MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 403-414

FINDING FINITE B_2-SEQUENCES WITH LARGER $m - a_m^{1/2}$

ZHENXIANG ZHANG

ABSTRACT. A sequence of positive integers $a_1 < a_2 < \cdots < a_m$ is called a (finite) B_2-sequence, or a (finite) Sidon sequence, if the pairwise differences are all distinct. Let

$$K(m) = \max(m - a_m^{1/2}),$$

where the maximum is taken over all m-element B_2-sequences. Erdős and Turán ask if $K(m) = O(1)$. In this paper we give an algorithm, based on the Bose-Chowla theorem on finite fields, for finding a lower bound of $K(p)$ and a p-element B_2-sequence with $p - a_p^{1/2}$ equal to this bound, taking $O(p^3 \log^2 pK(p))$ bit operations and requiring $O(p \log p)$ storage, where p is a prime. A search for lower bounds of $K(p)$ for $p \le p_{145}$ is given, especially $K(p_{145}) > 10.279$, where p_i is the ith prime.

1. INTRODUCTION

A sequence of positive integers $a_1 < a_2 < \cdots < a_m$ is called a (finite) B_2-sequence, or a (finite) Sidon sequence, if the pairwise differences are all distinct, or, in other words, if all the sums $a_i + a_j$ ($i = j$ is permitted) are different. Let m be the maximum number such that $a_m \le n$. It is known that

$$n^{1/2}(1 - \varepsilon) < m \le n^{1/2} + n^{1/4} + 1.$$

The upper bound is due to Lindstrom [6], improving a result of Erdős and Turán [2]. The lower bound is due to Singer [9]. Let

$$K(m) = \max(m - a_m^{1/2}), \tag{1.1}$$

where the maximum is taken over all m-element B_2-sequences. Erdős and Turán ask whether or not

$$K(m) = O(1). \tag{1.2}$$

Erdős offers \$500 for settling this equation [3, pp. 65-66].

In this paper we do not answer this question, but instead will give an algorithm for finding a lower bound of $K(p)$ and a p-element B_2-sequence with $p - a_p^{1/2}$ equal to this bound, taking $O(p^3 \log^2 pK(p))$ bit operations and requiring $O(p \log p)$ storage, where p is a prime. A search for lower bounds of

Received by the editor September 1, 1992 and, in revised form, January 19, 1993.
1991 *Mathematics Subject Classification*. Primary 11B75, 11Y16, 11Y55.
Key words and phrases. B_2-sequences, Erdős-Turán conjecture, Bose-Chowla theorem, finite fields, algorithms.

$K(p)$ for $p \le p_{145}$ is given, especially $K(p_{145}) > 10.279$, where p_i is the ith prime.

Our algorithm is based on the Bose-Chowla theorem for finite fields $GF(p^2)$. A direct search on a computer shows that probably for any $k > 0$, there would exist a p-element B_2-sequence with $p - a_p^{1/2} > k$.

2. Notations and main results

We denote by p a prime, and by p_i the ith prime. It is well known that [10, §37] corresponding to each prime p and natural number r there is a unique (up to isomorphism) finite field (Galois field) of p^r elements. We denote this field by $GF(p^r)$. The multiplicative group of the nonzero elements in the Galois field $GF(p^r)$, denoted by $GF^*(p^r)$, is cyclic with $p^r - 1$ elements. If d is a divisor of r, then $GF(p^d)$ is a subfield of $GF(p^r)$ and $GF^*(p^d)$ is a subgroup of $GF^*(p^r)$.

In this paper we need only the case when $r = 2$. In this case, $GF(p)$ is a subfield of $GF(p^2)$ and $GF^*(p)$ is a subgroup of $GF^*(p^2)$.

Let θ be a generator of $GF^*(p^2)$ (denoted by $GF^*(p^2) = (\theta)$),

$$A(p, \theta) = \{a\colon 1 \le a < p^2,\ \theta^a - \theta \in GF(p)\} \tag{2.1}$$

and

$$\overline{A}(p, \theta) = A(p, \theta) \cup \{p^2\}. \tag{2.2}$$

Then $\overline{A}(p, \theta)$ has $p+1$ elements, denoted by $1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2$. Let

$$D(p, \theta) = \{a_{i+1} - a_i\colon 1 \le i \le p\},$$

$$d(p, \theta) = \max\{d\colon d \in D(p, \theta)\}, \quad d(p) = \max d(p, \theta),$$

where the second maximum is taken over all generators of $GF^*(p^2)$, and define

$$k(p) = p - \sqrt{p^2 - d(p)}.$$

With the above notations, and $K(m)$ defined by (1.1), we state our main results as the following two theorems.

