Multiplication by n on elliptic curves over rings

Jinbi Jin
(Universiteit Leiden)

October 26, 2012

Main problem

Construct a triple of homogeneous polynomials defining multiplication by n on all projective Weierstrass curves over rings.

Results

For Weierstrass elliptic curves over fields: Already known *if* we restrict to *affine points* $(x : y : 1)$ (see [E])

Result unsuitable for direct generalisation to elliptic curves over arbitrary rings.

But it turns out that we can modify the polynomials to work for all points on elliptic curves over rings.

[E]: Andreas Enge, *Elliptic curves and their applications to cryptography - an introduction*

Example: Doubling formula (1/2)

Theorem

Let E be a Weierstrass curve over a ring R defined by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

where $a_1, a_2, a_3, a_4, a_6 \in R$. Let $P = (x : y : z)$ be a point on E. Then

$$2P = \big(\alpha_2(P) : \beta_2(P) : \gamma_2(P)\big),$$

where:

Example: Doubling formula (2/2)

$$\begin{aligned}
\alpha_2 = {} & 2xy^3 + 3a_1x^2y^2 + (a_1^2 - 2a_2)y^3z + (a_1^3 - 3a_1a_2 + 3a_3)xy^2z + (-2a_1^2a_2 + 2a_2^2 - 6a_4)x^2yz \\
& + (a_1a_2^2 - 3a_2a_3 - 3a_1a_4)y^2z^2 + (a_1^2a_2^2 - a_1^3a_3 - 2a_1a_2a_3 - 4a_1^2a_4 - 3a_3^2 + 2a_2a_4 - 18a_6)xyz^2 \\
& + (-a_1a_2^3 + a_1^2a_2a_3 + a_2^2a_3 - 3a_1a_3^2 + 4a_1a_2a_4 - 3a_3a_4 - 9a_1a_6)x^2z^2 \\
& + (a_1a_2^2a_3 - a_1^2a_3^2 - 3a_2a_3^2 - a_1a_3a_4 - 3a_1^2a_6 + 2a_4^2 - 6a_2a_6)yz^3 \\
& + (-a_1a_2a_3^2 - a_1a_2^2a_4 + 2a_1^2a_3a_4 - a_1^3a_6 - 2a_3^3 + a_2a_3a_4 + 4a_1a_4^2 - 3a_1a_2a_6 - 9a_3a_6)xz^3 \\
& + (-a_2a_3^3 + a_1a_3^2a_4 - a_1a_2^2a_6 + a_3a_4^2 - 3a_2a_3a_6 + 3a_1a_4a_6)z^4 \\
\beta_2 = {} & y^4 + a_1xy^3 + (a_1a_2 - 2a_3)y^3z + (a_1^2a_2 - a_2^2 - 3a_1a_3 + 3a_4)xy^2z \\
& + (-2a_1a_2^2 + 6a_1a_4)x^2yz + (a_2^3 - a_1a_2a_3 + a_1^2a_4 - 5a_2a_4 + 18a_6)y^2z^2 \\
& + (a_1a_2^3 - 2a_1^2a_2a_3 + a_1^3a_4 - a_2^2a_3 + 3a_1a_3^2 - 6a_1a_2a_4 + 3a_3a_4 + 27a_1a_6)xyz^2 \\
& + (-a_2^4 + 2a_1a_2^2a_3 - a_1^2a_2a_4 + 6a_2^2a_4 - 6a_1a_3a_4 + 9a_1^2a_6 - 9a_4^2)x^2z^2 \\
& + (a_2^3a_3 - a_1a_2a_3^2 + a_1^3a_6 + 2a_3^3 - 5a_2a_3a_4 - a_1a_4^2 + 3a_1a_2a_6 + 18a_3a_6)yz^3 \\
& + (a_1^2a_2a_3^2 - a_1^3a_3a_4 + a_1^4a_6 + 2a_2^2a_3^2 - a_1a_3^3 - a_2^3a_4 - 2a_1^2a_4^2 + 6a_1^2a_2a_6 - 6a_3^2a_4 + 3a_2a_4^2 + 9a_2^2a_6 - 27a_4a_6)xz^3 \\
& + (a_1a_2a_3^3 - a_1^2a_3^2a_4 + a_1^3a_3a_6 - a_3^4 + a_2a_3^2a_4 - 2a_1a_3a_4^2 - a_2^3a_6 + 6a_1a_2a_3a_6 - a_4^3 - 9a_3^2a_6 + 9a_2a_4a_6 - 27a_6^2)z^4 \\
\gamma_2 = {} & 8y^3z + 12a_1xy^2z + 6a_1^2x^2yz + (a_1^3 + 12a_3)y^2z^2 + (a_1^4 + 12a_1a_3)xyz^2 + (-a_1^3a_2 + 3a_1^2a_3)x^2z^2 \\
& + (a_1^3a_3 + 6a_3^2)yz^3 + (-a_1^3a_4 + 3a_1a_3^2)xz^3 + (-a_1^3a_6 + a_3^3)z^4
\end{aligned}$$

