Journal of
Mathematical
Inequalities

Volume 17, Number 4 (2023), 1323–1333

doi:10.7153/jmi-2023-17-86

REPRESENTATIONS OF ELEMENT AS SUM OF PRIMITIVE ROOT AND LEHMER NUMBER IN $\mathbb{Z}_p$

BO ZHANG, JIANKANG WANG, YONGLI SU AND ZHEFENG XU*

(*Communicated by A. Filipin*)

Abstract. Let p be an odd prime and $\mathbb{Z}_p$ the residue class ring modulo p. In this paper, we study representations of any element of $\mathbb{Z}_p$ as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$, and give an explicit inequality better than asymptotic formula for the number of representations. From this inequality, we obtained that each element of $\mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root for $p > 2.5 \times 10^{14}$. Moreover, using the algorithm we provided, we examined all the cases when $p < 10^6$ by computer. We also analyzed the time complexity of the algorithm and illustrated that it is extremely difficult to verify all the cases up to the bound 2.5×10^{14}, and conjectured that any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$ for all primes p except 2, 3, 5, 7, 11, 19, 31.

1. Introduction

Let $q > 2$ be an odd integer and $\mathbb{Z}_q$ denote the residue class ring modulo q. For any $x \in \mathbb{Z}_q$ with $(x,q) = 1$, there is one and only one $\bar{x} \in \mathbb{Z}_q$ that satisfies $x\bar{x} \equiv 1 \pmod{q}$, where x is a Lehmer number if x and $\bar{x}$ are of opposite parity. Let $\mathcal{L}(q)$ denote the set of Lehmer numbers in $\mathbb{Z}_q$, then we have

$$\mathcal{L}(q) = \{x | x \in \mathbb{Z}_q, (x,q) = 1, 2 \nmid (x + \bar{x})\}.$$

For an odd prime p, D. H. Lehmer proposed a problem to find $|\mathcal{L}(p)|$, or at least to say something nontrivial about it (see Problem F12 of [7]). W. P. Zhang [16] obtained an asymptotic estimate of the number of elements of $\mathcal{L}(p)$:

$$|\mathcal{L}(p)| = \frac{p}{2} + O(p^{\frac{1}{2}} \ln^2 p).$$

Many scholars also gave some interesting propositions about Lehmer numbers, see [9]–[12], [15]–[16]. Y. M. Lu and Y. Yi [10] define a generalization of Lehmer numbers, and studied the number of representations of an integer as sum of three generalized Lehmer numbers by applying circle method. Subsequently, I. E. Shparlinski [12] proved that

Mathematics subject classification (2020): 11A07, 11N69, 11L05.

Keywords and phrases: Residue class ring, Lehmer number, primitive root, representation, numerical computation.

[*] Corresponding author.

if N is sufficiently large, then N can be represented as the sum of two the generalized Lehmer numbers by using the estimation of exponential sums.

Let $\mathcal{G}(p)$ be the set of primitive roots modulo p. As shown in [13], for any given $g \in \mathcal{G}(p)$, Andrew Odlyzko asked what values of M we have such that each element of $\mathbb{Z}_p$ can be represented as the following form

$$g^x - g^y \pmod{p}, \ \ 1 \leqslant x, y \leqslant M.$$

Many scholars studied this question and gave lower bounds of M, see [1], [5]–[6].

S. W. Golomb [8] conjectured that there exists a constant q_0 such that for all $p > q_0$ every nonzero $n \in \mathbb{Z}_p$ can be represented as the sum of two primitive roots in $\mathbb{Z}_p$. J. P. Wang [14] solved the part of this conjecture. S. D. Cohen and G. L. Mullen [2] proved a generalization of Golomb's conjecture. Furthermore, for any given divisors k, l of $p-1$ and given nonzero $\gamma, \delta \in \mathbb{Z}_p$, S. D. Cohen and W. P. Zhang [3] obtained the asymptotic formula of the number of representations of $n \in \mathbb{Z}_p$ as $\gamma a^k + \delta b^l \pmod{p}$, where $(a,b) \in \mathcal{G}(p) \times \mathcal{G}(p)$. In this paper, we will study the representations of elements of $\mathbb{Z}_p$ as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$. Our question is, for any given element $n \in \mathbb{Z}_p$, how many pairs $(l, g) \in \mathcal{L}(p) \times \mathcal{G}(p)$ such that

$$n \equiv l + g \pmod{p}. \tag{1}$$

Let $F(n,p)$ denote the number of solutions of the equation (1). For any odd integer $m \geqslant 3$ define the positive number T_m by

$$T_m = \frac{2\sum_{j=1}^{(m-1)/2} \tan\left(\frac{\pi j}{m}\right)}{m \log m}.$$

