Multiplication and division on elliptic curves, torsion points and roots of modular equations

Semjon Adlaj

Having expressed the ratio of the length of the Lemniscate of Bernoulli to the length of its cocentred superscribing circle as the reciprocal of the arithmetic-geometric mean of 1 and $\sqrt{2}$, Gauss wrote in his diary, on May 30, 1799, that thereby "an entirely new field of analysis" emerges. Yet, up to these days, the study of elliptic functions (and curves) has been based on two traditional approaches (namely, that of Jacobi and that of Weiestrass), rather than a single unifying approach. Replacing artificial dichotomy by a, methodologically justified, single unifying approach does not only enable re-deriving classical results eloquently but it allows for undertaking new calculations, which did seem either unfeasible or too cumbersome to be explicitly performed. Here, we shall derive readily verifiable explicit formulas for carrying out highly efficient arithmetic on complex projective elliptic curves. We shall explicitly relate calculating the roots of the modular equation of level p to calculating the p-torsin points on a corresponding elliptic curve, and we shall re-bring to light Galois exceptional, never nearly surpassable and far from fully appreciated, impact.

An introduction: an integral, tightly cohesive subject of elliptic functions and elliptic curves

Given a parameter $\beta \in \mathbb{C} \setminus \{-1, 0, 1\}$, introduce *the Galois essential elliptic function*, as in [1, 2, 3, 4, 8, 9], that is a (meromorphic) function $\mathcal{R} = \mathcal{R}_\beta = \mathcal{R}_\beta(\cdot) = \mathcal{R}(\cdot, \beta)$, possessing a (double) pole at the origin and satisfying the differential equation

$$\mathcal{R}'^2 = 4\mathcal{R}\left(\mathcal{R} + \beta\right)\left(\mathcal{R} + 1/\beta\right). \tag{1}$$

Denote the lattice of the function $\mathcal{R}_\beta$ by Λ_β, and call the parameter β *the elliptic modulus*. The map

$$z \mapsto \left(1, \mathcal{R}_\beta(z), \mathcal{R}'_\beta(z)\right),$$

extends, with $0 \mapsto (0, 0, 1)$, to a map from the period-parallelogram $\mathbb{C}/\Lambda_\beta$ into the complex projective space $\mathrm{P}\mathbb{C}^2$. The (extended) map induces, onto its image $\mathbb{E}_\beta$, which we shall call *the associated elliptic curve*,[1] an isomorphism of Riemann surfaces, as well as, an isomorphism of groups.[2] This map, further, enables an identification (exploiting the j-invariant) of isomorphism classes of projective complex elliptic curves with homothety classes of lattices $\mathcal{L}/\mathbb{C}^\times$, which might, in turn, be identified with the fundamental domain $\Gamma\backslash\mathcal{H}$, for the action of the modular group $\Gamma := \mathrm{PSL}(2, \mathbb{Z})$, upon the upper half plane $\mathcal{H}$, as

[1] Without, necessarily, further specifying whether the association pertains to the elliptic function $\mathcal{R}_\beta$, its lattice Λ_β or the elliptic modulus β.

[2] The curve $\mathbb{E}_\beta$ is, thereby, said to be a one-dimensional complex Lie group.

is well explained in [17]. From now on, we exploit the identification of the points on the torus $\mathbb{C}/\Lambda_\beta$, which might be viewed as the domain of $\mathcal{R}_\beta$, with the points on the elliptic curve $\mathbb{E}_\beta$, which might be viewed as the image of the functional pair $(\mathcal{R}_\beta, \mathcal{R}'_\beta)$. Keeping in mind that the value of the function $\mathcal{R}_\beta$ determines, up to a sign, via equation (1), the value of its derivative $\mathcal{R}'_\beta$, we might further identify a pair of (not necessarily distinct) points on $\mathbb{E}_\beta$, sharing a first coordinate, with their corresponding pair of points in the domain of $\mathcal{R}_\beta$, which image (under $\mathcal{R}_\beta$) coincide with that very first coordinate.

Multiplication

Fix the elliptic modulus β, and express the defining equation for the (already introduced) elliptic curve $\mathbb{E}_\beta$ as

$$\mathbb{E}_\beta : \; y^2 = 4\,x\,q(x), \;\; q(x) := x^2 + 3\,\alpha\,x + 1, \;\; \alpha = \alpha(\beta) := \frac{\beta + 1/\beta}{3}.$$

The justification for such canonical representation of elliptic curves (not to be confused with the Weierstrass normal form) is provided in [3]. Two distinct points (x_1, y_1) and (x_2, y_2) might be summed (on $\mathbb{E}_\beta$) to a point (x_3, y_3), which first coordinate satisfy *the addition formula*

$$x_3 = \frac{1}{4\,x_1 x_2}\left(\frac{x_1\,y_2 - x_2\,y_1}{x_1 - x_2}\right)^2. \tag{2}$$

Now, denoting by $n \cdot (x, y)$ the multiplication of the point (x, y) by n, and denoting by $(n \cdot x, n \cdot y)$ the n-multiple of the point (x, y) on $\mathbb{E}_\beta$, so that $(n \cdot x, n \cdot y) = n \cdot (x, y)$, *the doubling formula* expresses the first coordinate $2 \cdot x$ of the point $2 \cdot (x, y)$, as calculated in [9],

$$2 \cdot x = \frac{p_2(x)}{q_2(x)}, \;\; p_2(x) := \left(\frac{x^2 - 1}{2}\right)^2, \;\; q_2(x) := x\,q(x).$$

When n is an arbitrary integer, the multiplication by n amounts to successively multiplying by its prime factors (counted with their respective multiplicities), so we want to deduce *a multiplication by an odd prime formula*. Assuming n to be odd (not necessarily prime!), exceeding 2, we might (recursively) deduce such a formula, expressing the first coordinate of the n-odd-multiple point as a degree n^2 fractional transformation of the first coordinate of the point to be multiplied, that is,

$$n \cdot x = \frac{p_n(x)}{q_n(x)}, \;\; p_n(x) := x^{n^2} r_n\left(\frac{1}{x}\right)^2, \;\; q_n(x) := r_n(x)^{\,2},$$

$$r_n(x) := \frac{(n-1)^2\,(x\,q_{n-1}(x) - p_{n-1}(x))}{n\,(n-2)\,r_{n-2}(x)}, \;\; r_1(x) :\equiv 1. \tag{3}$$

An explicit formula for $n \cdot x$ relies on an explicit formula for $(n-1) \cdot x$ as a fractional transformation with (coprime) polynomials p_{n-1} and q_{n-1} appearing in its numerator and denominator, respectively. Since n is odd, by assumption, the formula for $(n-1) \cdot x$ might always be attained via the doubling formula applied to $\left(\frac{n-1}{2}\right) \cdot x$. Note that the sequence $\{r_n : n \text{ is odd}\}$ need not be extended to include elements r_n with even indices, unlike p_n and q_n which are (successively) defined for all integer indices n (employing the doubling formula whenever the indices are even), and that, furthermore, if we choose the polynomials q_n to be monic for all even n then so do become all (subsequent) polynomials r_n (and q_n). The roots of each r_n are precisely the first coordinates of the points, aside from the identity point, on $\mathbb{E}_\beta$, of order dividing n, so, in particular, the degree of r_n is $(n^2 - 1)/2$, and if m divides n then the polynomial $r_m(x)$ divides the polynomial $r_n(x)$.

Division

The (monic) polynomial r_n, which we have introduced in the preceding section, has its coefficients in the field $\mathbb{F} := \mathbb{Q}(\alpha)$, that is, the field of rational functions in the transcendental (or algebraic) element α, introduced in the preceding section, over the field of rational numbers $\mathbb{Q}$.[3] When n is an odd prime, as we now opt as being the default assumption, the roots of r_n are the first coordinates of the points of order n on $\mathbb{E}_\beta$. The assumption which will not be lifted (throughout this article) that $\beta^2 \in \mathbb{C} \setminus \{0, 1\}$, or, equivalently, that $\alpha^2 \in \mathbb{C} \setminus \{4/9\}$, guarantees that the roots (of r_n) are pairwise distinct. We shall call the polynomial r_n *the division polynomial of level* n, and, whenever an emphasis on its dependence upon the elliptic modulus β is desired, we shall denote it as $r_n(\cdot, \beta)$, still being at large viewing it either as a function of two variables or as a β-parametric polynomial function in a single variable.

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

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

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:

$$r_n(x) = \prod_{m=0}^{n} r_{mn}(x).$$

The group of automorphisms $\mathrm{Aut}(\mathbb{F}[\gamma_m]/\mathbb{F})$ of each field extension $\mathbb{F}[\gamma_m]/\mathbb{F}$, $0 \leq m \leq n$, is cyclic of order $(n-1)/2$. One might, in fact, establish the isomorphism

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

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. The group $\mathbb{Z}_n^\times$ is generated by a primitive root modulo n, and the same root, after taking the quotient by the subgroup $\{\pm 1\}$, generates all $(n-1)/2$ elements of the quotient $\mathbb{Z}_n^\times/\{\pm 1\}$, which we might identify with the elements of $\mathrm{Aut}\left(\mathbb{F}[\gamma_m]/\mathbb{F}\right)$. The choice of a generator (of the latter group) does not, of course, restrict our unlimited freedom of designating any root, of a given elliptic polynomial r_{mn}, as γ_m, and then expressing all such $(n-1)/2$ roots as $l \cdot \gamma_m$, with $1 \leq l \leq (n-1)/2$. In other words, the field extension $\mathbb{F}[\gamma_m]$, while dependent upon the particular choice of the polynomial r_{mn} among the $n+1$ polynomial factors of r_n, it does not further depend upon the choice of γ_m as a root of r_{mn}.

Each of the $(n^2-1)/2$ (distinct) values $l \cdot \gamma_m : 1 \leq l \leq (n-1)/2,\ 0 \leq m \leq n$, viewed as values of $\mathcal{R}_\beta$, satisfy:

$$\mathcal{R}_\beta\left(n\mathcal{R}_\beta^{-1}(l \cdot \gamma_m)\right) = \infty.$$

Note that each pre-image $\mathcal{R}_\beta^{-1}(l \cdot \gamma_m)$ is a two-point subset (in the domain of $\mathcal{R}_\beta$). Thus, there are n^2 points (including 0, being a pole of $\mathcal{R}_\beta$), on the torus, $\mathbb{C}/\Lambda_\beta$ which if multiplied by n map, under $\mathcal{R}_\beta$, to one and the same point ∞, corresponding to the (additive) identity point on $\mathbb{E}_\beta$. To each r_{mn} we shall associate a line, through the origin (in $\mathbb{C}$), which image under $\mathcal{R}_\beta$ contains (all) the values $l \cdot \gamma_m$.

[3] No further restriction is imposed upon assuming that the coefficients of polynomials (in α) appearing in the numerator and the denominator of a rational expression, in $\mathbb{F}$, are integers.

