_4$

$\gamma \neq \gamma_4$

$$\left(\frac{\zeta^4 p_4(\frac{1}{\zeta})}{p_4(\zeta)}\right)^2$$

$p_4(x) = x^4 + 4\alpha x^3 + 2x^2 - \frac{1}{3} = x^3(x + 4\alpha) + 2\left(x - \frac{1}{\sqrt6}\right)\left(x + \frac{1}{\sqrt6}\right) =$

$= \left(x - \frac{1}{\sqrt6}\right)\left(x^3 + 2x + \frac{2}{\sqrt6}\right)$

пусть $4\alpha = -\frac{1}{\sqrt6}$, т.е $\alpha = -\ldots$

возьмём $\boxed{\gamma_4 = \frac{1}{\sqrt6}}$

Тогда $p_3(x) = x^3 + 2x + \frac{2}{\sqrt6}$, т.е $p_4(x) = (x - \gamma_4)\, p_3(x)$

Было со знаменателем, т.к $\gamma \neq \gamma_4 \Rightarrow$ γ есть корень $p_3(x)$

ζ есть корень $p_3(x)$

Не менее подсчитаем левую часть:

$$\left(\frac{\zeta^4 p_4(\frac{1}{\zeta})}{p_4(\zeta)}\right)^2 = \zeta\left(\frac{\zeta^4\left(\frac{1}{\zeta} - \frac{1}{\sqrt6}\right)p_3(\frac{1}{\zeta})}{\left(\zeta - \frac{1}{\sqrt6}\right)p_3(\zeta)}\right)^2 = \left(\frac{\zeta^3 p_3(\frac{1}{\zeta})}{p_3(\zeta)}\right)^2 \zeta\left(\frac{\left(1 - \frac{\zeta}{\sqrt6}\right)}{\left(\zeta - \frac{1}{\sqrt6}\right)}\right)^2$$

$$\frac{\zeta(\sqrt6 - \zeta)^2}{(\sqrt6\zeta - 1)^2} = \frac{\zeta(\zeta^2 - 2\sqrt6\zeta + 6)}{6\zeta^2 - 2\sqrt6\zeta + 1} = \frac{\zeta^3 - 2\sqrt6\zeta^2 + (6\zeta - 4\zeta) + 4\zeta + \frac{2}{\sqrt6} - \frac{2}{\sqrt6}}{6\zeta^2 - 2\sqrt6\zeta + 1} =$$

$$= \frac{p_3(\zeta) - \frac{2}{\sqrt6}(6\zeta^2 - 2\sqrt6\zeta + 1)}{6\zeta^2 - 2\sqrt6\zeta + 1} = \frac{p_3(\zeta)}{6\zeta^2 - 2\sqrt6\zeta + 1} - \frac{2}{\sqrt6}$$

$$\left(\frac{\zeta^3 p_3(\frac{1}{\zeta})}{p_3(\zeta)}\right)^2\left[\frac{\overset{=0}{p_3(\zeta)}}{6\zeta^2 - 2\sqrt6\zeta + 1} - \frac{2}{\sqrt6}\right] = -\frac{2}{\sqrt6}\left(\frac{\gamma^3 p_3(\frac{1}{\gamma})}{p_3(\gamma)}\right)^2 \cdot p_3^2(\zeta)$$

$(-2\gamma_4)$

$p_3^2(\zeta) = 0$

Constructing (mysterious) equalities

1. Introduction

In [1] the following 2 polynomials and a mysterious equality (abbreviated in the following with m. e.) are defined:

(1) $$p_4(x) := x^4 + 4\,\alpha\,x^3 + 2\,x^2 - \frac{1}{3}$$

(2) $$p_3(x) := x^3 + \left(\frac{1}{\gamma_i^{\,2}} - 4\right)x + 2\,\gamma_i$$

There it's proofed:

Let $\alpha \neq \pm 2/3$, let γ_i be any root of (1), $\gamma \neq \gamma_i$ any other root of (1) and ξ any root of (2), then for all 4 x 3 x 3 combinations of the roots the following equality holds:

(3) $$\frac{\zeta^9\, p_4\!\left(\frac{1}{\zeta}\right)^2}{p_4(\zeta)^2} = -\frac{2\,\gamma_i\,\gamma^6\, p_3\!\left(\frac{1}{\gamma}\right)^2}{p_3(\gamma)^2}$$

The left/right hand side is a rational function of γ_i, i.e. ϵ **Q** (γ_i)

These polynomials and the equality are related to the modular equation of level 3.

2. Constructing the equalities

Here the equalities are constructed in an elementary manner without any connection to elliptic functions or modular equations. But almost all examples are related to these.

Let $p_{a,k}(x)$ the polynomial of degree N, defined by the following equality:

(4.1) $$x^N\left(\frac{1}{x} - \gamma_i\right)^{(N-1)} = a\,\gamma_i^{\,k}\,(x - \gamma_i)^{(N-1)}$$

For $N \leq 0$ in (4.1) $p_{a,k}(x)$ is no polynomial, treating the polynomial in the numerator as "ansatz" leads to a second polynomial $r_{a,k}(x)$

(4.2) $$x\,(x - \gamma_i)^{(N-1)} = a\,\gamma_i^{\,k}\,x^{(N-1)}\left(\frac{1}{x} - \gamma_i\right)^{(N-1)}$$

Properties:
- the reciprocal polynomial i.e. $p_{a,k}(1/x) * x^N = p_{1/a,-k}(x)$
- the reciprocal polynomial $r_{a,k}(1/x) * x^N = r_{1/a,-k}(x)$
- $p_{a,k}(x)$ and the substitution $\gamma_i \to 1/\gamma_i \sim r_{a,-k}(x)$
- $r_{a,k}(x)$ and the substitution $\gamma_i \to 1/\gamma_i \sim p_{a,-k}(x)$

Define the 2 polynomials:

(4.3) $p_\gamma(x) := p_{a,k}(x)$ and γ be a root of $p_\gamma(x)$

(4.4) $p_\zeta(x) := p_{b,l}(x)$ and ξ be a root of $p_\xi(x)$

Using the 4 factorisations of appendix A leads to this equality:

(5) $$\frac{\zeta^N\, p_\gamma\!\left(\frac{1}{\zeta}\right)}{p_\gamma(\zeta)} = -\frac{\gamma^N\, p_\zeta\!\left(\frac{1}{\gamma}\right)}{p_\zeta(\gamma)} = \mathrm{Q}(\gamma_i)$$ a function of γ_i only

(5.1) $$\mathrm{Q}(\gamma_i) := \frac{a\,b\,\gamma_i^{\,(k+l)} - 1}{a\,\gamma_i^{\,k} - b\,\gamma_i^{\,l}}$$