Division polynomials and multiplication by n

The generic Weierstrass curve E/K (1/2)

$R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, 1/\Delta]$, where Δ is the usual elliptic discriminant.

K: algebraic closure of field of fractions of R.

E: elliptic curve over K defined by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

W: affine Weierstrass polynomial, i.e.

$$Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

The generic Weierstrass curve E/K (2/2)

Then recall:

$E(K)$ is an abelian group, with addition given by the chord-and-tangent rule, and with neutral element 0 the point at infinity.

$K(E)$ is field of fractions of $K[X,Y]/(W)$, where $X = x/z$ and $Y = y/z$.
$\mathrm{ord}_0(X) = -2$, $\mathrm{ord}_0(Y) = -3$.

$\Lambda\colon K(E) - 0 \to K - 0$, $f \mapsto \left((X/Y)^{-\mathrm{ord}_0 f} f\right)(0)$ (*leading coefficient*).

Multiplication by n on E/K (1/3)

Main reference: [E]

Definition

Let $n \in \mathbb{Z} - 0$. The *n-th division polynomial* Ψ_n is the unique element of $K(E) - 0$ with divisor $\sum_{P \in E[n]}([P] - [0])$ and leading coefficient n. In addition, we define $\Psi_0 = 0$.

Fact

The division polynomials satisfy the recurrence relation

$$\Psi_{m+n}\Psi_{m-n} = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2,$$

where $m, n \in \mathbb{Z}$.

Fact

For all $n \in \mathbb{Z}$, we have $\Psi_n \in R[X, Y]/(W)$.

Multiplication by n on E/K (2/3)

Define, for $n \in \mathbb{Z} - 0$,

$$\Phi_n = X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1} \quad \Omega_n = \frac{1}{2\Psi_n}\big(\Psi_{2n} - \Psi_n^2(a_1\Phi_n + a_3\Psi_n^2)\big).$$

In addition, define $\Phi_0 = \Omega_0 = 1$.

Fact

For all $n \in \mathbb{Z}$, we have $\Phi_n, \Omega_n \in R[X, Y]/(W)$. Moreover, we have $\Lambda\Phi_n = \Lambda\Omega_n = 1$ and $\operatorname{ord}_0 \Phi_n = -2n^2$, $\operatorname{ord}_0 \Omega_n = -3n^2$.

Multiplication by n on E/K (3/3)

Proposition

Let $n \in \mathbb{Z}$. Let $P \in E(K)$ be a point of E of the form $(x : y : 1)$. Then

$$nP = \big(\Phi_n(x,y)\Psi_n(x,y) : \Omega_n(x,y) : \Psi_n^3(x,y)\big)$$

Creating new polynomials (1/3)

Want to extend formula to all points.

Solution: homogenise formula with respect to suitable representatives modulo W.

Usual representatives (Y-degree at most 1) are not suitable.

Representatives with X-degree at most 2 are!

Look e.g. at homogenisations of

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Creating new polynomials (2/3)

Let $A_n, B_n, C_n \in R[X, Y]$ be the unique representatives of $\Phi_n \Psi_n$, Ω_n, Φ_n^3, resp., with X-degree at most 2.

$A_n,\ B_n,\ C_n$ have total degrees $n^2,\ n^2,\ n^2 - 1$, resp.

Define $\alpha_n = z^{n^2} A_n, \beta_n = z^{n^2} B_n, \gamma_n = z^{n^2} C_n \in R[x, y, z]_{n^2}$.

