The problem of Diophantus and Davenport*

Andrej Dujella†

Abstract. *In this paper we describe the author's results concerning the problem of the existence of a set of four or five positive integers with the property that the product of its any two distinct elements increased by a fixed integer n is a perfect square.*

Key words: *property of Diophantus, Diophantine quadruple, Pellian equation, Fibonacci numbers*

Sažetak. **Diofant - Davenportov problem.** *U članku su opisani autorovi rezultati vezani uz problem postojanja skupa od četiri ili pet prirodnih brojeva sa svojstvom da je produkt svaka dva različita elementa tog skupa uvećan za fiksan cijeli broj n jednak kvadratu nekog cijelog broja.*

Ključne riječi: *Diofantovo svojstvo, Diofantova četvorka, Pellova jednadžba, Fibonaccijevi brojevi*

1. Introduction

The Greek mathematician Diophantus of Alexandria studied the following problem: Find four (positive rational) numbers such that the product of any two of them increased by 1 is a perfect square. He obtained the following solution: $\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}$ (see [6]). The first set of four positive integers with the above property was found by Fermat, and it was $\{1, 3, 8, 120\}$. Euler gave the solution $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$, where $ab + 1 = r^2$ (see [5]).

Definition 1. *A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the property of Diophantus if $a_ia_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called a Diophantine m-tuple.*

Therefore, the Fermat's set is an example of a Diophantine quadruple, and the famous open question is whether there exists a Diophantine quintuple (quintuple = 5-tuple). The first result in that direction was proved in 1969 by Baker and Davenport [2]. They proved that if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, then d has to be 120. The same result was proved later by

*The lecture presented at the Mathematical Colloquium in Osijek organized by Croatian Mathematical Society – Division Osijek, April 4, 1997.

†Department of Mathematics, University of Zagreb, Bijenička cesta 30, HR-10000 Zagreb, Croatia, e-mail: `duje@cromath.math.hr`

Kanagasabapathy and Ponnudurai [24], Sansone [33] and Grinstead [19]. This result implies that the Diophantine triple $\{1, 3, 8\}$ cannot be extended to a Diophantine quintuple.

2. The problem of the extension of Diophantine triples

In 1979, Arkin, Hoggatt and Strauss [1] proved that every Diophantine triple $\{a, b, c\}$ can be extended to the Diophantine quadruple $\{a, b, c, d\}$. More precisely, if

$$ab + 1 = r^2, \qquad ac + 1 = s^2, \qquad bc + 1 = t^2,$$

then we can take

$$d = a + b + c + 2abc \pm 2rst.$$

Conjecture A. *In the above notation, d has to be $a + b + c + 2abc \pm 2rst$.*

It is easy to see that the validity of *Conjecture A* would imply that there does not exist a Diophantine quintuple. *Conjecture A* can be rephrased in the terms of Pellian equations.

Conjecture B. *If a, b, c, r, s, t are positive integers satisfying $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, then all solutions of the system of Pellian equations*

$$ay^2 - bx^2 = a - b, \qquad az^2 - cx^2 = a - c$$

are given by $|x| \in \{1, rs - at, rs + at\}$.

As it was mentioned before, Baker and Davenport verified the above conjectures for the triple $\{1, 3, 8\}$. Furthermore, Veluppillai [36] verified the conjectures for the triple $\{2, 4, 12\}$ and Kedlaya [25] for the triples $\{1, 3, 120\}$, $\{1, 8, 120\}$, $\{1, 8, 15\}$, $\{1, 15, 35\}$, $\{1, 24, 35\}$, and $\{2, 12, 24\}$. Recently, I verified the conjectures for two infinite families of Diophantine triples, namely, for all triples of the form $\{k, k + 2, 4k + 4\}$ (see [17]) and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$, $k \in \mathbb{N}$ (F_k denotes k^{th} Fibonacci number). Also, in the joint paper with A. Pethő [18], we verified the conjectures for all Diophantine triples of the form $\{1, 3, c\}$. Our result implies that the Diophantine pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple.