Then, we have the following results

THEOREM 1. *Let $p > 3$ be a prime. For any given element $n \in \mathbb{Z}_p$ we have the inequality*

$$\left| F(n,p) - \frac{\phi(p-1)}{2} \right| < \frac{3\phi(p-1)}{2(p-1)} T_p^2 2^{\omega(p-1)} \sqrt{p} \ln^2 p + 1.$$

where $\phi(m)$ is Euler totient function, $\omega(m)$ denotes the number of distinct prime factors of m.

From $\phi(p-1) < p-1$ and Lemma 2 in section 2, we have

COROLLARY 1. *Let p be a prime large enough. Then, there holds*

$$F(n,p) = \frac{\phi(p-1)}{2} + O\left(\sqrt{p} 2^{\omega(p-1)} \ln^2 p\right).$$

COROLLARY 2. *Any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$ if $p > 2.5 \times 10^{14}$.*

In section 4, according to the analysis of algorithm time complexity, if the prime p is selected as the order of 10^{14} magnitude, the time required to execute the algorithm is 1.44×10^{17} years by using the tianhe-2 supercomputer. Therefore, it is impossible to completely verify all prime numbers in limited time.

REMARK. When $p < 10^6$, we verify the representation of each element of $\mathbb{Z}_p$ by numerical computation, and find any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root except $p = 2, 3, 5, 7, 11, 19, 31$.

CONJECTURE 1. For all primes p except 2, 3, 5, 7, 11, 19, 31, any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$.

2. Some lemmas

In this section, we give some lemmas for the proof of theorem.

LEMMA 1. *Let χ be any Dirichlet character modulo an odd prime p. Then, for arbitrary integers n, r, s with $(rs, p) = 1$, we have*

$$\left|\sum_{x=1}^{p-1} \chi(x+n) \exp\left(\frac{rx + s\bar{x}}{p}\right)\right| < 3\sqrt{p}.$$

Proof. This is another form of Lemma 4 in [4]. □

LEMMA 2. *For any odd integer $m \geqslant 2$ we have*

$$\frac{2}{\pi}\left(\frac{0.548}{\ln m}\right) \leqslant T_m \leqslant \frac{2}{\pi}\left(1 + \frac{1.549}{\ln m}\right).$$

In particular, if $m \geqslant 1637$, then $T_m^2 \leqslant \frac{1}{2}$

Proof. See Lemma 1 of [4]. □

LEMMA 3. *Let p be an odd prime and let χ be any Dirichlet character modulo p. Then, for arbitrary integers n,*

$$\left|\sum_{x=1}^{p-1} (-1)^{x+\bar{x}} \chi(x+n)\right| < 3T_p^2 \sqrt{p} \ln^2 p$$

holds.

Proof. Notice that the trigonometric identity

$$\sum_{a=1}^{p} \exp\left(\frac{ma}{p}\right) = \begin{cases} p, & \text{if } (m,p) = p; \\ 0, & \text{if } (m,p) = 1; \end{cases}$$

then we have

$$\begin{aligned}
&\sum_{x=1}^{p-1}(-1)^{x+\bar{x}}\chi(x+n)\\
&=\frac{1}{p^2}\sum_{\substack{x=1\\ xb\equiv 1(\bmod p)}}^{p-1}\sum_{b=1}^{p-1}\chi(x+n)\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}(-1)^{c+d}\sum_{r=1}^{p}\exp\left(\frac{r(x-c)}{p}\right)\\
&\quad\times\sum_{s=1}^{p}\exp\left(\frac{s(b-d)}{p}\right)\\
&=\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left\{\sum_{x=1}^{p-1}\chi(x+n)\exp\left(\frac{rx+s\bar{x}}{p}\right)\right\}\\
&\quad\times\left\{\sum_{c=1}^{p-1}(-1)^c\exp\left(\frac{-rc}{p}\right)\right\}\left\{\sum_{d=1}^{p-1}(-1)^d\exp\left(\frac{-sd}{p}\right)\right\}. \qquad (2)
\end{aligned}$$