Creating new polynomials (3/3)

Theorem

Let $n \in \mathbb{Z}$, and let $P \in E(K)$ be a point. Then

$$nP = \big(\alpha_n(P) : \beta_n(P) : \gamma_n(P)\big).$$

Proof.

It suffices to check that $\beta_n(0) \neq 0$, which is true as $\beta_n \in y^{n^2} + xR[x,y,z] + zR[x,y,z]$. $\square$

Weierstrass curves over rings

Weierstrass polynomials and ring morphisms

A homogeneous Weierstrass polynomial over a ring S is of the form

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in S$ are such that $\Delta(a_1, a_2, a_3, a_4, a_6) \in S^\times$.

Hence the data of giving a homogeneous Weierstrass polynomial over S is equivalent to giving a ring morphism $R \to S$.

Elliptic curves over rings

Definition

Let S be a ring, and let E be a Weierstrass curve over S given by a homogeneous Weierstrass polynomial W.
The *set $E_0(S)$ of S-valued points in homogeneous coordinates* is the set of all $(x : y : z) \in S^3$ (up to scaling by a unit of S) satisfying $W(x, y, z) = 0$ and $Sx + Sy + Sz = S$.

Remark

- $E_0(S)$ usually is not the full set of S-valued points (to be defined later), but this is the case when $\operatorname{Pic} S = 1$ (which is the case e.g. when S is semi-local or factorial).
- Full set of S-valued points is an abelian group, but $E_0(S)$ is usually not closed under addition.

Example

Let $S = \mathbb{Z}[\sqrt{-5}]$, and let $K = \mathbb{Q}(\sqrt{-5})$. Consider the Weierstrass curve E over S given by $y^2z + xyz + yz^2 = x^3 + 4xz^2 - 6z^3$, and the two points

$$P = (9 : 23 : 1)$$
$$Q = (3411\sqrt{-5} : 26488 + 117\sqrt{-5} : -3645\sqrt{-5})$$

Then $P + Q$ is given (in $E(K)$) by

$$(61028487 + 104922279\sqrt{-5} : 120011054 - 171672039\sqrt{-5} : -127263527)$$

which is not in $E_0(S) \subseteq E(K)$.

Main theorem, simple form

However, $E_0(S)$ turns out to be closed under multiplication by n:

Main Theorem

Let $n \in \mathbb{Z}$. Let S be a ring, and let E be a Weierstrass curve over S. Let $P = (x : y : z) \in E_0(S)$. Then

$$nP = \big(\alpha_n(P) : \beta_n(P) : \gamma_n(P)\big).$$

Corollary in terms of division polynomials

Corollary

Let $n \in \mathbb{Z}$. Let S be a ring, and let E be a Weierstrass curve over S. Let $P = (x : y : 1) \in E_0(S)$ be an affine S-valued point of E. Then

$$nP = \big(\Phi_n(x, y)\Psi_n(x, y) : \Omega_n(P) : \Psi_n^3(P)\big).$$

Question: Is this statement already in the literature?

The projective plane over rings (1/3)

We want to describe $\mathbb{P}^2(S)$ for a ring S.

Recall:

Definition

Let S be a ring, and let M be an S-module. Then M is called *invertible* if there exist elements $f_1, \ldots, f_s \in S$ such that $Sf_1 + \cdots + Sf_s = S$, and $M_{f_i} \cong S_{f_i}$ as S_{f_i}-modules.

If M and N invertible, then $M \otimes N$ and $M^\vee = \mathrm{Hom}_S(M, S)$ invertible.

Moreover, $M \otimes M^\vee \cong S$ as S-modules.

The projective plane over rings (2/3)

Consider 4-tuples (M, m_0, m_1, m_2), where M is an invertible S-module, and $m_0, m_1, m_2 \in M$ such that $Sm_0 + Sm_1 + Sm_2 = M$.

$(M, m_0, m_1, m_2) \sim (N, n_0, n_1, n_2)$ if there exists an isomorphism $M \to N$ of S-modules mapping m_i to n_i.

If $M = S$, then we denote the class of (M, m_0, m_1, m_2) by $(m_0 : m_1 : m_2)$.

The projective plane over rings (3/3)

Proposition

The $\mathbb{P}^2(S)$ is the set of equivalence classes of 4-tuples (M, m_0, m_1, m_2) as described before.

If $\operatorname{Pic} S = 1$, then by definition, all invertible S-modules are trivial, so then all points in projective plane are given by homogeneous coordinates.

