ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 35, Number 5, 2006

ON Q-DERIVED POLYNOMIALS

R.J. STROEKER

ABSTRACT. A **Q**-derived polynomial is a univariate polynomial, defined over the rationals, with the property that its zeros, and those of all its derivatives are rational numbers. There is a conjecture that says that **Q**-derived polynomials of degree 4 with distinct roots for themselves and all their derivatives do not exist. We are not aware of a deeper reason for their non-existence than the fact that so far no such polynomials have been found. In this paper an outline is given of a direct approach to the problem of constructing polynomials with such properties. Although no **Q**-derived polynomial of degree 4 with distinct zeros for itself and all its derivatives was discovered, in the process we came across two infinite families of elliptic curves with interesting properties. Moreover, we construct some **K**-derived polynomials of degree 4 with distinct zeros for itself and all its derivatives for a few real quadratic number fields **K** of small discriminant.

1. Introduction. A polynomial $f \in \mathbf{Q}[x]$ of degree n with n rational zeros and such that all of its derivatives of positive degree have the same property is known as a **Q**-derived polynomial. It is easy to classify all such polynomials of degree at most 3. For instance,

$$\begin{aligned} f(x) &= 4x^3 - 4x^2 - 15x = x(2x+3)(2x-5) \\ f'(x) &= 12x^2 - 8x - 15 \ = \ (2x-3)(6x+5) \\ f''(x) &= 24x - 8 \end{aligned}$$

is a **Q**-derived polynomial of type $p_{1,1,1}$. By definition, the class $p_{m_1,\dots,m_s}$ contains all polynomials with s distinct zeros, where the ith zero has multiplicity m_i, $i = 1, \dots, s$, and $\sum_{i=1}^{s} m_i = n = \deg(f)$. Surprisingly, polynomials of type $p_{1,1,1,1}$ are unknown. More strongly, it is conjectured that such polynomials do not exist, see [**1**] and [**4**].

Conjecture 1.1. *There is no* **Q***-derived polynomial of type* $p_{1,1,1,1}$.

2000 AMS *Mathematics Subject Classification.* Primary 11G30.
Key words and phrases. **Q**-derived polynomial, elliptic curve.
Received by the editors on August 6, 2003, and in revised form on Jan. 12, 2004.

This conjecture is the only remaining obstacle in the course of a full classification of all quartic **Q**-derived polynomials, see [**4**]. In the closing lines of [**4**] it is observed that this paper's approach to proving the non-existence of **Q**-derived polynomials of type $p_{3,1,1}$ won't work for the $p_{1,1,1,1}$ case. Therefore, in the next section we shall outline a different, constructive way of attacking this remaining conjecture.

2. Q-derived polynomials of degree 4. Clearly, if $f(x)$ is **Q**-derived, then so is $g(x) = r_1 f(r_2(x + r_3))$ for any $r_i \in \mathbf{Q}$, $i = 1, 2, 3$, $r_2 \neq 0$. This observation implies that without loss of generality we may take $f'(0) = 0$, $f(1) = 0$, and f to be monic for suitable choices of r_3, r_2, r_1, respectively, provided f is **Q**-derived with at least two different zeros. From now on we assume this to be the case. Let

$$f(x) = (x-1)(x-a)(x-b)(x-c) \tag{1}$$

be **Q**-derived with $a, b, c \in \mathbf{Q}$ and $f'(0) = 0$, which yields

$$abc + ab + bc + ca = 0. \tag{2}$$

Further, f is **Q**-derived and so $f'(x) = 0$ and $f''(x) = 0$ have rational roots only. Because $f'(0) = 0$, this yields two quadratic polynomials with rational discriminants:

(3)
$$9(a+b+c+1)^2 - 32(ab+bc+ca+a+b+c) = \text{rational square}$$

(4)
$$9(a+b+c+1)^2 - 24(ab+bc+ca+a+b+c) = \text{rational square.}$$

Now we shall assume that $bc + b + c \neq 0$, for otherwise it follows from (2) that $b = c = 0$ and f cannot be of type $p_{1,1,1,1}$. These fs are adequately dealt with in [**1**]. For the same reason we assume $a \neq 0$, $b \neq 0$, and $c \neq 0$.