Theorem 1. *Given $k > 0$, if there exists a prime p with $k(p) > k$, or, in other words, with $d(p) > 2kp - k^2$, then there exists a p-element B_2-sequence $1 = b_1 < b_2 < \cdots < b_p = p^2 - d(p)$ with*

$$K(p) \ge k(p) = p - b_p^{1/2} > k.$$

Theorem 2. *There exists an algorithm for finding $k(p)$ (or $d(p)$) and a p-element B_2-sequence $\{b_i\}$ with $p - b_p^{1/2} = k(p)$, taking $O(p^3 \log^2 pK(p))$ bit operations and requiring $O(p \log p)$ storage.*

3. Proof of Theorem 1

To prove Theorem 1, we need four lemmas. The first lemma is just a special case of the Bose-Chowla theorem [1] obtained in 1962. Although the proof can be found in either [1] or [4, Chapter 2], we rewrite it here, since the idea in the proof will be used in the proofs of our theorems.

Lemma 3.1 (Bose-Chowla). *Both $A(p, \theta)$ and $\overline{A}(p, \theta)$ are B_2-sequences.*

Proof. Let $A(p, \theta) = \{a_i : 1 \le i \le p\}$ and $c(a) = \theta^a - \theta \in GF(p)$ for $a \in A(p, \theta)$. If $\{i, j\} \ne \{i', j'\}$, $1 \le i \le j \le p$, $1 \le i' \le j' \le p$, then

$$(\theta + c(a_i))(\theta + c(a_j)) - (\theta + c(a_{i'}))(\theta + c(a_{j'})) \ne 0. \tag{3.1}$$

For the left-hand side of (3.1), considered as a polynomial in θ with coefficients in $GF(p)$, is of degree at most one in θ and does not vanish identically, since there is at most one factorization of a monic polynomial into monic linear factors; whilst θ is of degree 2 over $GF(P)$. Thus, $\theta^{a_i+a_j} \ne \theta^{a_{i'}+a_{j'}}$, and then

$$a_i + a_j \not\equiv a_{i'} + a_{j'} \mod (p^2 - 1). \tag{3.2}$$

Therefore $a_i + a_j \ne a_{i'} + a_{j'}$, i.e., $A(p, \theta)$ is a B_2-sequence.

Now let $a_i, a_j, a_k \in A(p, \theta)$, $1 \le i, j, k \le p$. If $a_i + a_j = a_k + p^2$, then $\{i, j\} \ne \{1, k\}$ and

$$a_i + a_j \equiv a_k + 1 = a_k + a_1 \mod (p^2 - 1),$$

which contradicts (3.2). Thus, $\overline{A}(p, \theta)$ is also a B_2-sequence. □

Lemma 3.2. *Let $\overline{A}(p, \theta) = \{1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2\}$. Then*

$$\{a_{i+1}, a_{i+2}, \ldots, a_p, a_{p+1} = a_1 + p^2 - 1, a_2 + p^2 - 1, \ldots, a_i + p^2 - 1\}$$

is also a B_2-sequence for any i with $1 \le i \le p$.

Proof. This follows easily by (3.2). □

Lemma 3.3. *If $\{a_i\}$ is a B_2-sequence and $h < a_1$, then so is $\{a_i - h\}$.*

Proof. Obvious. □

Lemma 3.4. *Let $\overline{A}(p, \theta) = \{1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2\}$. Given t with $1 \le t \le p$, let $h = a_{t+1} - 1$. Then*

$$\{1 = b_1 < b_2 < \cdots < b_p = p^2 - (a_{t+1} - a_t)\}$$

is a B_2-sequence, where

$$b_i = \begin{cases} a_{t+i} - h, & 1 \le i \le p - t, \\ a_{t+i-p} + p^2 - 1 - h, & p - t < i \le p. \end{cases}$$

Proof. This follows by Lemmas 3.2 and 3.3. □

Remark. In the above lemma, if we choose t such that $d(p, \theta) = a_{t+1} - a_t$, then the sequence $\{b_i : 1 \le i \le p\}$ associated with this t has larger $p - b_p^{1/2}$.

Example 3.1. Let $p = 7$ and $\theta^2 = \theta - 3$; then $GF^*(p^2) = (\theta)$. We have $\overline{A}(p, \theta) = \{a_i\} = \{1, 2, 5, 11, 31, 36, 38, 49\}$ and $d(p, \theta) = a_5 - a_4$. Let

$$b_i = \begin{cases} a_{4+i} - 30, & 1 \le i \le 3, \\ a_{i-3} + 18, & 4 \le i \le 7. \end{cases}$$

Then $\{b_i\} = \{1, 6, 8, 19, 20, 23, 29\}$ is a B_2-sequence with $p - b_p^{1/2} = 1.614\ldots$.

Example 3.2. Let $p = 11$ and $\theta^2 = 9\theta - 6$; then $GF^*(p^2) = (\theta)$. We have $\overline{A}(p, \theta) = \{a_i\} = \{1, 7, 17, 32, 34, 45, 52, 66, 71, 74, 75, 121\}$ and

$d(p, \theta) = a_{12} - a_{11}$. Then $\{b_i\} = A(p, \theta) = \{1, 7, 17, 32, 34, 45, 52, 66, 71, 74, 75\}$ is a B_2-sequence with $p - b_p^{1/2} = 2.339\ldots$.