The set of points of an elliptic curve (1/2)

Definition

Let S be a ring, and let E be a Weierstrass curve over S, given by a homogeneous Weierstrass polynomial W. The *set $E(S)$ of S-valued points* is the set

$$\{(M, m_0, m_1, m_2) \in \mathbb{P}^2(S) : W(m_0, m_1, m_2) = 0 \text{ in } M^{\otimes 3}\}.$$

The set of points of an elliptic curve (2/2)

Let S be a ring, and let E be a Weierstrass curve over S.

$E(S)$ has the structure of an abelian group, with $0 = (0 : 1 : 0)$ as neutral element. (See [KM])

If S is a field, this is the group structure we already know.

For an S-algebra T, the composition $R \to S \to T$ defines an elliptic curve E'. In this case, $E(S) \to E'(T)$, $(M, m_0, m_1, m_2) \mapsto (M \otimes_S T, m_0 \otimes 1, m_1 \otimes 1, m_2 \otimes 1)$ is a group homomorphism.

[KM] N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*

Main theorem, full version

Main Theorem

Let $n \in \mathbb{Z}$. Let S be a ring, and let E be a Weierstrass curve over S. Let $P = (M, m_0, m_1, m_2) \in E(S)$. Then

$$nP = \left(M^{\otimes n^2}, \alpha_n(m_0, m_1, m_2), \beta_n(m_0, m_1, m_2), \gamma_n(m_0, m_1, m_2)\right).$$

Proof of main theorem

Outline of proof

Step 1: Use Theorem of the Cube to show the existence and uniqueness (up to units in R) of homogeneous polynomials of degree n^2 defining multiplication by n on all Weierstrass curves.

Step 2: Show, using the generic Weierstrass curve, that these polynomials can be taken to be $\alpha_n, \beta_n, \gamma_n$.

Proof of Step 1 implies Step 2 (1/5)

Suppose for the moment that:

- We know that there exist homogeneous polynomials $\alpha'_n, \beta'_n, \gamma'_n$ that define multiplication by n on all Weierstrass curves.
- We know that they are unique up to scaling by a common unit of R.

Then we will show that $\alpha_n, \beta_n, \gamma_n$ also define multiplication by n.

Proof of Step 1 implies Step 2 (2/5)

Recall:

$R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, 1/\Delta]$

K: algebraic closure of field of fractions of R

Let E be the generic Weierstrass curve.

Make a choice of $\alpha'_n, \beta'_n, \gamma'_n$. Note that $\alpha'_0 = \gamma'_0 = 0$, $\beta'_0 \in R^\times$.

Hence assume $n \neq 0$. Main idea: view $\theta_n = \beta_n/\beta'_n$ as rational function on E, and prove that it is in fact in $R^\times$.

Proof of Step 1 implies Step 2 (3/5)

Why does this suffice?

Note that for all $P \in E(K)$, we have

$$\left(\alpha'_n(P) : \beta'_n(P) : \gamma'_n(P)\right) = nP = \left(\alpha_n(P) : \beta_n(P) : \gamma_n(P)\right).$$

Hence $\alpha'_n/\gamma'_n = \alpha_n/\gamma_n$ and $\beta'_n/\gamma'_n = \beta_n/\gamma_n$ as rational functions on E. We deduce that

$$\frac{\alpha_n}{\alpha'_n} = \frac{\beta_n}{\beta'_n} = \frac{\gamma_n}{\gamma'_n} = \theta_n$$

as rational functions on E. Hence if $\theta_n \in R^\times$, then we are indeed done.

Proof of Step 1 implies Step 2 (4/5)

θ_n is a rational function with neither zeroes, nor poles, since for all $P \in E(K)$,

$$\big(\alpha_n'(P), \beta_n'(P), \gamma_n'(P)\big) \neq (0,0,0)$$
$$\big(\alpha_n(P), \beta_n(P), \gamma_n(P)\big) \neq (0,0,0).$$

We deduce that $\theta_n \in K^\times$.

The homogeneous Weierstrass polynomial W is monic in x, so $\big(R[x,y,z]/(W)\big)_{n^2}$ is a free R-module. As θ_n is a quotient of two elements of $\big(R[x,y,z]/(W)\big)_{n^2}$, which is also a constant, it follows that θ_n is in the field of fractions of R.