Special cases: k = 0 and a = 1 $\to$ Q () = 1, l = 0 and b = 1 $\to$ Q () = -1

Define the polynomial of degree N + 1:

(4.5) $$q_\gamma(x) := (x - \gamma_i)\,p_\gamma(x) = (x - \gamma_i)\,p_{a,k}(x)$$

Rising (5) to the $(N-1)^{th}$ power and using (4.4) and (4.5) for the left side yields

(5.2) $$\frac{\zeta^{(N^2)}\, q_\gamma\left(\frac{1}{\zeta}\right)^{(N-1)}}{q_\gamma(\zeta)^{(N-1)}} = \frac{b\,\gamma_i^{\,l}\,(-1)^{(N-1)}\,\gamma^{(N(N-1))}\,p_\zeta\left(\frac{1}{\gamma}\right)^{(N-1)}}{p_\zeta(\gamma)^{(N-1)}} = b\,\gamma_i^{\,l}\,Q(\gamma_i)^{(N-1)}$$

By construction this equality is valid **only** for γ_i the root of the **linear factor** of q_γ (x), but the m. e. is valid for all roots!

The same construction for the polynomials $r_{a,\,k}$ (x) (4. 2) changes almost nothing. Only (5.2) has to be replaced by:

(5.3) $$\frac{\zeta^{(N^2-2)}\, q_\gamma\left(\frac{1}{\zeta}\right)^{(N-1)}}{q_\gamma(\zeta)^{(N-1)}} = \frac{(-1)^{(N-1)}\,\gamma^{(N(N-1))}\,p_\zeta\left(\frac{1}{\gamma}\right)^{(N-1)}}{b\,\gamma_i^{\,l}\,p_\zeta(\gamma)^{(N-1)}}$$

this differs from (5.2) in the power of ξ on the left hand side and b, γ_i are in the denominator on the right hand side.

3. Conditions to be a mysterious equality i.e. an equality for all roots γ_i

Now we look for conditions under that (5.2) or (5.3) is an equality for all roots γ_i of q_γ (x).

At first some examples:

Example 1:

N = 3, a = - 1 / 3, k = -1, b, l = free (b ϵ **R**, l ϵ **Z**)

For these parameters and the specialisation b = - 2, l = 1
(5.2) is equals to (3), $p_{-2,\,1}$ (x) is proportional to p_3 (x) in (2)
and (4.3) q (x) = (x - γ_i) * $p_{-1/3,\,-1}$ (x) is proportional to

$$x^4 + x^3\left(-\frac{2}{\gamma_i} + \frac{1}{3}\frac{1}{\gamma_i^{\,3}} - \gamma_i\right) + 2\,x^2 - \frac{1}{3}$$

which of course by construction is reducible in Q (γ_i)

Setting the coefficient of x^3 to 4*α this is exactly p_4 (x) in (1).

This p_4 (x) is irreducible in **Q** (α) with Galois group S_4.

Now a sufficient condition (8):
If the degree N + 1 polynomial q_γ (x) in (4.3) after a rational reparametrisation by α is irreducible over **Q** (α) and the Galois group is at least 2-transitive then the equality (5.2) is fulfilled for all roots γ_i of q_γ (x) i.e. is a m.e.

These are exactly the polynomials and the m. e. from [1].

Comment to the parametrization of p_3 (x) and elliptic curves:

It can bee seen easily seen that this parametrization of p_3 (x) by b ϵ **R**, l ϵ **Z** is just a deformation of the coelliptic polynomial t_m (x) in [1] that causes a linaer transformation on the s_m () and therefore does not change the value of β_m^2. So this parametrized p_3 (x) is something like a generalised coelliptic polynomial? Of course the m. e. (5.2) with b and l then can be derived from the formula with $r_{j,\,n}$ (0) and t_m (0) in [1].

Example 2:

N = 2, a, k = free (a ϵ **R**, k ϵ **Z**), b = 1, l = 0

$$q_3(x) := (x-\alpha)\left(x^2\left(\frac{1}{x}-\alpha\right) - a\,\alpha^k\,(x-\alpha)\right) \quad p_2(x) := x^2 - 1$$

$$\frac{\zeta^4\, q_3\left(\frac{1}{\zeta}\right)}{q_3(\zeta)} = -\frac{\gamma^2\, p_2\left(\frac{1}{\gamma}\right)}{p_2(\gamma)}$$ (5.1) for N = 2

p_2 (x) is independent from γ_i, so ξ = ± 1, and the left hand side is equals 1
The right hand side is 1 for arbitrary γ, q_3 (x) could be replaced by an even more general polynomial (of arbitrary degree).

Though this is a little bit trivial example, this shows that condition (8) is not necessary (a reparametrisation of q_3 (x) to get irreducibility is not possible)

Example 3:

N = 1, a = free (a ϵ **R**), k = -1, b, l = free (b ϵ **R**, l ϵ **Z**)

$$q_2(x) := x^2 + x\left(-\frac{a}{\gamma_i} - \gamma_i\right) + a \qquad p_1(x) := x - b\,\gamma_i^{\,l}$$

$\zeta = b\,\gamma_i^{\,l}$ (5.1) for N = 1

reparameterising with $\alpha = -\frac{1}{6}\frac{a}{\gamma_i} - \frac{1}{6}\gamma_i$

leads to the irreducible (for a ≠ 9 * α^2) $q_2(x) := x^2 + 6\,x\,\alpha + a$

For a = 4 these are the polynomials and the equality related to the modular equation of level 4 (see table 1).

$$q_2\left(x+\frac{1}{x}\right)x^2 = x^4 + 6\,x^3\,\alpha + 6\,x^2 + 6\,x\,\alpha + 1$$

is the 4th degree equation for the primitive, nontrivial (± 1 are the trivial) 4-division points, see [2]. See the polynomials $R_{4,3}(x)$ and $S_{4,3}(x)$ in appendix B too.

level	$\mathbf{Z}_n^x$	N	a	k	remarks	q (x)	R / S
2	$\mathbf{Z}_2$	1	1	-1		$q_2(x) := x^2 + 3\,x\,\alpha + 1$	$R_{2,2}$
3	$\mathbf{Z}_2$	3	-1/3	-1		$q_4(x) := x^4 + 4\,x^3\,\alpha + 2\,x^2 - \frac{1}{3}$	R_3
4	$\mathbf{Z}_2$	1	4	-1		$q_2(x) := x^2 + 6\,x\,\alpha + 4$	$S_{4,3}$
6	$\mathbf{Z}_2^2$	3	-3	1	►	● $q_4(x) := x^4 - 6\,x^2 - 12\,x\,\alpha - 3$	$R_{6,1}$
							$?_{6,2}$
8	$\mathbf{Z}_2^2$	1	-1	1	$\gamma_i = \gamma_i - 4$	$q_2(x) := x^2 - 4\,x - 4 - 12\,\alpha$	$S_{8,1}$
12	$\mathbf{Z}_2^2$						$?_{12,1}$
24	$\mathbf{Z}_2^3$						$?_{24,1}$

Table 1: the examples to m. e. s

► use $pr_{a,k}(x)$ and formulas (4.x*) and (5.x*)
● reciprocal to $q_4(x)$ of level 3, the m.e. is now (5.3) with ξ^7 instaed of ξ^9 !

