Exercises on faster isogeny computation

Daniel J. Bernstein
11 September 2021

1. Optional further reading (surveys): von zur Gathen and Gerhard, *Modern computer algebra*; Brent and Zimmermann, *Modern computer arithmetic*; Bürgisser, Clausen, and Shokrollahi, *Algebraic complexity theory*; Bernstein, *Fast multiplication and its applications*; Bernstein and Lange, *Montgomery curves and the Montgomery ladder.*

2. In the following exercises, R is a commutative ring; each f_i is in R; each g_i is in R; each h_i is in R; $R[z]$ is the univariate polynomial ring over R; and $R[[z]]$ is the univariate power-series ring over R. Optional: Show that a set with elements $0, 1$, a unary operation $-$, and binary operations $+, \cdot$ is a commutative ring if and only if it satisfies every identity satisfied by $\mathbf{Z}$.

3. [Schoolbook polynomial multiplication over R.] Let n be a positive integer. Define $f = f_0 + f_1 z + \cdots + f_{n-1}z^{n-1} \in R[z]$ and $g = g_0 + g_1 z + \cdots + g_{n-1}z^{n-1} \in R[z]$. Define $h = fg$, and write h as $h_0 + h_1 z + \cdots + h_{2n-2}z^{2n-2}$. Given $f_0, \ldots, f_{n-1}$ and $g_0, \ldots, g_{n-1}$, "schoolbook multiplication" computes each h_i in the most obvious way: it computes $h_0 = f_0 g_0$ with 1 multiplication in R; it computes $h_1 = f_0 g_1 + f_1 g_0$ (assuming $n \ge 2$) with 2 multiplications in R and 1 addition in R; etc. How many multiplications in R does schoolbook multiplication take in total to obtain all of $h_0, \ldots, h_{2n-2}$? How many additions in R? Express your answers as polynomials in n, and check that these answers match 4 multiplications and 1 addition for $n = 2$. Do these multiplication and addition counts also hold for $n = 0$?

4. [Schoolbook multiplication, recursive view.] For each positive integer n, write $M_R(n)$ for the minimum length of a chain of multiplications, additions, and subtractions that, given any $f_0, f_1, \ldots, f_{n-1}, g_0, g_1, \ldots, g_{n-1}$ as input, produces $h_0, h_1, \ldots, h_{2n-2}$ as output, where

$$h_0 + \cdots + h_{2n-2}z^{2n-2} = (f_0 + \cdots + f_{n-1}z^{n-1})(g_0 + \cdots + g_{n-1}z^{n-1})$$

in $R[z]$. Show that $M_R(1) = 1$, and that $M_R(n+1) \le M_R(n) + 4n$.

5. [Karatsuba multiplication over R, simplest case.] Say $h = h_0 + h_1 z + h_2 z^2$ is the product of $f = f_0 + f_1 z$ and $g = g_0 + g_1 z$. Explain how to compute h_0, h_1, h_2, given f_0, f_1, g_0, g_1, using 3 multiplications rather than 4 multiplications. How many additions are there, counting subtractions as additions? How slow do multiplications in R need to be compared to additions for this to be a good tradeoff?

6. [Clumping.] The polynomial $f = f_0 + f_1 z + \cdots + f_{2n-1}z^{2n-1}$, where n is a positive integer, can be viewed as the image of the polynomial $F_0 + F_1 y \in R[z][y]$ under the $R[z]$-algebra morphism $R[z][y] \to R[z]$ that takes y to z^n, where $F_0 = f_0 + f_1 z + \cdots + f_{n-1}z^{n-1}$ and $F_1 = f_n + f_{n+1}z + \cdots + f_{2n-1}z^{n-1}$. If $g = g_0 + g_1 z + \cdots + g_{2n-1}z^{2n-1}$ is similarly viewed as the image of $G_0 + G_1 y$ for suitable G_0, G_1, then the product fg is the image of $(F_0 + F_1 y)(G_0 + G_1 y)$. If $(F_0 + F_1 y)(G_0 + G_1 y)$ is computed by Karatsuba multiplication over $R[z]$, and if each product in $R[z]$ is computed by schoolbook multiplication over R, then how many multiplications in R are used in total to obtain fg? How many additions? Did you include the cost of applying the morphism?