We are now ready to prove Theorem 1.

Proof of Theorem 1. Given $k > 0$, suppose there exists a prime p with $k(p) > k$. Let $GF^*(p^2) = (\theta)$ such that $d(p) = d(p, \theta)$. Let $\overline{A}(p, \theta) = \{1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2\}$ and $d(p, \theta) = a_{t+1} - a_t$ for some t with $1 \le t \le p$. Then the sequence $\{b_i\}$ in Lemma 3.4 is just what we want. □

4. Proof of Theorem 2

In this section, for a given prime p, we denote by $\text{order}(a)$ the order of a in $GF^*(p)$ or in $GF^*(p^2)$. To prove Theorem 2, we need seven lemmas.

Lemma 4.1. *Let $GF^*(p^2) = (\theta)$ and $\theta^2 = u\theta - v$. Then we have*
(I) $\theta^p + \theta = u$, $\theta^{p+1} = v$;
(II) $\theta^i \notin GF(p)$ *for* $1 \le i \le p$;
(III) $\text{order}(v) = p - 1$.

Proof. (I) This follows from the fact that θ and θ^p are two roots of $x^2 = ux - v$.

(II) This follows from the facts that $\text{order}(\theta) = p^2 - 1$ and the order of an element of $GF^*(p)$ is at most $p - 1$.

(III) This follows by (I) and the fact that $\text{order}(\theta) = p^2 - 1$. □

Lemma 4.2. *Let $\theta \in GF(p^2)$, $\theta^2 = u\theta - v$ with $u, v \in GF(p)$ and* $\text{order}(v) = p - 1$, *and $\theta^i \notin GF(p)$ for $1 \le i \le p$. Then we have $GF^*(p^2) = (\theta)$.*

Proof. Since $\theta^i \notin GF(p)$ for $1 \le i \le p$, we have that θ and θ^p are two different roots of $x^2 = ux - v$. Thus, $\theta^{p+1} = v$. Suppose $\text{order}(\theta) = m < p^2 - 1$. Let $m = (p+1)q + r$ with $0 \le r \le p$. If $r = 0$, then $\text{order}(\theta^{p+1}) \le q < p - 1$, which contradicts the condition that $\text{order}(v) = p - 1$. If $1 \le r \le p$, then $\theta^r = \theta^{m-(p+1)q} = (\theta^{p+1})^{-q} \in GF(p)$, which contradicts the condition that $\theta^i \notin GF(p)$ for $1 \le i \le p$.

Thus, we have $\text{order}(\theta) = p^2 - 1$, i.e., $GF^*(p^2) = (\theta)$. □

Lemma 4.3. *Let $\theta \in GF(p^2)$ and $\theta^2 = u\theta - \nu$ with $u, v \in GF(p)$. Then a necessary and sufficient condition for $GF^*(p^2) = (\theta)$ is that*

$$\text{order}(v) = p - 1 \quad \textit{and} \quad \theta^i \notin GF(p) \quad \textit{for } 1 \le i \le p.$$

Proof. This follows by Lemmas 4.1 and 4.2. □

Lemma 4.4. *We have $(p^2 - 1)/2 + p \in A(p, \theta)$.*

Proof. By Lemma 4.1 we have $\theta^{(p^2-1)/2+p} - \theta = -\theta^p - \theta \in GF(p)$. □

Lemma 4.5. *Let $\overline{A}(p, \theta) = \{1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2\}$. Then for any a_i with $p + 1 < a_i < p^2$, there exists some r_i with $1 \le r_i \le p$ such that $\theta^{r_i + a_{i+1} - a_i} - \theta^{r_i} \in GF(p)$. Moreover, we have $\theta^b - \theta^{r_i} \notin GF(p)$ for any b with $r_i < b < r_i + a_{i+1} - a_i$.*

Proof. Let $a_i = (p+1)t_i + r_i$ with $0 \le r_i \le p$. Since $\theta^{p+1}, \theta^{a_i} - \theta \in GF(p)$, we have $r_i \ne 0$, i.e., $1 \le r_i \le p$. Then $\theta^{r_i + a_{i+1} - a_i} - \theta^{r_i} = \theta^{a_{i+1} - (p+1)t_i} - \theta^{a_i - (p+1)t_i} = (\theta^{a_{i+1}} - \theta^{a_i})\theta^{(p+1)(-t_i)} \in GF(p)$.