Generally, for an arbitrary value $\eta \in \mathbb{C}$,[4] there are n^2 distinct values $x_j, 1 \le j \le n^2$ for which

$$\mathcal{R}_\beta \left(n \mathcal{R}_\beta^{-1}(x_j) \right) = \eta.$$

As before, the pre-image $\mathcal{R}_\beta^{-1}(x_j)$ is a two-point subset of the torus $\mathbb{C}/\Lambda_\beta$, as long as x_j is not a root of the cubic polynomial q_2, that is, as long as $x_j \in \mathbb{C}\backslash\{0, -\beta, -1/\beta\}$. The value η along with the n^2 values x, which we have labelled as $x_1, x_2, \ldots, x_{n^2}$, satisfy the polynomial

$$f_n(x, \eta) := n^2 \left(p_n(x) - \eta \, q_n(x) \right) =: \prod_{j=1}^{n^2} (x - x_j) \,, \tag{4}$$

which whenever η is fixed (along with the already fixed elliptic modulus β) might be viewed as a polynomial in the (single) variable x over the field $\mathbb{F}_\eta := \mathbb{F}(\eta)$. We shall then write $f_n(x)$ instead of $f_n(x, \eta)$, and the product on the rightmost side of (4), thereby, exhibits its n^2 roots, as being the roots of its n^2 monomial factors. The task of this section is calculating these roots for a given η.

The n^2-point set $\{x_j : 1 \le j \le n^2\}$ might be divided into n *collinear n-point subsets*, each aligned along the same direction vector, corresponding to one of the $n+1$ possible lines associated, as above, to one of the elliptic polynomials r_{mn}. Here we must emphasize that the use of the term collinear would not have been justified without the afore-indicated identification of the image of $\mathcal{R}_\beta$ with its pre-image, since, strictly speaking, the collinearity pertains to the pre-image points. Now, assuming that the n^2 values $\{x_j : 1 \le j \le n^2\}$ have been ordered, so as to reflect a particular alignment along n (parallel) lines, corresponding to a particular elliptic polynomial r_{mn}, say the first n values $\{x_j : 1 \le j \le n\}$ are the values of $\mathcal{R}_\beta$ along the line (in its domain) determined by any pre-image point, of the n values $\{x_j : 1 \le j \le n\}$, together with any pre-image point of the $(n-1)/2$ roots of that designated r_{mn}, and introducing the n-th degree (monic) coelliptic polynomial

$$t_m(x) := n \, x \, r_{mn}(x)^2 - 2 \, q_2'(x) \, r_{mn}'(x) \, r_{mn}(x) + 4 \, q_2(x) \left(r_{mn}'(x)^2 - r_{mn}''(x) \, r_{mn}(x) \right),$$

along with the n-th degree fractional transformation

$$s_m(x) := \frac{t_m(x)}{r_{mn}(x)^2}, \tag{5}$$

one might verify that s_m is an n-to-one function on the set $\{x_j : 1 \le j \le n^2\}$, with the subset $\{x_j : 1 \le j \le n\}$, in particular, being mapped (under s_m) to a single value, which we might denote by s_{m1}. Actually

$$\sum_{j=1}^{n} x_j = s_{m1},$$

that is, the n-value-sum (on the left hand side) coincides with the value of the n-th degree fractional transformation (on the right hand side) at any x_j, as long as $1 \le j \le n$. In fact, such an invariance, of the function s_m, might be employed in order to further divide the values $\{x_j : 1 \le j \le n^2\}$ into n collinear n-point subsets, each subset sharing a single image value (under s_m), successively, further denoted by $s_{m2}, \ldots, s_{mn}$. Letting m acquire all permissible values $0 \le m \le n$, we attain $n+1$ distinct

[4] The subsequent assertion (concerning the number n^2 of distinct values) holds for all $\eta \in \mathbb{C}\backslash\{0, -\beta, -1/\beta\}$. Here, we might already point out that, for each of the three indicated exceptions the number of distinct values is $(n^2+1)/2$.

divisions of the set $\{x_j : 1 \le j \le n^2\}$ into n collinear n-point subsets. Let w_m^k denote the elementary symmetric polynomial of degree k in the n variables $s_{m1}, s_{m2}, \ldots, s_{mn}$, that is

$$w_m^k := \sum_{l=1}^{n} s_{ml}^k,$$

and put

$$g_m(x) := x^n + \sum_{k=1}^{n-1} (-1)^k \, w_m^k \, x^{n-k}.$$

The coefficients w_m^k of g_m are, in fact, linear functions in η,[5] thus (in particular)

$$w_m^k = w_m^k(\eta) = w_m^k(0) + \beta \left(w_m^k(0) - w_m^k \left(-\frac{1}{\beta} \right) \right) \eta. \tag{6}$$

The polynomial f_n might now be factored (in $n+1$ distinct ways) into a product of n n-th degree polynomials:

$$f_n(x) = \prod_{l=1}^{n} h_{ml}(x), \;\; h_{ml}(x) := t_m(x) - s_{ml} \, r_{mn}(x)^2, \;\; 0 \le m \le n, \tag{7}$$

with the values s_{ml}, $1 \le l \le n$, being, now, viewed as roots of the polynomials g_m (for a fixed index m).

Once a root of f_n is calculated, the other $n^2 - 1$ roots might be obtained by adding to (and subtracting from) it the $(n^2-1)/2$ roots of r_n (all treated as first coordinated of points on $\mathbb{E}_\beta$) via the addition formula (2). Any pair of polynomials h_{ml}, which first indices (m) do not coincide with each other, has a first degree monomial as its greatest common divisor. A root of the latter monomial is, of course, a root of f_n. Thus, a root is expressible as a rational function, involving the coefficients of the afore-indicated polynomial pair h_{ml}. Yet, we shall present another path yielding greater conceptual insight into the algebraic structure of a root of f_n.

Let H denote a set of $n+1$ polynomials of degree n:

$$H = \left\{ h_m(x) = \sum_{k=0}^{n} a_{m\,n-k} \, x^k : \; 0 \le m \le n \right\}, \tag{8}$$

and call the matrix

$$A = \begin{pmatrix} a_{0\,0} & a_{0\,1} & \ldots & a_{0\,n} \\ a_{1\,0} & a_{1\,1} & \ldots & a_{1\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,0} & a_{n\,1} & \ldots & a_{n\,n} \end{pmatrix} \tag{9}$$

the matrix associated with H. Denote by H_j the n-subset $H \backslash \{h_j\}$, obtained by deleting the element h_j from the set H, and denote by A_{jk} the submatrix formed by deleting the $j+1$-st raw and the $k+1$-st column of the matrix A. Associate with the subset H_j the linear system

$$\sum_{k=1}^{n} a_{m\,n-k} \, x_k = -a_{mn}, \;\; 0 \le m \le n, \;\; m \ne j.$$

[5] We point out (superfluously, perhaps) that $s_m(x)$ was regarded as a function in the variable x, where x was taken to satisfy $n \cdot x = \eta$. We have not (yet) viewed s_m as a function of η.

Cramer rule might be invoked, to evaluate the variable x_1, of the latter linear system, as a ratio of two determinants:

$$x_1 = -\frac{\Delta_{jn-1}}{\Delta_{jn}}, \tag{10}$$

where Δ_{jk} is the determinant of the matrix A_{jk} (assuming here that the determinant Δ_{jn} in the denominator is non vanishing). Now, having already denoted by x_1 a root of f_n, we might further observe that such a root is simultaneously a root of $n+1$ polynomials h_{ml}, whose first indices run over all admissible values, $0 \leq m \leq n$, corresponding to $n+1$ distinct factorizations of f_n.[6] Since the second index (l), of each such polynomial h_{ml}, is determined by the first (assuming the root x_1 is fixed), we might regard this set as the set H, being given in (8). A necessary and sufficient condition for such an $n+1$ set of polynomials H to be that particular set, possessing the monomial $x - x_1$ as its greatest common divisor, which we shall call *the pinned set associated with the root* x_1, is the vanishing of the determinant Δ of its associated matrix A, given in (9), that is the condition

$$\Delta = 0.^7$$

Among the $(n+1)^n$ possible H-sets, obtained by picking a polynomial h_{ml} from each of the $n+1$ factorizations of f_n, given by (7), n^2 H-sets do satisfy the latter condition. Any of the $n+1$ n-subsets H_j (obtained by excluding any of the $n+1$ members), of a given pinned set H, might be associated with a linear system, as we have just described. No confusion, due to using the same symbol x_1 to denote a root of f_n, as well as, a variable, shared by $n+1$ linear systems, corresponding to $n+1$ distinct n-subsets of the pinned set, emerges since all $n+1$ evaluations turn out to coincide with one and the same value for x_1, being again regarded as a root of f_n.

The linear dependence of a pinned set H might be explicitly expressed as the identity

$$\sum_{m=0}^{n} (-1)^m \Delta_{mk}\, h_m(x) \equiv 0, \tag{11}$$

which, we emphasize, is valid for each k, $0 \leq k \leq n$. In other words, the space of row vectors, spanned by the set

$$\{(-\Delta_{m0},\, \Delta_{m1},\, \ldots\, ,\, -\Delta_{mn-1},\, \Delta_{mn}) : 0 \leq m \leq n\}$$

is one dimensional, reflecting the fact that all $n+1$ vectors, of the latter set, are collinear with the vector

$$u := \left(x_1^n,\, x_1^{n-1},\, \ldots\, ,\, x_1,\, 1\right).$$

The vector u is, of course, orthogonal to the row space of the matrix A, associated with the pinned set H, whereas the vector

$$v := (-\Delta_{0n},\, \Delta_{1n},\, \ldots\, ,\, -\Delta_{n-1n},\, \Delta_{nn})$$

is orthogonal to its column space. So, u^T is an eigenvector of A, and v^T is an eigenvector of A^T; both eigenvectors correspond to eigenvalue zero.

For each polynomials h_m, of a given pinned set H, each coefficient a_{m1} of x^{n-1} coincides with a value $-s_{ml}$, where the second index (l) is determined by the first (m). Thus, we might write (assuming the pinned set H is fixed) $a_{m1} = -s_m$, meaning that the value indicated by s_m is a particular predetermined value among the n candidate values s_{ml}, as the index l runs through n (permissible) options. Once

[6] That is, for each first index m, $0 \leq m \leq n$, a second index l, $1 \leq l \leq n$, for which x_1 is a root of h_{ml}, exists.

[7] Admittedly, such a condition, in and of itself, would be more satisfactory for elliptic curves over finite fields.

more, the notation chosen, here, is consistent with the notation that we adopted upon introducing the function s_m, via formula (5). Having fixed x_1, we merely agree to restrict the designation of the notation s_m from denoting a function to denoting its value at x_1, that is, we assign $s_m = s_m(x_1)$.

