Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Jacob T.B. Jr. Beard, J. Kevin Doyle, Kenneth I. Mandelberg

Square-separable primes and unitary perfect polynomials

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **68** (1980), n.5, p. 397–401.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1980_8_68_5_397_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1980.

Teoria dei numeri. — *Square-separable primes and unitary perfect polynomials.* Nota di JACOB T. B. BEARD, Jr. (*), J. KEVIN DOYLE (**) e KENNETH I. MANDELBERG (**), presentata (***) dal Socio G. ZAPPA.

RIASSUNTO. — I principali risultati di questa nota stabiliscono che tutti i numeri primi $p = 4t + 1 > 13$ e $p = 8t + 1$ con t dispari sono quadrato-separabili. Da precedenti risultati segue che per ciascuno di tali p e per ogni numero dispari $d > 1$, esistono infinite classi distinte di polinomi unitari perfetti non spezzati su GF (p^d). Sono allegati i risultati numerici degli studi sui primi quadrato-separabili col calcolatore.

1. INTRODUCTION

The main topic of this paper is the number-theoretic concept of square-separable primes [2], which concerns the distribution of quadratic residues modulo p. The concept has its origins elsewhere, as follows. The study of unitary perfect polynomials over finite fields [3]–[5] has led to the conjecture [4] that the number NSUP (p^d) of distinct p^d-equivalence classes of non-splitting unitary perfect polynomials over GF (p^d) is infinite for each prime p and each odd integer $d \geq 1$. The necessity of NSUP $(p^d) = \infty$ for each odd $d > 1$ follows from NSUP $(p) > 0$ whenever there exists a non-splitting unitary perfect polynomial over GF (p) whose irreducible factors in GF $[p, x]$ have degrees which are powers of 2 [4; pg. 297]. For primes $p = 2^e t + 1$ with t odd, such polynomials exist over GF (p) whenever $p < 97$, $e \leq 2$, or $e \geq 3$ and p is square-separable [5].

The principal results of this note establish the non-trivial portion of the Theorem stated below: that all primes $p = 4t + 1 > 13$ and $p = 8t + 1$, t odd, are square-separable. The Corollary follows from the Theorem and earlier results [3]–[5], and summarizes the current knowledge of NSUP (p^d). Finally, the Theorem lends some support to the conjecture [5] that for each $e \geq 3$, all but a finite number of primes $p = 2^e t + 1$, t odd, are square-separable.

THEOREM. *Let $p = 2^e t + 1$ be prime, t odd. Then p is square-separable whenever $e = 1$, $e = 2$ and $t > 3$, or $e = 3$.*

(*) Tennessee Technological University-Cookeville, Tennessee 38501 (U.S.A.). Written while this author was visiting at Emory University.

(**) Emory University-Atlanta, Georgia 30322 (U.S.A.).

(***) Nella seduta del 10 maggio 1980.

COROLLARY. NSUP $(p) > 0$ *and* NSUP $(p^d) = \infty$ *whenever one of the following holds*:

i) $p = 2$ *and* $d \not\equiv 0 \pmod 6$;

ii) $p = 2^e t + 1$ *with* t *odd,* $d > 1$ *odd,* $0 \leq e \leq 3$;

iii) $p = 17$ *and* $d > 1$ *odd*;

iv) $p = 2^e t + 1$ *is square-separable with* $d > 1$ *odd,* $e \geq 4$.

In addition NSUP $(2) \geq 33$, NSUP $(3) \geq 16$, NSUP $(5) \geq 7$, NSUP $(7) \geq 3$, *and* NSUP $(11) \geq 2$.

The Theorem follows immediately from Theorem 1 and Theorem 2 which we prove in Section 2. In Section 3 we give some results of computer studies which establish the existence of over 250,000 square-separable primes satisfying iv) of the Corollary with t odd and $4 \leq e \leq 9$.