Now suppose $\theta^b - \theta^{r_i} \in GF(p)$ for some b with $r_i < b < r_i + a_{i+1} - a_i$. Let $b' = b + (p+1)t_i$. Then we have $a_i < b' < a_{i+1}$ and

$$\theta^{b'} - \theta^{a_i} = \theta^{(p+1)t_i}(\theta^b - \theta^{r_i}) \in GF(p),$$

which contradicts (2.1) or (2.2). □

Lemma 4.6. *For a pair of* $u, v \in GF(p)$ *with* $\operatorname{order}(v) = p-1$, *let* $\theta^2 = u\theta - v$. *Then it takes* $O(p\log^2 p)$ *bit operations to check if* $GF^*(p^2) = (\theta)$. *Moreover, if* $GF^*(p^2) = (\theta)$ *has been checked, then it takes* $O(p\log^2 pk(p))$ *bit operations to get* $d(p, \theta)$.

Proof. Let $\theta^i = u_i\theta - v_i$ with $u_i, v_i \in GF(p)$. Then $u_1 = 1$, $u_2 = u$, and

$$u_{i+1} = u_i u - u_{i-1}v \pmod p \quad \text{for } i \geq 2. \tag{4.1}$$

By a conventional algorithm [5, Chapter 4], [8, pp. 33–44], it takes $O(\log^2 p)$ bit operations for computing each u_i. By Lemma 4.3, to check if $GF^*(p^2) = (\theta)$, we need (only) to compute u_i for $1 \leq i \leq p$ and to check that none of them is zero. This can be done in $O(p\log^2 p)$ bit operations.

Now suppose $GF^*(p^2) = (\theta)$ has been checked. We use $O(p\log p)$ storage to save all u_i for $1 \leq i \leq p$.

For $i > p$, let $i = (p+1)t + r$, where $0 \leq r \leq p$; then

$$u_i = \begin{cases} 0, & r = 0, \\ v^t u_r \pmod p, & 1 \leq r \leq p, \end{cases} \tag{4.2}$$

by Lemma 4.1. Since u_r $(1 \leq r \leq p)$ are stored, they need not be recomputed. The quantity v^t can be computed by recurrence: $v^t = v^{t-1}v \pmod p$.

By Lemma 4.5 and the above descriptions of the computation of u_i, we have

$$d(p, \theta) = \max_{1\leq i\leq p} \{s - i \colon s \text{ is the least integer such that } s > i \text{ and } u_s = u_i\}. \tag{4.3}$$

We use the following procedure in pseudocode to get $d(p, \theta)$:

```
BEGIN
  j ← 0; s ← 1; α(1) ← 1; d(p, θ) ← 0;
  For i := 2 To p − 1 Do α(i) ← 0;
  While j < p Do
    Begin
      s ← s + 1; If (p + 1)|s Then s ← s + 1;
      If s > p Then calculate u_s by (4.2);
      If α(u_s) > 0 Then
        begin
          j ← j + 1; b ← s − α(u_s);
          If b > d(p, θ) Then d(p, θ) ← b;
          If s > p Then α(u_s) ← 0
        end;
      If s ≤ p Then α(u_s) ← s
    End
END;
```

In the procedure the values of $\alpha(i)$ for $1 \le i \le p$ are stored and changed from time to time. It requires $O(p \log p)$ storage, since $0 \le \alpha(i) \le p$. By (4.3), to get $d(p, \theta)$, the u_s are calculated for s at most equal to $s = p + d(p, \theta)$. Thus, the procedure will be terminated in $O(d(p, \theta) \log^2 p)$ or $O(p \log^2 pk(p))$ bit operations. □

Remark 4.1. In the procedure, as s increases, there may be several values of s $(\le p)$ for which the u_s have a same value, say, w. Assign $\alpha(w)$ to be the latest value of s with $u_s = w$. When we find a larger s with $u_s = w$, we get a new member of the set of (4.3): $b = s - \alpha(w)$. The variable j is the number of integers in the set of (4.3) which have been compared for taking the maximum for $d(p, \theta)$.

Example 4.1. Let $p = 7$ and $\theta^2 = \theta - 3$; then $GF^*(p^2) = (\theta)$ as in Example 3.1. Let $\alpha(1) = 1$ and $\alpha(i) = 0$ for $2 \le i \le 7$. Then the variables in the procedure will be evaluated as follows:

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
u_s	1	1	5	2	1	2	6	0	3	3	1	6	3	6	4	0	2	2	3	4	2	4	5
$\alpha(u_s)$	1	2	3	4	5	6	7				0	0					0						0
b		1			3	2					6	5					11						20
j	0	1			2	3					4	5					6						7
$d(p, \theta)$	0	1			3						6						11						20

We obtain, without calculating a_i, $d(7, \theta) = 20$, as in Example 3.1.

