MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 208
OCTOBER 1994, PAGES 767-771

COMPUTING DIVISION POLYNOMIALS

JAMES McKEE

ABSTRACT. Recurrence relations for the coefficients of the nth division polynomial for elliptic curves are presented. These provide an algorithm for computing the general division polynomial without using polynomial multiplications; also a bound is given for the coefficients, and their general shape is revealed, with a means for computing the coefficients as explicit functions of n.

1. INTRODUCTION

Let k be a field with characteristic $\neq 2$ or 3. Given $a, b \in k$ with $4a^3 + 27b^2 \neq 0$, let E be the elliptic curve over k defined (as a projective plane curve over k) by the affine equation

$$y^2 = x^3 + ax + b,$$

with the special point being the point at infinity.

With the usual abelian group law on E, we have the notion of a multiplication-by-n map, for any integer n, denoted $[n]$. For positive integers n, we define *division polynomials* $f_n \in \mathbb{Z}[a, b][x]$ by the recursion formulae (cf. [4, p. 200])

$$\begin{aligned}
&f_1 = 1, \\
&f_2 = 2, \\
&f_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\
&f_4 = 4x^6 + 20ax^4 + 80bx^3 - 20a^2x^2 - 16abx - 32b^2 - 4a^3, \\
&f_{2m} = f_m(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)/2, \qquad m \geq 3, \\
&f_{4l+1} = (x^3 + ax + b)^2 f_{2l+2}f_{2l}^3 - f_{2l-1}f_{2l+1}^3, \qquad l \geq 1, \\
&f_{4l+3} = f_{2l+3}f_{2l+1}^3 - (x^3 + ax + b)^2 f_{2l}f_{2l+2}^3, \qquad l \geq 1.
\end{aligned} \tag{1}$$

The vanishing of $f_n(x)$ for n odd, or of $yf_n(x)$ for n even, characterizes the kernel of $[n]$. As a polynomial in x, f_n has degree $\chi(n)$, where $\chi(n) = (n^2-1)/2$ if n is odd, and $\chi(n) = (n^2-4)/2$ if n is even. The relation between f_n and Weber's ψ_n [3, p. 105] is that $f_n = \psi_n$ for n odd, and $f_n = \psi_n/y$ for n even.

If x is given weight 1, a is given weight 2, and b is given weight 3, then all the terms in $f_n(a, b, x)$ have weight $\chi(n)$. Thus, the coefficient of $x^{\chi(n)-1}$

Received by the editor September 28, 1992 and, in revised form, December 23, 1992, July 12, 1993, and September 14, 1993.

1991 *Mathematics Subject Classification*. Primary 14H52; Secondary 11G99, 11Y16.

This work was supported by a studentship from the Science and Engineering Research Council.

must be 0, and we have

$$f_n(a, b, x) = \alpha_{0,0}(n)x^{\chi(n)} + \alpha_{1,0}(n)ax^{\chi(n)-2} + \alpha_{0,1}(n)bx^{\chi(n)-3} + \cdots + \alpha_{r,s}(n)a^r b^s x^{\chi(n)-2r-3s} + \cdots,$$

where $\alpha_{r,s}(n) \in \mathbb{Z}$.

In this paper we give recurrence relations for the coefficients of a *fixed* division polynomial; these can be used to compute the coefficients $\alpha_{r,s}(n)$ *as functions of* n and to compute the general nth division polynomial $f_n(a, b, x)$ using $O(n^6)$ integer operations. The recurrence relations also provide bounds for the coefficients and reveal their general shape.

2. Statement of Main Lemma and deduction of results

Define $\alpha_{r,s}(n) = 0$ if either r or s is negative, or if $2r + 3s > \chi(n)$. Then $f_n(a, b, x) = \sum_t \beta_t(n)x^t$, where

$$\beta_t(n) = \sum_{2r+3s=\chi(n)-t} \alpha_{r,s}(n)a^r b^s \in \mathbb{Z}[a, b].$$

Main Lemma. *For* n *odd, and any* $i \in \mathbb{Z}$,

$$(i+3)(i+2)b\beta_{i+3}(n) - (i+2)(2n^2/3 - 3/2 - i)a\beta_{i+2}(n) + ((n^2 - 2i)(n^2 - 2i - 1)/4)\beta_i(n) - 3n^2 b\frac{\partial \beta_{i+1}(n)}{\partial a} + (2n^2a^2/3)\frac{\partial \beta_{i+1}(n)}{\partial b} = 0, \tag{2}$$

and, with $d = 2r + 3s$, *for any* $r, s \in \mathbb{Z}$,

$$\begin{aligned} d(d+1/2)\alpha_{r,s}(n) = {} & ((n^2+3)/2 - d)(n^2/6 - 1 + d)\alpha_{r-1,s}(n) \\ & - ((n^2+5)/2 - d)((n^2+3)/2 - d)\alpha_{r,s-1}(n) \\ & + 3(r+1)n^2\alpha_{r+1,s-1}(n) \\ & - (2(s+1)n^2/3)\alpha_{r-2,s+1}(n). \end{aligned} \tag{3}$$

