Monogenic Fields Arising from Torsion on Elliptic Curves

T. Alden Gassert, Hanson Smith, and Katherine E. Stange

arXiv id: 1708.03953, presenter email: hanson.smith@colorado.edu

Objective and Background

The connection between torsion points on elliptic curves with complex multiplication and class fields is well-documented. We investigated whether number fields obtained by adjoining torsion points of elliptic curves without complex multiplication have unique properties. Specifically, we discover a family of number fields arising from elliptic curves with rational 4-torsion that is monogenic, i.e. the ring of integers admits a power basis.

The problem of describing all monogenic number fields is called *Hasse's problem*. Since it was posed in the 1960's there has been a good deal of work put into the problem; however, this seems to be the first time that elliptic curves have been used as a method of attack.

Terminology

Tate's normal form of an elliptic curve with a rational point of order 4 is given by

$$E : y^2 + (\alpha + 8\beta)xy + \beta(\alpha + 8\beta)^2 y = x^3 + \beta(\alpha + 8\beta)x^2$$

where $\alpha, \beta \in \mathbb{Q}$ and $(0, 0)$ is the point of order 4. By changing coordinates, we may assume $\alpha, \beta \in \mathbb{Z}$ are coprime. The invariants are

$$\Delta = \beta^4(\alpha - 8\beta)(\alpha + 8\beta)^7, \quad j = \frac{(\alpha^2 - 48\beta^2)^3}{\beta^4(\alpha - 8\beta)(\alpha + 8\beta)}.$$

Let $E[n]$ be the group of n-torsion points on E. Suppose n is odd. We define the *nth division polynomial* to be

$$\Psi_n(x) = n \prod_{P \in E[n]\setminus\{\mathcal{O}\}}{}' (x - x(P))$$

where the prime indicates we only include one of each pair P and $-P$ in the product.

Let K be the number field obtained by adjoining a root, θ, of some irreducible polynomial $f(x)$ of degree n. Suppose the ring of integers of K, $\mathcal{O}_K$, admits the basis $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$. A basis of this form is called a *power basis* and in this case we say K is *monogenic*. In other words we have $\mathcal{O}_K = \mathbb{Z}[\theta]$.

An Example

Consider the elliptic curve in Tate Normal form

$$E : y^2 + 23xy + 23^2 y = x^3 + 23x^2.$$

Here $\alpha = 15$ and $\beta = 1$, so $\Delta = 7 \cdot 23^7$ and $j = \dfrac{(15^2 - 48)^3}{7 \cdot 23}$. Further, we have

$$\Psi_3(x) = 3x^4 + 621x^3 + 36501x^2 + 839523x + 6436343.$$

Let θ be a root of $\Psi_3(x)$. Our result shows that $K = \mathbb{Q}(\theta)$ is monogenic. However, $\mathbb{Z}[\theta]$ does not yield all of $\mathcal{O}_K$. To find a generator of our power basis, we change to the Fueter form

$$T_1^2 = 4T^3 + 23T^2 + 4T.$$

Now $\Psi_3(x)$ becomes

$$F_3(T) = T^4 - 6T^2 - 15T - 3.$$

Letting τ be a root of $F_3(T)$ that lies in K, we have

$$\begin{array}{ccccc} K = \mathbb{Q}(\theta) & \supset & \mathcal{O}_K = \mathbb{Z}[\tau] \\ | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$$

Results

Let E be an elliptic curve defined over $\mathbb{Q}$ such that some twist E' of E has a 4-torsion point defined over $\mathbb{Q}$. Then the following are equivalent:

- E' has reduction types I_1^* and I_1 only;
- E has j-invariant with squarefree denominator except a possible factor of 4.
- E has j-invariant $j = \frac{(\alpha^2-48)^3}{(\alpha-8)(\alpha+8)}$, where $\alpha \in \mathbb{Z}$, $\alpha \pm 8$ are squarefree.

Let K_n be the field defined by adjoining the x-coordinate of an n-torsion point of E. If any of the above hypotheses holds, then K_3 is monogenic with a generator given by a root of $T^4 - 6T^2 - \alpha T - 3$. In particular, the field K_3 has discriminant $-27(\alpha - 8)^2(\alpha + 8)^2$.

Methods

We consider an arbitrary elliptic curve E with a rational point of order 4 in Tate normal form. Let p be a prime of bad reduction. First, we apply Tate's algorithm to determine the Kodaira type of E. Now, we use a paper by the third author [2] or an explicit computation to find the p-adic valuation of the odd division polynomials, $\Psi_n(x)$, evaluated at the singular point modulo p.

Next we change coordinates to the Fueter form [1] of E. Applying

$$(x, y) = \left(\frac{a\beta}{T} - a\beta, \frac{1}{2}\left(\frac{(a\beta)^{\frac{3}{2}} T_1}{T^2} - \frac{a^2\beta}{T}\right)\right)$$

one obtains

$$T_1^2 = T\left(4T^2 + \frac{\alpha}{\beta}T + 4\right).$$

Under this change of coordinates $\Psi_3(x)$ becomes

$$F_3(T) = T^4 - 6T^2 - \frac{\alpha}{\beta}T - 3.$$

Let τ be a root of $F_3(T)$ and let $K = \mathbb{Q}(\tau)$. Here we apply the Montes algorithm. The Montes algorithm computes $v_p([\mathcal{O}_K : \mathbb{Z}[\tau]])$ by counting lattice points below certain Newton polygons. Noting the degree of $F_3(T)$ and the fact that reduction modulo $p \neq 3$ is injective on $E[3]$ if E is nonsingular modulo p, we consider only $p = 2, 3$ and p for which E has bad reduction. Requiring that $\beta = 1$ and $\alpha \pm 8$ are squarefree ensures that $v_p([\mathcal{O}_K : \mathbb{Z}[\tau]]) = 0$ for all p dividing the discriminant of $F_3(T)$. Thus we conclude K is monogenic.

References

[1] Ph. Cassou-Noguès and M. J. Taylor. *Elliptic functions and rings of integers*, volume 66 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1987.

[2] Katherine E. Stange. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.*, 68(5):1120–1158, 2016.