I will outline the proof of our result. First of all, observe that the condition that $\{1, 3, c\}$ is a Diophantine triple implies that $c = c_k$, where recurrence sequence (c_k) is defined by

$$c_1 = 8, \quad c_2 = 120, \quad c_{k+2} = 14c_{k+1} - c_k + 8.$$

Let k be the minimal positive integer, if such exists, for which the statement is not valid. Then $k \geq 3$ and our proof begins by proving that $k \leq 75$. We have to solve the following system of Pellian equations:

$$z^2 - c_k x^2 = 1 - c_k, \qquad 3z^2 - c_k y^2 = 3 - c_k.$$

For any fixed k the solutions of each of these equations belong to the union of the sets of members of finitely many linear recurrence sequences. We first localize the initial terms of the recurrence sequences provided that the above system is soluble. Here we use congruence condition modulo c_k. In the second step we consider the remaining sequences modulo c_k^2 and rule out all but two equations in terms of linear recurrence sequences. Then we transform the exponential equations into inequalities for linear forms in three logarithms of algebraic numbers, which depend on the parameter k. A comparison of the theorem of Baker and Wüstholz [3] with the lower bounds for the solutions obtained from the congruence condition modulo c_k^2 finishes the proof that $k \leq 75$. Finally, we prove the statement for $3 \leq k \leq 75$ by using a version of the reduction procedure due to Baker and Davenport [2].

3. Generalization of the problem of Diophantus and Davenport

Definition 2. *Let n be an integer. A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the property $D(n)$ if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called a Diophantine m-tuple (with the property $D(n)$), or P_n-set of size m.*

Several authors considered the problem of the existence of Diophantine quadruples with the property $D(n)$ for an arbitrary integer n. In 1985, Brown [4], Gupta and Singh [20] and Mohanty and Ramasamy [28] proved independently that if $n \equiv 2 \pmod 4$, then there does not exist a Diophantine quadruple with the property $D(n)$.

In 1993, I proved that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$, and if $n \notin S \cup T$, where $T = \{-15, -12, -7, 7, 13, 15, 21, 24, 28, 32, 48, 60, 84\}$, then there exist at least two different Diophantine quadruples with the property $D(n)$ (see [7, Theorems 5 and 6] and [8, p. 315]).

For $n \in S$ the question of the existence of Diophantine quadruples with the property $D(n)$ is still unanswered. Let us mention that in [4, 25, 27], it was proved that some particular Diophantine triples with the property $D(-1)$ cannot be extended to Diophantine quadruples with the same property. The conjecture is that for $n \in S$ there does not exist a Diophantine quadruple with the property $D(n)$. In [13], some consequences of this conjecture were considered.

The above mentioned results from [7] were proved by considering the following cases:

$$n = 4k + 3, \ \ n = 8k + 1, \ \ n = 8k + 5, \ \ n = 8k, \ \ n = 16k + 4, \ \ n = 16k + 12.$$

In any of these cases, we can find two sets with the property $D(n)$ consisted of the four polynomials in k with integral coefficients. For example, the sets

$$\{1, k^2 - 2k + 2, k^2 + 1, 4k^2 - 4k - 3\},$$

$$\{1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13\}$$

have the property $D(4k + 3)$. The elements from the sets S and T are exceptions because we can get the sets with nonpositive or equal elements for some values of k.

The formulas of the similar type were systematically derived in [10]. These formulas were used in [12] and the above results are generalized to the set of Gaussian integers. Using the two-parametric formulas for Diophantine quadruples from [10], in [16], some improvements of the results of [7] were obtained. It was proved that if $|n|$ is sufficiently large and $n \equiv 1 \pmod 8$, or $n \equiv 4 \pmod{32}$, or $n \equiv 0 \pmod{16}$, then there exist at least six, and if $n \equiv 8 \pmod{16}$, or $n \equiv 13, 21 \pmod{24}$, or $n \equiv 3, 7 \pmod{12}$, then there exist at least four distinct Diophantine quadruples with the property $D(n)$.

Let U denote the set of all integers n, not of the form $4k+2$, such that there exist at most two distinct Diophantine quadruples with the property $D(n)$. One open question is whether the set U is finite or not. From the results from [16] it follows that if $n \in U$ and $|n| > 48$, then $n \equiv 3 \pmod 4$, or $n \equiv 12 \pmod{16}$, or $n \equiv 5 \pmod 8$, or $n \equiv 20 \pmod{32}$. In [15], it was proved that if $n \in U \setminus \{-9, -1, 3, 7, 11\}$ and $n \equiv 3 \pmod 4$, then the integers $|n-1|/2$, $|n-9|/2$ and $|9n-1|/2$ are primes, and either $|n|$ is prime or n is the product of twin primes. Also, if $n \in U \setminus \{-27, -3, 5, 13, 21, 45\}$ and $n \equiv 5 \pmod 8$, then the integers $|n|$, $|n-1|/4$, $|n-9|/4$ and $|9n-1|/4$ are primes.