Two particular instances of identity (11) are

$$\sum_{m=0}^{n}(-1)^m\Delta_{mk} = 0,\ \sum_{m=0}^{n}(-1)^m\Delta_{mk}\, s_m = 0,$$

the first of which reflects that the polynomials h_m are monic, and means that the coordinates of the vector v sum to zero. We conclude this section by pointing out that a vector proportional to u might be obtained by (successively) applying Gram-Schmidt orthogonalization to the rows of A, with the last row replaced by the vector $(0, \ldots, 0, 1)$.[8] However, for a given pinned set, the value of a root x_1 is most efficiently calculated via employing the formula

$$\sum_{m=0}^{n} s_m = n\, x_1 + n^2\, \eta. \tag{12}$$

Explicit halving and thirding formulas

Formulas for halving points on elliptic curves were derived in [9]. Extending the notation $n\cdot x$ to indicate the first coordinate of a point (on $\mathbb{E}_\beta$) multiplied by a number n, which we shall, temporarily, permit to acquire integer, as well as, rational values, the halving (multivalued) formula might be expressed as

$$\frac{1}{2}\cdot x = w \pm \sqrt{w^2-1},\ w := x \pm \sqrt{q(x)}.$$

The leftmost side might assume 4 possible (generally, pairwise distinct) values corresponding to two branches of the square root function being twice applied, upon calculating the values on right-hand side. The three exceptions are, as expected, the roots of q_2. Each yielding two *halves*. Namely, the three pairs ± 1, $-\beta \pm \sqrt{\beta^2-1}$, and $-1/\beta \pm \sqrt{1/\beta^2-1}$ are the halves of 0, $-\beta$ and $-1/\beta$, respectively, giving, in total, six distinct first coordinates of points of order four on $\mathbb{E}_\beta$. One might proceed to calculate the coordinates of the points of order eight, as was done in [10].

We proceed to employ the results of the preceding section in order to derive explicit *thirding* formulas. The points of order 3 (on $\mathbb{E}_\beta$) satisfy the polynomial

$$r_3(x) = x^4 + 4\,\alpha\, x^3 + 2\, x^2 - \frac{1}{3} = \prod_{m=0}^{3}(x-\gamma_m)\,. \tag{13}$$

Each of the four (distinct) values $\gamma \in \{\gamma_m : m = 0, 1, 2, 3\}$, viewed as values of $\mathcal{R}_\beta$, satisfy:

$$\mathcal{R}_\beta\left(3\mathcal{R}_\beta^{-1}(\gamma)\right) = \infty.$$

Note that each pre-image $\mathcal{R}_\beta^{-1}(\gamma)$ is a two-point subset (in the domain of $\mathcal{R}_\beta$). Thus, there are 9 points (including 0, being a pole of $\mathcal{R}_\beta$), on the torus, $\mathbb{C}/\Lambda_\beta$ which if tripled map under $\mathcal{R}_\beta$ to one and the

[8] Recall that the monomial $x - x_1$ is the greatest common divisor of the polynomials in the pinned set H, so that the vector $(0, \ldots, 0, 1)$ is not spanned by the row space of A, and, if "orthogonalized" to this space, yields a vector proportional to u.

same point ∞. Generally, for an arbitrary value η, there are nine distinct values $x = x_j, 1 \le j \le 9$, satisfying

$$\mathcal{R}_\beta\left(3\mathcal{R}_\beta^{-1}(x)\right) = \eta.$$

As before, the pre-image $\mathcal{R}_\beta^{-1}(x)$ is a two-point subset of the torus $\mathbb{C}/\Lambda_\beta$, as long as $x \in \mathbb{C}\backslash\{0, -\beta, -1/\beta\}$. When the value η is fixed its 9 *thirds* $x_1, x_2, \ldots, x_9$ satisfy the polynomial

$$f_3(x) = \prod_{j=1}^{9}(x - x_j) = 9\left(p_3(x) - \eta\, q_3(x)\right) =$$

$$= x^9 - 9\,\eta\, x^8 - 12\left(6\,\alpha\,\eta + 1\right)x^7 - 12\left(3(4\,\alpha^2 + 1)\,\eta + 2\,\alpha\right)x^6 - 6\left(24\,\alpha\,\eta - 5\right)x^5$$
$$-6\left(5\,\eta - 24\,\alpha\right)x^4 + 12\left(2\,\alpha\,\eta + 3\,(4\,\alpha^2 + 1)\right)x^3 + 12\left(\eta + 6\,\alpha\right)x^2 + 9\,x - \eta,$$

with coefficients in the (base) field $\mathbb{F}_\eta$, as defined in the preceding section. Here, we might state that the multiplication (on $\mathbb{E}_\beta$) by a fixed rational non-integer number is not a single-valued function,[9] thereby, in particular, justifying the notation

$$\frac{1}{3}\cdot\eta = \{x_j : 1 \le j \le 9\}.$$

The fractional transformations, introduced in (5), are cubic when $n = 3$:

$$s_m(x) = \frac{t_m(x)}{(x - \gamma_m)^2},\ t_m(x) = x^3 + \left(\frac{1}{\gamma_m^2} - 4\right)x + 2\,\gamma_m,\ 0 \le m \le 3. \tag{14}$$

Picking an index value m, the nine-point set $\{x_j : 1 \le j \le 9\}$ might be divided into three *collinear* triplets, each aligned along the same direction vector (corresponding here, as described in the preceding section, to the monomial $x - \gamma_m$), each triple sharing the same image value (under s_m), successively denoted by s_{m1}, s_{m2} and s_{m3}. Letting the index m assume 4 possible values, we attain 4 distinct divisions of the set $\{x_j : 1 \le j \le 9\}$.

The coefficients of the polynomial

$$g_m(x) = x^3 - w_m^1\, x^2 + w_m^2\, x - w_m^3,$$

lie in $\mathbb{F}_\eta[\gamma_m]$, and, exploiting formulas (6), are readily calculated:

$$w_m^1 = s_{m1} + s_{m2} + s_{m3} = 9\,\eta,\ w_m^2 = s_{m1}\,s_{m2} + s_{m2}\,s_{m3} + s_{m3}\,s_{m1} = 6\,c_m\,\eta - \frac{3}{\gamma_m^2},$$

$$w_m^3 = s_{m1}\,s_{m2}\,s_{m3} = c_m^2\,\eta + \frac{2}{\gamma_m^3},$$

where

$$c_m := -3\left(\gamma_m + 4\,\alpha\right) = \frac{6\gamma_m^2 - 1}{\gamma_m^3}.$$

The discriminant w_m of the polynomial g_m might be regarded as a function w in the variables γ_m and η: $w_m := w(\gamma_m, \eta)$, where

$$w(\gamma, \eta) = -\frac{108(9\gamma^2 - 1)^2 q_2(\eta)}{\gamma^9} = -11664\left(7\,\gamma^3 + 21\,\alpha\gamma^2 + \left(15 - 24\,\alpha^2\right)\gamma + 16\,\alpha^3 - 12\,\alpha\right)q_2(\eta).$$

[9] Division of points on $\mathbb{E}_\beta$ by an integer n might, of course, be viewed as multiplication by the rational $1/n$.

The roots of the cubic polynomial g_m might, thus, be expressed via radical functions of its coefficients:

$$s_{ml} = 3\,\eta + \frac{9\,\eta^2 - 2\,c_m\,\eta + 1/\gamma_m^2}{e_{ml}} + e_{ml},$$

$$e_{ml} = \sqrt[3]{27\,\eta^3 - 9\,c_m\,\eta^2 + (27 - 6\,c_m(\alpha+\gamma_m))\,\eta + 1/\gamma_m^3 + \sqrt{-w_m/108}}\;\zeta^l,\; 1 \le l \le 3,$$

where ζ is a primitive cube root of unity: $\zeta^3 = 1 \ne \zeta$. Since $\alpha^2 \ne 4/9$, $\gamma_m^2 \ne 1/9$ and the discriminant w_m vanishes iff $q_2(\eta) = 0$ iff $\eta \in \{0, -\beta, -1/\beta\}$. Note that two of the three roots s_{ml} are swapped by switching from a branch, of the square root function (applied to $-w_m/108$) in the expression for e_{ml}, to the other, while the third root (of g_m) remains unaltered.

The polynomial f_3 might now be factored (in four distinct ways) into a product of three cubic polynomials:

$$f_3(x) = \prod_{l=1}^{3} h_{ml}(x),\;\; h_{ml}(x) := t_m(x) - s_{ml}\,(\gamma_m - x)^2,\;\; 1 \le l \le 3.$$

Once a root of f is calculated the other eight roots might be obtained by adding to (and subtracting from) it the four roots of r_3 (all treated as first coordinates of points on $\mathbb{E}_\beta$) via the addition formula (2). We shall suggest four ways to calculating a root x_1 of f_3. Firstly, a root might be obtained as a root of any cubic polynomial $h_{ml}(x) = x^3 + a_1x^2 + a_2x + a_3$, and thereby expressed as an element in a radical extension of the field, generated by its coefficients:

$$x_1 = b - \frac{a_1}{3} + \frac{a_1^2 - 3\,a_2}{9\,b},$$

where

$$b := \sqrt[3]{\sqrt{-a/108} - a_1^3/27 + a_1a_2/6 - a_3/2},\; a := a_1^2a_2^2 + 18\,a_1a_2a_3 - 4\,a_1^3a_3 - 4\,a_2^3 - 27\,a_3^2.$$

Secondly, a root might be obtained as root of a first degree polynomial, namely a greatest common divisor of any pair of cubic polynomials h_{ml}, whose first indices (m) do not match with each other, and thereby is expressible as a rational function of the coefficients of the chosen pair of cubic polynomials. So, if a cubic polynomial pair h_1 and h_2 is chosen, where

$$h_m(x) = x^3 + a_{m1}\,x^2 + a_{m2}\,x + a_{m3}, \tag{15}$$

then a root x_1 might be calculated as

$$x_1 = \frac{(a_{12} - a_{22})(a_{23} - a_{13}) + a_{11}a_{21}(a_{13} + a_{23}) - a_{13}a_{21}^2 - a_{11}^2a_{23}}{(a_{11} - a_{21})(a_{23} - a_{13}) - a_{11}a_{21}(a_{12} + a_{22}) + (a_{12} - a_{22})^2 + a_{12}a_{21}^2 + a_{11}^2a_{22}} =$$

$$= \frac{(1+4\gamma_1\gamma_2)(s_1+s_2) - \left(\frac{1}{\gamma_2^2}+4\right)\gamma_1^2s_1 - \left(\frac{1}{\gamma_1^2}+4\right)\gamma_2^2s_2 + 2\left(\left(\left(1 - \gamma_1\gamma_2 + \frac{(\gamma_1-\gamma_2)(s_2-s_1)}{2}\right)s_1s_2 + \left(\frac{1}{\gamma_1} - \frac{1}{\gamma_2}\right)^2\right)(\gamma_1+\gamma_2) + \left(\gamma_1^3 - \gamma_2\right)s_1^2 + \left(\gamma_2^3 - \gamma_1\right)s_2^2\right)}{\left(\frac{1}{\gamma_1^2} - \frac{1}{\gamma_2^2} + 2(\gamma_1s_1 - \gamma_2s_2)\right)^2 + \left(2(\gamma_1-\gamma_2)(1 - s_1s_2) + \left(\gamma_2^2 - \frac{1}{\gamma_1^2} + 4\right)s_2 - \left(\gamma_1^2 - \frac{1}{\gamma_2^2} + 4\right)s_1\right)(s_1 - s_2)},$$

where the last expression is attained by recalling that $a_{m1} = -s_m$, $a_{m2} = 1/\gamma_m^2 - 4 + 2\,s_m\gamma_m$ and $a_{m3} = 2\,\gamma_m - s_m\gamma_m^2$.