Next we eliminate a from (2) and each of the equations in (3) and (4) separately. Working with Maple, this can be conveniently done using Groebner bases with total degree order (a, b, c) for each pair. Setting $b = 1/t$ and $c = (U-1)/(t+1)$ and adjusting for rational squares gives

two similar parametric families of elliptic curves with corresponding quartic equations

$$E_1(t): \quad V^2 = U^4 - \left(\frac{14}{3}T + 2\right)U^3 + \left(9T^2 + \frac{14}{3}T - \frac{5}{9}\right)U^2 - \left(\frac{14}{3}T + 2\right)U + 1 \tag{5}$$

$$E_2(t): \quad W^2 = U^4 - 2(T+1)U^3 + \left(9T^2 + 2T + \frac{1}{3}\right)U^2 - 2(T+1)U + 1 \tag{6}$$

where we write $T = (t^2+t+1)/3t$ for convenience. These curves have to be investigated for rational points with common abscissa. We have to keep in mind however that not all pairs of points with common abscissa qualify. For instance, the points $(U, V) = (0, \pm 1)$ and $(U, W) = (0, \pm 1)$ give rise to $bc + b + c = 0$, which we excluded. This can be seen as follows. If U is the common abscissa of two points, one on each of the curves $E_1(t)$ and $E_2(t)$, see (5) and (6), then combining $b = 1/t$ with $c = (U-1)/(t+1)$ gives $bc + b + c = U/t$, which vanishes with U. Observe that for $U \neq 0$ we have

$$a = -\frac{U-1}{U(t+1)}, \quad b = \frac{1}{t}, \quad c = \frac{U-1}{t+1}. \tag{7}$$

There are many solutions to the fourth degree **Q**-derived problem with multiple zeros. Corresponding points for such solutions may be obtained by equating any two elements of the set $\{1, a, b, c\}$. Proceeding in this way[1] we obtained the following U-values for these points.

$$U = \frac{1}{t+2}\ (a=1), \quad t+2\ (c=1), \quad \frac{t}{2t+1}\ (a=b), \quad \frac{2t+1}{t}\ (b=c), \quad -1\ (c=a) \tag{8}$$

Further, two or more of these U values can only be equal for $t \in \{1, -1, -3, -1/3\}$. Consequently, we may expect these families of elliptic curves to have many rational points, which suggests a rank of at least 1 for all rational values of t, with a few obvious exceptions.

What we hope to find is an explicit rational point $P(t)$ with abscissa $U(t)$, which is a point on one of these two curves for all t, and which corresponds to a point $Q(t)$ on the other curve that can be forced to have the same abscissa $U(t)$ for a suitably chosen rational value t. If such a point exists, and if it does not correspond to a solution with multiple zeros, then we have found a $\mathbf{Q}$-derived polynomial of degree 4 and of type $p_{1,1,1,1}$. So we have to investigate the properties of these two families of elliptic curves.

3. Two families of elliptic curves. The curve $E_1(t)/\mathbf{Q}$ has the Weierstraß equation

$$\begin{aligned} Y^2 - 2(7T+3)XY - 36(7T+3)Y \\ = X^3 + 2(16T^2-7)X^2 - 324X - 648(16T^2-7) \end{aligned} \tag{9}$$

and a Weierstraß equation for $E_2(t)/\mathbf{Q}$ is

$$\begin{aligned} Y^2 - 6(T+1)XY - 108(T+1)Y \\ = X^3 + 6(12T^2-1)X^2 - 324X - 1944(12T^2-1). \end{aligned} \tag{10}$$

Recall that $T = (t^2+t+1)/3t$. The discriminant of $E_1(t)/\mathbf{Q}$ is

$$2^{18}3^4(T-1)^2(T+1)^2(9T+7)^2(3T+1)(27T-23).$$

It readily follows that $E_1(t)$ is non-singular and hence elliptic for $t \notin \{0, 1, -1, -3, -1/3\}$. Further, for transcendental T we have $E_1(\mathbf{Q}(T))_{\text{tor}} \cong \mathbf{Z}_2$ with non-trivial torsion point $P_0(t)$ with coordinates $(X, Y) = (-18, 0)$ on the cubic (9).

Considering $U = -1, t, t+2$, see (8), and the point producing maps $t \mapsto 1/t$ and $(U, V) \mapsto (1/U, V/U^2)$, we find a collection of points belonging to the subgroup of $E_1(t)(\mathbf{Q})$ generated by two points of infinite order, say $P_1(t)$ with coordinates $(U, V) = (-1, 3T + 7/3)$ on the quartic (5) and $(X, Y) = (96T + 78, -192T^2 - 576T - 384)$ on the cubic (9), and $P_2(t)$ with $(U, V) = (2+1/t, -2(t+1)(t-1)(3t+1)/3t^2)$ on (5) and $(X, Y) = (-16t - 2, 32(t-1)(t^2-2t-2)/3t)$ on (9). These points need not be independent for all t, but often they are. Therefore we have (see also the paragraph immediately below Theorem 3.2):

Theorem 3.1. *The curve $E_1(t)/\mathbf{Q}$ is elliptic for all $t \notin \{0, 1, -1, -3, -1/3\}$. For these values of t its torsion group has a subgroup of order 2 and its rank is at least 1.*