Proof of Step 1 implies Step 2 (5/5)

Note that R is factorial.

Hence write $\theta_n = f/g$ with $f, g \in R$ having no common factors. Then $f\beta'_n = g\beta_n$ in $\left(R[x,y,z]/(W)\right)_{n^2}$. Hence g divides all coefficients of β'_n.

But for $P = (0:1:0)$, we have $\left(\alpha'_n(P), \beta'_n(P), \gamma'_n(P)\right) = (0:1:0)$, so the y^{n^2}-coefficient of β'_n is a unit. Hence g is a unit as well; $\theta_n \in R - 0$.

This implies that θ_n divides all coefficients of β_n. But $\Lambda\Omega_n = 1$ and $\operatorname{ord}_0 \Omega_n = -3n^2$, so the coefficient of y^{n^2} in β_n is 1. Hence $\theta_n \in R^\times$. $\square$

Outline of proof

Step 1: Use Theorem of the Cube to show the existence and uniqueness (up to units in R) of homogeneous polynomials of degree n^2 defining multiplication by n on all Weierstrass curves.

Step 2: Show, using the generic Weierstrass curve, that these polynomials can be taken to be $\alpha_n, \beta_n, \gamma_n$. $\leftarrow$ **Done!**

Elliptic curves over schemes (1/3)

Recall:

Let A be a ring, and let $f \in A[x_0, \ldots, x_n]$ be homogeneous of degree d. Let $P = \operatorname{Proj} A[x_0, \ldots, x_n]/(f)$.

Then, for all schemes X over $\operatorname{Spec} A$, we identify the set $P(X) = \operatorname{Hom}_{\mathrm{Sch}/A}(X, P)$ with the set of equivalence classes of $(n+2)$-tuples $(\mathcal{L}, s_0, \ldots, s_n)$ such that $f(s_0, \ldots, s_n) = 0 \in \mathcal{L}^{\otimes d}$.

Here, $\mathcal{L}$ is an invertible sheaf on $\mathcal{O}_X$, and the s_i global sections of $\mathcal{L}$ generating $\mathcal{L}$.

Elliptic curves over schemes (2/3)

Definition

Let S be a scheme. An *elliptic curve* over S is a triple $(E, \pi, 0)$, where

- $\pi\colon E \to S$ is a smooth proper morphism of schemes, and all its geometric fibres are connected curves of genus 1;
- $0\colon S \to E$ is a section of π, the *zero section*.

Elliptic curves over schemes (3/3)

Now let A be a ring, and let $R \to A$ be a ring morphism. Then the scheme $E = \operatorname{Proj} A[x, y, z]/(W)$, together with the section $0 = (0 : 1 : 0) \in E(A)$, is an elliptic curve. We call elliptic curves of this kind *Weierstrass curves*.

Note that Weierstrass curves over A come with an embedding into $\mathbb{P}^2_A$.

Fact ([KM])

- *Every elliptic curve is, (Zariski) locally on the base, isomorphic to a Weierstrass curve.*
- *Every elliptic curve is a group scheme.*

Proof of Step 1 (1/9)

Main idea to prove existence and uniqueness (up to units in R) of homogeneous polynomials defining multiplication by n on Weierstrass curves:

Consider a *universal point* on a *universal Weierstrass curve*.

Proof of Step 1 (2/9)

Let E be the elliptic curve over R given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

We call E the *universal elliptic curve*. Note that it corresponds to the identity map on R.

Moreover, we call the point $P^{\text{univ}} \in E(E)$ given by the identity map on E the *universal point* on E. Note that $P^{\text{univ}} = \big(\mathcal{O}_E(1), x, y, z\big)$.

We want to determine nP^{univ}, as a 4-tuple $(\mathcal{L}, s_0, s_1, s_2)$.

Proof of Step 1 (3/9)

Let μ_n denote the multiplication-by-n map on E.

As the identity on E corresponds to $\left(\mathcal{O}_E(1), x, y, z\right)$ in $E(E)$, we know that

$$nP^{\text{univ}} = \left(\mu_n^*\mathcal{O}_E(1), \mu_n^* s_0, \mu_n^* s_1, \mu_n^* s_2\right)$$

Hence we want to determine $\mu_n^*\mathcal{O}_E(1)$. We do this using the *Theorem of the Cube*.