Thirdly, a root might be calculated as a common root of three-polynomial subset of a pinned set H. So, denoting the polynomials of this pinned set by h_m, $0 \le m \le 3$, and denoting their coefficients via

that same expression (15), which we have already applied to the first pair h_1 and h_2, we shall then extract the value of the root x_1 as the third component of the vector solution of the linear system

$$\begin{pmatrix} 1 & a_{11} & a_{12} \\ 1 & a_{21} & a_{22} \\ 1 & a_{31} & a_{32} \end{pmatrix} \begin{pmatrix} x_3 \\ x_2 \\ x_1 \end{pmatrix} = - \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix}.$$

The system might be solved either via Gauss elimination, or, explicitly, by applying Cramer rule (10):

$$x_1 = -\frac{\Delta_{02}}{\Delta_{03}},\ \Delta_{02} = \begin{vmatrix} 1 & -s_1 & \gamma_1(2 - s_1\gamma_1) \\ 1 & -s_2 & \gamma_2(2 - s_2\gamma_2) \\ 1 & -s_3 & \gamma_3(2 - s_3\gamma_3) \end{vmatrix},\ \Delta_{03} = \begin{vmatrix} 1 & -s_1 & \gamma_1(2s_1 - c_1) \\ 1 & -s_2 & \gamma_2(2s_2 - c_2) \\ 1 & -s_3 & \gamma_3(2s_3 - c_3) \end{vmatrix}.$$

As discussed in the preceding section, the components labeled x_2 and x_3 do, respectively, coincide with the square and the cube of the root x_1. Furthermore, a vector collinear with the vector $(x_1^3, x_1^2, x_1, 1)$ might be obtained by "orthogonalizing" the vector $(0, 0, 0, 1)$ with respect to the space spanned by the three-vectors set $\{(1, a_{m1}, a_{m2}, a_{m3}) : 1 \leq m \leq 3\}$.

Fourthly and finally, a root might be obtained as a linear function of the four coefficients (of x^2) $a_{m1} = -s_m$, corresponding to the four polynomials h_m, $0 \leq m \leq 3$, of the pinned set H, using formula (12):

$$x_1 = \frac{1}{3}\sum_{m=0}^{3} s_m - 3\,\eta = \eta + \sum_{m=0}^{3} \frac{9\,\eta^2 - 2\,c_m\,\eta + 1/\gamma_m^2}{3\,e_m} + \frac{e_m}{3},$$

where e_m is understood to match that particular value, among the three values e_{ml}, $1 \leq l \leq 3$, via which s_m is obtained as a radical function of the coefficients of the cubic polynomial g_m.

The modular equation and a tribute to Galois

Put $d(x) := x - 1/x$, and $d^2(x) := x + 1/x - 2$. Let d^2 denote the discriminant of the quadratic polynomial $q(x)$, which coincides with the discriminant of the cubic polynomial $q_2(x)$, so $d^2 = d(\beta)^2 = d^2(\beta^2)$. The homothety class of the lattice Λ_β is represented by a (unique) point τ in the fundamental domain $\Gamma\backslash\mathcal{H}$, as we alluded to in the introduction. The (Klein) modular invariant j, which maps the upper half plane $\mathcal{H}$ onto $\mathbb{C}$, is a modular form of weight zero. Its domain might be extended to include all rational real points, as well as, the point at (complex) infinity. All these points map (under j) to (complex) infinity. We shall emphasize that the modular invariant j is a (holomorphic) bijection between the (or any) extended fundamental domain and the Riemann sphere $\mathbb{C} \cup \infty$.[10] The domain of j might be further extended to include the lower half plane via setting $j(-\tau) = j(\tau)$. The value of j at a point τ, corresponding to the homothety class of the lattice Λ_β is

$$j(\tau) = \frac{4\,(d^2 + 1)^3}{27\,d^2}, \tag{16}$$

and since the said discriminant d^2 is invariant under the substitutions $\beta \mapsto -\beta$ and $\beta \mapsto 1/\beta$, so must be $j(\tau)$. Moreover, $j(\tau)$ is invariant under the substitutions $\beta \mapsto \sqrt{1 - \beta^2}$. Thus, the homothety class of the lattice Λ_β as β^2 undergoes the inversions (meaning linear fractional transformations of order 2)

$$S : x \mapsto \frac{1}{x},\ T : x \mapsto 1 - x, \tag{17}$$

[10] The latter statement merely defines a modular form of weight zero.

is preserved. The latter two inversions generate a (6 element) group isomorphic with the symmetry group S_3 of a triangle. The three functional (trigonometric) pairs

$$\{-\tan^2, -\cot^2\},\ \{\sin^2, \cos^2\},\ \{\csc^2, \sec^2\}$$

might be viewed as the three vertices, which are rotated via either the composition $S \circ T$ or its inverse $T \circ S$. The first vertex is invariant under the action of S which transposes the second vertex with the third, while the second vertex is invariant under the action of T which transposes the third vertex with the first, and the third is invariant under the action of the third inversion

$$S \circ T \circ S = T \circ S \circ T : x \mapsto \frac{x}{x-1}$$

which transposes the first vertex with the second. Generally, twelve distinct values of β correspond to a single point τ in the fundamental domain. The exceptions are the values, corresponding to the *corners* of the fundamental domain. These are the six values $\beta \in \{\pm i, \pm 1/\sqrt{2}, \pm\sqrt{2}\}$, corresponding to $\tau = i := \sqrt{-1}$, and the four values $\beta \in \{\pm i\zeta,\ \pm i\zeta^2\}$, corresponding to $\tau = \zeta$.[11] An isomorphism between elliptic curves as their elliptic modulus β undergoes permissible transformations (generated by S and T) might explicitly be given as a linear map between first coordinates. Evidently, the isomorphism corresponding to the transformation $\beta \to 1/\beta$ is given by the identity map $x \mapsto x$, and the isomorphism corresponding to the transformation $\beta \to -\beta$ is given by the map $x \mapsto -x$. The isomorphism corresponding to the transformation $\beta \to \sqrt{1-\beta^2}$ is given by the map $x \mapsto -(\beta x + 1)/\sqrt{1-\beta^2}$. Alternatively denoting the elliptic modulus β by $\sin\theta$,[12] the latter map between first coordinates

$$l(x) = -x\tan\theta - \sec\theta \tag{18}$$

is said to induce an isomorphism of elliptic curves, as the elliptic modulus β undergoes the transformation $\sin\theta \to \cos\theta$.[13]

Since two elliptic moduli β and $1/\beta$ correspond to a single elliptic function $\mathcal{R}_\beta$ (and to a single elliptic curve $\mathbb{E}_\beta$), only six elliptic functions $\mathcal{R}$ correspond to twelve values of the elliptic modulus, corresponding to a single point τ in the fundamental domain. Only three distinct functions $\mathcal{R}$ correspond to the exceptional value $\tau = i$, and only two distinct functions $\mathcal{R}$ correspond to the exceptional value $\tau = \zeta$. The term elliptic modulus, endowed upon the parameter β, is now seen to coincide with the same term appearing in connection with the Jacobi elliptic functions. The Jacobi elliptic sine function, corresponding to elliptic modulus β and denoted by $\mathrm{sn}_\beta = \mathrm{sn}_\beta(\cdot)$, satisfies the differential equation

$$\mathrm{sn}_\beta'^2 = \left(1 - \mathrm{sn}_\beta^2\right)\left(1 - \beta^2\mathrm{sn}_\beta^2\right),$$

and coincides, up to homothety and translation (of its argument), with a square root of the function $\mathcal{R}$ (analytically continued). Explicitly,

$$\beta\,\mathrm{sn}_\beta\left(\frac{z}{\sqrt{\beta}}\right)^2 = \frac{1}{\mathcal{R}_{-\beta}(z)} = \mathcal{R}\left(z + \sqrt{\beta}\,z_0, -\beta\right),^{14}\ z_0 := \frac{\pi i}{2M(\beta)},$$

[11] A reformulation involving α (instead of β) would be less cumbersome, perhaps, and so we give it here. Generally, six distinct values of α correspond to a single point τ in the fundamental domain. The exceptions are the three values $\alpha \in \{0, \pm 1/\sqrt{2}\}$, corresponding to $\tau = i$, and the two values $\alpha \in \{\pm 1/\sqrt{3}\}$, corresponding to $\tau = \zeta$.

[12] The angle θ is then called *the modular angle*.

[13] One readily verifies that the inverse of the linear map l is $l^{-1}(x) = -x\cot\theta - \csc\theta$ correspond to the (reverse) transformation of the elliptic modulus $\cos\theta \to \sin\theta$.

[14] Note that the leftmost side of the equality is unaltered by switching from a branch of the square root function, applied to β, in the expression for the argument of the (known to be odd) function sn_β, to the other.

where $M(x)$ is the arithmetic-geometric mean of 1 and x; enlightening details about the function M are presented in [13]. As the elliptic modulus $\beta = \sin\theta$ undergoes the transformations, which we earlier discussed, corresponding elliptic functions $\mathcal{R}(\cdot, -\sin\theta)$, $\mathcal{R}(\cdot, i\tan\theta)$ and $\mathcal{R}(\cdot, -\sec\theta)$ coincide, up to homothety, translation and multiplicative constants, with the squares of the Jacobi elliptic functions sn_β, cn_β and dn_β. Putting $\kappa := 2i\csc(2\theta)$, the squares of the latter two Jacobi elliptic functions might be, explicitly, expressed as

$$\mathrm{cn}_\beta(z)^2 = 1 - \frac{\kappa}{\mathcal{R}\left(z/\sqrt{\kappa},\, i\tan\theta\right) + i\tan\theta} = i\cot\theta\,\mathcal{R}\left(\frac{z+z_0}{\sqrt{\kappa}},\, i\tan\theta\right),$$

$$\mathrm{dn}_\beta(z)^2 = 1 + \frac{\sin\theta\tan\theta}{\mathcal{R}\left(\sqrt{-\cos\theta}\,z,\, -\sec\theta\right) - \sec\theta} = \cos\theta\,\mathcal{R}\left(\sqrt{-\cos\theta}\,(z+z_0),\, -\sec\theta\right).$$[15]

Respectively, they satisfy the differential equations

$$\mathrm{cn}_\beta'^2 = \left(1-\mathrm{cn}_\beta^2\right)\left(1-\beta^2+\beta^2\mathrm{cn}_\beta^2\right),\ \mathrm{dn}_\beta'^2 = \left(1-\mathrm{dn}_\beta^2\right)\left(\beta^2-1+\mathrm{dn}_\beta^2\right),$$

as well as, the functional equations

$$\mathrm{sn}_\beta^2 + \mathrm{cn}_\beta^2 \equiv 1 \equiv \beta^2\mathrm{sn}_\beta^2 + \mathrm{dn}_\beta^2.$$