The language of this note is that of [2], [3]–[5]. Briefly, for monic polynomials $A, B \in GF[q, x]$, $q = p^d$, $d \geq 1$, the polynomial B is a *unitary divisor* of A provided $(A, A/B) = 1$, and A is *unitary perfect* over GF (q) if the sum of the distinct unitary divisors in GF $[q, x]$ of A equals A. For any $A, B \in GF[q, x]$, the polynomial A is *q-equivalent* to B whenever $A = B^{p^l}$ for some integer l. A non-splitting polynomial over GF (q) is a monic polynomial over GF (q) which does not factor in GF $[q, x]$ as a product of linear irreducibles.

Continuing, for the remainder of this note let $p = 2^e t + 1 > 2$ be prime with t odd, and represent GF (p) by the ring $Z_p = \{0, 1, 2, \cdots, p - 1\}$ of integers *modulo* p. From [2], the prime p is called *s-square-separable* if s is a positive divisor of t such that each (closed) integer interval $[\theta^\sigma, \theta^{\sigma'}]$ contains a quadratic residue *modulo* p, where θ is a primitive root *modulo* p, θ^σ and $\theta^{\sigma'}$ are odd powers of θ^s, and $\theta^\sigma < \theta^{\sigma'}$ under the "ordering" $1 < 2 < \cdots < p - 1$ on the multiplicative group $Z_p^* = \{1, \cdots, p - 1\}$ of the field Z_p. The prime p is *square-separable* if it is s-square-separable for some s. Our technique of proof is to show that the primes considered in this note are t-square-separable, the Theorem holding pathologically in the case $e = 1$. As usual, $\left(\frac{a}{p}\right)$ denotes the Legendre symbol of a *modulo* p.

The reader is cautioned that *unless it is clearly indicated* to the contrary, *no modular arithmetic is performed during our arguments*; rather, the calculations involve integer (or occasionally, real) arithmetic.

2. MAIN RESULTS

The contrasting cases $e = 2$ (Theorem 1) and $e = 3$ (Theorem 2) are severed for emphasis. However, both cases appeal to the following result, $[x]$ denoting the greatest integer function of the real number x.

LEMMA. *Let* $n, h > 0$ *be integers. Then the integer interval* $(n, n + h)$ *contains a perfect square if and only if* $([\sqrt{n}] + 1)^2 < n + h$.

THEOREM 1. *Let* $p = 4t + 1$ *be prime with* $t > 3$ *odd. Then* p *is square-separable.*

Proof. Let θ be a primitive root *modulo* p, and let $\gamma \in \{\theta^t, \theta^{3t}\} \subset Z_p^*$ such that $\gamma < \gamma^3$. Observe $\gamma^2 \equiv -1 \pmod{p}$ and $\gamma^3 \equiv -\gamma \pmod{p}$. Let $\gamma = (p-k)/2$ where k is odd, so that $\gamma^3 = (p+k)/2 = \gamma + k$. Then $1 \equiv \gamma^4 \equiv \frac{p-k}{2} \cdot \frac{p+k}{2} \equiv -\frac{k^2}{4} \pmod{p}$ so that $k^2 \equiv -4 \pmod{p}$, say $mp = k^2 + 4$. Note that $m \geq 1$ is odd, and $k \geq 5$ since $t > 3$. If $m \geq 3$, then $p \leq (k^2+4)/3$ so that

$$\frac{p-k}{2} = \frac{k^2 - 3k + 4}{6} < \frac{k^2 - 2k + 1}{4} = \left(\frac{k-1}{2}\right)^2$$

$$[\sqrt{\gamma}] \leq \sqrt{\gamma} = \sqrt{\frac{p-k}{2}} < \frac{k-1}{2},$$

$$([\sqrt{\gamma}] + 1)^2 = [\sqrt{\gamma}]^2 + 2[\sqrt{\gamma}] + 1 < \gamma + k.$$

Thus $[\gamma, \gamma^3]$ contains a perfect square by the Lemma. Hence assume $m = 1$, so that $p = k^2 + 4$. Since k is odd, then $k \equiv 1, 3 \pmod{4}$.

