BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 24, Number 2, April 1991

A COMPLETE SOLUTION TO THE POLYNOMIAL 3-PRIMES PROBLEM

GOVE W. EFFINGER AND DAVID R. HAYES

I. INTRODUCTION

By the "classical 3-primes problem" we mean: *can every odd number* ≥ 7 *be written as a sum of three prime numbers*? This problem was attacked with spectacular success by Hardy and Littlewood [8] in 1923. Using their famous *Circle Method* and assuming the Generalized Riemann Hypothesis, they proved that there exists a positive number N such that every odd integer $n \geq N$ is a sum of three primes. In 1937, Vinogradov [12] employed his ingenious methods for estimating exponential sums to prove the Hardy-Littlewood conclusion without invoking the Riemann Hypothesis. The result is therefore known as Vinogradov's Theorem. Vinogradov's proof actually implies a computable value for N, raising the possibility that the classical 3-primes problem can be completely settled by computation. For example, by carefully estimating the errors in Vinogradov's proof, Borodzkin [2] showed that one can take

$$N = 3^{3^{15}}.$$

Unfortunately, this value is far beyond the minimum that would make the problem accessible to even the fastest computers.

If instead of $\mathbf{Z}$ we consider the ring $\mathbf{F}_q[x]$ of polynomials in a single variable x over the finite field $\mathbf{F}_q$ of q elements, we can easily formulate, in direct analogy to the classical 3-primes problem, a *polynomial* 3-*primes problem.* To this end we observe that the analog of prime number is irreducible polynomial, of positive number is monic polynomial, and we need also:

Definition. A monic polynomial M over $\mathbf{F}_q$ is called *even* if $q = 2$ and if M is divisible by x or $x + 1$; otherwise M is called *odd* (so, for all $q \neq 2$, all M are odd).

Received by the editors April 30, 1990 and, in revised form, August 28, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11P32, 11T55.
The second author was supported in part by NSF Grant DMS-8903512.

It is easy to show that there exist even monic polynomials of arbitrarily high degree which *cannot* be written as a sum of three monic irreducibles [5]. Moreover, just as 1, 3, and 5 in the classical setting are "too small" to have the desired representation, so in the polynomial setting are all linear polynomials (over all finite fields) and quadratic polynomials of the form $x^2 + \alpha$ over *even* finite fields "too small" to have the desired representation [5]. Thus we must omit these cases from consideration.

Definition. A monic polynomial M over $\mathbf{F}_q$ of degree r is said to be a *3-primes polynomial* if it can be written as a sum of three irreducible monic polynomials over $\mathbf{F}_q$, one of degree r and the other two of lesser degree.

The following theorem provides a *complete* solution to the polynomial 3-primes problem:

The Polynomial 3-Primes Theorem. *Every odd monic polynomial M of degree $r \geq 2$ over every finite field $\mathbf{F}_q$ (except the case $M = x^2 + \alpha$ with q even) is a 3-primes polynomial.*

The proof of this theorem falls naturally into three parts:

1. An Asymptotic Theorem analogous to Vinogradov's Theorem in the classical setting.
2. Subtheorems which reduce the cases not covered by the Asymptotic Theorem to a finite, tractable number.
3. A computer check of all remaining cases.

In the remainder of this announcement, we summarize these three parts.

II. The Asymptotic Theorem

A complete exposition of the proof of the following theorem is contained in [7]. See also [3] and [10].

Asymptotic Theorem. *For every degree $r \geq 5$ there exists a q_r, depending on r and decreasing as r increases, such that if $q \geq q_r$, then every odd monic polynomial of degree r over $\mathbf{F}_q$ is a 3-primes polynomial. Moreover, we have $q_r = 2$ for all sufficiently large r.*

The method of proof is the Hardy-Littlewood Circle Method adapted to the function field setting. The analog for the unit circle $\mathbf{T}$ is the adèle class group $\mathbf{C}_k = \mathbf{A}_k/k$ with $k = \mathbf{F}_q(x)$ (cf. [11]).

The normalized Haar measure dt on the compact k-vector space $\mathbf{C}_k$ is a natural replacement for the complex path integral around $\mathbf{T}$. After the choice of the generator x of k, there is a canonical additive character $E\colon \mathbf{A}_k \to \mathbf{T}$ which is defined as follows

$$E(t) = e_q(\operatorname{res}(t\,dx)) \quad \text{for } t \in \mathbf{A}_k,$$

where e_q is the usual additive character on $\mathbf{F}_q$. By the residue theorem, the discrete subgroup k of $\mathbf{A}_k$ lies in the kernel of E, and so E can be regarded as a character on $\mathbf{C}_k$.