7. [Striding.] The polynomial $f = f_0 + f_1 z + \cdots + f_{2n-1}z^{2n-1}$, where n is a positive integer, can alternatively be viewed as the image of the polynomial $(f_0 + f_1 z) + (f_2 + f_3 z)y + (f_4 + f_5 z)y^2 + \cdots \in R[z][y]$ under the $R[z]$-algebra morphism $R[z][y] \to R[z]$ that takes

y to z^2. If a product in $R[z][y]$ is computed by schoolbook multiplication over $R[z]$, and if each product in $R[z]$ is computed by Karatsuba multiplication over R, then how many multiplications in R are used in total to obtain fg? How many additions? Is this faster or slower than Exercise 6?

8. [Karatsuba multiplication, general case.] Show that $M_R(2n) \le 3M_R(n) + 8n - 4$. Show that $M_R(n) \in O(n^{\log_2 3})$. What is the smallest value of n for which this exercise produces smaller upper bounds on $M_R(n)$ than schoolbook multiplication?

9. What's the chance that we've carried out all of the above analyses correctly? How can we increase this chance? Would this increase the time taken for the analyses?

10. Literature-search exercise: Why do hundreds of papers refer to Karatsuba multiplication as "Karatsuba–Ofman" multiplication? Why are they wrong? What does this tell you about the scientific process?

11. [Refined Karatsuba multiplication.] A 1976 paper "Practical fast polynomial multiplication" by Moenck includes a claim that "with care" one can obtain $M_R(2n) \le 3M_R(n)+7n$ from Karatsuba's method. This is, for almost all n, better than the bound $M_R(2n) \le 3M_R(n) + 8n - 4$ from Exercise 8. No details were provided in the 1976 paper; Moenck's OS-360 card decks were discarded long ago; and a random sample of several subsequent papers on the topic consistently says 8, not 7. Does the 7 sound plausible? Show that the claim is correct: even better, $M_R(2n) \le 3M_R(n) + 7n - 3$.

12. [Toom multiplication, simplest case beyond Karatsuba.] The product $h = h_0 + h_1z + h_2z^2 + h_3z^3 + h_4z^4$ of $f = f_0 + f_1z + f_2z^2$ and $g = g_0 + g_1z + g_2z^2$ satisfies $h(1) = f(1)g(1)$, $h(2) = f(2)g(2)$, and $h(3) = f(3)g(3)$. Explain how to compute $6h_0, 6h_1, 6h_2, 6h_3, 6h_4$ from $f_0, f_1, f_2, g_0, g_1, g_2$ using 5 multiplications. Optional: How many additions did you use?

13. Assume that 6 is invertible in R. Define $M'_R(n)$ the same way as $M_R(n)$, except for also allowing constants (elements of R) as extra inputs: e.g., computing $f_0g_0/2$ takes two multiplications given $f_0, g_0, 1/2$. Show that $M'_R(n) \in O(n^{\log_3 5})$.

14. Optional: An addition chain is typically defined as a finite sequence $c_0, \ldots, c_\ell$ such that $c_0 = 1$ and such that, for each $i \in \{1, \ldots, \ell\}$, there exist $j, k \in \{0, \ldots, i-1\}$ with $c_i = c_j + c_k$. This is supposed to be a model of an exponentiation algorithm that computes, for each i in turn, the c_ith power of its input. How many doublings are in the addition chain $1, 2, 3, 4, 7$? How would you modify the definition so that this question has a clear answer? How would you formalize the definitions of $M_R(n)$ and $M'_R(n)$?

15. [Toom multiplication, general case.] Let ϵ be a positive real number. Show that there is a positive integer i such that if $1, 2, \ldots, i$ are invertible in R then $M'_R(n) \in O(n^{1+\epsilon})$. How does i relate to ϵ?

16. Show that $M'_R(n)$ is bounded above by $n^{1+o(1)}$ if all positive integers are invertible in R.

17. Toom (1963) actually stated a multiplication algorithm for n-bit integers rather than n-coefficient polynomials. Cook (1966) wrote that "it turns out that the same method works for multiplying polynomials" over "any finite field". Should this be called "Toom–Cook multiplication" rather than "Toom multiplication"?

18. Exhibit a choice of R for which $M_R(n)$ is sublinear in n.

19. For the remaining exercises, assume that multiplying two n-coefficient polynomials uses $O(n \log n)$ operations. Optional literature-search exercises: Who should be credited for showing that $M'_R(n) \in O(n \log n \log\log n)$? Who should be credited for showing that $M_R(n) \in O(n \log n \log\log n)$? How close are we to knowing that $M_R(n) \in O(n \log n)$? Who should be credited for the joke that the sound of an analytic number theorist drowning is "log log log log log"?