Questions:
- are there other $p_{a,k}(x)$ than in table 1 that fulfil the condition (8)?
- can the coelliptic polynomials $t_m(x)$ for p = 5, 7, … in [1] parametrized too, so β_m^2 does not change?

Appendices

Appendix A: Factorising the $p_\xi(x)$ and $p_\gamma(x)$ for roots

Now the p (x)´s (4.1) for γ, ξ with different arguments can be expressed as products, due to the special form (4):

(6.1) $p_\zeta(\gamma) = p_\zeta(\gamma) - p_\gamma(\gamma)$

Adding multiples of the defining equation for γ does not change the right hand side, but this cancels the term γ^N with highest degree, the right hand side now factors

(7.1) $p_\zeta(\gamma) = -(\gamma-\gamma_i)^{(N-1)}(-a\,\gamma_i^{\,k} + b\,\gamma_i^{\,l})$

(6.2) $p_\zeta\left(\frac{1}{\gamma}\right) = p_\zeta\left(\frac{1}{\gamma}\right) + \frac{b\,\gamma_i^{\,l}\,p_\gamma(\gamma)}{\gamma^N}$

the constant term with γ^0 is canceled, the right hand side now factors

(7.2) $p_\zeta\left(\frac{1}{\gamma}\right) = \frac{(\gamma-\gamma_i)^{(N-1)}(-a\,b\,\gamma_i^{\,(k+l)} + 1)}{\gamma^N}$

(6.3) $p_\gamma(\zeta) = p_\gamma(\zeta) - p_\zeta(\zeta)$

the term with ξ^N is canceled, the right hand side now factors

(7.3) $p_\gamma(\zeta) = (\zeta-\gamma_i)^{(N-1)}(-a\,\gamma_i^{\,k} + b\,\gamma_i^{\,l})$

(6.4) $p_\gamma\left(\frac{1}{\zeta}\right) = p_\gamma\left(\frac{1}{\zeta}\right) + \frac{a\,\gamma_i^{\,k}\,p_\zeta(\zeta)}{\zeta^N}$

the constant term with ξ^0 is canceled, the right hand side now factors

(7.4) $p_\gamma\left(\frac{1}{\zeta}\right) = \frac{(\zeta-\gamma_i)^{(N-1)}(-a\,b\,\gamma_i^{\,(k+l)} + 1)}{\zeta^N}$

Remark:

Instead of (6.1) this $p_\zeta(\gamma) = p_\zeta(\gamma) - \frac{a\,\gamma_i^{\,k}\,p_\gamma(\gamma)}{b\,\gamma_i^{\,l}}$ could be used too, this cancels the term with γ^0 instead of γ^N and factorises too. The result is equals to (7.1) using the defining equality (4) for $p_{b,l}(x)$. Similar for the 3 cases (6.2) – (6.4)

For the polynomials r (x) (4.2) slightly different results are obtained, but the result is the same quotients.

Appendix B: Division points for the essential elliptic curve E_β

The essential elliptic curve: $y^2 - 4x^3 - 12\alpha x^2 - 4x$

Some addition formulas (only for the x-components):

∞	0	-β	-1/β
x	$\frac{1}{x}$	$-\frac{x\beta+1}{x+\beta}$	$-\frac{x+\beta}{x\beta+1}$

The doubling formula:

$$x_2 := \frac{(x-1)^2(x+1)^2}{y^2} \qquad y_2 := \frac{2(x-1)(x+1)R_{4,3}(x)}{y^3}$$

The tripling formula:

$$x_3 := \frac{x R_{6,1}(x)^2}{R_3(x)^2} \qquad y_3 := \frac{y R_{6,1}(x) R_{6,2}(x)}{R_3(x)^3}$$

The equations of the primitive division points:

The following table lists the polynomials for the 7 levels with unit group $\mathbf{Z}_2^{\ k}$

column # : number of primitive division points, for level > 2 each x-division point exists twice (for ± y), s the sum all degrees is only # / 2

For reciprocal polynomials the polynomials S (x) of half degree are given R (x) = S (x + 1 / x).

The ?R (x) polynomials of degree 3 are the cubic resolvents of degree 4 polynomials

level	#	R (x)
2	3	$R_{2,1} := x$
		$R_{2,2} := x^2 + 3\alpha x + 1$
3	8	$R_3 := 3x^4 + 6x^2 + 12x^3\alpha - 1$
		$RR_3 := 3x^3 - 6x^2 + 4x - 8 + 16\alpha^2$

4	12	$R_{4,1} := x - 1$
		$R_{4,2} := x + 1$
		$R_{4,3} := x^4 + 6\alpha x^3 + 6x^2 + 6\alpha x + 1$
		$S_{4,3} := x^2 + 6\alpha x + 4$
		$RR_{4,3} := (x-2)(x^2 - 4x + 36\alpha^2 - 12)$
6	24	*** $R_{6,1} := x^4 - 6x^2 - 12\alpha x - 3$
		*** $RR_{6,1} := x^3 + 6x^2 + 12x + 72 - 144\alpha^2$
		$R_{6,2} := x^8 + 12\alpha x^7 + 28x^6 + 84\alpha x^5 + x^4(6 + 144\alpha^2) + 84\alpha x^3 + 28x^2 + 12\alpha x + 1$
		$S_{6,2} := x^4 + 12\alpha x^3 + 24x^2 + 48\alpha x + 144\alpha^2 - 48$
		$SR_{6,2} := x^3 - 24x^2 + 192x + 18432\alpha^2 - 4608 - 20736\alpha^4$
		$T_{6,2,1} := 4x^3\beta^2 + \beta + 4x + 6x^2\beta + x^4\beta$
		$TR_{6,2,1} := x^3 - 6x^2 + 12x + 24 - 16\beta^2 - \frac{16}{\beta^2}$
		$T_{6,2,2} := 4x\beta^2 + \beta + 6x^2\beta + 4x^3 + x^4\beta$
		$TR_{6,2,2} := TR_{6,2,1}$
8	48	$R_{8,1} := x^4 - 4x^3 + x^2(-12\alpha - 2) - 4x + 1$
		$S_{8,1} := x^2 - 4x - 12\alpha - 4$
		$R_{8,2} := x^4 + 4x^3 + x^2(12\alpha - 2) + 4x + 1$
		$S_{8,2} := x^2 + 4x + 12\alpha - 4$
		$R_{8,3} := x^{16} + 24x^{15}\alpha + x^{14}(88 + 72\alpha^2) + 840x^{13}\alpha + x^{12} + \dots$
		$S_{8,3} := x^8 + 24\alpha x^7 + (80 + 72\alpha^2)x^6 + 672\alpha x^5 + (-416 + 3456\alpha^2)x^4 + \dots$
12	96	$R_{12,1} := x^8 + 8x^7 + x^6(-20 + 72\alpha) + x^5(56 - 96\alpha + 144\alpha^2) + \dots$
		$S_{12,1} := x^4 + 8x^3 + (-24 + 72\alpha)x^2 + (32 - 96\alpha + 144\alpha^2)x + 16 + 96\alpha - 144\alpha^2$
		$R_{12,2} := x^8 - 8x^7 + x^6(-20 - 72\alpha) + x^5(-56 - 96\alpha - 144\alpha^2) + \dots$
		$S_{12,2} := x^4 - 8x^3 + (-24 - 72\alpha)x^2 + (-32 - 96\alpha - 144\alpha^2)x + 16 - 96\alpha - 144\alpha^2$
		$R_{12,3} := x^{32} + 48\alpha x^{31} + x^{30}(144\alpha^2 + 432) + 7440x^{29}\alpha + \dots$