For $t \in \mathbf{A}_k$, we introduce the functions

$$F_r(t) = \sum_{\deg P = r} E(Pt) \quad \text{and} \quad H_r(t) = \sum_{\deg P < r} E(Pt)$$

and observe in the familiar way that $F_r(t) \cdot H_r^2(t)$ is a generating function for the number of representations $N(M)$ of the monic polynomial M as a 3-primes polynomial. Therefore

$$N(M) = \int_D F_r(t) H_r^2(t) E(-Mt)\, dt$$

where $D \subset \mathbf{A}_k$ is any fundamental domain for $\mathbf{C}_k$. It remains to estimate $F_r(t)$ by simpler functions and to choose D so that the error term is as small as possible. In estimating $F_r(t)$, one can imitate the original Hardy-Littlewood line of attack because the analog of the Generalized Riemann Hypothesis is a consequence of Weil's celebrated proof of the Riemann Hypothesis for smooth projective curves over $\mathbf{F}_q$. The resulting approximation to $F_r(t)$ is good when the denominator

$$\partial(t) = \prod_{\text{all } P} P^{\operatorname{Max}\{0,\, -v_P(t_P)\}}$$

of the adèle t satisfies

$$\deg \partial(t) \le r/2 \quad \text{and} \quad v_\infty(t_\infty) > r/2 + \deg \partial(t),$$

where ∞ is the infinite place of k. The union D of all $t \in \mathbf{A}_k$ which satisfy these relations is the analog of the Farey dissection, and this D is indeed a fundamental domain for $\mathbf{C}_k$. Just as in the Hardy-Littlewood approach to the classical 3-primes problem, "minor arcs" are not required.

The end result of the work is an asymptotic formula for $N(M)$ with a very good error term

$$N(M) = (1/r)(L_{r-1}(q))^2 S(M) + O(q^{7r/4}/((q-1)(r-1)))$$

where

$$L_{r-1}(q) = \sum_{1\le i\le r-1} q^i/i$$

and $S(M)$ is the "singular series." The Asymptotic Theorem then follows from the facts that

$$L_{r-1}(q) \ge q^r/((q-1)(r-1))$$

and that $S(M)$ is bounded below by a strictly positive constant which is independent of q.

Now it is possible to make a careful evaluation of the constant in the error term of the asymptotic formula above, obtaining for each $r \ge 5$ a lower bound for q_r (see [7]). The results of this evaluation are summarized in the following table. (This data is, of course, the polynomial analog of Borodzkin's astronomical N.)

NUMERIC RESULTS FOR THE ASYMPTOTIC THEOREM

For odd monic polynomials of degree $r =$	The 3-Primes Conjecture is true provided that $q \ge$
2 – 4	not covered by Asymptotic Theorem
5	2,231,753
6	2933
7	311
8	97
9	47
10	29
11	23
12	17
13	13
14	11
15	9
16	8
17 – 20	7
21 – 24	5
25 – 33	4
34 – 41	3
42 and up	2

It remains then to "fill in" these remaining cases.

III. THE SUBTHEOREMS

The first subtheorem covers the low degree cases at the top of Table 1.

Subtheorem 1. *Every odd monic polynomial M of degree $r = 2, 3, 4$, or 5 over every finite field $\mathbf{F}_q$ is a 3-primes polynomial except for the case $M = x^2 + \alpha$, q even. Every monic polynomial* *of degree* $r = 6$ *is a* 3*-primes polynomial provided that* $q \geq 19$. *Every monic polynomial of degree* $r = 7$ *is a* 3*-primes polynomial provided that* $q \geq 211$ *but* $q \neq 256$.

See [4] and [5] for the q odd and q even cases respectively. The methods employed are primarily affine geometry over finite fields (as in Artin [1]), although the cases $r = 6$ and $r = 7$, q odd require in addition the Riemann Hypothesis for certain *nonabelian* Artin L-functions.

Combining Subtheorem 1 with the Asymptotic Theorem does indeed reduce the polynomial 3-primes problem to a finite calculation, but as it stands an intractable one. For example, to check the 3^{33} monic polynomials of degree 33 over $\mathbf{F}_3$ at a rate of one per millisecond would require about 176 years. More mathematics is needed.

