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 ≤ 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 $\gamma_i \to 1 / \gamma_i$ ~ $r_{a,\,-k}$ (x)
- $r_{a,\,k}$ (x) and the substitution $\gamma_i \to 1 / \gamma_i$ ~ $p_{a,\,-k}$ (x)

Define the 2 polynomials:

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

(4.4) $p_\zeta(x) := p_{b,\,l}(x)$ and ξ be a root of p_ξ (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 → Q () = 1, l = 0 and b = 1 → 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) $$\frac{\zeta^{(N^2)}\, q_\gamma\!\left(\frac{1}{\zeta}\right)^{(N-1)}}{q_\gamma(\zeta)^{(N-1)}} = \frac{b\,\gamma_i^{\,l}\,(-1)^{(N-1)}\,\gamma^{(N(N-1))}\, p_\zeta\!\left(\frac{1}{\gamma}\right)^{(N-1)}}{p_\zeta(\gamma)^{(N-1)}} = b\,\gamma_i^{\,l}\, \mathrm{Q}(\gamma_i)^{(N-1)}$$

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

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

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

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**)

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

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

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

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

Table 2: polynomials for the division points of E_β

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

Special values: $j = 1$, $\alpha = \pm 1 / \sqrt{2}$, $\beta = \pm \sqrt{2}, \pm 1 / \sqrt{2}$
$j = 0$, $\alpha = \pm 1 / \sqrt{3}$, $\beta = \sqrt{3} / 2 \pm i / 2 = 12^{th}$ 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