Here, one must also bear in mind a simple and basic functional equation

$$\mathcal{R}(iz,\, \beta) = -\mathcal{R}(z,\, -\beta).$$

An explicit fast inverse k of the modular invariant j was given in [2, 5, 6, 7] as a composition

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

where

$$k_0(x) := \frac{i\,M\left(\sqrt{1-x^2}\,\right)}{M(x)},\ k_1(x) := \frac{\sqrt{x+4}-\sqrt{x}}{2},\ k_2(x) := \frac{3}{2}\left(\frac{x}{k_3(x)} + k_3(x)\right) - 1,$$

$$k_3(x) := \sqrt[3]{\sqrt{x^2-x^3}-x}.$$[16]

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 Γ. 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

[15] Alternatively, using the inversion L, which appears later in this article, we have

$$\mathrm{cn}_\beta(z)^2 = i\cot\theta\,L\left(\mathcal{R}\left(\sqrt{\frac{\sin(2\theta)}{2i}}\,z,\, i\tan\theta\right),\, -i\tan\theta\right),\ \mathrm{dn}_\beta(z)^2 = \cos\theta\,L\left(\mathcal{R}\left(\sqrt{-\cos\theta}\,z,\, -\sec\theta\right),\, \sec\theta\right).$$

[16] A verification, of this explicit inverse, was carried out by Helmut Ruhland and is made accessible at the web site provided at the end of footnote 39.

the modular group Γ 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,

$$\forall x \in \mathbb{C},\ j \circ k\,(x) = x,^{17}$$

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

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 $j(i) = 1$. So, we point out that the (set) values of the composition, $k_1 \circ k_2$ at 0 and 1, coincide with exceptional (set) values of β at $\tau = \zeta$ and $\tau = i$, respectively. 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 $i \in k(1) = k_0 \circ k_1(1/2)$.[18]

Recalling our default assumption 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, as explained in [18], 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 $\mathbb{Q}(j(\tau))$,[19] and we shall call its roots, *the roots of the modular equation of level* n. Now, let the value of $j(\tau)$ be given by equation (16) then the values

$$j_m := \frac{4\,(d_m^2+1)^3}{27\,d_m^2},\ d_m^2 := d^2(\beta_m^2),\ \beta_m^2 := \frac{s_m(-\beta) - s_m(0)}{s_m(-1/\beta) - s_m(0)},\ 0 \le m \le n, \tag{19}$$

where $s_m(\cdot)$ is the fractional transformation given by equation (5), are the roots of the modular equation of level n. Evidently, 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 in (17). 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. One might be satisfied to verify that a value of one of the roots j_m would coincide with $j(n\tau)$. The elliptic curves $\mathbb{E}_\beta$ and $\mathbb{E}_{\beta_m}$ are said to be related by *cyclic isogeny* of degree n.

The projective special linear group $G_n := \mathrm{PSL}(2, \mathbb{Z}_n)$, where $\mathbb{Z}_n$ is the (prime) field of integers modulo n (which we had earlier introduced), is the Galois group of the modular equation of level n. Not merely a Galois group in the conventional sense, but is the Galois group in a most spectacular sense. Galois, who was apparently the discoverer of finite fields, indicated, in his last letter [14],[20] sufficient and necessary

[17] 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.

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

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

[20] This letter, addressed to Chevalier, on the eve of Galois' (so-called) duel (which, perhaps, simpler and more accurately described by Alfred, who did not let anyone disturb the final moments with his older brother Évariste, as murder) May 30, 1832, was eloquently described by Hermann Weyl as "the most substantial piece of writing in the whole literature of mankind".

condition for *depressing*[21] the degree of the modular equation of prime level. For this very purpose he did introduce the, being discussed, projective special linear groups over prime fields G_n, and observed that they were simple for all primes strictly exceeding the prime 3.[22] For primes $n \geq 5$, he pointed out the three exceptions for which the groups G_n possessed subgroups of indices coinciding with the cardinality of the field n. These were the primes 5, 7 and 11. For any prime n strictly exceeding 11, proper subgroups of index $n+1$, and no lower (as we were also told by Galois), are guaranteed to exist in G_n. Equivalently said,[23] a modular equation, of prime level $n \geq 5$, is depressible, from degree $n+1$ to degree n (and no lower), 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},[24] Galois must, in particular, be solely credited for solving the general quintic via exhibiting it as a modular equation of level 5. While Galois' contribution for formulating sufficient and necessary criterion for solubility of an algebraic equation via radicals was brought to light by Liouville, his decisive contribution to actually solving the quintic (before Hermite and Klein did) is, surprisingly, too poorly recognized (if not at all unrecognized)![25] Betti, in 1851 [11], futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results, and, in 1854 [12], went on to show that Galois' construction yields a solution to the quintic via elliptic functions.[26] One might associate with each quintic, given in Bring-Jerrard form, a corresponding value for the (Jacobi) elliptic modulus β, as Hermite did, in 1858 [15], implementing this very Galois' construction, which time has come to clarify. The group G_5 acts (naturally) on the projective line $\mathrm{P}\mathbb{Z}_5$, which six elements we shall, following Galois, label as 0, 1, 2, 3, 4 and ∞. Then collecting them in a triple-pair $\{(0,\infty), (1,4), (2,3)\}$, the group G_5 is seen to generate four more triple-pairs $\{(1,\infty), (2,0), (3,4)\}$, $\{(2,\infty), (3,1), (4,0)\}$, $\{(3,\infty), (4,2), (0,1)\}$, $\{(4,\infty), (0,3), (1,2)\}$. Together, the five triple-pairs constitute the five-element set upon which G_5 acts.[27] Galois did not (in his last letter) write down the four triple-pairs, which we did

[21]This well-established term means lowering. Its conception is a simple (yet ingenious) idea with which Galois alone must be fully credited, and, as we shall soon see, is the single most crucial (yet rarely brought to awareness) step towards actually solving the quintic.

[22]The very concept of simplicity, being again introduced by Galois, provides the basic principle in classifying (finite) groups. We note here that the projective special linear group is simple for all finite, not necessarily prime, fields except the fields $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

[23]The equivalence, of statement that follows to the few statements preceding it, was established by Galois.

[24]For $n = 5, 7, 11$, the subgroup of index n in G_n turns 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.

[25]Galois' brother Alfred and schoolmate Auguste Chevalier managed to involve Liouville (who was 135 weeks elder to Galois) in disentangling the manuscripts, which they faithfully copied and forwarded to several mathematicians (including Gauss and Jacobi). 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 has 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".

[26]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. For the sake of being fair to a few exceptional mathematicians, we must cite (without translating to English) Grothendick (as a representative), who (in his autobiographical book Récoltes et Semailles) graciously admits that "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)."

[27]Indeed, it is the five-element set (not merely a five-element set) which Hermite had no choice but to employ. Galois'

write after the first, and we now, guided by his conciseness and brevity, confine ourselves to writing down only the first pair-set that he presented for each of the two remaining cases, where $n = 7$ and $n = 11$, respectively: $\{(0,\infty), (1,3), (2,6), (4,5)\}$ and $\{(0,\infty), (1,2), (3,6), (4,8), (5,10), (9,7)\}$. Unlike the case $n = 5$, an alternative might be presented for $n = 7$, which is $\{(0,\infty), (1,5), (2,3), (4,6)\}$, and for $n = 11$, which is $\{(0,\infty), (1,6), (3,7), (4,2), (5,8), (9,10)\}$. *The absolute invariant* for the action of the subgroup Γ_2, of the modular group Γ, consisting of linear fractional transformations congruent to the identity modulo 2, is β^2. A fundamental domain $\Gamma_2\backslash\mathcal{H}$ for the action of Γ_2, might be obtained by subjecting a fundamental domain $\Gamma\backslash\mathcal{H}$ (of Γ) to the action of the quotient group $\Gamma/\Gamma_2 \cong S_3$.[28] In particular, β^2 viewed as function on $\mathcal{H}$, is periodic, with period 2. The definition of the modular equation, initially introduced for the invariant j, might be extended to other invariants such as β^2 or $\beta^{1/4}$. Sohnke, in a remarkable work [19], had determined the modular equations for $\beta^{1/4}$, for all odd primes up to, and including, the prime 19. That work, along with Betti's work, inspired Hermite to (successfully) relate a (general) quintic, in Bring-Jerrard form, to a modular equation of level 5, yet he had little choice but to admit the importance of a sole Galois idea (in depressing the degree of the modular equation).[29] The modular polynomial for $\beta^{1/4}$, of level 5, is

$$\phi_5(x,y) := x^6 - y^6 + 5\,x^2y^2\,(x^2 - y^2) + 4\,x\,y\,(1 - x^4y^4), \tag{20}$$

and the period of $\beta^{1/4}$ (as an analytically continued function) is 16. Denoting the roots of $\phi_5(x,\, y = \beta^{1/4}(\tau))$, for a fixed $\tau \in \mathcal{H}$, by

$$y_5 = \beta^{1/4}(5\,\tau),\ y_m = -\beta^{1/4}\left(\frac{\tau + 16\,m}{5}\right),\ 0 \le m \le 4,$$

one calculates the minimal polynomial for $x_1 := (y_5 - y_0)(y_4 - y_1)(y_3 - y_2)\,y$. It turns out to be

$$x^5 - 2000\,\beta^2\,(1-\beta^2)^2\,x + 1600\sqrt{5}\,\beta^2\,(1-\beta^2)^2\,(1+\beta^2).$$

Thereby, a root of the quintic

$$x^5 - x + c,\ c := \frac{2\,(1+\beta^2)}{5^{5/4}\sqrt{\beta(1-\beta^2)}} = \frac{2\,(1+y^8)}{5^{5/4}\,y^2\sqrt{1-y^8}},$$ [30]

is

$$\frac{\sqrt{5}\,c\,x_1}{4\,(1+\beta^2)} = \frac{x_1}{2\,\sqrt{5\sqrt{5}\,\beta(1-\beta^2)}} = \frac{(y_5 - y_0)(y_4 - y_1)(y_3 - y_2)}{2\,y\,\sqrt{5\sqrt{5}\,(1-y^8)}},$$

construction for each of the two remaining cases, where $n = 7$ or $n = 11$, allows an alternative, as will, next, be exhibited.

[28]The latter quotient group coincides with G_2 which is isomorphic with S_3.

[29]Hermite had apparently adopted Cauchy's catholic and monarchist ideology, much in contrast to Galois' passionate rejection of social prejudice. In 1849, Hermite submitted a memoir to the French Academy of Sciences on doubly periodic functions, crediting Cauchy, but a priority dispute with Liouville prevented its publication. Hermite was then elected to the French Academy of Sciences on July 14, 1856, and (likely) acquainted, by Cauchy, with ideas stemming from (but not attributed to) Galois "lost" papers. T. Rothman made a pitiful attempt in "Genius and Biographers: The Fictionalization of Evariste Galois", which appeared in the American Mathematical Monthly, vol. 89, 1982, pp. 84-106 (and, sorrowly, received the Lester R. Ford Writing Award in 1983) to salvage Cauchy's reputation (unknowingly) suggesting further evidence of Cauchy's cowardice, and surprising us, along the way, with many (unusual but ill substantiated and biased) judgements telling us much about T. Rothman himself, but hardly anything trustworthy about anyone else!