4. Diophantine quadruples with the property $D(l^2)$

From Euler's result mentioned in the introduction it follows that there exists an infinite number of Diophantine quadruples with the property $D(1)$. Let l be an integer. Multiplying all elements of a set with the property $D(1)$ by l we obtain a set with the property $D(l^2)$. Accordingly, there exists an infinite number of Diophantine quadruples with the property $D(l^2)$.

In [7], I proved the stronger result. Namely, for any set $\{a, b\}$ with the property $D(l^2)$, where ab is not a perfect square, there exists an infinite number of Diophantine quadruples of the form $\{a, b, c, d\}$ with the property $D(l^2)$. The proof of this result is based on the construction of the double sequences $y_{n,m}$ and $z_{n,m}$ which are defined in [7] by second order recurrences in each index. Solving these recurrences we obtain

$$\begin{aligned} y_{n,m} &= \frac{l}{2\sqrt{b}}\{(\sqrt{a}+\sqrt{b})[\frac{1}{l}(k+\sqrt{ab})]^n(s+t\sqrt{ab})^m \\ &+ (\sqrt{b}-\sqrt{a})[\frac{1}{l}(k-\sqrt{ab})]^n(s-t\sqrt{ab})^m\}, \\ z_{n,m} &= \frac{l}{2\sqrt{a}}\{(\sqrt{a}+\sqrt{b})[\frac{1}{l}(k+\sqrt{ab})]^n(s+t\sqrt{ab})^m \\ &+ (\sqrt{a}-\sqrt{b})[\frac{1}{l}(k-\sqrt{ab})]^n(s-t\sqrt{ab})^m\}, \end{aligned}$$

where s and t are positive integers satisfying the Pell equation $s^2 - abt^2 = 1$. The desired quadruples have the form $\{a, b, x_{n,m}, x_{n+1,m}\}$, where

$$x_{n,m} = (y_{n,m}^2 - l^2)/a = (z_{n,m}^2 - l^2)/b\,.$$

In general, $x_{n,m}$ is a rational number, but in [14], it was proved that if $n \in \{-1, 0, 1\}$ and $(n, m) \notin \{(-1, 0), (-1, 1), (0, -1), (0, 0), (1, -2), (1, -1)\}$, then $x_{n,m}$ is a positive integer.

Example 1.

$$1 \cdot 7 + 3^2 = 4^2$$

In this case, $x_{-2,m}$, $x_{-1,m}$, $x_{0,m}$, $x_{1,m} \in \mathbb{Z}$ *and the following sets have the property* $D(9)$*:*

$$\{1, 7, 40, 216\},\ \{1, 7, 216, 1080\},\ \{1, 7, 1080, 5320\},\ \{1, 7, 11440, 56160\},\ \ldots$$

If we have the pair of identities of the form: $ab + l^2 = k^2$ and $s^2 - abt^2 = 1$, then we can construct the sequence $x_{n,m}$ and obtain an infinite number of Diophantine quadruples with the property $D(l^2)$. There are several pairs of identities for Fibonacci and Lucas numbers which have the above form. For example,

$$\begin{aligned} 4F_{n-1}F_{n+1} + F_n^2 &= L_n^2, \\ (F_n^2 + F_{n-1}F_{n+1})^2 - 4F_{n-1}F_{n+1} \cdot F_n^2 &= 1 \end{aligned}$$

and

$$\begin{aligned} 4F_{n-2}F_{n+2} + L_n^2 &= 9F_n^2, \\ (F_n^2 + F_{n-2}F_{n+2})^2 - 4F_{n-2}F_{n+2} \cdot F_n^2 &= 1. \end{aligned}$$

Applying our construction to these pairs of identities we get e. g. the set

$$\{2F_{n-1},\ 2F_{n+1},\ 2F_{n-2}F_{n-1}F_n^3,\ 2F_n^3F_{n+1}F_{n+2}\}$$

with the property $D(F_n^2)$ and the set

$$\{2F_{n-2},\ 2F_{n+2},\ 2F_{n-1}F_nL_n^2L_{n+1},\ 2L_{n-1}F_nL_n^2L_{n+1}\}$$

with the property $D(L_n^2)$ (see [8]).

Several authors considered the connections of the problem of Diophantus and Davenport and (generalized) Fibonacci numbers (see [9, 21, 22, 23, 26, 30, 31, 32, 34, 35]). These papers are mainly devoted to various generalizations of the result of Hoggatt and Bergum [21] that the set

$$\{F_{2k},\ F_{2k+2},\ F_{2k+4},\ 4F_{2k+1}F_{2k+2}F_{2k+3}\}$$

has the property $D(1)$.

5. Rational Diophantine quintuples

In [11], generalizing the result of Arkin, Hoggatt and Strauss [1], I proved the following theorem.