Lemma 4.7. *Given $u, v \in GF(p)$ such that $GF^*(p^2) = (\theta)$ and $d(p, \theta) = d(p)$ with $\theta^2 = u\theta - v$, it takes $O(p^2 \log^2 p)$ bit operations to get a p-element B_2-sequence $\{b_i\}$ with $b_p = p^2 - d(p)$.*

Proof. Let u_i be defined as in the proof of Lemma 4.6. Then by (2.1) and (2.2) we have

$$\overline{A}(p, \theta) = \{i : 1 \le i \le p^2, \ u_i = 1\}.$$

By (4.1) and (4.2), it takes $O(p^2 \log^2 p)$ bit operations to calculate u_i and to check if $u_i = 1$ for $1 \le i \le p^2$. After $\overline{A}(p, \theta)$ is known, the time for getting a B_2-sequence $\{b_i\}$ with $b_p = p^2 - d(p)$ is negligible $(O(p \log p)$ bit operations) by Lemma 3.4. □

Now we are ready to prove Theorem 2.

Proof of Theorem 2. Given a prime p, let $g = g(p)$ be the least primitive root of p. Let $v = g^s \pmod p$ for odd s with $1 \le s < p - 1$ and $(s, p - 1) = 1$; then $\operatorname{order}(v) = p - 1$. The number of pairs of u, v with $\operatorname{order}(v) = p - 1$ is $(p-1)\varphi(p-1) < p^2$, where $\varphi(\cdot)$ is the Euler φ-function. Thus, by Lemma 4.6 it takes $O(p^3 \log^2 p)$ bit operations to find all pairs of u, v such that $GF^*(p^2) = (\theta)$ with $\theta^2 = u\theta - v$. It is clear that the time for calculating $g^s \pmod p$ by recurrence and for checking if $(s, p - 1) = 1$ by the Euclidean algorithm [8, pp. 58–68] is negligible.

Since there are in total $\varphi(p^2 - 1) < p^2$ generators in $GF^*(p^2)$, it takes another $O(p^3 \log^2 pk(p))$ bit operations to find $d(p)$ or $k(p)$ by Lemma 4.6.

Since $k(p) \le K(p)$, the total time for finding $k(p)$ or $d(p)$ is $O(p^3 \log^2 pK(p))$ bit operations, while the time for finding a B_2-sequence $\{b_i\}$ with $p - b_p^{1/2} = k(p)$ is negligible by Lemma 4.7.

By the proofs of Lemmas 4.6 and 4.7, we see that the space required is $O(p \log p)$ bytes. $\square$

Remark 4.2. The least primitive root $g = g(p)$ of p is usually found quite fast in the manner described in [7, pp. 105–106].

5. Description of the algorithm

In this section we will implement the algorithm for finding $k(p)$. To speed things up, we need some more lemmas.

Lemma 5.1. *We have* $D(p, \theta) = D(p, \theta^{-p})$.

Proof. Let $h = (p^2 - 1)/2 + p$; then $h \in A(p, \theta) \cap A(p, \theta^{-p})$ by Lemma 4.4. Let

$$\overline{A}(p, \theta) = \{1 = a_1 < a_2 < \cdots < a_p < a_{p+1} = p^2\}$$

and $h = a_t$ for some t with $1 < t \leq p$. Then

$$(\theta^{-p})^{h-(a_i-a_1)} - (\theta^{-p})^h = (\theta^{-h+a_i-a_1} - \theta^{-h})^p$$
$$= (-\theta^{-p+a_i-a_1} + \theta^{-p})^p = \left(\frac{\theta - \theta^{a_i}}{\theta^{p+1}}\right)^p \in GF(p)$$

for $1 \leq i \leq t$ by Lemma 4.1. Similarly,

$$(\theta^{-p})^{h+p^2-1-(a_i-a_1)} - (\theta^{-p})^h \in GF(p)$$

for $t \leq i \leq p$. Thus,

$$\overline{A}(p, \theta^{-p}) = \{h - (a_i - a_1) \colon 1 \leq i \leq t\} \cup \{h + p^2 - 1 - (a_i - a_1) \colon t \leq i \leq p\};$$

therefore, $D(p, \theta) = D(p, \theta^{-p})$. $\square$

Example 5.1. Let $p = 7$ and $\theta^2 = \theta - 3$ as in Example 3.1. Then $h = 31$, $t = 5$, $(\theta^{-p})^2 = 5\theta^{-p} - 5$, $\overline{A}(p, \theta^{-p}) = \{1, 21, 27, 30, 31, 42, 44, 49\}$, $D(p, \theta) = \{1, 3, 6, 20, 5, 2, 11\} = D(p, \theta^{-p})$.

Example 5.2. Let $p = 11$ and $\theta^2 = 9\theta - 6$ as in Example 3.2. Then $h = 71$, $t = 9$, $(\theta^{-p})^2 = 7\theta^{-p} - 2$, $\overline{A}(p, \theta^{-p}) = \{1, 6, 20, 27, 38, 40, 55, 65, 71, 117, 118, 121\}$, $D(p, \theta) = \{6, 10, 15, 2, 11, 7, 14, 5, 3, 1, 46\} = D(p, \theta^{-p})$.