[30]One must note that the constant coefficient c is invariant under the inversions $\beta \mapsto -1/\beta$ and $\beta \mapsto (1-\beta)/(1+\beta)$. Here, the composition of the latter two inversions is another inversion. The corresponding four-point orbit in a fundamental domain $\Gamma_2\backslash\mathcal{H}$ is generated via the mapping $\tau \mapsto 2/(2-\tau)$.

and so is expressible via the coefficients λ_m and μ_m of the elliptic polynomials $r_{m5}(x) =: x^2 - \lambda_m x + \mu_m$, $0 \le m \le 5$. In fact, the polynomials r_{m5} might be so ordered so that, for each m, the value β_m^2 coincides with y_m^8. The (general) expression for $y_m^8 = \beta_m^2$, as given in (19), might be rewritten for the special case $n = 5$ as

$$y_m^8 = \frac{s(\lambda_m,\, \mu_m,\, \beta)}{\beta^4 s(\lambda_m,\, \mu_m,\, 1/\beta)},$$

where

$$s(\lambda,\, \mu,\, x) = \left(\frac{1+\lambda\, x}{\mu} + x^2\right)\left(4\,\lambda + \left(\frac{2\,\lambda^2}{\mu} + 4 + 5\,\mu\right) x + \lambda\left(\frac{2}{\mu} + 3\right) x^2 + x^3\right),$$

and the coefficients $\lambda_m = \gamma_m + (2\cdot\gamma_m)$ and $\mu_m = \gamma_m(2\cdot\gamma_m)$ satisfy

$$\prod_{m=0}^{5}\left(x^2 - \lambda_m\, x + \mu_m\right) = x^{12} + \frac{62\, x^{10}}{5} - 21\, x^8 - 60\, x^6 - 25\, x^4 - 10\, x^2 + \frac{1}{5} +$$

$$+12\,\alpha\, x^3\left(x^8 + 4\, x^6 - 18\, x^4 - \frac{92\, x^2}{5} - 7\right) + 144\,\alpha^2\, x^4\left(\frac{x^6}{5} - 3\, x^2 - 2\right) - \frac{1728\,\alpha^3\, x^5}{5} = r_5(x).$$

The roots γ_m and $2\cdot\gamma_m$, $0 \le m \le 5$, of the division polynomial r_5 might be highly efficiently calculated via the algorithm provided in [9]. Calculating a pair, say γ_0 and γ_5, suffices, of course, for calculating all twelve roots via applying the addition formula (2), along with the doubling formula.

Nowadays, oblivion has entirely replaced marvelling at Galois key step, towards solving the quintic, in depressing the degree of the modular equation, of level 5, from 6 to 5,[31] and Galois is merely mentioned, along with Abel, for determining that the quintic is not solvable via radicals. With this paper, we hope that this (crippled) view of Galois (deeply constructive) theory would finally come to an end.

Let, for example, $\tau = 2\, i$, $\alpha = 2$, $\beta = \left(\sqrt{2} - 1\right)^2$. The corresponding quintic is

$$x^5 - x + \frac{3\sqrt{2\sqrt{2}}}{5\sqrt{\sqrt{5}}}.$$

The corresponding division polynomial $r_5(x)$ factors over $\mathbb{Q}[\sqrt{5}]$ into three quartic polynomial-factors:

$$r_5(x) = \left(x^4 + 4\left(3 + \sqrt{5}\right) x^3 + 6\left(5 + 2\sqrt{5}\right) x^2 - 4\left(29 + 13\sqrt{5}\right) x + 9 + 4\sqrt{5}\right)$$

$$\left(x^4 + \frac{18\, x^2}{5} + \frac{8\, x}{5} + \frac{1}{5}\right)\left(x^4 + 4\left(3 - \sqrt{5}\right) x^3 + 6\left(5 - 2\sqrt{5}\right) x^2 - 4\left(29 - 13\sqrt{5}\right) x + 9 - 4\sqrt{5}\right).$$

Each (quartic) factor is an elliptic polynomial pair product. They are (with their argument omitted) $r_{55} r_{50}$, $r_{54} r_{51}$ and $r_{53} r_{52}$, respectively. The (corresponding) modular polynomial $\phi_5\left(x, y = \beta^{1/4} = \sqrt{\sqrt{2} - 1}\right)$ factors, over $\mathbb{Q}[y]$, into a quadratic and a quartic polynomial-factor:

$$\phi_5\,(x, y\,) = \left(x^2 + y^{-2}\right)\left(x^4 + 4\, y^3\left(1 - y^2\, x^2\right) x - 2\, y^4\, x^2 - y^8\right),$$

and the six roots (of the modular polynomial) might be accordingly expressed and ordered:

$$y_0 = -\sqrt{\frac{\sqrt{2}\left(2 + \sqrt{5}\right) - \chi(-1)}{\chi(1)}},\ y_1 = -i\sqrt{\sqrt{2} + 1},\ y_2 = \sqrt{\frac{\sqrt{2}\left(2 - \sqrt{5}\right) - \chi(i)}{\chi(-i)}}.$$

[31] For example, S. Vlăduţ (wrongfully) attributes, in his book "Kronecker's Jugendtraum and Modular Functions" (published by Gordon and Breach in 1991), to Hermite showing the equivalence of the general quintic to the modular equation of level 5.

$$y_3 = \sqrt{\frac{\sqrt{2}\,(2-\sqrt{5}\,)-\chi(-i)}{\chi(i)}},\ y_4 = i\sqrt{\sqrt{2}+1},\ y_5 = \sqrt{\frac{\sqrt{2}\,(2+\sqrt{5}\,)-\chi(1)}{\chi(-1)}},$$ [32]

where

$$\chi(\epsilon) := 3 + 2\,\sqrt{\sqrt{5}\,\epsilon}.$$

Exploiting the identities

$$\beta = \left(\sqrt{2}-1\right)^2 = \left(\sqrt{10}-3\right)\left(\sqrt{5}-2\right)\left(3\sqrt{2}+\sqrt{5}-2\right),$$

$$\chi(1)\,\chi(-1) = \left(\sqrt{5}-2\right)^2 = \left(3\sqrt{2}+\sqrt{5}+2\right)\left(3\sqrt{2}-\sqrt{5}-2\right).$$

$$\chi(i)\,\chi(-i) = \left(\sqrt{5}+2\right)^2 = \left(3\sqrt{2}+\sqrt{5}-2\right)\left(3\sqrt{2}-\sqrt{5}+2\right),$$

along with the alternative expressions

$$y_0 = -\frac{\sqrt{-(i+1)\chi(i)}+\sqrt{(i-1)\chi(-i)}}{\sqrt{2\,\chi(1)}},\ y_5 = \frac{\sqrt{(i-1)\chi(i)}+\sqrt{-(i+1)\chi(-i)}}{\sqrt{2\,\chi(-1)}},$$

$$y_2 = \frac{\sqrt{2\,\chi(-i)}}{\sqrt{(1+i)\chi(1)}-\sqrt{(1-i)\chi(-1)}},\ y_3 = \frac{\sqrt{2\,\chi(i)}}{\sqrt{(1-i)\chi(1)}-\sqrt{(1+i)\chi(-1)}},$$

one finds out that

$$x_1 = -8\,\sqrt{5}\,\beta,$$

and, so, a root of our quintic is

$$\frac{-8\,\sqrt{5}\,\beta}{2\,\sqrt{5\sqrt{5}\,\beta(1-\beta^2)}} = \frac{-2}{\sqrt{\sqrt{10}}}.$$

Along the way, we might calculate the (five) discriminants

$$d^2(\beta^2) = d^2(\beta_1^2) = d^2(\beta_4^2) = 32,\ d^2(\beta_0^2) = \frac{32\,\chi(-1)}{\chi(1)^5},\ d^2(\beta_2^2) = \frac{32\,\chi(i)}{\chi(-i)^5},\ d^2(\beta_3^2) = \frac{32\,\chi(-i)}{\chi(i)^5},\ d^2(\beta_5^2) = \frac{32\,\chi(1)}{\chi(-1)^5},$$

observing that they are sixth powers of the respective values

$$2^{5/6},\ \frac{\sqrt{5}-1}{2^{1/6}\chi(1)},\ \frac{\sqrt{5}+1}{2^{1/6}\chi(-i)},\ \frac{\sqrt{5}+1}{2^{1/6}\chi(i)},\ \frac{\sqrt{5}-1}{2^{1/6}\chi(-1)},$$

and, so using equation (16), we might calculate five special values of the modular invariant:

$$j\left(\frac{5\,i}{2}\right) = j_0 = \left(\sqrt{5}+2\right)^{20}\chi(-1)^6\left(238\,\sqrt{5}-60\sqrt{\sqrt{5}}-\frac{861}{2}\right)^3,\ j(2\,i) = j_1 = j_4 = \left(\frac{11}{2}\right)^3,$$

$$j\left(\frac{5\,i-1}{4}\right) = j_2 = -\left(\sqrt{5}-2\right)^{20}\chi(i)^6\left(238\,\sqrt{5}-60\sqrt{\sqrt{5}}\,i+\frac{861}{2}\right)^3,$$

$$j\left(\frac{5\,i+1}{4}\right) = j_3 = -\left(\sqrt{5}-2\right)^{20}\chi(-i)^6\left(238\,\sqrt{5}+60\sqrt{\sqrt{5}}\,i+\frac{861}{2}\right)^3,$$

[32] The image of the square root is assumed, here (but not necessarily earlier!), to be unambigiously taken in the right half-plane, including the boundary of the upper quadrant but excluding it for the lower quadrant.

$$j\left(10\,i\right)=j_5=\left(\sqrt{5}+2\right)^{20}\chi(1)^6\left(238\,\sqrt{5}+60\sqrt{\sqrt{5}}-\frac{861}{2}\right)^3.^{33}$$