		$S_{12,3} := x^{16} + 48\,x^{15}\,\alpha + (144\,\alpha^2 + 416)\,x^{14} + 6720\,x^{13}\,\alpha + \ldots$
24	384	$S_{24,1} := x^{16} - 32\,x^{15} + (-1248\,\alpha - 352)\,x^{14} + (-8064\,\alpha - 2688 - 16128\,\alpha^2)\,x^{13} + \ldots$
		$S_{24,2} := x^{16} + 32\,x^{15} + (1248\,\alpha - 352)\,x^{14} + (-8064\,\alpha + 2688 + 16128\,\alpha^2)\,x^{13} + \ldots$
		$R_{24,3} := x^{128} + 192\,x^{127}\,\alpha + (2880\,\alpha^2 + 6848)\,x^{126} + (13824\,\alpha^3 + 505920\,\alpha)\,x^{125} + \ldots$

Table 2: polynomials for the division points of E_β

*** $R_{6,1}$ is reciprocal to R_3

Special values: $j = 1$, $\alpha = \pm 1/\sqrt{2}$, $\beta = \pm\sqrt{2}, \pm 1/\sqrt{2}$
$j = 0$, $\alpha = \pm 1/\sqrt{3}$, $\beta = \sqrt{3}/2 \pm i/2$ = 12th unit roots with re > 0

The following table shows, how a polynomial splits for the half/third of the points

level		1 / 2 div. points	
2	$R_{2,1}$	$R_{4,1}$, $R_{4,2}$	
	$R_{2,2}$	$R_{4,3}$	
3	R_3	$R_{6,1}$, $R_{6,2}$	R_3
4	$R_{4,1}$	$R_{8,1}$	
	$R_{4,2}$	$R_{8,2}$	
	$R_{4,3}$	$R_{8,3}$	
6	$R_{6,1}$	$R_{12,1}$, $R_{12,2}$	
	$R_{6,2}$	$R_{12,3}$	
12	$R_{12,1}$	$R_{24,2}$	
	$R_{12,2}$	$R_{24,1}$	
	$R_{12,3}$	$R_{24,3}$	

level		1 / 3 div. points	
2	$R_{2,1}$	$R_{6,1}$	$R_{2,1}$
	$R_{2,2}$	$R_{6,2}$	$R_{2,2}$
4	$R_{4,1}$	$R_{12,2}$	$R_{4,1}$
	$R_{4,2}$	$R_{12,1}$	$R_{4,2}$
	$R_{4,3}$	$R_{12,3}$	$R_{4,3}$
8	$R_{8,1}$	$R_{24,1}$	$R_{8,1}$
	$R_{8,2}$	$R_{24,2}$	$R_{8,2}$
	$R_{8,3}$	$R_{24,3}$	$R_{8,3}$

Table 3: splitting of the polynomial of division points

References

[1] S. Adlaj (Computing Centre of RAS, Moscow), Modular Polynomial Symmetries, talk at the 17th Workshop on Computer Algebra, may 21 - 22, 2014, Dubna

[2] S. Adlaj, Eighth Lattice Points Preprint, arXiv:1110.1743v1 [math.NT] 8 Oct 2011

Helmut Ruhland, 06. Aug. 2014

e-mail : Helmut.Ruhland50@web.de

An essential elliptic function and its associated curve

Associate to a fixed (elliptic modulus) $\beta \in \mathbb{C} \setminus \{-1, 0, 1\}$ a value $\alpha = \alpha(\beta) := (\beta + 1/\beta)/3$ and

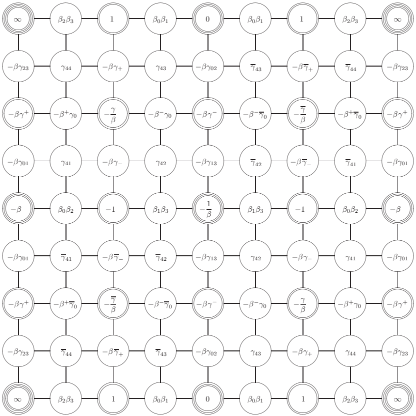
- a (cubic) polynomail $q(x) := x^3 + 3\,\alpha\,x^2 + x$,
- an elliptic function $\mathcal{R}_\beta$, with a (double) pole at zero, satisfying the differential equation

$$x'^2 = 4\,q(x),$$

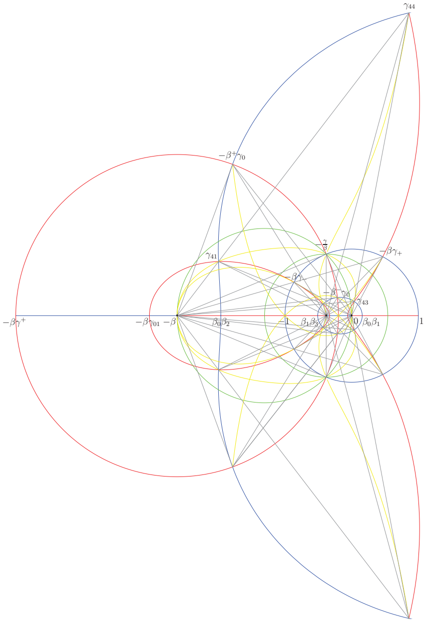
- Λ_β: the lattice of $\mathcal{R}_\beta$,
- a complex (projective) elliptic curve (associated with $\mathcal{R}_\beta$)

$$E_\beta : y^2 = 4\,q(x).$$

Attention! The latter (canonical) form ought not be confused with "the Weierstrass normal form". The justification for deviating from the (much) established convention is given in [1, 2].