For any integer r with $(r,p)=1$,

$$\sum_{a=1}^{p-1}(-1)^a\exp\left(\frac{-ar}{p}\right)=\frac{1-\exp\left(\frac{r}{p}\right)}{1+\exp\left(\frac{r}{p}\right)}=\frac{i\sin\left(\frac{\pi r}{p}\right)}{\cos\left(\frac{\pi r}{p}\right)}.$$

Moreover,

$$\sum_{a=1}^{p-1}\left|\frac{\sin\left(\frac{\pi a}{p}\right)}{\cos\left(\frac{\pi a}{p}\right)}\right|=2\sum_{j=1}^{(p-1)/2}\tan\left(\frac{\pi j}{p}\right)=T_p p\ln p.$$

According to (2) and Lemma 1, it follows that

$$\begin{aligned}
\left|\sum_{x=1}^{p-1}(-1)^{x+\bar{x}}\chi(x+n)\right|&=\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{x=1}^{p-1}\chi(x+n)\exp\left(\frac{rx+s\bar{x}}{p}\right)\right|\\
&\quad\times\left|\sum_{c=1}^{p-1}(-1)^c\exp\left(\frac{-rc}{p}\right)\right|\left|\sum_{d=1}^{p-1}(-1)^d\exp\left(\frac{-sd}{p}\right)\right|\\
&\leqslant\frac{3\sqrt{p}}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\frac{\sin\left(\frac{\pi r}{p}\right)}{\cos\left(\frac{\pi r}{p}\right)}\right|\left|\frac{\sin\left(\frac{\pi s}{p}\right)}{\cos\left(\frac{\pi s}{p}\right)}\right|\\
&<3T_p^2\sqrt{p}\ln^2 p.
\end{aligned}$$

This proves Lemma 3. □

LEMMA 4. *Let p be an odd prime, c be an integer with $(c,p)=1$. Then*

$$\sum_{d\mid p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}e\left(\frac{h\ ind\ c}{d}\right)=\begin{cases}\dfrac{p-1}{\phi(p-1)}, & \text{if } c \text{ is a primitive root modulo } p;\\ 0, & \text{otherwise.}\end{cases}$$

where ind c satisfies $c \equiv g^{ind\ c} \pmod{p}$ *for a fixed primitive root modulo* p^{α}*,* $\mu(c)$ *is the Möbius function.*

Proof. See [16]. □

3. Proof of theorems

We will use above lemmas to prove our results. Firstly, we make a simple transformation of $F(n,p)$. In the process of proof, let $\mathcal{L} = \mathcal{L}(p)$ and $\mathcal{G} = \mathcal{G}(p)$ for convenience. In fact, $|\mathcal{G}| = \phi(p-1)$ and

$$|\mathcal{L}| = \frac{p-1}{2} - \frac{1}{2}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}.$$

From the definition of $F(n,p)$, we can write

$$\begin{aligned}
F(n,p) = & \sum_{\substack{a=1 \\ a\in\mathcal{L} \\ a+b\equiv n(\bmod p)}}^{p-1}\sum_{\substack{b=1 \\ b\in\mathcal{G}}}^{p-1} 1 \\
= & \frac{1}{p}\sum_{c=1}^{p}\exp\left(\frac{-cn}{p}\right)\sum_{\substack{a=1 \\ a\in\mathcal{L}}}^{p-1}\exp\left(\frac{ac}{p}\right)\sum_{\substack{b=1 \\ b\in\mathcal{G}}}^{p-1}\exp\left(\frac{bc}{p}\right) \\
= & \frac{(p-1)\phi(p-1)}{2p} + \frac{1}{p}\sum_{c=1}^{p-1}\exp\left(\frac{-cn}{p}\right)\sum_{\substack{a=1 \\ a\in\mathcal{L}}}^{p-1}\exp\left(\frac{ac}{p}\right)\sum_{\substack{b=1 \\ b\in\mathcal{G}}}^{p-1}\exp\left(\frac{bc}{p}\right) \\
& -\frac{\phi(p-1)}{2p}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}} \\
= & \frac{(p-1)\phi(p-1)}{2p} + E(n,p). \qquad (3)
\end{aligned}$$