Theorem 1. *Let* q, a_1, a_2, a_3, a_4 *be rational numbers such that* $a_ia_j + q^2 = b_{ij}^2$, $b_{ij} \in \mathbb{Q}$*, for all* $1 \leq i < j \leq 4$*. Assume that* $a_1a_2a_3a_4 \neq q^4$*. Then the rational number* $a_5 = A/B$*, where*

$$\begin{aligned} A &= q^3[2b_{12}b_{13}b_{14}b_{23}b_{24}b_{34} + qa_1a_2a_3a_4(a_1 + a_2 + a_3 + a_4) \\ &+ 2q^3(a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4) + q^5(a_1 + a_2 + a_3 + a_4)], \end{aligned}$$

$$B = (a_1a_2a_3a_4 - q^4)^2\,,$$

has the property that $a_ia_5 + q^2$ *is a square of a rational number for* $i = 1, 2, 3, 4$. *To be more precise, for* $i \in \{1, 2, 3, 4\}$ *it holds:*

$$a_ia_5 + q^2 = (q\frac{a_ib_{jk}b_{jl}b_{kl} + qb_{ij}b_{ik}b_{il}}{a_1a_2a_3a_4 - q^4})^2\,,$$

where $\{i, j, k, l\} = \{1, 2, 3, 4\}$.

As a corollary we get the result that for all Diophantine quadruples $\{a_1, a_2, a_3, a_4\}$ with the property $D(1)$ there exists a positive rational number a_5 such that a_ia_5+1 is a square of a rational number for $i = 1, 2, 3, 4$.

Since the signs of b_{ij} are arbitrary, we have two choices for a_5. Let a_5^+ and a_5^- denote these two numbers, and let a_5^+ be the number which corresponds to the case where all b_{ij} are nonnegative.

Example 2. *If we apply the construction from* Theorem 1 *to Fermat's set* $\{1, 3, 8, 120\}$, *we obtain* $a_5^+ = \frac{777480}{2879^2}$, $a_5^- = 0$. *For Diophantus' original set* $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$ *we obtain* $a_5^+ = \frac{1557225246720}{42521^2}$ *and* $a_5^- = \frac{-4387246080}{42521^2}$, *and for the set* $\{4, 21, 69, 125\}$ *with the property* $D(400)$ *we obtain* $a_5^+ = 384$, $a_5^- = -\frac{4032000}{1129^2}$.

The construction from *Theorem 1* can be interpreted using the group low on elliptic curves. Namely, consider the elliptic curve

$$y^2 = (a_1x + q^2)(a_2x + q^2)(a_3x + q^2). \tag{1}$$

The points $P = (a_4, b_{14}b_{24}b_{34})$ and $Q = (\frac{q^4}{a_1a_2a_3}, \frac{q^3b_{12}b_{13}b_{23}}{a_1a_2a_3})$ are rational points on the curve (1). Now, the numbers a_5^+ and a_5^- are just the first coordinates of the points $P \pm Q$ on (1). See [37] for more details about the connection of the problem of Diophantus and Davenport and the theory of elliptic curves.

Let us finish the paper with some open questions.

Since it is not known whether there exists a Diophantine quintuple with the property $D(1)$, one may ask what is the least positive integer n_1, and what is the greatest negative integer n_2, for which there exists a Diophantine quintuple with the property $D(n_i)$, $i = 1, 2$. Certainly $n_1 \leq 256$ and $n_2 \geq -255$, since the sets $\{1, 33, 105, 320, 18240\}$ and $\{5, 21, 64, 285, 6720\}$ have the property $D(256)$, and the set $\{8, 32, 77, 203, 528\}$ has the property $D(-255)$ (see also [29]).

The definition of a Diophantine m-tuple can be extended to the subsets of $\mathbb{Q}$. Let q be a rational number. We call a set $M = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{Q}\setminus\{0\}$ *a rational Diophantine* m*-tuple with the property* $D(q)$ if the product of any two distinct elements of M increased by q is equal to the square of a rational number. It follows easily from [7, Theorem 5] that for every rational number q there exists a rational Diophantine quadruple with the property $D(q)$. Thus we came to the following open question: For which rational numbers q there exists a rational Diophantine quintuple with the property $D(q)$?

And finally, an open question is whether there exists a rational number $q \neq 0$ such that there exists a rational Diophantine sextuple with the property $D(q)$.

References

[1] J. Arkin, V. E. Hoggatt, E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17**(1979), 333–339.

[2] A. Baker, H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$*, Quart. J. Math. Oxford Ser. (2) **20**(1969), 129–137.