In the case $k \equiv 1 \pmod{3}$, let $l = (k+1)/2$ and note that l is odd. Since $k = \gamma^3 - \gamma \equiv 2\gamma^3 \pmod{p}$, then $\left(\frac{k}{p}\right) = 1$ as $\left(\frac{2}{p}\right) = \left(\frac{\gamma^3}{p}\right) = -1$. If $\left(\frac{l}{p}\right) = 1$ then $\left(\frac{kl}{p}\right) = 1$. and $kl \in [\gamma, \gamma^3]$ since

$$\gamma = \frac{p-k}{2} = \frac{k^2 - k + 4}{2} < \frac{k^2 + k}{2} = kl < \frac{k^2 + k + 4}{2} = \frac{p+k}{2} = \gamma^3.$$

If $\left(\frac{l}{p}\right) = -1$ then $\frac{p-l}{2}$ is a quadratic residue *modulo* p since $\left(\frac{-1}{p}\right) = 1$, and $\frac{p-l}{2} \in [\gamma, \gamma^3]$ by

$$(*) \qquad \gamma = \frac{p-k}{2} < \frac{p-(k+1)/2}{2} = \frac{p-l}{2} = \frac{k^2 - l + 4}{2} < \frac{k^2 + k + 4}{2} = \gamma^3.$$

In the case $k \equiv 3 \pmod{4}$ let $l = (k+3)/2$ and again note l is odd. If $\left(\frac{l}{p}\right) = -1$ then $\frac{p-l}{2}$ is a quadratic residue *modulo* p, and $\frac{p-l}{2} \in [\gamma, \gamma^3]$ as in (*). If $\left(\frac{k-2}{p}\right) = -1$ then $\frac{p-(k-2)}{2}$ suffices similarly. Finally, suppose $\left(\frac{l}{p}\right) = \left(\frac{k-2}{p}\right) = 1$ so that $\left(\frac{l(k-2)}{p}\right) = 1$.

Since $k \geq 5$, we have $k^2 - k + 4 \leq k^2 + k - 6$, so that

$$\gamma = \frac{p-k}{2} = \frac{k^2-k+4}{2} \leq \frac{k^2+k-6}{2} =$$

$$l(k-2) < \frac{k^2+k+4}{2} = \frac{p+k}{2} = \gamma^3 .$$

Thus $l(k-2) \in [\gamma, \gamma^3]$ and the proof is completed.

The restriction $t > 3$ in Theorem 1 cannot be removed, since [2, 3] and [5, 8] do not contain quadratic residues *modulo* 5 and *modulo* 13 respectively.

THEOREM 2. *Let $p = 8t + 1$ be prime, t odd. Then p is square-separable.*

Proof. Let θ be a primitive root *modulo* p, and let $\gamma \in Z_p^*$ be an odd power of θ^t such that $\gamma < \gamma^3, \gamma^5, \gamma^7$. Observe that $\gamma^4 \equiv -1 \pmod{p}$, $\gamma^5 \equiv -\gamma \pmod{p}$, and $\gamma^7 \equiv -\gamma^3 \pmod{p}$. Hence we may choose $\varphi \in \{\gamma^3, \gamma^7\}$ such that $\gamma < \varphi < p - \varphi < \gamma^5$. Then $\frac{p-1}{2} \in [\varphi, p-\varphi]$ and $\frac{p-1}{2}$ is a quadratic residue *modulo* p since $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$. Moreover, any quadratic residues *modulo* p in $[\gamma, \varphi]$ and $[p-\varphi, \gamma^5]$ occur in pairs since $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$. Hence it suffices to show that $[\gamma, \varphi]$ contains a perfect square. Let $k = \varphi - \gamma$. Then

$$(\gamma^2 - 1)^4 \equiv -4 \equiv (\gamma^6 - 1)^4 \pmod{p},$$

$$4 \equiv -4\gamma^4 \equiv (\gamma^3 - \gamma)^4 \equiv (\gamma^7 - \gamma)^4 \pmod{p},$$