Next, we estimate the error term $E(n,p)$, and have

$$\begin{aligned}
E(n,p) = & \frac{1}{2p}\sum_{c=1}^{p-1}\exp\left(\frac{-cn}{p}\right)\sum_{a=1}^{p-1}\left(1-(-1)^{a+\bar{a}}\right)\exp\left(\frac{ac}{p}\right)\sum_{\substack{b=1 \\ b\in\mathcal{G}}}^{p-1}\exp\left(\frac{bc}{p}\right) \\
& -\frac{\phi(p-1)}{2p}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}} \\
= & \frac{\phi(p-1)}{2p(p-1)}\sum_{c=1}^{p-1}\exp\left(\frac{-cn}{p}\right)\sum_{a=1}^{p-1}\left(1-(-1)^{a+\bar{a}}\right)\exp\left(\frac{ac}{p}\right) \\
& \times\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1 \\ (h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\exp\left(\frac{bc}{p}\right) - \frac{\phi(p-1)}{2p}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}
\end{aligned}$$

$$
\begin{aligned}
&= -\frac{\phi(p-1)}{2p(p-1)}\sum_{c=1}^{p-1}\exp\left(\frac{-cn}{p}\right)\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\exp\left(\frac{bc}{p}\right)\\
&\quad -\frac{\phi(p-1)}{2p(p-1)}\sum_{c=1}^{p-1}\exp\left(\frac{-cn}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\exp\left(\frac{ac}{p}\right)\\
&\quad \times\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\exp\left(\frac{bc}{p}\right)-\frac{\phi(p-1)}{2p}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\\
&= -\Sigma_1-\Sigma_2-\Sigma_3. \qquad (4)
\end{aligned}
$$

By calculating each term in (4), for $n \neq 0$ we have

$$
\begin{aligned}
|\Sigma_1| &= \left|\frac{\phi(p-1)}{2p(p-1)}\sum_{c=1}^{p}\exp\left(\frac{-cn}{p}\right)\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\exp\left(\frac{bc}{p}\right)\right.\\
&\quad \left. -\frac{\phi(p-1)}{2p(p-1)}\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\right|\\
&\leqslant \frac{\phi(p-1)}{2p-2}\left|\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ n}{d}\right)\right|\\
&\quad +\frac{\phi(p-1)}{2p(p-1)}\left|\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\right|\\
&\leqslant \frac{1}{2}+\frac{\phi(p-1)}{2p}\\
&< \frac{3}{4}. \qquad (5)
\end{aligned}
$$

If $n=0$ then we also have $|\Sigma_1| < \frac{3}{4}$. For Σ_2 and Σ_3, we can write

$$
\begin{aligned}
&\Sigma_2+\Sigma_3\\
&= \frac{\phi(p-1)}{2p(p-1)}\sum_{c=1}^{p}\exp\left(\frac{(a+b-n)c}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)\\
&\quad -\frac{\phi(p-1)}{2p(p-1)}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\sum_{b=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ b}{d}\right)+\frac{\phi(p-1)}{2p}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\\
&= \frac{\phi(p-1)}{2(p-1)}\sum_{\substack{a=1\\a\neq n}}^{p-1}(-1)^{a+\bar{a}}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ n-a}{d}\right).
\end{aligned}
$$

From the fact that the map which takes a with $(a,p)=1$ to $e\left(\frac{h\,ind\,a}{d}\right)$ is a Dirichlet character modulo p with order d and Lemma 3, it follows that

$$|\Sigma_2+\Sigma_3| \leqslant \frac{\phi(p-1)}{2(p-1)}\left|\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{a=1}^{p-1}(-1)^{a+\bar{a}}\chi_{h,d}(n-a)\right|$$
$$< \frac{3\phi(p-1)}{2(p-1)}T_p^2 2^{\omega(p-1)}\sqrt{p}\ln^2 p. \tag{6}$$

Combining (4)–(6) we have

$$|E(n,p)| < \frac{3\phi(p-1)}{2(p-1)}T_p^2 2^{\omega(p-1)}\sqrt{p}\ln^2 p+\frac{3}{4}. \tag{7}$$

From (3) and (7), we immediately get

$$\left|F(n,p)-\frac{\phi(p-1)}{2}\right| < \frac{3\phi(p-1)}{2(p-1)}T_p^2 2^{\omega(p-1)}\sqrt{p}\ln^2 p+1.$$

So Theorem 1 is proved.