The values of the essential elliptic function $\mathcal{R}$, satisfying the differential equation $\mathcal{R}'^2 = 4\mathcal{R}\,(\mathcal{R}+\beta)\,(\mathcal{R}+1/\beta)$, for $\beta > 1$, whose lattice is Λ, at the nodes of the lattice $\Lambda/8$.

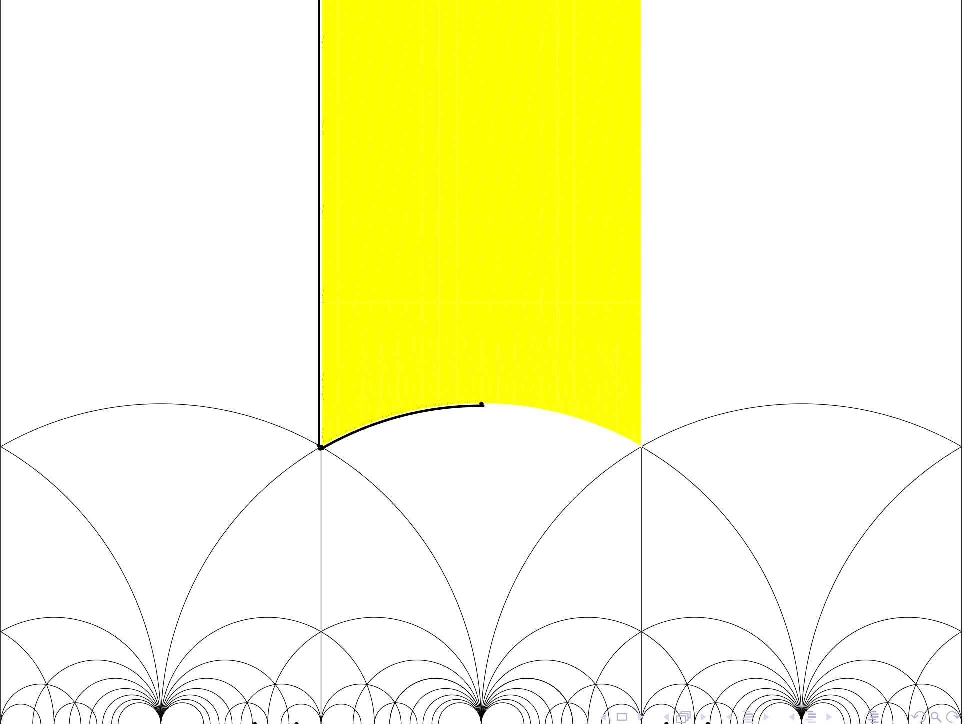


Two correspondences

The map

$$\mathbb{C}/\Lambda_\beta \to E_\beta$$
$$\mathrm{z} \mapsto (\mathcal{R}_\beta(\mathrm{z}), \mathcal{R}'_\beta(\mathrm{z})),$$

which turns out being an isomorphism of Riemann surfaces, as well as, an isomorphism of groups, enables an identification (exploiting the modular j-invariant) of isomorphism classes of projective complex elliptic curves with the homothety classes of lattices $\mathcal{L}/\mathbb{C}^\times$, which might, in turn, be identified with the fundamental domain $\mathcal{D} := \mathrm{PSL}(2,\mathbb{Z})\backslash\mathcal{H}$ for the action of the modular group $\mathrm{PSL}(2,\mathbb{Z})$ upon the (extended) upper half plane $\mathcal{H}$.



An explicit analytic inverse of the modular invariant

An explicit analytic inverse k of the modular invariant j was given in [3] as a composition

$$k := k_0 \circ k_1 \circ k_2,$$

where

$$k_0(x) := \frac{i\, M\left(\sqrt{1-x^2}\,\right)}{M(x)}, \;\; k_1(x) := \frac{\sqrt{x+4}-\sqrt{x}}{2},$$

$$k_2(x) := \frac{3}{2}\left(\frac{x}{k_3(x)} + k_3(x)\right) - 1,$$

$$k_3(x) := \sqrt[3]{\sqrt{x^2-x^3}-x},$$

and $M(x)$ is the arithmetic-geometric mean of 1 and x.

Key properties of the inverse of the modular invariant

Strictly speaking, the function M is (doubly) infinitely-valued as its calculation entails choosing one of two branches of the square root function at infinitely many steps. Consequently, the function k is, as well, an infinitely-valued function. However, its values, up to a sign, differ by the action of the modular group $\mathrm{PSL}(2,\mathbb{Z})$. We mean that by flipping the sign, if necessary, we might assume that the function k never assumes values in the lower half plane, and, furthermore, its values might be brought via the action of the modular group $\mathrm{PSL}(2,\mathbb{Z})$ to a single value in the (or any) fundamental domain. In other words, while k is not strictly a left inverse of j, it is a right inverse, that is,

$$\forall x \in \mathbb{C},\ j \circ k\,(x) = x,$$ [1]

for the modular invariant j does not separate points, in its domain, as long as they differ by the action of the modular group $\mathrm{PSL}(2,\mathbb{Z})$, and no troubles arise in extending the latter equality to the whole Riemann sphere, including the point at (complex) infinity.

[1] An analogy is afforded by a branch of the logarithmic function which is (regradless of the choice of the branch) a right (but not left) inverse of the exponential function. While the values of the logarithm, at a given point, constitute a discrete subset of a line, the values of the functions k and M do not. We have already indicated that the function M is (doubly) infinitely-valued, suggesting that its values (at a given point) constitute a discrete subset of $\mathbb{C}$ (not contained in any one-dimensinal subset over $\mathbb{R}$), and so is the function k.

Verifying the formula for the inverse k at (the image of j at the corners of the fundamental domain) 0 and 1

Before we move on to the modular equation, we must clarify the calculation of the inverse function k for the two special values of j at the corners: $j(\zeta) = 0$ and $j(i) = 1$.[2] So, we point out that the (set) values of the composition, $k_1 \circ k_2$ at 0 and 1, coincide with set values of the elliptic moduli β at $\tau = \zeta$ and $\tau = i$, which, respectively, are the four values $\beta \in \{\pm i\zeta, \pm i\zeta^2\}$ and the six values $\beta \in \{\pm i, \pm 1/\sqrt{2}, \pm\sqrt{2}\}$. Certainly, k_2 has a removable singularity at zero and must be evaluated to -1 there, whereas $k_2(1) = 1/2$. Thus, $\zeta \in k(0) = k_0 \circ k_1(-1)$, and $i \in k(1) = k_0 \circ k_1(1/2)$.[3]

[2] We denoted by ζ a primitive cube root of unity, so $\zeta^3 = 1 \neq \zeta$.