In fact, $E_1(t)$ can have three points of order 2, a situation that can be parameterized as follows. Setting $Y = (7T+3)X + 18(7T+3)$ in (9) leads to

$$(X+18)(X^2 + (81T^2 + 42T - 23)X + 306T^2 + 756T + 414) = 0.$$

For the second factor to be rationally solvable, its discriminant needs to be a perfect square, which means

$$(3T+1)(27T-23)(9T+7)^2 = \text{rational square}.$$

As none of the factors in the left-hand side can vanish, and replacing T by $(t^2+t+1)/3t$, we find that $(9t-7)^2+32 =$ rational square. This finally yields the parametrization

$$\frac{1+t}{1-t} = u - \frac{2}{u}, \quad \text{for} \quad u \in \mathbf{Q} \quad \text{but} \quad u \neq 0, \pm 1, \pm 2.$$

The lower bound 1 for the rank is best possible as can be seen from the table below.

The curve $E_2(t)/\mathbf{Q}$ has discriminant

$$2^{14}3^8(3T^2-1)^2(3T+1)(9T-5)(27T^2+18T+19),$$

and we check that $E_2(t)$ is non-singular for all $t \neq 0$. Again, for transcendental T we have $E_2(\mathbf{Q}(T))_{\text{tor}} \cong \mathbf{Z}_2$ with non-trivial torsion point $(X,Y) = (-18, 0)$ on the cubic (10). We have

Theorem 3.2. *The curve $E_2(t)/\mathbf{Q}$ is elliptic for all $t \neq 0$. For $t \neq 0$ its torsion group has a subgroup of order 2 and its rank is at least 1.*

The point $P = (X,Y) = (18, 0)$ is on both curves (9) and (10). This point cannot be of finite order. On the curve (9) we have $-P = (18, 72(7T+3))$ and $7T+3 \neq 0$, so that P cannot be of order 2. More tedious arguments, using Maple and *Apecs*, show that P cannot be of order $3, 4, 5, 6, 7, 8, 9, 10$ or 12 either. For instance, setting $x[2P] = -x[P]$ gives $T = -2$ or $T = -5/8$, both of which are impossible, so that P cannot be of order 3. And so on. By Mazur's theorem we then conclude that P cannot be of finite order. In the same way we check this for the second curve.

In the table below we have gathered information on the curves $E_1(t)$ and $E_2(t)$ for all 125 values of t in $\mathbf{Q} \cap [-1, 1]$ of height at most 20 and with $t \neq 0, -1, 1, -3, -1/3$. The computations were carried out with Ian Connell's Maple package *Apecs* 6 [**2**]. We also ran John Cremona's *mwrank* [**3**] under Linux to verify *Apecs*' results. For only three values of t, namely $t = -2/11, -5/8, 4/5$, we were unable to find a guaranteed value for the rank of $E_1(t)/\mathbf{Q}$. The best we can do in this respect is to say that the ranks of these three curves are 1, 2, or 3.

TABLE 1. Number of curves $E_i(t)$, $i = 1, 2$, for 125 values of t.

	Torsion group		Rank			
	$\mathbf{Z}_2$	$\mathbf{Z}_2 \times \mathbf{Z}_2$	1	2	3	4
E_1	120	5	3	80	38	4
E_2	125	0	*39	63	18	5

The * means that three curves counted here may have rank 2 or 3, instead of 1.

4. Finding suitable rational points. As we explained at the end of Section 2, we approach the problem of finding a $\mathbf{Q}$-derived polynomial of type $p_{1,1,1,1}$ by selecting a point on $E_1(t)$ (5) for general t and trying to force its abscissa $U(t)$ to be the abscissa of a point on $E_2(t)$ (6) for a suitable choice of t. This works as follows. We take any linear combination of $P_0(t)$, $P_1(t)$ and $P_2(t)$ (see the previous section), extract its coordinate $U(t)$ and substitute this into (6), which then can be written as $F(t) = Z^2$ for $Z \in \mathbf{Q}(t)$. Next we try to find a suitable rational point on this elliptic or generally hyperelliptic equation. This search is much simplified by the very fast program *ratpoints* of Michael Stoll [**5**], which we need to extend to cover $\deg(F) > 10$. In fact, we did our calculations with all 127 points $P(t) = c_0 P_0(t) + c_1 P_1(t) + c_2 P_2(t)$ for integers c_i with $c_0 = 0, 1$ and c_i $(i = 1, 2)$ between -3 and 4, and with *ratpoints* searching up to height 100000. The highest degree of F we came across was 76. Unfortunately, we did not find any $p_{1,1,1,1}$-type polynomial. We give a few examples.