Subtheorem 2. *If* q *and* r *are relatively prime, then it suffices to check for* 3*-primes representations only of polynomials with first coefficient* 0 *and second coefficient* 0, 1, *and, for* q *odd, some fixed quadratic nonresidue.*

Again, see [4] and [5]. This result says we can replace q^2 checks by two (for q even) or three (for q odd) checks. It helps substantially for the larger q's remaining to be checked, but not much for the smaller q's. For these, the following result is crucial:

Subtheorem 3. *Among monic polynomials of degree* r *over* F_q, *there exist irreducible polynomials with every possible choice of first* s *coefficients provided that*

$$r/2 > s + \log_q(s+1).$$

See the proof of Theorem 9.3 of [9]. This result says that given M of degree r, we can find an irreducible P_1 of degree r such that $M - P_1$ is monic of degree not much larger than $r/2$. For example, in the case $q = 3$, $r = 33$, we are assured by Subtheorem 3 of the existence of a P_1 such that $M - P_1$ is monic of degree 19. The combination of the Asymptotic Theorem together with the three subtheorems has now reduced the problem to a tractable computation.

IV. The computer check

Application of all the preceding results reduces the polynomial 3-primes problem to the following: for 85 separate combinations of q and r (for example $q = 256$ $r = 5$, $q = 199$ $r = 4, \ldots, q = 2$ $r = 25$, etc.), we must check that every monic polynomial (except for odd polynomials when $q = 2$) with first coefficient 0 and second coefficient 0, 1, and (for odd q) a fixed quadratic nonresidue is a sum of *two* monic irreducible polynomials. This is still a large computation requiring a powerful computer. One of us (Effinger) programmed the IBM 3090 Supercomputer at the Cornell National Supercomputing Facility to check these remaining cases. Algorithms were designed to:

1. generate lists of irreducible polynomials, and
2. check off the sums of appropriate pairs of irreducibles.

For the former both the Berlekamp factorization algorithm for $\mathbf{F}_q[x]$ and an "extension field" algorithm were employed. For the latter extensive indexing was used. See [6] for the details of the algorithm design.

On December 19, 1989, the IBM 3090 completed the list of the 85 cases which needed to be checked. A total of 64.8 hours of central processing was needed. A complete solution to the polynomial 3-primes problem was then at hand.

The authors gratefully acknowledge the support of the Cornell National Supercomputing Facility, which generously provided access to its computers and user support resources.

REFERENCES

1. E. Artin, *Geometric algebra*, Interscience Publishers, New York, 1957.
2. K. G. Borodzkin, K voprosu o postoyanni I. M. Vinogradov, *Trudy tretego vsesoiuznogo matematiceskogo siezda* **1** (1956), Moskva.
3. M. Car, *Le problem de Goldbach pour l'anneau des polynomes sur un corps fini*, C. R. Acad. Sci. Paris Ser. A **273** (1971), 201–204.
4. G. W. Effinger, *A Goldbach theorem for polynomials of low degree over odd finite fields*, Acta Arithmetica **42** (1983), 329–365.
5. ——, *A Goldbach* 3*-primes theorem for polynomials of low degree over finite fields of characteristic* 2, J. Number Theory **29** (1988), 345–363.
6. ——, *The polynomial* 3*-primes conjecture*, Computer Assisted Analysis and Modeling on the IBM 3090, MIT Press, Cambridge, MA. (to appear).
7. G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Univ. Press, England (to appear).
8. G. H. Hardy and J. E. Littlewood, *Some problems of 'partitio numerorum': On the expression of a number as a sum of primes*, Acta Math. (Stockholm) **44** (1923), 1–70.
9. D. R. Hayes, *The distribution of irreducibles in* $GF[q, x]$, Trans. Amer. Math. Soc. **117** (1965), 101–127.

10. ———, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.

11. J. G. M. Mars, *Sur l'approximation du nombre de solutions de certaines equations Diophantiennes*, Ann. Sci. École Norm. Sup. 4^e Ser. **6** (1973), 357–388.

12. I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Comptes Rendues (Doklady) de l'Academy des Sciences de l'URSS, Tome **15** (1937), 191–294.

Department of Mathematics and Computer Science, Skidmore College, Saratoga Springs, New York, 12866
E-mail address: EFFINGER@AMY.SKIDMORE.EDU

Department of Mathematics and Statistics, University of Massachusetts at Amherst, Amherst, Massachusetts 01003
E-mail address: DHAYES@MATH.UMASS.EDU