[3] Implying, unsurprisingly, that the values 0 and 1 are fixed by the (identity) function $j \circ k$.

The Inverse of the Modular Invariant j(τ)

1. Introduction

In [1], page 1 the following inverse of the modular invariant j(τ) presented at the CCRAS (Moscow, Russia) is given:

(1) $k_0(x) = \frac{G(1, \sqrt{1-x^2})\, I}{G(1, x)}$

(2) $k_1(x) = \frac{\sqrt{x+4}}{2} - \frac{\sqrt{x}}{2}$

(3) $k_2(x) = \frac{3}{2}\frac{x}{k_3(x)} + \frac{3}{2} k_3(x) - 1$

(4) $k_3(x) = (\sqrt{x^2 - x^3} - x)^{(1/3)}$

(5) $k_0(k_1(k_2(j)))$

(2 *) $k_1(x)^2 = \frac{x}{2} + 1 - \frac{\sqrt{x\,(x+4)}}{2}$ the square of k_1 (x)

The equation for k_3 (j) is:

(6) $x^6 + 2\,x^3\, j + j^3$

If x is a solution, also j / x is a solution (the – sign for the square root in (4))

The equation for k_2 (k_3 (j)) is:

(7) $x^3 + 3\,x^2 + x\left(-\frac{27\, j}{4} + 3\right) + 1$

The degree of this equation is only 3, because in (3) k_3 (j) and j / k_3 (j) yield the same k_2 (j) !

The equation for k_1 (k_2 (k_3 (j))) ^ 2 (formula (2 *)) is:

(8) $1 - 3\,x + \left(6 - \frac{27\, j}{4}\right)x^2 + \left(-7 + \frac{27\, j}{2}\right)x^3 + \left(6 - \frac{27\, j}{4}\right)x^4 - 3\,x^5 + x^6$

The formula (8) above is equivalent to the equation for λ in formula (3.3) in [2]:

$$J(\tau) := \frac{4}{27}\frac{(\lambda^2(\tau) - \lambda(\tau) + 1)^3}{\lambda^2(\tau)(\lambda(\tau) - 1)^2}.$$

So $k_1(j) = \sqrt{\lambda}$

The well known inverse of the modular invariant in the appendix A of[2]:

$$\tau = \mathrm{i}\ \frac{{}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; 1-\lambda\right)}{{}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \lambda\right)}.$$

So formula (1) with the inverse of the modular invariant in terms of the arithmetic – geometric mean G (1, x) follows from the well known identity:

$G(1, \sqrt{\lambda}) = {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \lambda\right)$

References

[1] S. Adlaj, An inverse of the modular invariant
Preprint arXiv:1110.3274v1 [math.NT] (14 Oct 2011)

[2] K. Vogeler & M. Flohr, Pure Gauge SU(2) Seiberg-Witten Theory and Modular Forms
Preprint, arXiv:hep-th/0607142v2 (17 Jul 2007)

Helmut Ruhland, 9. June 2014

E-mail address: Helmut.Ruhland50@web.de

The modular equation

Assume, unless indicated otherwise, that n is an odd prime. The functional pair $(j(\tau), j(n\tau))$ is known to be algebraically dependent (over $\mathbb{Q}$), and is said to satisfy *the modular polynomial of level n*, that is

$$\Phi_n(j(\tau), j(n\tau)) \equiv 0,$$

where the modular polynomial Φ_n possesses integer (rational) coefficients. Moreover, Φ_n is symmetric in its two variables, that is $\Phi_n(x, z) = \Phi_n(z, x)$. When τ is fixed, and so is $j(\tau)$, the polynomial $\Phi_n(j(\tau), x)$ might be viewed as a polynomial in a single variable x over the (base) field $\mathbb{Q}(j(\tau))$,[4] and we shall call its roots, *the roots of the modular equation of level n*.

[4] In fact, it might be viewed as a polynomial over the ring $\mathbb{Z}[j(\tau)]$.

Galois criterion for depressing the degree of the modular equation

A modular equation, of prime level $n \geq 5$, is depressible, from degree $n+1$ to degree n (and no lower), iff (its group) $\mathrm{PSL}(2, \mathbb{Z}_\mathrm{n})$ possesses a subgroup of index n iff $n \in \{5, 7, 11\}$. Via explicitly constructing a permutation representation for the three exceptional groups, embedding them, respectively, in the three alternating groups A_5, A_7 and A_{11},[5] Galois must, in particular, be solely credited for solving the general quintic via exhibiting it as a modular equation of level 5.

[5] For $n = 5, 7, 11$, the subgroup of index n in $\mathrm{PSL}(2, \mathbb{Z}_\mathrm{n})$ turn out to be isomorphic to A_4, S_4 and A_5, respectively. These are precisely the symmetry groups of the platonic solids. The tetrahedron, being self-dual, has A_4 as its symmetry group. S_4 is the symmetry group for the hexahedron and the octahedron, whereas A_5 is the symmetry group for the dodecahedron and the icosahedron.

Three suppressed and forgotten "snapshots" of history

In 1830, Galois competed with Abel and Jacobi for the grand prize of the French Academy of Sciences. Abel (posthumously) and Jacobi were awarded (jointly) the prize, whereas all references to Galois' work (along with the work itself!) have (mysteriously) disappeared. The very fact that Galois' lost works contained contributions to Abelian integrals is either unknown (to many) or deemed (by some) no longer relevant to our contemporary knowledge.

Liouville acknowledged in September 1843 that he "recognized the entire correctness of the method", which was, subsequently (in 1846), published in the Journal de Mathématiques Pures et Appliquées XI, giving birth to Galois theory. Liouville declared an intention to proceed with publishing the rest of Galois' papers. Yet, most unfortunately, subsequent publication never ensued, and neither Gauss nor Jacobi had ever fulfilled Galois modest request to merely announce the significance (tacitly alleviating the burden of judging the correctness) of his (not necessarily published) contributions. In 1847, Liouville published (instead) his own paper "Leçons sur les fonctions doublement périodiques".

In 1851, in a paper published in Annali di Tortolini, Betti futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results. Then, in 1854, Betti showed that Galois' construction yields a solution to the quintic via elliptic functions.

