RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2014.40S.069

ScienceAsia 40S (2014): **69–72**

Towards the construction of elliptic curves over $\mathbb{Q}$ with high rank and a point of order 5

Fahd M. Alshammari

King Suad University, College of Science, Department of Mathematics, P.O.Box 2455 Riyadh 11451, Saudi Arabia

e-mail: fmobarak@ksu.edu.sa

Received 13 Feb 2014
Accepted 9 Jun 2014

ABSTRACT: By representing a genus one curve as a plane curve with five double points, we are able to construct a 3-parameter family of genus one curves over $\mathbb{Q}$ with Jacobians having a torsion subgroup isomorphic to Z_5. This leads, by specializing the parameters, to elliptic curves over $\mathbb{Q}$ of the Mordell-Weil group with high rank and with a torsion subgroup isomorphic to $\mathbb{Z}_5$. We also show this family contains as a subfamily the principal homogeneous space parameterizing elliptic curves with a rational point of order 5, namely $X_1(5)$. We explicitly describe these families by equations in the Weierstrass form.

KEYWORDS: Mordell-Weil group

BASIC CONSTRUCTION

Let $S = \{P_0, P_2, \ldots, P_4\}$ be a set of 5 points in the projective plane $\mathbb{P}^2(F)$ with the property that no three are co-linear, we call such a set in general position. Although most of the results hold over an arbitrary field F, for our interests and for simplicity we assume F is a subfield of the complex numbers or even just the rational numbers. A plane quintic having only ordinary double points at the points P_i has geometric genus $\frac{1}{2}(5-1)(5-2)-5 = 1$ (see Ref. 1). On the other hand we have the following lemma.

Lemma 1 *The vector space of quintic forms in three variables with double points on S has dimension 6.*

Proof: The vector space of degree n forms in $k+1$ has dimension $\binom{n+k}{k}$, because this is the number of combinations of n elements (with repletion) which can be taken from a set of $k+1$ elements. Hence the dimension of the vector space of all quintic forms in 3 variables is 21. Now to have double points on S, each point of S imposes 3 independent linear conditions, namely the vanishing of the first order partial derivatives which, by Euler's formula, implies the vanishing of the form (see Ref. 1 for more details). Hence the dimension of the vector space of quintic forms with double points on S is 21–15 = 6. □

We now find a basis for this vector space. For $i = 0, 1, \ldots, 4$ let L_i be the line through P_i and P_{i+1} and K_i be the line through P_i and P_{i+2} where the indices are considered modulo 5. Using the same symbols to denote the line equations, the product of each set of linear forms is a quintic which will be denoted as follows.

Definition 1 Given a set $S \subseteq \mathbb{P}^2$ of 5 points in general position, a union of five lines described above is called a *pentagon on S* and we refer to the points of S as its vertices.

Given a set S of five points in general position, the following facts are immediate:

(i) If P is a pentagon then the union of the remaining 5 lines is also a pentagon on S which will be called the pentagon opposite to P and is denoted by P^{op}.

(ii) There are exactly 12 pentagons on S which come in 6 pairs of the form (P, P^{op}).

(iii) P and P^{op} meet outside the set S in exactly five points giving the set $T = \{q_0, q_2, \ldots, q_4\}$. We will use the following notation. For $i = 0, 1, \ldots, 4$, q_i is the point of intersection of L_i and K_{i+2}, where again the indices are taken mod 5.

If we fix a form for each of the 12 pentagons then the following lemma shows in particular that these 12 forms generate the vector space of quintic forms with double points on S.

Lemma 2 *Let S be a set of five points in general position. There is a set of 6 pentagons on S so that their defining forms are linearly independent. Hence these forms generate a vector space of quintic forms with double points on S.*

Proof: Let $S = \{P_0, P_1, P_2, P_3, P_4\}$ and P be a pentagon on S. Let

$$P = \prod_{i=0}^{4} L_i$$

be a defining form for the pentagon P so that L_i is the form defining the line through P_i and P_{i+1} ($i = 0, 1, \ldots, 4$ and the indices are taken mod 5). Then we can write

$$P^{\text{op}} = \prod_{i=0}^{4} K_i$$

for the opposite pentagon so that K_i is the form defining the line through P_i and P_{i+2} ($i = 0, 1, \ldots, 4$ and the indices are taken mod 5). We claim that the following forms are linearly independent:

$$\begin{aligned} A_1 &= P \\ A_2 &= P^{\text{op}} \\ A_3 &= L_1 L_3 L_4 K_0 K_1 \\ A_4 &= L_0 L_2 L_4 K_1 K_2 \\ A_5 &= L_0 L_2 L_3 K_0 K_4 \\ A_6 &= L_0 L_1 L_3 K_2 K_3. \end{aligned}$$