Proof of Step 1 (4/9)

Theorem (Theorem of the Cube, [R])

Let X be an abelian scheme (e.g. an elliptic curve) over a scheme S, and let T be any S-scheme. Furthermore, let $a_1, a_2, a_3 \in X_S(T)$, and let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module. Then the invertible $\mathcal{O}_T$-module

$$\bigotimes_{I \subseteq \{1,2,3\}} \left(\sum_{i \in I} a_i \right)^* \mathcal{L}^{(-1)^{\# I}}$$

is trivial.

[R]: M. Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes*

Proof of Step 1 (5/9)

Expanded:

$$0^*\mathcal{L}$$

$$\otimes\, a_1^*\mathcal{L}^{-1} \otimes a_2^*\mathcal{L}^{-1} \otimes a_3^*\mathcal{L}^{-1}$$

$$\otimes\, (a_1 + a_2)^*\mathcal{L} \otimes (a_1 + a_3)^*\mathcal{L} \otimes (a_2 + a_3)^*\mathcal{L}$$

$$\otimes\, (a_1 + a_2 + a_3)^*\mathcal{L}^{-1}$$

Proof of Step 1 (6/9)

Corollary

Let $n_1, n_2, n_3 \in \mathbb{Z}$. Then the invertible $\mathcal{O}_E$-module

$$\bigotimes_{I \subseteq \{1,2,3\}} \mu^*_{\sum_{i \in I} n_i} \mathcal{O}_E(1)^{(-1)^{\#I}}$$

is trivial.

Proof of Step 1 (7/9)

Proposition

Let $n \in \mathbb{Z}$. Then $\mu_n^* \mathcal{O}_E(1) = \mathcal{O}_E(n^2)$.

Proof.

For $n \in \{-1, 0, 1\}$, this is trivial.

Hence it suffices to show that for all positive n, we have $\mu_n^* \mathcal{O}_E(1) = \mathcal{O}_E(n^2)$; this is done by induction, using the Theorem of the Cube.
To get the case $n = 2$, we apply the corollary with $n_1 = n_2 = 1$, $n_3 = -1$.
To get the case $n = k + 1$, we apply the corollary with $n_1 = k$, $n_2 = n_3 = 1$. □

Proof of Step 1 (8/9)

Corollary

Let $n \in \mathbb{Z}$. Then there exist homogeneous elements $\alpha'_n, \beta'_n, \gamma'_n$ of degree n^2 in $R[x, y, z]/(W)$ such that

$$nP^{\text{univ}} = (\mathcal{O}_E(n^2), \alpha'_n, \beta'_n, \gamma'_n).$$

These elements are unique up to a common unit of R.

Proof of Step 1 (9/9)

Corollary

Let E be a Weierstrass curve over a ring A, let T be a scheme over A. Furthermore, let $n \in \mathbb{Z}$ and $P = (\mathcal{L}, s_0, s_1, s_2) \in E(T)$. Then, for $\alpha'_n, \beta'_n, \gamma'_n$ as in the previous corollary,

$$nP = \left(\mathcal{L}^{\otimes n^2}, \alpha'_n(s_0, s_1, s_2), \beta'_n(s_0, s_1, s_2), \gamma'_n(s_0, s_1, s_2)\right)$$

Outline of proof

Step 1: Use Theorem of the Cube to show the existence and uniqueness (up to units in R) of homogeneous polynomials of degree n^2 defining multiplication by n on all Weierstrass curves. $\leftarrow$ **Done!**

Step 2: Show, using the generic Weierstrass curve, that these polynomials can be taken to be $\alpha_n, \beta_n, \gamma_n$. $\leftarrow$ **Done!**

Summary of main results

Theorem

Let $n \in \mathbb{Z}$. Let S be a ring, and let E be a Weierstrass curve over S. Let $P = (M, m_0, m_1, m_2) \in E(S)$. Then

$$nP = \left(M^{\otimes n^2}, \alpha_n(m_0, m_1, m_2), \beta_n(m_0, m_1, m_2), \gamma_n(m_0, m_1, m_2)\right).$$

Corollary

Let $n \in \mathbb{Z}$. Let S be a ring, and let E be a Weierstrass curve over S. Let $P = (x : y : z) \in E_0(S)$. Then

$$nP = \left(\alpha_n(P) : \beta_n(P) : \gamma_n(P)\right).$$