Elliptic polynomials as factors of the division polynomial

Denote by $\mathbb{F} := \mathbb{Q}(\alpha)$ the base field of the polynomial r_n, which roots are the first coordinates of the points (on $\mathbb{E}_\beta$) of order n. Call r_n the division polynomial of level n. The field $\mathbb{F}[\gamma_m]$, obtained by adjoining a root γ_m of r_n to the base field $\mathbb{F}$, is the splitting field for *the elliptic polynomial of level n*

$$r_{mn}(x) := \prod_{l=1}^{(n-1)/2} (x - l \cdot \gamma_m) .$$

where the dot is used to indicate the multiplication of the first coordinate to yield the first coordinate of the l-multiple (on $\mathbb{E}_\beta$). The polynomial r_{mn} divides r_n, and the first index (m) of r_{mn} might be employed to designate $n+1$ pairwise coprime elliptic polynomial factors of r_n:

$$r_n(x) = \prod_{m=1}^{n+1} r_{mn}(x).$$

Coelliptic polynomials

The group of automorphisms $\mathrm{Aut}(\mathbb{F}[\gamma_m]/\mathbb{F})$ of each field extension $\mathbb{F}[\gamma_m]/\mathbb{F}$, $1 \leq m \leq n+1$, is cyclic of order $(n-1)/2$. One might, in fact, establish the isomorphism

$$\mathrm{Aut}\,(\mathbb{F}[\gamma_m]/\mathbb{F}) \cong \mathbb{Z}_n^\times/\{\pm 1\},$$

where the group, on the right hand side of the isomorphism, denoted by $\mathbb{Z}_n^\times$ is the multiplicative subgroup of $\mathbb{Z}_n$: the (prime) field of integers modulo n. To (each) elliptic polynomial $r_{m\,n}$ we shall associate a coelliptic polynomial

$$t_m(x) := n\,x\,r_{m\,n}(x)^2 - 2\,q'(x)\,r'_{m\,n}(x)\,r_{m\,n}(x) +$$

$$+4\,q(x)\left(r'_{m\,n}(x)^2 - r''_{m\,n}(x)\,r_{m\,n}(x)\right).$$

Calculating the roots of the modular equation

Now, let (for a fixed $\tau \in \mathcal{D}$) the value of $j(\tau)$ be given by

$$j(\tau) = \frac{4\,(d+1)^3}{27\,d}, \;\; d = d(\beta^2) := (\beta - 1/\beta)^2\,,$$

then the roots of the modular equation, of level n, are

$$j_m := \frac{4\,(d_m+1)^3}{27\,d_m}, \;\; d_m := d(\beta_m^2),$$

$$\beta_m^2 := \frac{s_m(-\beta) - s_m(0)}{s_m(-1/\beta) - s_m(0)}, \;\; 1 \le m \le n+1,$$

where $s_m(\cdot)$ is the n-th degree fractional transformation given by

$$s_m(x) := \frac{t_m(x)}{r_{m\,n}(x)^2}.$$

An action of S_3

Each such root j_m is invariant as β_m^2 is subjected to the action of the triangle group S_3, which is generated by the two inversions S and T given by

$$S : x \mapsto \frac{1}{x}, \;\; T : x \mapsto 1 - x.$$

This action on β_m^2 corresponds to the action of S_3 as the permutation group of the three symbols $\{0, \beta, 1/\beta\}$, appearing on the right hand side of the defining expression for β_m^2.

The elliptic curves $\mathbb{E}_\beta$ and $\mathbb{E}_{\beta_m}$ are said to be related by *cyclic isogeny* of degree n.

The modular equation of level 3 and 5

$$\Phi_3(x,y) = 2176782336\, x^3y^3 - 2811677184\,(x^3y^2 + y^3x^2) - 729\,(x^4 + y^4) + 779997924\,(x^3y + y^3x) - 1886592284694\, x^2y^2 - 15552000\,(x^3 + y^3) - 3754781568000\,(x^2y + y^2x) - 110592000000\,(x^2 + y^2) + 188194816000000\, x\, y - 262144000000000\,(x + y).$$

$$\Phi_3^*(x,y) = x^3y^3 - 2232\,(x^3y^2 + x^2y^3) - x^4 - y^4 + 1069956\,(x^3y + xy^3) - 2587918086\, x^2y^2 - 36864000\,(x^3 + y^3) - 8900222976000\,(x^2y + y^2x) - 452984832000000\,(x^2 + y^2) + 770845966336000000\, x\, y - 1855425871872000000000\,(x + y).$$ **(Smith 1879)**

$$\Phi_5(x,y) = 8916100448256\, x^5y^5 - 19194382909440\,(x^5y^4 + y^5x^4) + 13589034024960\,(x^5y^3 + y^5x^3) - 4974647446705766400\, x^4y^4 - 3505336473600\,(x^5y^2 + y^5x^2) - 186414787904261990400\,(x^4y^3 + y^4x^3) - x^6 - y^6 + 246683410950\,(x^5y + y^5x) - 383083609779811215375\,(x^4y^2 + y^4x^2) + 441206965512914835246100\, x^3y^3 - 1136117760\,(x^5 + y^5) - 74387615108118528000\,(x^4y + y^4x) - 155662551263777381813760000\,(x^3y^2 + y^3x^2) - 430254526762844160\,(x^4 + y^4) + 6445377289996473512755200\,(x^3y + y^3x) - 17116440602335505090150400000\, x^2y^2 - 54313315434020926285414400\,(x^3 + y^3) - 70845528472506632188723200000\,(x^2y + y^2x) - 750608416927050074633011200\,(x^2 + y^2) + 29617595563122405481849552896\, x\, y - 3457795560648760910413824000\,(x + y) - 53096261712733607223623680000.$$

$$\Phi_5^*(x,y) = x^5y^5 - 3720\,(x^5y^4 + y^4x^5) + 4550940\,(x^5y^3 + y^5x^3) - 1665999364600\, x^4y^4 - 2028551200\,(x^5y^2 + y^5x^2) - 107878928185336800(x^4y^3 + y^4x^3) - x^6 - y^6 + 246683410950\,(x^5y + y^5x) - 383083609779811215375\,(x^4y^2 + y^4x^2) + 441206965512914835246100\, x^3y^3 - 1963211489280\,(x^5 + y^5) - 1285417989068288163840000\,(x^4y + y^4x) - 26898488858380731577417728000\,(x^3y^2 + y^3x^2) - 128473313284142445625344 0\,(x^4 + y^4) + 1924579346189282996551082311680000\,(x^3y + y^3x) - 5110941777552418083110765199360000\, x^2y^2 - 28024477782843952780432156529786880 0\,(x^3 + y^3) - 36554736583949629295706472332656640000\,(x^2y + y^2x) - 6692500042627997708487149415015068467200\,(x^2 + y^2) + 264073457076620596259715790247978782949376\, x\, y - 53274330803424425450420160273356509151232000\,(x + y) - 141359947154721358697753474691071362751004672000.$$ **(Berwick 1916)**