To see this, suppose we have a linear relation

$$\sum_{i=1}^{6} a_i A_i = 0.$$

By evaluating the left-hand side of the equation at the point of intersection of the lines L_0 and K_2 we find that $a_3 = 0$, since all the forms A_i where $i \neq 3$ vanish at this point and $A_3 \neq 0$ there. Then put $a_3 = 0$ and evaluate at the point of intersection of the lines L_3 and K_0 to get $a_4 = 0$. Similarly, putting $a_3 = a_4 = 0$ and evaluating at the point of intersection of the lines L_4 and K_2 implies that $a_5 = 0$. Continue in this pattern to see that the evaluation at the point of intersection of L_4 and L_2 implies that $a_6 = 0$. Finally, it follows that $a_1 = 0$ and hence the forms A_i are linearly independent. □

We will consider the family of curves given by the equation

$$Q: \quad P + \mu P^{\text{op}} = 0$$

where μ is a non-zero rational number. If $\tilde{Q}$ is the normalization of Q then $\tilde{Q}$ is genus one curve and the space of holomorphic differentials on $\tilde{Q}$ has a nice general description given by the following lemma.

Lemma 3 *Let the curve Q have affine equation $q(x, y) = 0$, and let the coordinates are chosen so that q_y does not vanish identically. Let $\tilde{Q}$ be the normalization of Q, then the space of holomorphic differentials on $\tilde{Q}$ is generated by the differential form:*

$$\omega = \frac{g(x,y)d\,x}{q_y(x,y)} = \frac{-g(x,y)d\,y}{q_x(x,y)}$$

where $g(x, y)$ is the corresponding affine equation for the conic G through the points of S.

Sketch of proof We only give a sketch of the proof, for more details see Ref. 1 p. 360. First to avoid complications discussing points at infinity, write ω using homogenous coordinates, i.e., $x = X/Z$, and $y = Y/Z$. Then ω has the homogenous form

$$\omega = \frac{G(X,Y,Z)(Z d\,X - X d\,Z)}{Q_Y(X,Y,Z)}.$$

MAIN RESULTS

To select our five points forming S, we note the following result about points in general position.

Proposition 1 *The divisors of degree zero supported on the five points of T represent 5-torsion in the Jacobian of Q.*

Proof: We show that the points q_i for $i = 0, 1, \ldots, 4$ are 5-torsion points by explicitly finding rational functions f_{ij} such that $\text{div}(f_{\text{ij}}) = 5q_i - 5q_{\text{j}}$. Using the lines L_i and K_i, we have the following intersection cycles

$$\begin{aligned} L_i \cdot Q &= 2P_i + 2P_{i+1} + q_i \\ K_i \cdot Q &= 2P_i + 2P_{i+2} + q_{i+3} \end{aligned}$$

where the indices are taken mod 5 for $i = 0, 1, \ldots, 4$. It follows that we have the divisor

$$\text{div}\left(\frac{L_1 L_3^2 K_0^3 K_4}{L_0^2 L_2 K_2^3 K_3}\right) = 5q_3 - 5q_0.$$

Adding 1 (mod 5) to the indices of the lines of the rational function on the left we get a rational functions f_{ij} with following divisors

$$\begin{aligned} \text{div}(f_{41}) &= 5q_4 - 5q_1 \\ \text{div}(f_{02}) &= 5q_0 - 5q_2 \\ \text{div}(f_{13}) &= 5q_1 - 5q_3 \\ \text{div}(f_{41}) &= 5q_2 - 5q_4. \end{aligned}$$

The remaining desired rational functions are found by multiplying or dividing these five rational functions. □

Since any four points (with no three are collinear) in $\mathbb{P}^2$ are projectively equivalent to the points $p_0 =$

$(0:0:1)$, $p_1=(1:0:1)$, $p_2=(0:1:1)$, and $p_3=(1:1:1)$. We will choose for S the points p_0, p_1, p_2, p_3, and $p_4=(a:b:1)$.

Now for $i=0,1,\ldots,4$ the affine forms for the lines L_i are given respectively by y, $-x+1-y$, $y-1$, $x-xb+b-y+ay-a$, and $xb-ay$. On the other hand, the affine forms for the lines K_i are given respectively by $-x$, $-x+1$, $x-xb+ay-a$, $x-y$, and $xb-ay+y-b$. So that the curve Q is now given by the affine form

$$\begin{aligned} y(-x+1-y)(y-1)(x-xb+b-y+ay-a)\\ \times(xb-ay)-t(-x+1)(x-xb+ay-a)\\ \times(x-y)(xb-ay+y-b)\end{aligned}$$

Now by construction we have the following theorem.

Theorem 1 *The above affine form defines a genus one curve Q over the field $\mathbb{Q}(a,b,t)$ whose Jacobian contains 5-torsion subgroup represented by the points q_0, q_1, q_2, q_3, and q_4 with coordinates given respectively by*

$$\begin{aligned}\Big(-\frac{a}{-1+b}:0:1\Big),\Big(\tfrac{1}{2}:\tfrac{1}{2}:1\Big),\Big(\frac{a-1+b}{b}:1:1\Big),\\ \Big(0:\frac{-b+a}{a-1}:1\Big),\ \Big(1:\frac{b}{a}:1\Big).\end{aligned}$$

We show now that this family 'contains' $X_1(5)$.