Lemma 5.2. *If* $GF^*(p^2) = (\theta)$, $\theta^2 = u\theta - v$ *with* $u, v \in GF(p)$, *then the minimum polynomial of* θ^{-p} *over* $GF(p)$ *is* $x^2 = wx - v^{-1}$ *for some* $w \in GF(p)$.

Proof. Let $x^2 = wx - t$ be the minimum polynomial of θ^{-p} over $GF(p)$ with $w, t \in GF(p)$. Then by Lemma 4.1 we have

$$t = (\theta^{-p})^{p+1} = (\theta^{p+1})^{-p} = (v^p)^{-1} = v^{-1}. \quad \square$$

Lemma 5.3. *Given a prime* p, *let* $g = g(p)$ *be the least primitive root of* p. *To find* $d(p)$, *we need only compare those* $d(p, \theta)$ *with* $\theta^2 = u\theta - v$, $u, v \in GF(p)$, *and*

$$(5.1) \qquad v = g^s \pmod{p} \quad \textit{for some } s \textit{ with } (s, p-1) = 1 \textit{ and } 1 \leq s < \frac{p-1}{2}.$$

Proof. This follows by Lemmas 4.1, 5.1, and 5.2. $\square$

Lemma 5.4. *We have* $A(p, \theta) = A(p, \theta^p)$.

Proof. This follows from the fact that both θ and θ^p have the same minimum polynomial over $GF(p)$. □

Lemma 5.5. *Given a prime p, let m_1 be the number of distinct sets $D(p, \theta)$ and m_2 the number of pairs of $u, v \in GF(p)$ such that*

$$v \text{ satisfying } (5.1), \text{ if } \theta^2 = u\theta - v, \text{ then } GF^*(p^2) = (\theta).$$

Then we have $m_1 \le m_2 = \varphi(p^2-1)/4$.

Proof. This follows by Lemmas 5.1, 5.2, 5.3, 5.4 and the fact that the group $GF^*(p^2)$ has $\varphi(p^2-1)$ generators. □

Lemma 5.6. *Given a prime p, if $GF^*(p^2) = (\theta)$, $\theta^2 \doteq u\theta - v$, with $u, v \in GF(p)$, then*

$$(u2^{-1})^2 - v \text{ is a quadratic nonresidue of } p. \tag{5.2}$$

Proof. This follows from the fact that

$$x^2 - ux + v = (x - u2^{-1})^2 - ((u2^{-1})^2 - v)$$

is irreducible over $GF(p)$. □

Remark 5.1. From Lemmas 5.3 and 5.6 we see that, given a prime p, to find $d(p)$, we need only, for those pairs of $u, v \in GF(p)$ satisfying (5.1) and (5.2), check if $GF^*(p^2) = (\theta)$ with $\theta^2 = u\theta - v$, and find $d(p, \theta)$ by Lemma 4.6; then take the maximum of them.

With the above preparation, we describe our algorithm in the following pseudocode:

```
REPEAT
  read a prime p and its least primitive root g = g(p) from a disk file;
  d(p) ← 0; count ← 0;
  For each pair of u, v ∈ GF(p) satisfying (5.1) and (5.2) do
    BEGIN
      Check if GF*(p^2) = (θ) with θ^2 = uθ − v by Lemma 4.3;
        (cf. the proof of Lemma 4.6)
      If GF*(p^2) = (θ) with θ^2 = uθ − v then
        Begin
          count ← count + 1; find d(p, θ) by Lemma 4.6;
          If d(p, θ) > d(p) then
            begin
              d(p) ← d(p, θ); save u, v
            end
        End
    END;
  k(p) ← p − sqrt(p^2 − d(p));
  output p, g, count, d(p), k(p), u, v
UNTIL p = p_145;
```

Remark 5.2. If $count \neq \varphi(p^2-1)/4$ for some p in the output, then there must be some errors in the program by Lemma 5.5.

6. Numerical results: $k(p)$ for $p \le p_{145}$

On an SCC486 (a compatible IBM PC/AT486), it takes about 120 hours to get $k(p)$ and related values for $p \le p_{145}$ in Table 1.