Four special values of the modular invariant

Suppose that j is (correctly) normalized with $j(i) = 1$, then

$$j\left(\frac{4\,(5\,i \pm 1)}{13}\right) =$$

$$= \left(\frac{(1-\sqrt{5}\,)^{37}}{2^{39}}\left(1190448488 - 858585699\,\sqrt{2} - 540309076\,\sqrt{5} + 374537880\,\sqrt{10} + \right.\right.$$

$$\left.\left. \pm\, i\sqrt{\sqrt{5}}\left(693172512 - 595746414\,\sqrt{2} - 407357424\,\sqrt{5} + 240819696\,\sqrt{10}\right)\right)\right)^3,$$

$$j\left(\frac{5\,(4\,i \pm 1)}{17}\right) =$$

$$= \left(\frac{(1-\sqrt{5}\,)^{37}}{2^{39}}\left(1190448488 + 858585699\,\sqrt{2} - 540309076\,\sqrt{5} - 374537880\,\sqrt{10} + \right.\right.$$

$$\left.\left. \pm\, i\sqrt{\sqrt{5}}\left(693172512 + 595746414\,\sqrt{2} - 407357424\,\sqrt{5} - 240819696\,\sqrt{10}\right)\right)\right)^3.$$

These special values (along with other values) were derived in an article titled "Multiplication and division on elliptic curves, torsion points and roots of modular equations" and forwarded for publication yesterday!

The equality E as a (simplest non-trivial) special case

Denote the roots of a coelliptic polynomial t_m by ξ_k, $1 \leq k \leq n$, and pick an index j so that $1 \leq j \leq n+1$ and $j \neq m$. One then finds that, for any given root γ of the elliptic polynomial $r_{j\,n}$, the equality

$$\xi_k^{n^2} \left(r_n \left(\frac{1}{\xi_k} \right) / r_n(\xi_k) \right)^2 =$$

$$= -r_{j\,n}(0)^{2n}\, t_m(0) \prod_{l=1}^{(n-1)/2} \left(t_m \left(\frac{1}{l \cdot \gamma} \right) / t_m(l \cdot \gamma) \right)^2$$

merely reflects two (out of many) distinct ways of calculating one and the same the coordinate on E_β. In other words, as k runs through n values on the left-hand side of the equality, whereas γ runs through $(n-1)/2$ values for each of the n possibles values for j, all $n(n+1)/2$ permissible values (thus obtained) turn out to coincide with one and the same.

Back to equality E and (merely) a single step beyond

- $$\xi^9\left(\frac{r_3(1/\xi)}{r_3(\xi)}\right)^2=-2\gamma_m\left(\frac{\gamma^3\, t_m(1/\gamma)}{t_m(\gamma)}\right)^2,$$
$$r_3(x):=x^4+4\,\alpha\,x^3+2\,x^2-\frac{1}{3}=\prod_{m=1}^{4} r_{m3}(x),\ \ r_{m3}(x)=x-\gamma_m,$$
$$t_m(x):=x^3+\left(\frac{1}{\gamma_m^2}-4\right)x+2\,\gamma_m,\ \ t_m(\xi)=r_3(\gamma)=0\neq r_{m3}(\gamma).$$
- $$\xi^{25}\left(\frac{r_5(1/\xi)}{r_5(\xi)}\right)^2=-2\,\lambda_m\,\mu_m\left(\mu^5 t_m\left(\frac{1}{\gamma}\right)t_m\left(\frac{1}{2\cdot\gamma}\right)/\left(t_m\left(\gamma\right)t_m(2\cdot\gamma)\right)\right)^2,$$
$$r_5(x)=x^{12}+\frac{62\,x^{10}}{5}-21\,x^8-60\,x^6-25\,x^4-10\,x^2+\frac{1}{5}+12\,\alpha\,x^3\left(x^8+4\,x^6-18\,x^4-\frac{92\,x^2}{5}-7\right)+$$
$$+144\,\alpha^2\,x^4\left(\frac{x^6}{5}-3\,x^2-2\right)-\frac{1728\,\alpha^3\,x^5}{5}=\prod_{m=1}^{6} r_{m5}(x),\ \ r_{m5}(x)=x^2-\lambda_m\,x+\mu_m=(x-\gamma_m)(x-2\cdot\gamma_m),$$
$$t_m(x)=x^5+\left(4+3\,\lambda_m^2-10\,\mu_m+12\,\lambda_m\,\alpha\right)x^3-2\left(\lambda_m+2\,\lambda_m\,\mu_m+24\,\mu_m\,\alpha\right)x^2+$$
$$+\left(2\,\lambda_m^2-12\,\mu_m+5\,\mu_m^2+12\,\lambda_m\,\mu_m\,\alpha\right)x+2\,\lambda_m\,\mu_m,\ \ t_m(\xi)=r_5(\gamma)=0\neq r_{m5}(\gamma).$$

Two quotes from "Récoltes et Semailles" by Grothendieck

"Je suis persuadé d'ailleurs qu'un Galois serait allé bien plus loin encore que je n'ai été. D'une part à cause de ses dons tout à fait exceptionnels (que je n'ai pas reçus en partage, quant à moi)."

"Mais au delà de ces différences accidentelles, je crois discerner à cette "marginalité" une cause commune, que je sens essentielle. Cette cause, je ne la vois pas dans des circonstances historiques, ni dans des particularités de "tempérament" ou de "caractère" (lesquels sont sans doute aussi différents de lui à moi qu'ils peuvent l'être d'une personne à une autre), et encore moins certes au niveau des "dons" (visiblement prodigieux chez Galois, et comparativement modestes chez moi). S'il y a bien une "parenté essentielle", je la vois à un niveau bien plus humble, bien plus élémentaire."

A few references to related works by the speaker and two pitifully written (anti)references to Galois biography

1. Adlaj S. Tether equilibria in a linear parallel force field // 4^{th} IYR Workshop on Geometry, Mechanics and Control, Ghent, Belgium, Jan. 11-13, 2010. http://www.wgmc.ugent.be/adlaj.pdf.

2. Adlaj S. Eighth lattice points // arXiv:1110.1743 (2011).

3. Adlaj S. An inverse of the modular invariant // arXiv:1110.3274 (2011).

4. Adlaj S. Iterative algorithm for computing an elliptic integral // Issues on motion stability and stabilization (2011), 104–110 (in Russian).

5. Adlaj S. Mechanical interpretation of negative and imaginary tension of a tether in a linear parallel force field // Sixth Polyakhov Readings: Selected works of the international scientific conference on Mechanics, Saint-Petersburg, Jan. 31 – Feb. 3, 2012, 13–18.

Rothman T. Genius and Biographers: The Fictionalization of Evariste Galois // The American Mathematical Monthly, vol. 89, 1982, 84-106. (This article, sorrowly, recieved the Lester R. Ford Writing Award, 1983).

Кованцов Н. Математика и романтика. Киев: Вища школа, 1976, 96 с. (Another mundane view of Galois biography by another pseudo-expert.)