Theorem 2 *With the substitutions $a=2$ and $b=3$, the above defines a genus one curve Q over the field $\mathbb{Q}(t)$ whose Jacobian is the modular elliptic curve $X_1(5)$.*

Proof: Using maple software we calculated the Jacobian in Weierstrass form

$$\begin{aligned}x^3+\big(-\tfrac{27}{256}-\tfrac{189}{128}t^2-\tfrac{27}{256}t^4+\tfrac{81}{84}t-\tfrac{81}{64}t^3\big)x\\ -\tfrac{27}{2048}t^6-\tfrac{2025}{2048}t^2-\tfrac{27}{2048}+\tfrac{243}{1024}t+y^2\\ -\tfrac{2025}{2048}t^4-\tfrac{243}{1024}t^5=0\end{aligned}$$

with j-invariant

$$-\frac{\left(1-12t+12t^3+14t^2+t^4\right)}{t^5\left(11t-1+t^2\right)}.$$

Now going back to the curve Q that represents an infinite 3-parameter family of genus one curves over $\mathbb{Q}$. By specializing the parameters, we modify this family and get other families with more rational points on them. Indeed a simple way to do this is by basically substituting the coordinates of any point (x,y) and solving the parameter t in terms of a and b. For example, using the affine point (3,2) will produce a 2-parameter family given by the affine form

$$\begin{aligned}y(-x+1-y)(y-1)(x-xb+b-y+ay-a)\\ \times(xb-ay)-\frac{2}{3}\frac{1}{(3-3b+a)(-b+a-1)}\\ \times\Big((1-2b+a)(-3b+2a)x(-x+1)\\ \times(x-xb+ay-a)(x-y)(xb-ay+y-b)\Big).\end{aligned}$$

By another rational point substitution, say (1,13), for (x,y) and solving for b in terms of a, the result is a 1-parameter family given by the form

$$\begin{aligned}y(-x+1-y)(y-1)(x-13xa+12a-y+ay)\\ \times(13xa-ay)+\frac{74}{3}\frac{1}{(3-38a)(-12-1)}\\ \times(1-25a)ax(-x+1)(x-13ax+ay-a)\\ \times(x-y)(13xa-ay+y-13a).\end{aligned}$$

Now this family has lots of smooth rational points. Using Mazur's classification of the Mordell-Weil groups of rational points on an elliptic curve[2], one concludes that the Jacobian of the above curve over $\mathbb{Q}(a)$ has positive rank and a subgroup of the torsion points isomorphic to $\mathbb{Z}_5$. We then use the program MAPLE to calculate the Jacobian and represent it by the following Weierstrass form.

$$\begin{aligned}x^3+\big(&-1875313186498431044352a^{12}\\ &+7731869513246851415040a^{11}\\ &-1217227157475263114208a^{10}\\ &+8875065530934155344896a^9\\ &-2778879875742156730752a^8\\ &+2124012315388685230008a^7\\ &+900300969806897 3184a^6\\ &-196896060658495 4112a^5\\ &+9349509008174587 2a^4\\ &+1085215555120320a^3-276569761691808a^2\\ &+8526936360384a-80951927472\big)x\\ &-4943968379370907549600331780096a^{18}\\ &+3035729545081811813648378666188 80a^{17}\\ &-7828560503413393784688041318645 76a^{16}\\ &+1090644782663773822407639896604672a^{15}\\ &-8745766256488321394895587575910 40a^{14}\end{aligned}$$

$$
\begin{aligned}
&+ 3924665127756972752284099700858888a^{13}\\
&- 84186051647810149948417519933440^{12}\\
&+ 3617229355755020670244737650688a^{11}\\
&+ 836923249645110539394962978 30a^{10}\\
&- 7862726838623571454331930 1120a^{9}\\
&- 1703921229822764330592574464a^{8}\\
&+ 3400469839243717812269568 00a^{7}\\
&+ 8743336451331398302613 76a^{6}\\
&- 8595021013594332778206 72a^{5}\\
&+ 4596393029433980261760a^{4}\\
&+ 1923455392105068836352a^{3}\\
&- 8231673487417563456 0a^{2}\\
&+ 14007027782047558912a\\
&- 8865207481313664 + y^{2}.
\end{aligned}
$$

□

From the above construction and the fact that the specializing map is an injective group homomorphism for infinitely many values of the parameter, see Ref. 3, we have the following theorem.

Theorem 3 *The elliptic curve over $\mathbb{Q}(a)$ with equation given by the above form has Mordell-Weil group with rank at least one and a torsion subgroup isomorphic to $\mathbb{Z}_5$. Thus by specializing rational values for a we have produced infinitely many elliptic curves over $\mathbb{Q}$ with Mordell-Weil group having torsion subgroup isomorphic to $\mathbb{Z}_5$ and rank at least 1.*

Acknowledgements: This project was supported by King Saud University, Deanship of Scientific Research, College of Science Research Centre.

REFERENCES

1. Brieskorn E, Knörrer H (1986) *Plane Algebraic Curves*, Birkhäuser Verlag, Basel.
2. Campbell G (1999) Finding elliptic curves and families of elliptic curves over $\mathbb{Q}$ of large rank. Dissertation, Rutgers Univ.
3. Silverman JH (1994) *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, New York.