Example 4.1. For $P(t) = P_0(t) + P_1(t) + P_2(t)$ we have $U(t) = 1/(t+2)$, which corresponds to $a = 1$. Substitution of $U(t) = 1/(t+2)$ into (6) yields

$$F_1(t) := 3(t^4 + 4t^3 + 4t^2 + 3) = \left(\frac{3t(t+2)^2}{2(t+1)}\, W\right)^2.$$

The elliptic curve $Z^2 = F_1(t)$ has rank 2, but every rational point of this curve corresponds to a **Q**-derived polynomial with a double root 1.

Example 4.2. Take $P(t) = P_0(t) + 3P_1(t) - P_2(t)$. Then $U(t) = (5t+4)/(2t^2+2t-1)$ and substitution of this $U(t)$ into (6) results in

$$\begin{aligned} F_2(t) &:= 3(67t^8 + 228t^7 + 306t^6 - 92t^5 - 63t^4 + 276t^3 + 214t^2 + 24t + 12) \\ &= \left(\frac{3t(2t^2+2t-1)^2}{2(t+1)}\, W\right)^2. \end{aligned}$$

Searching for rational points on the curve $Z^2 = F_2(t)$ with *ratpoints-1.5* we only find the finite rational points corresponding to $t = 1, -1, -3, -4/5$, all four values giving rise to inadmissible situations, the last one notably $U = 0$.

Observe that for rational t we generally get a **K**-derived polynomial of type $p_{1,1,1,1}$ over the quadratic field **K**. For instance, setting $t = -2$ finds such a polynomial over $\mathbf{K} = \mathbf{Q}(\sqrt{3})$. The roots of this polynomial are $[a, b, c, d] = [3/2, -1/2, 3, 1]$.

5. K-derived polynomials for some number fields K. In this section we give some examples of **K**-derived polynomials of type $p_{1,1,1,1}$ over the number field **K** of small discriminant. Obviously, for a suitable $U(t)$, any rational t will generally give a **K**-derived polynomial of type $p_{1,1,1,1}$ over a quadratic number field **K**. There is however no reason for the discriminant of **K** to be small. We have already given an example of such a polynomial over $\mathbf{K} = \mathbf{Q}(\sqrt{3})$ in Example 4.2.

Example 5.1. Setting $U(t) = t$ in (6) gives

$$W^2 = \frac{4}{3}\,(t^2+1)^2$$

so that for each $t \neq 0, 1, -1$ the polynomial with roots (7)

$$[a, b, c, d] = \left[-\frac{t-1}{t(t+1)}, \frac{1}{t}, \frac{t-1}{t+1}, 1 \right]$$

is a $\mathbf{K}$-derived polynomial of type $p_{1,1,1,1}$ over $\mathbf{K} = \mathbf{Q}(\sqrt{3})$.

Example 5.2. The U-value of $P(t) = P_0(t) - P_1(t) + P_2(t)$ is

$$U(t) = \frac{2t^2 + 2t - 1}{5t + 4}.$$

Let $\mathbf{K} = \mathbf{Q}(\sqrt{D})$ for squarefree D. The following t-values give different $\mathbf{K}$-derived polynomials of type $p_{1,1,1,1}$ for the relevant D as shown in the table below.

TABLE 2. Some $\mathbf{K}$-derived polynomials of type $p_{1,1,1,1}$ over a quadratic number field $\mathbf{K} = \mathbf{Q}(\sqrt{D})$ of small discriminant.

D	t
3	1/7, 2/3
$3 \cdot 31 \cdot 37$	$-7/17$, 1/4, 1/2, 4
$37 \cdot 103$	$-2/7$, 3
9931	$-3/7$, 10

Acknowledgment. I am grateful to an unknown referee for pointing out several errors, and for making valuable suggestions for further research.

ENDNOTE

1. The choice $b = 1$ leads to $t = 1$ and the curve $E_1(1)$ is not elliptic.

REFERENCES

1. R.H. Buchholz and J.A. MacDougall, *When Newton met Diophantus*: *A study of rational-derived polynomials and their extension to quadratic fields*, J. Number Theory **81** (2000), 210–233.

2. I. Connell's *Apecs*-6.1 is available at the web site http://www.math.mcgill.ca in the directory /connell/public/apecs/.

3. J. Cremona's *mwrank* is available at the web site http://www.maths.nott.ac.uk in the directory /personal/jec/ftp/progs/.

4. E.V. Flynn, *On* **Q**-*derived polynomials*, Proc. Edinburgh Math. Soc. **44** (2001), 103–110.

5. M. Stoll, The program *ratpoints* is based on an idea of Noam Elkies, with many improvements by Colin Stahlke and Michael Stoll (version 1.5, 23 April 2001).

Econometric Institute, Erasmus University, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands
E-mail address: stroeker@few.eur.nl