We might now let $\tau=i$, $\beta=\sqrt{2}$, and observe that the modular polynomial $\phi_5\left(x,y=\beta^{1/4}=\sqrt{\sqrt{\sqrt{2}}}\right)$ factors, over $\mathbb{Q}[y]$, into a quadratic and a quartic polynomial-factor:

$$\phi_5\left(x,y=\sqrt{\sqrt{\sqrt{2}}}\right)=\left(x^2-y^5x+y^2\right)\left(x^4-3\,y^5x^3-2\,y^2x^2+y^7x-y^4\right),$$

before confirming that the roots of the latter quartic polynomial-factor

$$\frac{\epsilon^2\sqrt{5}+1}{y^3\left(\epsilon\,\sqrt{\sqrt{5}}-1\right)},\ \epsilon=\{1,\,-i,\,i,\,-1\},$$

are, respectively, obtainable as fourth roots of the values

$$\frac{\sqrt{2}\left(\epsilon^2\sqrt{5}+2\right)}{\chi(-\epsilon)},$$

which, in turn, are (as they ought to be) the images of the four afore-calculated values β_0, β_2, β_3 and β_5 (where β was $3-2\sqrt{2}$) if subjected to the (fourth order) linear fractional transformation

$$\frac{1+\beta_m}{1-\beta_m},\ m\in\{0,\,2,\,3,\,5\}.$$

The four corresponding values of the discriminants are

$$d^2\left(\frac{2\left(\epsilon^2\sqrt{5}+2\right)^2}{\chi(-\epsilon)^2}\right)=\frac{\chi(\epsilon)^5}{2\,\chi(-\epsilon)}=32\left(\frac{\chi(\epsilon)}{\sqrt{5}-\epsilon^2}\right)^6.$$

Two more special values of the modular invariant are calculated by (reapplying) formula (16) to a discriminant from, firstly, the complex-conjugate ($\epsilon=\pm i$) pair, and, secondly, the real-valued ($\epsilon=\pm1$) pair:

$$j\left(\frac{5\,i+1}{2}\right)=\left(\frac{2927-1323\,\sqrt{5}}{2}\right)^3,\ j\left(5\,i\right)=\left(\frac{2927+1323\,\sqrt{5}}{2}\right)^3.$$

One might infer, from equation (19), that the modular polynomial, of level 2, $\Phi_2(x,\,z)$ vanishes at

$$(x,\,z_l)=\frac{4}{27}\left(\frac{\left(d^2+1\right)^3}{d^2},\,\frac{\left(d_l^2+1\right)^3}{d_l^2}\right),\ l\in\{0,1,2\},$$

where

$$\left(d_0^2,\,d_1^2,\,d_2^2\right)=16\left(\frac{1}{d^2},\,-\frac{d}{\beta^3},\,\beta^3\,d\right),\ d=d(\beta)=\beta-\frac{1}{\beta}.$$

For $x\in\{j_0,\,j_2,\,j_3,\,j_5\}$ we have already calculated the (two) corresponding values z_0. Concluding this section, we calculate the corresponding values z_1 and z_2, so put

$$\psi(\delta,\epsilon):=\frac{\sqrt{5}+1}{8\,\chi(\epsilon)^6}\left(57272-34011\,\delta\,\sqrt{2}+4\left(101-5463\,\delta\,\sqrt{2}\right)\epsilon^2\sqrt{5}+\right.$$

[33] These special values might be expressed as cubes if one notes that $\sqrt{5}\pm2=\left(\sqrt{5}\pm1\right)^3/8$.

$$-18\left(800+111\,\delta\,\sqrt{2}+4\left(100+27\,\delta\,\sqrt{2}\right)\epsilon^2\sqrt{5}\right)\epsilon\,\sqrt{\sqrt{5}}\Big)=$$

$$\frac{\left(\epsilon^2\sqrt{5}+1\right)^{37}}{2^{39}}\left(1190448488-858585699\,\delta\sqrt{2}+540309076\,\epsilon^2\sqrt{5}-374537880\,\delta\,\epsilon^2\sqrt{10}-\epsilon\,\sqrt{\sqrt{5}}\left(693172512-595746414\,\delta\sqrt{2}+407357424\,\epsilon^2\sqrt{5}-240819696\,\delta\,\epsilon^2\sqrt{10}\right)\right)=$$

$$=\frac{1}{8}\Big(129569705555681708+57945333889427292\,\epsilon^2\sqrt{5}-\epsilon\,\sqrt{\sqrt{5}}\left(86648484409011792+38750380257176208\,\epsilon^2\sqrt{5}\right)+$$

$$-9\,\delta\sqrt{2}\left(10179957492752331+4552615392370507\,\epsilon^2\sqrt{5}-\epsilon\,\sqrt{\sqrt{5}}\left(6807747878350206+3044517405934206\,\epsilon^2\sqrt{5}\right)\right)\Big),$$

and observe that

$$z_1(j_m)=\frac{4}{27}\left(\frac{2^{8/3}d(\beta_m)^{2/3}}{\beta_m^2}-\frac{\beta_m}{2^{4/3}d(\beta_m)^{1/3}}\right)^3=\psi(-1,\epsilon)^3,$$

$$z_2(j_m)=\frac{4}{27}\left(2^{8/3}\beta_m^2\,d(\beta_m)^{2/3}+\frac{1}{2^{4/3}\beta_m\,d(\beta_m)^{1/3}}\right)^3=\psi(1,\epsilon)^3,$$

where $\epsilon\in\{1,\,-i,\,i,\,-1\}$ correspond, respectively, to $m\in\{0,\,2,\,3,\,5\}$, as before, and verify that

$$j\left(\frac{5\,i}{4}\right)=z_1(j_0),\ j\left(\frac{20\,i+5}{17}\right)=z_1(j_2),\ j\left(\frac{20\,i-5}{17}\right)=z_1(j_3),\ j\,(20\,i)=z_1(j_5),$$

$$j\left(\frac{5\,i+2}{4}\right)=z_2(j_0),\ j\left(\frac{20\,i+4}{13}\right)=z_2(j_2),\ j\left(\frac{20\,i-4}{13}\right)=z_2(j_3),\ j\left(\frac{10\,i+1}{2}\right)=z_2(j_5).$$

Instead of a conclusion: few motivating calculations towards many more

Given a parameter $\gamma\in\mathbb{C}\setminus\{\pm1\}$ and a variable x introduce an inversion L as

$$L(x,\gamma):=\frac{\gamma x-1}{x-\gamma}.$$

By calling L an inversion, we tacitly assume the parameter γ being fixed. The inversion $L(\cdot,\gamma)$ swaps the point 1 with -1, whereas *the dual inversion* $L(x,\cdot)$ fixes, for a fixed argument $x\in\mathbb{C}$, the points -1 and 1. The inversion L ought to be viewed as a conformal bijection, from the Riemann sphere $\mathbb{C}\cup\infty$ onto itself, which coincides with its own inverse, that is,

$$\forall x\in\mathbb{C}\cup\infty,\ L(L(x,\gamma),\gamma)=x. \tag{21}$$

The inversion L satisfy two properties we'll call *skew commutativity* and *skew associativity*,[34] meaning that, $\forall x\in\mathbb{C}\cup\infty$, the two respective identities

$$L(x,\,\gamma)=-L(\gamma,\,x),\ L\,(L(x,\gamma),\,\delta)=L(-x,\,L(\gamma,\delta)),$$

hold. Together, these two properties are equivalent to another property-pair

$$L(x,\,\gamma)=-L(-x,-\gamma),\ L\,(L(x,\gamma),\,\delta)=-L(L(\gamma,\delta),-x).$$

[34]The non-associative division algebra of octonions $\mathbb{O}$, sometimes referred to as Cayley algebra, inevitably springs to mind. The terms "skew commutative" and "skew associative" are rarely used nowadays, upon describing the octonions $\mathbb{O}$, often replaced, respectively, by the terms "anti-commutative" and "anti-associative". The latter term is even more frequently replaced by "alternative".

Identity (21) might, in fact, be regarded as the (special) case of skew associativity, corresponding to $\delta = \gamma$. Observing that $L(1/\gamma, \gamma) = 0$ and $L(0, \gamma) = 1/\gamma$, the cases $\delta = 1/\gamma$ and $\delta = 0$ might be emphasized as the identities

$$L\left(L(x,\gamma),\, \frac{1}{\gamma}\right) = \frac{1}{x},\ \frac{1}{L\,(x,\gamma)} = L\left(\frac{1}{x},\, \gamma\right) = L\left(x,\, \frac{1}{\gamma}\right).$$

The Klein four-group, which fixes the differential equation (1) as described in [3], is generated by any two of its three non-trivial elements, which are

$$x \mapsto \frac{1}{x},\ x \mapsto L(x, -\delta),\ \delta \in \left\{\beta,\, \frac{1}{\beta}\right\}. \tag{22}$$

These three inversions are permuted if conjugated by the map l, given in (18). Explicitly,

$$l\left(\frac{1}{l(x,\delta)}, \sqrt{1-\delta^2}\right) = L\left(x, -\frac{1}{\delta}\right).$$

$$l\left(L\left(l(x,\delta), -\sqrt{1-\delta^2}\right), \sqrt{1-\delta^2}\right) = L(x, -\delta).$$

$$l\left(L\left(l(x,\delta), -\frac{1}{\sqrt{1-\delta^2}}\right), \sqrt{1-\delta^2}\right) = \frac{1}{x}.$$

Put

$$L_n\,(x,\delta) := x \prod_{\gamma:\, r_n(\gamma,\delta)=0} L(x,\gamma)^2,$$

and observe that the multiplication by an odd integer n of a first coordinate x of a point on $\mathbb{E}_\beta$, given by (3), must commute with the three inversions given by (22), that is,

$$n \cdot x = L_n\,(x,\delta) = 1/L_n\left(\frac{1}{x}, \delta\right) = L\left(L_n\left(L(x,-\delta),\delta\right), -\delta\right),\ \delta \in \left\{\beta,\, \frac{1}{\beta}\right\},$$

and we must also have

$$L_n\,(x,\delta) = -L_n\,(-x,-\delta) = l\left(L_n\left(l(x,\delta), \sqrt{1-\delta^2}\right), \sqrt{1-\delta^2}\right) = l\left(L_n\left(l(x,\delta), \frac{1}{\sqrt{1-\delta^2}}\right), \sqrt{1-\delta^2}\right).$$

The latter formula merely reflects the fact that multiplication is respected by isomorphisms (of elliptic curves), thereby obviating the second and the third equality along with the first.[35]

Calculating directly the sum

$$\sum_{m=0}^{n} s_m(x) = n(n+1)\,x - \frac{2\,q_2'(x)\,r_n'(x)\,r_n(x) - 4\,q_2(x)\,(r_n'(x)^2 - r_n''(x)\,r_n(x))}{r_n(x)^2},$$

and applying the multiplication (by an odd prime n) formula to the last summand in formula (12), we might deduce the functional equation

$$n^2 x^{n^2} r_n\left(\frac{1}{x}\right)^2 = n^2 x\, r_n(x)^2 - 2\,q_2'(x)\,r_n'(x)\,r_n(x) + 4\,q_2(x)\left(r_n'(x)^2 - r_n''(x)\,r_n(x)\right),$$

[35] One might opt a more technical route of deducing the latter formula, aided with the formulas for conjugating the inversion L with the linear map l, given above.

from which we, in turn, deduce the following system of equations

$$n^2\gamma^{n^2} r_n\left(\frac{1}{\gamma}\right)^2 = 4\, q_2(\gamma)\, r_n'(\gamma)^2,$$

as γ runs through the roots of r_n.