Table 1

i	p_i	$g(p_i)$	count	$d(p_i)$	$k(p_i)$	u	v
3	5	2	2	13	1.535 ···	1	2
4	7	3	4	20	1.614 ···	1	3
5	11	2	8	46	2.339 ···	7	2
6	13	2	12	57	2.416 ···	2	6
7	17	3	24	89	2.857 ···	9	5
8	19	2	24	103	2.937 ···	9	13
9	23	5	40	140	3.276 ···	4	20
10	29	2	48	201	3.701 ···	7	19
11	31	3	64	195	3.323 ···	1	24
12	37	2	108	250	3.548 ···	6	32
13	41	6	96	307	3.932 ···	15	19
14	43	3	120	341	4.167 ···	4	19
15	47	5	176	404	4.514 ···	11	23
16	53	2	216	429	4.214 ···	44	26
17	59	2	224	439	3.845 ···	7	42
18	61	2	240	586	5.008 ···	58	10
19	67	2	320	617	4.774 ···	12	18
20	71	7	288	699	5.106 ···	6	59
21	73	5	432	646	4.567 ···	22	5
22	79	3	384	717	4.676 ···	61	74
23	83	2	480	793	4.923 ···	76	15
24	89	3	480	818	4.720 ···	23	59
25	97	5	672	1000	5.299 ···	63	58
26	101	2	640	1024	5.203 ···	6	53
27	103	5	768	912	4.526 ···	11	86
28	107	2	936	1018	4.867 ···	56	72
29	109	6	720	1128	5.303 ···	3	40
30	113	3	864	1121	5.074 ···	108	43
31	127	3	1152	1364	5.488 ···	23	109
32	131	2	960	1271	4.944 ···	10	119
33	137	3	1408	1417	5.273 ···	92	6
34	139	2	1056	1741	6.410 ···	74	26
35	149	2	1440	1618	5.532 ···	109	51
36	151	6	1440	1874	6.338 ···	135	140
37	157	5	1872	1649	5.342 ···	93	142
38	163	2	2160	1737	5.418 ···	76	122
39	167	5	1968	2279	6.968 ···	21	159
40	173	2	2352	1997	5.871 ···	89	46
41	179	2	2112	2055	5.835 ···	88	165
42	181	2	1728	2151	6.042 ···	126	128
43	191	19	2304	2306	6.135 ···	158	63
44	193	5	3072	2460	6.481 ···	116	153
45	197	2	2520	2283	5.882 ···	68	179
46	199	3	2400	2283	5.821 ···	143	148
47	211	2	2496	2888	6.958 ···	22	174
48	223	3	3456	2930	6.669 ···	200	20
49	227	2	4032	3093	6.918 ···	108	66
50	229	6	3168	3527	7.834 ···	80	194
51	233	3	4032	2899	6.306 ···	98	155
52	239	7	3072	2977	6.311 ···	115	173
53	241	7	3520	3527	7.432 ···	116	68
54	251	6	3600	3059	6.169 ···	208	202
55	257	3	5376	3413	6.728 ···	120	132

TABLE 1 (continued)

i	p_i	$g(p_i)$	count	$d(p_i)$	$k(p_i)$	u	v
56	263	5	5200	3467	6.675 ···	113	194
57	269	2	4752	3249	6.108 ···	7	132
58	271	6	4608	3502	6.540 ···	203	210
59	277	5	6072	3567	6.515 ···	17	179
60	281	3	4416	3809	6.861 ···	265	42
61	283	3	6440	3838	6.864 ···	191	226
62	293	2	6048	3891	6.716 ···	168	42
63	307	5	5760	4589	7.567 ···	245	267
64	311	17	5760	4455	7.246 ···	225	103
65	313	10	7488	4208	6.795 ···	178	14
66	317	2	8112	4222	6.730 ···	123	237
67	331	3	6560	4587	7.003 ···	59	90
68	337	10	7488	4661	6.987 ···	116	248
69	347	2	9632	5226	7.613 ···	54	264
70	349	2	6720	4429	6.404 ···	242	166
71	353	3	9280	5229	7.485 ···	6	212
72	359	7	8544	5270	7.416 ···	292	183
73	367	6	10560	5512	7.587 ···	121	341
74	373	2	9600	5408	7.321 ···	64	135
75	379	2	7776	4995	6.648 ···	242	284
76	383	5	12160	5223	6.880 ···	60	140
77	389	2	9216	5712	7.412 ···	219	375
78	397	5	11880	6649	8.464 ···	222	46
79	401	3	10560	5577	7.015 ···	10	19
80	409	21	10240	6290	7.763 ···	90	132
81	419	2	8640	6141	7.393 ···	219	96
82	421	2	10080	6102	7.310 ···	231	39
83	431	7	12096	6582	7.704 ···	57	426
84	433	5	12960	6403	7.457 ···	419	201
85	439	15	11520	6517	7.486 ···	11	74
86	443	2	13824	7167	8.164 ···	82	332
87	449	3	11520	6830	7.671 ···	237	166
88	457	13	16416	6562	7.236 ···	92	328
89	461	2	10560	6647	7.266 ···	198	251
90	463	3	13440	6512	7.086 ···	265	349
91	467	2	16704	6761	7.295 ···	339	295
92	479	13	15232	8175	8.610 ···	176	13
93	487	3	19440	7606	7.872 ···	106	368
94	491	2	13440	7584	7.784 ···	267	447
95	499	7	16400	8624	8.717 ···	208	417
96	503	5	18000	7206	7.214 ···	99	266
97	509	2	16128	7608	7.529 ···	38	440
98	521	3	16128	7779	7.519 ···	282	239
99	523	2	21840	8655	8.340 ···	520	446
100	541	2	19440	8535	7.946 ···	139	2
101	547	2	19584	8626	7.942 ···	510	241
102	557	2	24840	8541	7.720 ···	466	346
103	563	2	25760	9215	8.244 ···	234	388
104	569	3	20160	8655	7.656 ···	200	149
105	571	3	17280	9260	8.166 ···	473	537
106	577	5	26112	8991	7.844 ···	326	137
107	587	2	24528	10535	9.043 ···	188	11
108	593	3	25920	9371	7.954 ···	417	41
109	599	7	21120	9467	7.955 ···	329	62
110	601	7	20160	10156	8.509 ···	72	317
111	607	3	28800	11562	9.599 ···	263	345
112	613	2	29376	9583	7.866 ···	416	362
113	617	3	24480	10881	8.881 ···	542	12
114	619	2	24480	10272	8.353 ···	120	488
115	631	3	22464	9804	7.817 ···	411	270

