Euclidean Methods for Cubic and Quartic Jacobi Symbols

Eric Bach [1] Bryce Sandlund [2]

[1]University of Wisconsin-Madison

[2]University of Waterloo

Previous Work

Binomial congruences and feasibility tests

Power Residues

- The multiplicative group of the finite field $\mathbf{Z}_p$ is cyclic.
- Let $\gcd(p,q)=1$. If $x^r \equiv q$ is solvable mod p, we say that q is an r-th power residue mod p.
- The quadratic case ($r=2$).
  - Jacobi symbol $(q|p)$: tells you if q is a quadratic residue mod p or not.
  - Quadratic reciprocity (Gauss): When p, q are odd primes, $(q|p)$ and $(p|q)$ are related.
- Jacobi symbol can be computed rapidly using the Euclidean algorithm:

$$u = qv + 2^k r, \qquad r \text{ odd.}$$

Cubic and Quartic Residues

- Reciprocity laws for 3rd and 4th powers explored by Gauss, Jacobi and their followers.
- Eisenstein (1844): first "code" for quartic Jacobi symbol, based on Euclidean algorithm. Cubic version only written down much later (Williams/Holte 1977).
- Bit complexity for n-bit "Euclidean" gcd algorithms in $\mathbf{Z}[\rho]$, $\mathbf{Z}[i]$:
  - $O(nM(n))$ for least-remainder alg in $\mathbf{Z}[i]$ (Caviness/Collins 1976)
  - $O(n^2)$ for alg in $\mathbf{Z}[i]$ that approximates least remainders (Collins 1992).
- Earlier, approximate remainders used in more intricate $O(n^2)$ procedures to compute gcd ideals in quadratic fields (Kaltofen/Rolletschek 1989).
- These upper bounds extend to "Euclidean" Jacobi symbol algs (folklore).

What We Did

Bounds for the bit complexity of some cubic/quartic Jacobi symbol algorithms that use long division.

A Bit Complexity Upper Bound

- Complete self-contained proof of $O(n^2)$ bit complexity for Williams-Holte using approximate least remainders.
- We extend alg to handle inputs that aren't relatively prime.
- Similar treatment for $\mathbf{Z}[i]$.

Upper Bounds are Tight

- Linear recurrence to define a sequence of "bad" input pairs, similar to Fibonacci numbers for Euclidean alg in $\mathbf{Z}$.
- Williams/Holte alg uses $\Omega(nM(n))$ bops, using *any* reasonable norm formula.
- Even if division is free, Williams/Holte needs $\Omega(n^2)$ bops, just to write down remainders.

What's the Best Power Residue Test?

- Contrary to belief, the "best" cubic and quartic residue tests need not involve reciprocity.
- For testing if $x^r \equiv a \bmod p$ ($r = 3, 4$), the Jacobi symbol alg uses a prime ideal factor of p in $\mathbf{Z}[\rho]$ (or $\mathbf{Z}[i]$).
- To thus factor p, you must compute $\sqrt{-3}$ (or $\sqrt{-1}$) mod p. Fastest known methods use exponentiation, which is $O(nM(n))$.
- 19th century soln: look up p in precomputed tables of quadratic forms.
- Today's soln: For one test, use Euler's criterion. For many tests (same p), use reciprocity.

Algorithms with Quotient Constraints

- Eisenstein (1844) computed Jacobi symbol in $\mathbf{Z}$ using even quotients:

$$u = qv + r, \qquad q \text{ even.}$$

- Bit complexity is worst-case exponential (Shallit 1990).
- Smith (1859) gave similar alg for $\mathbf{Z}[i]$, based on

$$u = qv + r, \qquad q \text{ divisible by } 1+i$$

- Claimed, but did not prove, his division step is feasible.

Our Results on These

- Smith-style division is feasible and efficient.
- Smith's quartic symbol algorithm is also exponential, since

$$(4k+1) = 2(4k-3) - (4k-7).$$

- We extended it to cubic Jacobi symbols, using

$$u = qv + r, \qquad q \text{ divisible by } 1-\rho$$

  in $\mathbf{Z}[\rho]$.
- Harder to analyze. We resorted to the "tools of ignorance."
  - Tried all inputs with $|\text{coefficients}| \le 10$.
  - Maintained "record values" for iteration counts.
  - For $u = (3k+2)\rho$, $v = 1 + (3k+3)\rho$, # of iterations is $4k+3$.
- Cubic algorithm has a cycle of 4 repeated quotients

$$-2-\rho, \quad -1-2\rho, \quad 2+\rho, \quad -2-\rho.$$

  (Verified by symbolic execution.)
- So n-bit inputs can force $\Omega(2^{n/2})$ iterations.

Open Questions

- Find exact worst case for least-remainder cubic and quartic Jacobi symbol algs.
- Study the "dynamics" of the constrained-quotient algorithms.
  - Smith's quartic alg has a quotient cycle of length 1.
  - Is 4 the shortest cycle length for the cubic algorithm?

To Learn More

To obtain the full paper, contact the authors.
We plan to put it on arXiv soon.

References

- B. F. Caviness and G. E. Collins, Proc. ACM Symp. Symb. Alg. Comp., 1976.
- G. E. Collins, J. Symb. Comp., 1992.
- G. Eisenstein, J. reine angew. Math., 1844. (4 papers.)
- E. Kaltofen and H. Rolletschek, Math. Comp., 1989.
- H. J. S. Smith, Report on the Theory of Numbers (I), 1859.
- J. O. Shallit, J. Symb. Comp., 1990.
- H. C. Williams and R. C. Holte, Math. Comp., 1977.

Acknowledgement

This research was supported in part by NSF: CCF-1420750.

Contact Information

- Eric Bach: bach@cs.wisc.edu
- Bryce Sandlund: bcsandlund@uwaterloo.ca

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

UNIVERSITY OF WATERLOO