For n *even, we have similarly*

$$(i+3)(i+2)b\beta_{i+3}(n) - (i+2)(2n^2/3 - 5/2 - i)a\beta_{i+2}(n) + ((n^2 - 2i - 3)(n^2 - 2i - 4)/4)\beta_i(n) - 3n^2 b\frac{\partial \beta_{i+1}(n)}{\partial a} + (2n^2a^2/3)\frac{\partial \beta_{i+1}(n)}{\partial b} = 0, \tag{4}$$

and

$$\begin{aligned} d(d+1/2)\alpha_{r,s}(n) = {} & (n^2/2 - d)(n^2/6 - 1/2 + d)\alpha_{r-1,s}(n) \\ & - ((n^2+2)/2 - d)(n^2/2 - d)\alpha_{r,s-1}(n) \\ & + 3(r+1)n^2\alpha_{r+1,s-1}(n) \\ & - (2(s+1)n^2/3)\alpha_{r-2,s+1}(n). \end{aligned} \tag{5}$$

TABLE 1

n	Computed maximum number of decimal digits in $\alpha_{r,s}(n)$	Bound on number of digits implied by (6)
6	5	22
12	22	93
24	90	381

Corollary 1. *There holds*

$$\log(1+|\alpha_{r,s}(n)|) = O(n^2),$$

where the implied constant is independent of r and s.

Proof. Let B_d be a bound for $|\alpha_{r,s}(n)|$ over $2r+3s \le d$. We have $B_0 = B_1 = n$, and from (3) and (5) we deduce that

$$B_d \le \frac{n^2(d+n^2/2)}{d^2} B_{d-1},$$

for $d \ge 2$ and $n \ge 5$, and the cases $n < 5$ can be checked directly. Hence,

$$\begin{aligned}|\alpha_{r,s}(n)| \le B_{\chi(n)} &\le \frac{n^{n^2}(n^2-1/2)!}{[((n^2-1)/2)!]^2(n^2/2+1)!} \\ &\sim 2^{(3n^2+1)/2} e^{n^2/2}/\pi n^3 .\end{aligned} \tag{6}$$

Taking logarithms gives the desired bound. □

Remark. This corollary suggests that the maximum number of digits in the coefficients of f_n should grow like n^2. This is reflected in Table 1.

Corollary 2. *There holds*

$$\alpha_{r,s}(n) = P_{r,s}(n) + (-1)^n Q_{r,s}(n),$$

where $P_{r,s}$ and $Q_{r,s}$ are both odd polynomials in $\mathbb{Q}[n]$ (i.e., only odd powers of n occur), $P_{r,s}$ has degree at most $4r+6s+1$, and $Q_{r,s}$ has degree at most $4r+6s-3$. The denominators of $P_{r,s}$ and $Q_{r,s}$ are $(4r+6s+1)$-smooth (i.e., they have no prime divisors greater than $4r+6s+1$).

Proof. Induction on $2r+3s$, using (3) and (5). □

Remark. Using (3) and (5), one can compute explicit formulae for any desired $\alpha_{r,s}(n)$, e.g.,

$$\alpha_{1,0}(n) = \begin{cases} \frac{1}{60}n(n^2-1)(n^2+6), & n \text{ odd}, \\ \frac{1}{60}n(n^2-4)(n^2+9), & n \text{ even}. \end{cases}$$

Corollary 3. *The general division polynomial $f_n(a, b, x)$ can be computed using $O(n^6)$ multiplications and divisions (of integers with $O(n^2)$ digits by integers with $O(\log n)$ digits) and $O(n^6)$ additions (of integers with $O(n^2)$ digits).*

Proof. Set $x = 1$. Starting with $\beta_{\chi(n)}(n) = n$, and $\beta_t(n) = 0$ for $t > \chi(n)$, one can use (2) or (4) as appropriate to compute $\beta_t(n)$ for $t = \chi(n)-1, \chi(n)-2, \dots, 0$. Each application of (2) or (4) requires $O(n^4)$ integer operations of the type given in the statement of the corollary (using Corollary 1 to bound the coefficients), and $O(n^2)$ applications are needed. □