For Corollary 2, if $n\in\mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_q$ then $F(n,p)>0$. Thus, $\sqrt{p}>3T_p^2 2^{\omega(p-1)}\ln^2 p$. From Lemma 2 we have $p>e^{e^{3.5}}\approx 2.5\times 10^{14}$.

4. Numerical computation

In this section, we will verify whether each element in $\mathbb{Z}_p=\{0,1,2,\cdots,p-1\}$ can be represented as the sum of a Lehmer number and a primitive root.

4.1. Lehmer numbers and primitive roots

First, we need to calculate the Lehmer number set $\mathcal{L}=\mathcal{L}(p)=\{l_1,l_2,\cdots,l_k\}$ and a primitive root g module p.

Based on the definition of Lehmer number. The key to find Lehmer numbers is to find $\bar{x}\in\mathbb{Z}_p$ for non-zero element $x\in\mathbb{Z}_p$, then we just need to judge whether x and $\bar{x}$ is opposite to parity. Since $\bar{x}$ satisfies $x\bar{x}\equiv 1 \pmod p$, there are $p-1$ cases for $\bar{x}$ as follows,

$$x\bar{x}=p+1, x\bar{x}=2p+1,\cdots,x\bar{x}=(p-1)p+1$$

For $\bar{x}$ must belong to $\{2,3,\cdots,p-1\}$, the only thing we need to do is verifying whether one of the upper $p-1$ cases belong to $\{2,3,\cdots,p-1\}$.

Algorithm 1 *Finding Lehmer numbers*

```
Input: A prime $p$, define a 3-dimension zero matrix: $out = zeros(p-2,3)$,
    put $\{2,3,\cdots,p-1\}$ in the first column;
Output: Lehmer number set $\mathcal{L}$.
for $j = 1,2,\cdots,p-2$ do
    $out(j,1) = j+1$
end for
for $j = 1,2,\cdots,p-2$ do
    if $out(j,3) == 0$ then
        for $i = 1,2,\cdots,p-2$ do
            $x = out(j,1)$; $x\_inv = (ip+1)/x$;
            if $1 < x\_inv < p$ & $x\_inv$ is an integer & $x + x\_inv \equiv 1 \pmod 2$ then
                $out(j,2) = x\_inv$; $out(j,3) = 1$; $out(x\_inv-1,2) = x$;
                $out(x\_inv-1,3) = 1$; terminate loop(i)
            end if
        end for
    end if
end for
for $j = 1,2,\cdots,p-2$ do
    if $out(j,3) = 1$ then
        put $out(j,1) \in \mathcal{L}$;
    end if
end for
```

Time Complexity Analysis of Algorithm 1. The second step of the algorithm only performs the assignment operation, the operational time may not be considered. The third step of the algorithm has two layers of loops. The outer loop (j loop) needs to be executed $p-2$ times, and the inner loop (i loop) needs to be executed at most $p-1$ times. Inside the loop, statement $x\_inv = \frac{ip+1}{x}$ $(1 \leqslant i \leqslant p-1)$ includes one multiplication and one division; at the same time, in the subsequent judgment statements, whether x_inv is an integer can generally be judged by module 1 remainder, including one division; while $x + x\_inv \equiv 1 \pmod 2$ includes one addition and one division. Thus, each loop includes three divisions, one multiplication and one addition. So, the algorithm performs a total of $3(p-1)(p-2)$ divisions, $(p-1)(p-2)$ multiplications and $(p-1)(p-2)$ additions, and the time complexity is $O(p^2)$.

For primitive roots, we calculate $c^{q_i} \pmod p$ $(1 \leqslant i \leqslant k)$ for all proper divisors $\{q_1, q_2, \cdots, q_k\}$ of $\phi(p-1)$ one by one. As long as there is a certain one $c^{q_i} \equiv 1 \pmod p$, it shows that c is not a primitive root module p. If all $c^{q_i} \not\equiv 1 \pmod p$ then c is a primitive root.