We shall refrain from delving into explicit calculations of (all) the coefficients w_m^k, $1 \le k \le n$, yet we carry a calculation for the (last) coefficient w_m^n, thereby demonstrating that such calculations might be worthwhile to pursue in the near future. The coefficient w_m^n might be expressed as

$$w_m^n(\eta) = c_{mn}^2\,(\eta - \eta_{mn})\,, \tag{23}$$

and calculating it, being a linear function of η, amounts to calculating the two constants c_{mn} and η_{mn}. These are

$$c_{mn} = n\prod_{l=1}^{(n-1)/2} s_m(l\cdot\gamma),\ \eta_{mn} = -\frac{s_m(0)}{n^2}\prod_{l=1}^{(n-1)/2}\left(s_m\left(\frac{1}{l\cdot\gamma}\right)/s_m\left(l\cdot\gamma\right)\right)^2,$$ [36]

where γ is a (fixed) root of r_n/r_{mn}, that is,

$$r_n(\gamma) = 0 \neq r_{mn}(\gamma).$$

And, as γ runs through $n(n-1)/2$ permissible values, while restricted to satisfy the latter condition, both constants c_{mn} and η_{mn} remain unaltered. So, as we already know, both coefficients are elements of the field $\mathbb{F}[\gamma_m]$, where γ_m is a root of r_{mn}.[37] Alternative expressions are

$$c_{mn}^2 = \beta\left(w_m^n(0) - w_m^n(-1/\beta)\right),\ \frac{1}{\eta_{mn}} = \beta\left(\frac{w_m^n(-1/\beta)}{w_m^n(0)} - 1\right).$$

Denote the roots of the coelliptic polynomial t_m by ξ_k, $1 \le k \le n$, and pick an index j so that $0 \le j \le n$ and $j \neq m$. One then finds that, for any given root γ of r_{jn}, the equality[38]

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

merely reflects two (out of many) distinct ways of calculating one and the same the value $\eta_{mn} = n\cdot\xi_k$. 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 (jointly obtained on both sides) turn out to coincide with one and the same. The latter identity supplies an example of identities, while conceptually simple, quite cumbersome to verify, even when aided with an up-to-date

[36] For a less cumbersome notation, we have avoided using two indices for (either) the function s_m (or t_m), leaving its dependence upon n being tacitly assumed. Once the right hand side of each equality is calculated, the double indices endow the dependence, of the two values c_{mn} and η_{mn}, with explicity.

[37] The coefficients c_{mn} and η_{mn} are, in fact, elements of the (smaller) field which (merely) contains the coefficients of r_{mn}.

[38] Here, as was the case with the deduced functional equation for the division polynomial r_n and the system of equations that followed it, the primality of n is not necessary but its oddness is (as we have not even bothered with defining division polynomials with even indices). My immediate family, that is my wife, son and daughter must be credited for prompting this footnote. Most of the pertinent calculations were carried out by my wife Anja, and must be brought to light in another article.

symbolic computation software, implemented on contemporary machines. Perhaps, one ought to start with verifying the case, where $n = 3$, that is the case

$$\xi_k^9 \left(r_3 \left(\frac{1}{\xi_k} \right) / r_3(\xi_k) \right)^2 = -2\,\gamma_m \left(\gamma^3\, t_m \left(\frac{1}{\gamma} \right) / t_m(\gamma) \right)^2, \tag{24}$$

where r_3 and t_m are given in (13) and (14), respectively.[39] The three values on the left-hand side, as k acquires the values 1, 2, 3, and the three values on the right-hand side, as γ runs through the three other than γ_m roots of r_3, coincide with the value

$$\eta_{m3} = -\frac{2\,\gamma_m^3}{(6\,\gamma_m^2 - 1)^2} = \frac{2\,(16\,\alpha(13 - 48\,\alpha^2) - 4(7 + 528\,\alpha^2)\gamma_m + 48\,\alpha(1 - 96\,\alpha^2)\gamma_m^2 - (13 + 1152\,\alpha^2)\gamma_m^3)}{(1 - 96\,\alpha^2)^2}.$$

Four distinct invariants η_{m3}, $0 \le m \le 3$, correspond to each $\alpha \ne \pm 2/3$. With γ being a root of r_{jn}, $j \ne m$, as before, we might also derive the identities

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

$$\prod_{k=1}^{n} r_n(\xi_k) = 2^{n-1} \prod_{l=1}^{(n-1)/2} q_2(l \cdot \gamma_m)\, r_n'(l \cdot \gamma_m)^2\, s_m(l \cdot \gamma)^n.$$

The left-hand side of the latter equality is recognized as the resultant of the polynomials t_m and r_n. Rewriting it for the case, where $n = 3$, yields an expression for the resultant as a cube

$$\prod_{k=1}^{3} r_3(\xi_k) = \left(4\, q_2(\gamma_m)\, s_m(\gamma) \right)^3 =$$

$$= 64 \left(-28/27 + 7\,\alpha^2/3 - 12\,\alpha^4 + \alpha \left(4/3 - 27\,\alpha^2 \right) \gamma_m + \left(20/3 - 31\,\alpha^2 \right) \gamma_m^2 - 8\,\alpha^3\,\gamma_m^3 \right).$$

We conclude by remarking that $c_{mn} = 0$ iff $\eta_{mn} = \infty$. In this case w_m^n is constant (no longer dependent upon η), and the polynomial $t_m(x)$ divides the polynomial $r_n(x)$. But t_m would possess a common root with r_n iff it possess a (precisely one) common root with each factor r_{jn}, $0 \le j \le n$, $j \ne m$.[40] The expression for the coefficient w_m^n, given in (23), would then have to be replaced by

$$w_m^n(\eta) = w_m^n(0) = s_m(0) \prod_{l=1}^{(n-1)/2} s_m \left(\frac{1}{l \cdot \gamma} \right)^2, \quad \prod_{l=1}^{(n-1)/2} t_m\,(l \cdot \gamma) = 0,$$

[39] The latter (simplest) equality was subjected to several numerical verifications by Mikhail Malykh (FNM MSU, Moscow, Russia), who subsequently applied Sage and Maple standard simplification procedures to the difference (of the right and the left hand side) with negative result (that is, the difference was not recognized by the machine as being zero)! After presenting the equality on April 16, 2014 at the 7th International Polynomial Computer Algebra Conference in St. Petersburg, Russia, Sergei Meshveliani (PSI RAS, Pereslavl-Zalessky, Russia) suggested explicit procedures, based on Gröbner basis techniques, in order to yield the desired simplification, which he outlined on May 21, 2014 at the 17th Workshop on Computer Algebra in Dubna, Russia [16]. Later, in private correspondence, Helmut Ruhland presented a straightforward (no machine requiring) constructive proof, which I (with his permission) presented on the joint MSU-CCRAS Computer Algebra Seminar on September 24, 2014 [5]. The presentation, containing his proof, was titled "Torsion points on elliptic curves and modular polynomial symmetries" and is freely accessible via the world wide web at http://www.ccas.ru/sabramov/seminar/doku.php.

[40] Note that $t_m(\gamma_m) = 4\, q_2(\gamma_m)\, r'_{mn}(\gamma_m)^2$ never vanishes.

where γ is (again) a root of r_n/r_{mn}. The latter condition must be satisfied by any such root, so (in other words) it is the condition of vanishing of the resultant of the polynomials t_m and r_{jn} for each $j \neq m$, $0 \leq j \leq n$. For $n = 3$, the three conditions $t_0(\gamma_j) = 0$, $j \in \{1, 2, 3\}$, are equivalent to the (single) condition that $\gamma_0^2 = 1/6$.[41] The coefficients w_0^2 and w_0^3, then, acquire the (independent of η) constant values $-3/\gamma_0^2 = -18$ and $2/\gamma_0^3$, respectively.

References

[1] Adlaj S. Galois elliptic function and its symmetries. In Vassiliev N.N. (ed.) 12th International Conference on Polynomial Computer Algebra, pp. 11–17. St. Petersburg department of Steklov Institute of Mathematics, St. Petersburg (2019).

[2] Adlaj S. On the second memoir of Évariste Galois' last letter. Computer Tools in Science and Education **4**, 5–20 (2018)

[3] Adlaj S. Thread equilibrium in a linear parallel force field. LAP LAMBERT, Saarbrucken (2018) (in Russian).

[4] Adlaj S. An analytic unifying formula of oscillatory and rotary motion of a simple pendulum (dedicated to 70th birthday of Jan Jerzy Slawianowski). In Mladenov I. Ludu A. Yoshioka A. (eds.) Proc. Int. Conf. "Geometry, Integrability, Mechanics and Quantization", pp. 160–171. Avangard Prima, Sofia, Bulgaria (2015).

[5] Adlaj S. Torsion points on elliptic curves and modular polynomial symmetries. Presented at the joined MSU-CCRAS Computer Algebra Seminar on September 24, 2014. Available at `http://www.ccas.ru/sabramov/seminar/lib/exe/fetch.php?media=adlaj140924.pdf`.

[6] Adlaj S. Modular Polynomial Symmetries. In Vassiliev N.N. (ed.) 7th International Conference on Polynomial Computer Algebra, pp. 4–5. St. Petersburg department of Steklov Institute of Mathematics, St. Petersburg (2014).

[7] Adlaj S. Elliptic and coelliptic polynomials // 17th Workshop on Computer Algebra, Dubna, Russia, May 21-22, 2014. Available at `http://compalg.jinr.ru/Dubna2014/abstracts2014_files/1159.pdf`.

[8] Adlaj S. Mechanical interpretation of negative and imaginary tension of a tether in a linear parallel force field. In Selected Works of the International Scientific Conference on Mechanics "Sixth Polyakhov Readings", pp. 13–18. Saint-Petersburg State University, Saint-Petersburg (2012).

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

[10] Adlaj S. Eighth lattice points // arXiv:1110.1743.

[11] Betti E. Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo // Dagli Annali di Scienze matimatiche e fisiche, t. II (Roma, 1851): 5–19.

[41] The corresponding value of α, here, is $-\gamma_0/4$.

[12] Betti E. Un teorema sulla risoluzione analitica delle equazioni algebriche // Dagli Annali di Scienze matimatiche e fisiche, t. V (Roma, 1854): 10–17.

[13] Cox D. The arithmetic-geometric mean of Gauss. Mathématique, 30 (1984): 275–330.

[14] Galois É. "Lettre de Galois à M. Auguste Chevalier" // Journal de Mathématiques Pures et Appliquées XI (1846): 408-–415.

[15] Hermite C. "Sur la résolution de l'équation du cinquième degré" // Comptes Rendus de l'Académie des Sciences XLVI(I) (1858): 508-–515.

[16] Meshveliani S. D. Computer proof for a "mysterious" equality for quartic roots // 17th Workshop on Computer Algebra, Dubna, Russia, May 21-22, 2014. Available at `http://compalg.jinr.ru/Dubna2014/abstracts2014_files/1199.pdf`.

[17] Serre J-P. A Course in Arithmetic. New York: Springer-Verlag, 1973.

[18] Shimura G. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton, NJ: Princeton University Press, 1981.

[19] Sohnke L.A. Aequationes modulares pro transformatione Functionum Ellipticarum // Journal für die reine und angewandte Mathematik, **16** (1837): 97–130. ISSN 0075-4102.