[3] A. Baker, G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442**(1993), 19–62.

[4] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45**(1985), 613–620.

[5] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, New York, 1966, 513–520.

[6] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers*, (I. G. Bashmakova, Ed.), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

[7] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65**(1993), 15–27.

[8] A. Dujella, *Diophantine quadruples for squares of Fibonacci and Lucas numbers*, Portugaliae Math. **52**(1995), 305–318.

[9] A. Dujella, *Generalized Fibonacci numbers and the problem of Diophantus*, Fibonacci Quart. **34**(1996), 164–175.

[10] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328**(1996), 25–30.

[11] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81**(1997), 69–79.

[12] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32**(1997), 1-10.

[13] A. Dujella, *On the exceptional set in the problem of Diophantus and Davenport*, in: *Application of Fibonacci Numbers, Vol. 7*, Kluwer, Dordrecht, to appear.

[14] A. Dujella, *A problem of Diophantus and Pell numbers*, in: *Application of Fibonacci Numbers, Vol. 7*, Kluwer, Dordrecht, to appear.

[15] A. Dujella *A problem of Diophantus and Dickson's conjecture*, in: *Proceedings of the Number Theory Conference, Eger, 1996*, de Gruyter, Berlin, to appear.

[16] A. Dujella, *Some estimates of the number of Diophantine quadruples*, Publ. Math. Debrecen, to appear.

[17] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51**(1997), 311-322.

[18] A. Dujella, A. Pethő, *Generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), to appear.

[19] C. M. Grinstead, *On a method of solving a class of Diophantine equations*, Math. Comp. **32**(1978), 936–940.

[20] H. Gupta, K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. **5**(1985), 799–804.

[21] V. E. Hoggatt, G. E. Bergum, *A problem of Fermat and the Fibonacci sequence*, Fibonacci Quart. **15**(1977), 323–330.

[22] A. F. Horadam, *Generalization of a result of Morgado*, Portugaliae Math. **44**(1987), 131–136.

[23] B. W. Jones, *A second variation on a problem of Diophantus and Davenport*, Fibonacci Quart. **16**(1978), 155–165.

[24] P. Kanagasabapathy, T. Ponnudurai, *The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$*, Quart. J. Math. Oxford Ser. (2) **26**(1975), 275–278.

[25] K. S. Kedlaya, *Solving constrained Pell equations*, Math. Comp., to appear.

[26] C. Long, G. E. Bergum, *On a problem of Diophantus*, in: *Application of Fibonacci Numbers, Vol 2*, (A. N. Philippou, A. F. Horadam and G. E. Bergum, Eds.), Kluwer, Dordrecht, 1988, pp. 183–191.

[27] S. P. Mohanty, A. M. S. Ramasamy, *The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$*, J. Number Theory **18**(1984), 356–359.

[28] S. P. Mohanty, A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23**(1985), 36–44.

[29] V. K. Mootha, *On the set of numbers $\{14, 22, 30, 42, 90\}$*, Acta Arith. **71**(1995), 259–263.

[30] J. Morgado, *Generalization of a result of Hoggatt and Bergum on Fibonacci numbers*, Portugaliae Math. **42**(1983-1984), 441–445.

[31] J. Morgado, *Note on a Shannon's theorem concerning the Fibonacci numbers and Diophantine quadruples*, Portugaliae Math. **48**(1991), 429–439.

[32] J. Morgado, *Note on the Chebyshev polynomials and applications to the Fibonacci numbers*, Portugaliae Math. **52**(1995), 363–378.

[33] G. Sansone, *Il sistema diofanteo $N+1 = x^2$, $3N+1 = y^2$, $8N+1 = z^2$*, Ann. Math. Pure Appl. (4) **111**(1976), 125–151.

[34] A. G. Shannon, *Fibonacci numbers and Diophantine quadruples: Generalizations of results of Morgado and Horadam*, Portugaliae Math. **45**(1988), 165–169.

[35] Gh. Udrea, *A problem of Diophantos-Fermat and Chebyshev polynomials of the second kind*, Portugaliae Math. **52**(1995), 301–304.

[36] M. Veluppillai, *The equations $z^2 - 3y^2 = -2$ and $z^2 - 6x^2 = -5$*, in: *A Collection of Manuscripts Related to the Fibonacci sequence*, (V. E. Hoggatt and M. Bicknell-Johnson, Eds.), The Fibonacci Association, Santa Clara, 1980, pp. 71–75.

[37] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jahresber. Deutsch. Math. Verein. **92**(1990), 58–76.