TABLE 1 (continued)

i	p_i	$g(p_i)$	*count*	$d(p_i)$	$k(p_i)$	u	v
116	641	3	27136	12084	9.496 ···	461	384
117	643	11	27984	11568	9.059 ···	251	126
118	647	5	31104	12778	9.951 ···	488	511
119	653	2	34992	11480	8.850 ···	505	399
120	659	2	22080	10055	7.673 ···	370	594
121	661	2	26400	10021	7.624 ···	643	333
122	673	5	32256	12220	9.140 ···	656	290
123	677	2	34944	11634	8.647 ···	348	515
124	683	5	32400	11277	8.305 ···	286	79
125	691	3	30272	11769	8.569 ···	501	507
126	701	2	25920	12928	9.282 ···	458	523
127	709	2	32480	11043	7.830 ···	661	282
128	719	11	34368	12114	8.474 ···	80	674
129	727	5	31680	12768	8.834 ···	300	475
130	733	6	43920	12512	8.585 ···	187	92
131	739	3	34560	11965	8.140 ···	669	590
132	743	5	37440	13163	8.911 ···	700	467
133	751	3	36800	12105	8.102 ···	500	257
134	757	2	40824	13094	8.698 ···	132	656
135	761	6	36288	14077	9.305 ···	625	198
136	769	11	30720	12146	7.938 ···	462	247
137	773	2	48384	14417	9.382 ···	143	273
138	787	2	50960	13937	8.904 ···	452	588
139	797	2	42768	13333	8.408 ···	480	537
140	809	3	43200	13307	8.266 ···	82	653
141	811	3	36288	14428	8.944 ···	625	346
142	821	2	43520	13836	8.470 ···	186	233
143	823	3	55488	15272	9.331 ···	763	221
144	827	2	45936	13987	8.500 ···	87	708
145	829	2	43296	16938	10.279 ···	825	306

7. SUMMARY

Since $k(p_{145}) = 10.279\ldots$ and $p_{145} = 829$, there exists an 829-element B_2-sequence $\{b_i\}$ with $829 - b_{829}^{1/2} > 10.279$. By the proofs of Theorems 1 and 2, it is easy (actually it takes 4′16″ on an IBM PC/XT) to get all elements of $\{b_i\}$. To save space, we give only the first and the last ten elements as follows:

1 1738 3183 3419 4949 5710 6177 6522 7229 8380

....

664432 664834 665138 665902 666010 667081 667206 668286 670235 670303

From Table 1 in §6, it is reasonable to conjecture that

(7.1) given $k > 0$, there exists an integer m such that $K(m) > k$.

Clearly, (7.1) contradicts (1.2). We hope that in a future paper, either (7.1) or (1.2) will be proved (i.e., the other will be disproved).

ACKNOWLEDGMENT

I thank the referee for helpful comments that improved the paper.

BIBLIOGRAPHY

1. R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962–63), 141–147.

2. P. Erdős and P. Turán, *On a problem of Sidon in additive number theory and on some related problems*, J. London. Math. Soc. **16** (1941), 212–215; Addendum, **19** (1944), 208.

3. Richard K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1981.
4. H. Halberstam and K. F. Roth, *Sequences*, Oxford Univ. Press, New York, 1966.
5. D. E. Knuth, *The art of computer programming: Semi-numerical algorithms*, Vol. 2, 2nd ed., Addison-Wesley, Reading, MA, 1981.
6. B. Lindstrom, *An inequality for B_2-sequences*, J. Combin. Theory **6** (1969), 211–212.
7. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Boston, 1985.
8. K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Reading, MA, 1984.
9. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.
10. B. L. Van der Waerden, *Modern algebra*, English transl., Ungar, New York, 1949.

Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, P.R. China

State Key Laboratory of Information Security, Graduate School USTC, 100039 Beijing, P.R. China

Laboratoire Théorie des Nombres et Algorithmique, Département de Mathématiques, Université de Limoges, 87060 Limoges, France

E-mail address: `zxzhang@cict.fr`