Algorithm 2 *Finding primitive roots*

```
Input: A prime $p$, all proper divisors $\{q_1,q_2,\cdots,q_k\}$ of $\phi(p-1)$;
Output: A primitive root $g$.
for $n = 2,\cdots,p-1$ do
    flag=1; $t = n$;
    for $k = 2,\cdots,q_m$ do
        $t \equiv t \times n \pmod p$;
        **if** $t = 1$ **then**
            $flag = 0$; terminate loop(k)
        **end if**
    **end for**
    **if** $flag = 1$ **then**
        then $g = n$; terminate loop(n)
    **end if**
**end for**
```

Time Complexity Analysis of Algorithm 2. The main part of the algorithm consists of two layers of loops. The outer loop needs to be executed at most $p-2$ times, and the most executed times of inner loop is equal to maximum prime factor, its possible value is $p/2$. Inside the loop the calculation is $t \times n$, then module p, that includes one multiplication and one division. Therefore, during the execution of the algorithm, the total number of multiplication and division operations is at most $p(p-1)$ times, thus the time complexity is $O(p^2)$.

4.2. Represented as the sum of a Lehmer number and a primitive root

For any $n \in \mathbb{Z}_p$, we should traverse the elements $l_i \ (1 \leqslant i \leqslant k)$ in $\mathcal{L}$, and calculate the difference between n and l_i. Denote $a_i \equiv n - l_i \pmod{p}$. Now, we only need to check whether a_i is a primitive root, if it is, then n can be represented, otherwise it cannot be represented. We know that if g is a primitive root module p then all primitive roots can be expressed as the set $\{g^j | 1 \leqslant j \leqslant p-1, (j, p-1) = 1\}$. So we can find all numbers j that is coprime with $p-1$, then check whether a_i is equal to g^j.

Algorithm 3 *Verification that any element $n \in \mathbb{Z}_p$ is represented as the sum of a Lehmer number and a primitive root*

Input: A prime p, $\mathcal{L}(p) = \{l_1, l_2, \cdots, l_k\}$, a primitive root g module p;
Output: Whether $n \in \mathbb{Z}_p$ can be represented.

```
**for** $n = 0, 1, 2, \cdots, p-1$ **do**
    flag=0
    **for** $l = l_1, l_2, \cdots, l_k$ **do**
        $a \equiv n - l_i \pmod{p}$;
        **for** $j = 1, 2, \cdots, p-2$ **do**
            **if** $(j, p-1) = 1$ and $g^j \equiv a \pmod{p}$ **then**
                flag=1 terminate loop(l)
            **end if**
        **end for**
        **if** flag=0 **then**
            output (n cannot be decomposed) terminate loop(n)
        **end if**
    **end for**
**end for**
```

Time Complexity Analysis of Algorithm 3. The execution process of the algorithm includes three layers of loops. In the innermost layer, it is necessary to verify whether j and $p-1$ is coprime or not first, here, in order to judge the coprime, we use the algorithm of rolling division, and the time complexity of rolling division is

$O(\log p)$, then we need to calculate g^j, because the step size of j is 2, each cycle only needs to multiply g^2 on the basis of the previous calculation. Thus, the calculation g^j requires at most $\frac{p-1}{2}$ multiplications. Obviously, the time complexity of calculating g^j is much higher than that of judging coprime, so it can be considered that the number of multiplications in the innermost layer is about $\frac{p-1}{2}$. The maximum number of the middle layer is the number of elements in Lehmer number set, which is about $\frac{p-1}{2}$. The maximum number of the outermost layer is p, so the whole number of multiplication calculation times is $\frac{(p-1)p^2}{4}$, and the time complexity is $O(p^3)$.

In view of the time complexity of $O(p^3)$ and the number of multiplications $\frac{(p-1)p^2}{4}$, we should use the tianhe-2 supercomputer, which has the fastest calculation speed reaching 54.9 million billion times per second at present, that is 5.49×10^{16} times per second. If the prime is selected as the order of 10^{14} magnitude, the time required to execute the above algorithm is $\frac{0.25\times10^{42}}{5.49\times10^{16}} \approx 4.55 \times 10^{24}$ seconds, to convert into years, that is $\frac{4.55\times10^{24}}{365\times24\times60\times60} \approx 1.44 \times 10^{17}$ years.

Using algorithm 3, we have fully verified for primes below the order of 10^6 magnitude, the algorithm runs on a computer being configured by inter core (TM) cpui5-8250,1.8Gz, The calculation time is listed in Table 1 and all primes which cannot be represented are given in Table 2.