20. [Power-series multiplication.] Let $f = f_0 + f_1 z + f_2 z^2 + \cdots$ and $g = g_0 + g_1 z + g_2 z^2 + \cdots$ be two elements of the power-series ring $R[[z]]$. Write the product $h = fg$ as $h_0 + h_1 z + h_2 z^2 + \cdots$. Explain how to compute $h_0, \ldots, h_{n-1}$, given $f_0, \ldots, f_{n-1}$ and $g_0, \ldots, g_{n-1}$, in $O(n \log n)$ operations.

21. [An iteration for power-series reciprocal.] Let f, g be two elements of the power-series ring $R[[z]]$. Assume that $fg \in 1 + O(z^n)$ where n is a positive integer; here $O(z^n)$ means the set of power series of the form $h_n z^n + h_{n+1} z^{n+1} + \cdots$. Show that $fG \in 1 + O(z^{2n})$ where $G = 2g - fg^2$.

22. [Simpson's method, usually miscredited to Newton.] Simpson (1740) introduced the following iteration for finding roots of a function φ, unifying and generalizing previous iterations for polynomials φ: if x is close to a root then, under reasonable assumptions, $x - \varphi(x)/\varphi'(x)$ is closer, where φ' is the derivative of φ. Show that the iteration $g \mapsto G$ in Exercise 21 is a special case of Simpson's iteration.

23. [Power-series reciprocal, continued.] Define $f = f_0 + f_1 z + f_2 z^2 + \cdots \in R[[z]]$, and assume that f_0 is invertible in R. Explain how to compute the coefficients of $1, z, \ldots, z^{n-1}$ in $1/f$, given $1/f_0, f_0, f_1, \ldots, f_{n-1}$, in $O(n \log n)$ operations.

24. [Polynomial division.] Define $f = f_0 + f_1 z + \cdots + f_n z^n$ and $g = g_0 + g_1 z + \cdots + g_{2n-1} z^{2n-1}$. Assume that f_n is invertible in R. Explain how to compute the coefficients of $\lfloor g/f \rfloor$ and $g \bmod f$, given $1/f_n, f_0, f_1, \ldots, f_n, g_0, g_1, \ldots, g_{2n-1}$, in $O(n \log n)$ operations.

25. If someone gives you a machine that quickly divides a $2n$-coefficient polynomial by a degree-n polynomial, but you actually want to quickly divide a $3n$-coefficient polynomial by a degree-n polynomial, what do you do?

26. [Product trees.] Explain how to compute the coefficients of $(f_0 + g_0 z) \cdots (f_{n-1} + g_{n-1} z)$, given $f_0, g_0, \ldots, f_{n-1}, g_{n-1}$, in $O(n(\log n)^2)$ operations.

27. [Remainder trees.] Define $f = f_0 + f_1 z + \cdots + f_{n-1} z^{n-1}$. Explain how to compute the values $f(g_0), f(g_1), \ldots, f(g_{n-1})$, given $f_0, \ldots, f_{n-1}, g_0, \ldots, g_{n-1}$, in $O(n(\log n)^2)$ operations.

28. [Modular factorials.] If $f = (z+1)(z+2)\cdots(z+n)$ then $f(0)f(n)\cdots f(n^2 - n) = (n^2)!$. Explain how to compute $a!$ in $\mathbf{Z}/m$, given positive integers a, m, using $O(a^{1/2}(\log a)^2)$ operations in $\mathbf{Z}/m$. Optional: Explain how to use binary search on a to find a prime factor of m using $m^{1/4+o(1)}$ operations, assuming $m > 1$.

29. [Modular q-factorials.] Explain how to compute, given positive integers q, a, m, the product $(1-q)(1-q^2)(1-q^3)\cdots(1-q^a)$ in $\mathbf{Z}/m$ using $O(a^{1/2}(\log a)^2)$ operations in $\mathbf{Z}/m$. Explain how to compute the product of $1 + q + \cdots + q^{i-1}$ for $i \in \{1, 2, \ldots, a\}$ at this speed given also an inverse of $1 - q$ in $\mathbf{Z}/m$. Optional: Can you drop the invertibility assumption?