so that $k^4 \equiv 4 \pmod{p}$ independent of φ, and $k^2 \pm 2 \equiv 0 \pmod{p}$. Let $mp = k^2 \pm 2$. Since $p \equiv 1 \pmod{8}$ and $k^2 \pm 2 \equiv 2, 3, 6, 7 \pmod{8}$, then $m \geq 2$. Note $\frac{p-1}{2} > \gamma + k$ and $k = \sqrt{mp \pm 2} \geq \sqrt{mp - 2} \geq \sqrt{2p-2} > \sqrt{2p-2} - 1$. Hence

$$(k+1)^2 > 2p - 2,$$

$$(k-1)^2 > 2p - 2 - 4k,$$

$$\left(\frac{k-1}{2}\right)^2 > \frac{p-1}{2} - k > \gamma,$$

$$k > 2\sqrt{\gamma} + 1,$$

$$\varphi = \gamma + k > (\sqrt{\gamma} + 1)^2 > ([\sqrt{\gamma}] + 1)^2,$$

and we conclude by the Lemma that $[\gamma, \varphi]$ contains a perfect square. Regar-

ding the proof of Theorem 2: we note that on setting $\gamma = \frac{p-(l+2k)}{2}$ and $\varphi = \frac{p-l}{2}$ one can obtain $k \equiv \frac{l^2 \pm 4}{2l} \pmod{p}$, from which it follows that $k^2 \equiv 2 \pmod{p}$ when $\varphi = \gamma^3$ and $k^2 \equiv -2 \pmod{p}$ when $\varphi = \gamma^7$.

There is numerical evidence (Section 3) suggesting that all primes $p = 2^4 t + 1 > 17$, t odd, are square-separable. It is not now clear that an elementary proof of this result may be obtained.

3. NUMERICAL RESULTS

With the support of Emory University, the authors have made computer studies which establish the existence of precisely 253,814 square-separable primes among the 253,960 primes $p = 2^e t + 1$ having t odd, $1 < t < 10^6$ for $4 \leq e \leq 7$, and $1 < t < 10^5$ for $e = 8,9$. For each e and t as just stated, the Table below gives: (1) the number of primes $p = 2^e t + 1$, (2) the number of these primes (1) which are not square-separable, and (3) the numbers $t_3 (n_3)\, t_2 (n_2)\, t_1 (n_1)\, \mathbf{t_0}$; where $t_3 < t_2 < t_1$ are the three largest known values of t such that p is not square-separable, (n_i) is the number of t satisfying $t_i < t \leq t_{i-1}$ with p square-separable, and $\mathbf{t_0}$ is the largest known t for which p is square-separable. Some additional data on the distribution of non-square-separable primes is given in [1].

e	(1)	(2)	(3)
4	64,335	0	-
5	61,657	4	11 (1) 29 (365) 3,989 (61,287) **999,983**.
6	58,981	15	93,009 (1,398) 115,353 (44,982) 888,547 (6,184) **999,999**.
7	56,769	27	99,035 (11,935) 301,361 (11,782) 511,377 (26,580) **699,999**.
8	6,218	38	19,095 (3,120) 69,673 (418) 76,531 (1,347) **99,957**.
9	6,000	64	71,481 (323) 77,169 (460) 85,191 (825) **99,993**.

REFERENCES

[1] J. T. B. BEARD, Jr. (1979) - *Square-separable primes*, « A.M.S. Notices », *26*, A-200.

[2] J. T. B. BEARD, Jr. (1980) - *Are all primes* $32k + 17$ $(k > 0)$ *square separable?*, « Amer Math. Monthly », to appear.

[3] J. T. B. BEARD, Jr. (1977) - *Unitary perfect polynomials over* GF(q), « Rend. Acc. Naz. Lincei », LXII, 417-422.

[4] J. T. B. BEARD, Ir., A. T. BULLOCK, and M. S. HARBIN (1977) - *Infinitely many perfect and unitary perfect polynomials*, « Rend. Acc. Naz. Lincei », LXII, 294-303.

[5] J. T. B. BEARD, Jr., and M. S. HARBIN (1979) - *Non-splitting unitary perfect polynomials over* GF (q), « Rend. Acc. Naz. Lincei », LXVI, 179-185.