Table 1: *Calculation Time*

Range of prime	Time (second)
[2,5000]	452.976560
[5001,10000]	2760.886042
[10001,11000]	1123.306742
[11001,12000]	1169.932487

Table 2: *Numbers which cannot be represented*

Prime	Lehmer numbers	Primitive roots	Number which cannot be expressed
3	[]	[2]	0,1,2
5	[2,3]	[2,3]	2,3
7	[]	[3,5]	0,1,2,3,4,5,6
11	[3,4,7,8]	[2,6,7,8]	7,8
19	[4,5,14,15]	[2,3,10,13,14,15]	2,3,4,12,13
31	[12,13,18,19]	[3,11,12,13,17,21,22,24]	7,13,14,17,18,19,20,27,28

For example: if we select $p = 11$, and subtract the elements in Lehmer number set with 7 respectively, then we have $7 - \{3,4,7,8\} = \{4,3,0,10\}$ module 11, each number of $\{4,3,0,10\}$ do not belong to primitive root module 11, so 7 cannot be expressed as the sum of a Lehmer number and a primitive root module 11. Conversely if we subtract the elements in Lehmer set with 5 respectively. Conversely if $p = 5$, we can get $5 - \{3,4,7,8\} = \{2,1,9,8\}$, because number 2 and 8 belong to primitive root set, we have $5 = 3$(Lehmer number)$+2$(primitive root), and $5 = 8$(Lehmer number)$+8$(primitive root).

Acknowledgement. The authors are very grateful to the anonymous referee for the very careful reading of the manuscript and valuable comments. This work is supported by National Natural Science Foundation of China No. 11971381.

REFERENCES

[1] J. CILLERUELO, ANA ZUMALACÁRREGUI, *An additive problem in finite fields with powers of elements of large multiplicative order*, Rev. Mat. Comput., **27** (2014) 501–508.

[2] S. D. COHEN, G. L. MULLEN, *Primitive elements in Costas arrays*, Appl. Algebra Eng. Comm. Comput, **2** (1991) 45–53.

[3] S. D. COHEN, W. P. ZHANG, *Sums of two exact powers*, Finite Fields Appl., **8** (2002) 471–477.

[4] S. D. COHEN, T. TRUDGAIN, *Lehmer numbers and primitive roots modulo a prime*, J. Number Theory, **203** (2019) 68–79.

[5] C. V. GARCIA, *A note on an additive problem with powers of a primitive root*, Bol. Soc. Mat. Mexicana, **11** (2005) 1–4.

[6] M. Z. GARAEV, KA-LAM KUEH, *Distribution of special sequences modulo a large prime*, Int. J. Math. Math. Sci., **50** (2003) 3189–3194.

[7] R. K. GUY, *Unsolved Problems in Number Theory*, 3rd. edn, Springer-Verlag, New York, 2004.

[8] S. W. GOLOMB, *Algebraic constructions for costas arrays*, J. Comb. Theory, **37** (1984) 13–21.

[9] S. R. LOUBOUTIN, J. RIVAT, A. SARKOZY, *On a Problem of D. H. Lehmer*, Proc. Amer. Math. Soc., **135** (2007) 969–975.

[10] Y. M. LU, Y. YI, *Partitions involving D. H. Lehmer numbers*, Monatsh. Math., **159** (2010) 45–58.

[11] I. E. SHPARLINSKI, *On a generalisation of a Lehmer problem*, Math. Z., **263** (2009) 619–631.

[12] I. E. SHPARLINSKI, A. WINTERHOF, *Partitions into two Lehmer numbers*, Monatsh. Math., **160** (2010) 429–441.

[13] M. VÂJÂITU, A. ZAHARESCU, *Differences between powers of a primitive root*, Int. J. Math. Math. Sci. **29** (2002), 325–331.

[14] J. P. WANG, *On Golomb's conjectures*, Sci. Sinica Ser. A **31** (1988) 152–161.

[15] Z. F. XU, W. P. ZHANG, *On a problem of D. H. Lehmer over short intervals*, J. Math. Anal. Appl., **320** (2006) 756–770.

[16] W. P. ZHANG, *A problem of D. H. Lehmer and its generalization (II)*, Compositio Math., **91** (1994) 47–56.

(Received September 13, 2022)

Bo Zhang
School of Mathematics, Northwest University
Xi'an, China

Jiankang Wang
School of Mathematics, Northwest University
Xi'an, China
and
Research Center for Number Theory and Its Applications
Northwest University
Xi'an, China

Yongli Su
School of Mathematics, Northwest University
Xi'an, China

Zhefeng Xu
School of Mathematics, Northwest University
Xi'an, China
and
Research Center for Number Theory and Its Applications
Northwest University
Xi'an, China