3. A comparison with the traditional means for computing f_n

For specific values of a and b, using the recursion formulae (1) seems to be the best (i.e., quickest) method for computing $f_n(a, b, x)$. For computing the general division polynomial $f_n(a, b, x) \in \mathbb{Z}[a, b][x]$, however, this approach is very slow. By homogeneity, it suffices to compute $f_n(a, b, 1)$. The most time-consuming step is the final use of (1), which involves multiplying together polynomials in two variables, of degree $O(n^2)$ in each, so having $O(n^4)$ terms. Thus $O(n^8)$ multiplications of integer coefficients are needed, if one uses "ordinary" polynomial multiplication. By using divide and conquer [1, pp. 62–64] this can be reduced to $O(n^{4\log_2 3}) = O(n^{6.34})$ multiplications of integer coefficients (with $O(n^2)$ digits). Using FFT techniques [1, pp. 252 ff.] we can further reduce this to $O(n^4(\log n)^2)$ multiplications of integer coefficients. Thus, using (1) with FFT would be *ultimately* faster than (2)/(4), but, for reasonable values of n, using (2)/(4) is better.

Using PARI-GP on a Sun 3/60 workstation, we timed the last step in using (1) to compute f_n for a few values of n ($t_1(n)$ in Table 2—this is an underestimate for the time to compute $f_n(a, b, 1)$). By comparison, $t_2(n)$ in Table 2 gives the time taken to compute $f_n(a, b, 1)$ from scratch, using (2) or (4) as appropriate. The polynomial $f_{25}(a, b, 1)$ has 8269 terms with coefficients up to 97 decimal digits long. For small n, using (1) beats using (2)/(4), but the latter method soon becomes better.

TABLE 2. Comparing $t_1(n)$, an underestimate of the time taken to compute $f_n(a, b, 1)$ using (1), with $t_2(n)$, the time taken using (2) or (4) as appropriate

n	$t_1(n)$	$t_2(n)$
10	1s	6s
15	29s	47s
20	2 min 44s	3 min 5s
23	13 min 31s	9 min 29s
25	27 min 23s	15 min 29s

4. Proof of lemma

First suppose n is odd. Fricke, in [2, p. 191], derives a partial differential equation for ψ_n, which for n odd translates directly into a partial differential equation for f_n:

$$(x^3 + ax + b)\frac{\partial^2 f_n}{\partial x^2} - ((n^2 - 3/2)x^2 + (2n^2/3 - 1/2)a)\frac{\partial f_n}{\partial x} - 3n^2 b\frac{\partial f_n}{\partial a} + (2n^2a^2/3)\frac{\partial f_n}{\partial b} + n^2(n^2 - 1)xf_n/4 = 0. \tag{7}$$

He comments that this provides linear relations between the coefficients of f_n, which together with $\alpha_{0,0}(n) = n$ suffice to determine f_n, but he complains that this "freilich schon bei $n = 5$ einen erheblichen Aufwand von Rechnung erfordert", implying that this is not a profitable approach. Here we disagree. Our aim is to make the solution more explicit. Note that although (7) is derived over $\mathbb{C}$ using complex-variable methods, it is just a formal identity in

$\mathbb{Z}[1/6, a, b][x]$ and as such holds over any field with characteristic not dividing 6.

Equating coefficients of x^{i+1} in (7) gives (2), at least for $i \geq 0$, but since $\beta_t = 0$ for $t < 0$ one soon checks that (2) holds for negative i too.

Set $i = (n^2 - 1)/2 - 2r - 3s$ in (2); then equating coefficients of $a^r b^s$ gives (3).

For n even, replace f_n by $y f_n$ in (7), giving

$$(x^3 + ax + b)\frac{\partial^2 f_n}{\partial x^2} - ((n^2 - 9/2)x^2 + (2n^2/3 - 3/2)a)\frac{\partial f_n}{\partial x} + ((n^2 - 3)(n^2 - 4)x/4)f_n - 3n^2 b\frac{\partial f_n}{\partial a} + (2n^2a^2/3)\frac{\partial f_n}{\partial b} = 0.$$

Equating coefficients of x^{i+1} gives (4) for $i \geq 0$, but again this extends to all i.

Set $i = (n^2 - 4)/2 - 2r - 3s$ in (4); then equating coefficients of $a^r b^s$ gives (5). □

Acknowledgments

I should like to thank Richard Pinch and an anonymous referee for their helpful comments.

Bibliography

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, MA, 1974.
2. R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Vol. 2, Teubner, Leipzig, 1922.
3. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, New York, 1986.
4. H. Weber, *Lehrbuch der Algebra*. III, 3rd ed., Chelsea, New York, 1961.

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB2 1SB, England

E-mail address: `jfm@pmms.cam.ac.uk`