30. [Addition on Montgomery curves.] Assume that R is a field, that 2 is invertible in R, and that A, B are elements of R with $B(A^2 - 4) \neq 0$. Assume that $P, Q, P+Q, P-Q$ are nonzero points on the elliptic curve $By^2 = x^3 + Ax^2 + x$. Write $x_1 = x(P)$ and $x_2 = x(Q)$. Solve the exercise from Joost Renes saying that $x(P+Q)x(P-Q) = (x_1 x_2 - 1)^2/(x_1 - x_2)^2$, and show that

$$(z - x(P+Q))(z - x(P-Q)) = z^2 + \frac{F_1(x_1,x_2)}{F_0(x_1,x_2)}z + \frac{F_2(x_1,x_2)}{F_0(x_1,x_2)}$$

for biquadratic polynomials F_0, F_1, F_2 satisfying $x_0^2F_0(x_1,x_2)+x_0F_1(x_1,x_2)+F_2(x_1,x_2) = (x_0x_1-1)^2+(x_0x_2-1)^2+(x_1x_2-1)^2-2x_0x_1x_2(x_0+x_1+x_2+2A)-2$.

31. [Fast resultants, step 1.] Define F_0 as in Exercise 30. Define

$$\Delta = F_0(g_0,z)F_0(g_1,z)\cdots F_0(g_{n-1},z) \in R[z].$$

Explain how to compute the coefficients of Δ, given $A, g_0, \ldots, g_{n-1}$, using $O(n(\log n)^2)$ operations.

32. [Fast resultants, step 2.] In Exercise 30, assume that $P_1, P_2, \ldots, P_n$ and $Q_1, Q_2, \ldots, Q_n$ are nonzero curve points. Explain how to compute the product $\prod_{i,j} F_0(x(P_i), x(Q_j))$ using $O(n(\log n)^2)$ operations, given $A, x(P_1), \ldots, x(P_n), x(Q_1), \ldots, x(Q_n)$.

33. [Elliptic resultants, step 1.] In Exercise 30, assume that $P_1, P_2, \ldots, P_n$ and $Q_1, Q_2, \ldots, Q_n$ are nonzero curve points, and let α be an element of R. Explain how to compute

$$\prod_{i,j}(\alpha^2F_0(x(P_i),x(Q_j)) + \alpha F_1(x(P_i),x(Q_j)) + F_2(x(P_i),x(Q_j)))$$

using $O(n(\log n)^2)$ operations, given $\alpha, A, x(P_1), \ldots, x(P_n), x(Q_1), \ldots, x(Q_n)$.

34. [Elliptic resultants, step 2.] In Exercise 30, assume that $P_1, P_2, \ldots, P_n$ and $Q_1, Q_2, \ldots, Q_n$ are nonzero curve points, and assume for each i, j that $P_i + Q_j \neq 0$ and $P_i - Q_j \neq 0$. Let α be an element of R. Include division in R as one of the allowed operations. Explain how to compute $\prod_{i,j}(\alpha - x(P_i+Q_j))(\alpha - x(P_i - Q_j))$ using $O(n(\log n)^2)$ operations, given $\alpha, A, x(P_1), \ldots, x(P_n), x(Q_1), \ldots, x(Q_n)$.

35. [Covering kernels efficiently.] In Exercise 30, assume that P has order at least 64. Find integers $p_1, p_2, p_3, p_4, q_1, q_2, q_3, q_4$ such that each $P_i = p_iP$ is nonzero; each $Q_i = q_iP$ is nonzero; and the 32 points $P_i + Q_j$ and $P_i - Q_j$ are the 32 points $P, 3P, 5P, 7P, \ldots, 63P$ in some order.

36. [Kernel polynomials.] In Exercise 30, assume that P has odd order ℓ. Define $\Psi \in R[z]$ as the polynomial $\prod_{1\le i\le(\ell-1)/2}(z - x(iP))$. Explain how to rewrite $\Psi(\alpha)$ for $\ell = 67$ in the form $(\alpha - x(2P))\prod_{i,j}(\alpha - x(P_i+Q_j))(\alpha - x(P_i-Q_j))$, and how to rewrite $\Psi(\alpha)$ for $\ell = 71$ in the form $(\alpha - x(2P))(\alpha - x(4P))(\alpha - x(6P))\prod_{i,j}(\alpha - x(P_i+Q_j))(\alpha - x(P_i - Q_j))$, where i, j each range through $\{1, 2, 3, 4\}$.