Mathematical
Inequalities
& Applications
Volume 27, Number 3 (2024), 669–678 doi:10.7153/mia-2024-27-46

PARTITIONS INTO m–TH LEHMER NUMBERS AND k–TH POWER RESIDUES IN $\mathbb{Z}_p$

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

(*Communicated by M. Praljak*)

Abstract. Let p be a prime, $\mathbb{Z}_p^* = \{1,2,\ldots,p-1\}$, m,c be integers with $m \geqslant 2$, and $\mathscr{L}_m(c) = \{x|x \in \mathbb{Z}_p^*, 2 \nmid (x+(cx^m)_p)\}$, where $(cx^m)_p$ denotes the least positive residue modulo p. In this paper, we study the representation of any element of $\mathbb{Z}_p$ as sum of a m-th Lehmer number $l \in \mathscr{L}_m(c)$ and a k-th power residue in $\mathbb{Z}_p$, and give an inequality for the number of representations. Moreover, using the algorithm we provided, we examined all the cases for some pairs (k,m) 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 of p for larger km.

1. Introduction

Let p be an odd prime, $\mathbb{Z}_p^* = \{1,2,\ldots,p-1\}$. For any integer $x \in \mathbb{Z}_p^*$, there exists a unique $\bar{x} \in \mathbb{Z}_p^*$ such that $x\bar{x} \equiv 1 \pmod{p}$. If $x \in \mathbb{Z}_p^*$ and $\bar{x}$ are of opposite parity, then we call x a Lehmer number. Let $L(p)$ the set of Lehmer numbers modulo p, that is

$$L(p) = \{x \mid x\bar{x} = 1, x, \bar{x} \in \mathbb{Z}_p^*, 2 \nmid (x+\bar{x})\}.$$

D. H. Lehmer asked us to find $L(p)$ or at least to say something nontrivial about it (see Problem F12 of [4]). Zhang [10, 11] obtained an asymptotic estimate of the number of elements of $L(p)$:

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

Many scholars have proven other interesting properties about $L(p)$; for details see [5]–[8].

Bourgain, et al [1] defined E and O the set of even and odd residues modulo p respectively,

$$E = \{2,4,6,\cdots,p-1\}, \qquad O = \{1,3,5,\cdots,p-2\}.$$

For a positive integer m and any integer c with $p \nmid c$, let

$$\mathscr{N}_m(c) = \#\{x \in E : (cx^m)_p \in O\}$$

Mathematics subject classification (2020): 11A07, 11N69, 11L05.
Keywords and phrases: m-th Lehmer number, k-th residue, representation.
* Corresponding author.

where $(cx^m)_p$ denotes the smallest positive residue of cx^m modulo p. Let $\exp(x) = e^{2\pi ix}$. For $m \geqslant 2$, they [1, Theorem 1.1] gave

$$\left|\mathscr{N}_m(c) - \frac{p}{4}\right| \leqslant \frac{1}{\pi}\Phi'(m)\min\left\{\ln\left(\frac{356p}{\Phi'(m)}\right), \ln(5p)\right\}, \tag{1}$$

where

$$\Phi'(m)\begin{cases} = \frac{\Phi(m)}{2}, & \text{if } m \text{ is even;} \\ \leqslant \frac{1}{2}\Phi(m) + \frac{1}{\pi}\ln(5p)\Phi(m,1), & \text{if } m \text{ is odd;} \end{cases}$$

$$\Phi(m) = \max_{1\leqslant a\leqslant p-1}\left|\sum_{x=1}^{p-1}\exp\left(\frac{ax^m}{p}\right)\right|,$$

$$\Phi(m,1) = \max_{1\leqslant a,b\leqslant p-1}\left|\sum_{x=1}^{p-1}\exp\left(\frac{ax^m+bx}{p}\right)\right|,$$

and

$$\Phi'(m) = \max_{1\leqslant a\leqslant p-1}\left|\sum_{x=1}^{\frac{p-1}{2}}\exp\left(\frac{ax^m}{p}\right)\right|.$$

Furthermore, Xu [9] considered the distribution of the difference of an integer and its m-th power modulo a positive integer q over incomplete intervals. Let λ, δ be any real numbers with $0 < \lambda, \delta \leqslant 1$, $q > \max\{[\frac{1}{\lambda}], [\frac{1}{\delta}]\}$ and $m \geqslant 2$ be integers. Define

$$S_{m,q,\lambda,\delta} = \#\{a : 1 \leqslant a \leqslant \lambda q, (a,q) = 1, |a - (a^m)_q| \leqslant \delta q\}.$$

Xu gave some asymptotic formulas for

$$\sum_{a\in S_{m,q,\lambda,\delta}} \left|a - (a^m)_q\right|^k.$$

Define a generalization of Lehmer numbers by

$$\mathscr{L}_m(c) = \{x \mid x \in \mathbb{Z}_p^*, 2 \nmid (x + (cx^m)_p)\}.$$

We call $x \in \mathscr{L}_m(c)$ a m-th Lehmer number and $x \in \mathscr{L}_m(1)$ a classical m-th Lehmer number. From (1), it is straightforward to obtain an asymptotic estimate of the number of elements of $\mathscr{L}_m(c)$. If m is odd then we have

$$\left|\#\mathscr{L}_m(c) - \frac{p-1}{2}\right| < \frac{2}{\pi}\Phi'(m)\min\left\{\ln\left(\frac{356p}{\Phi'(m)}\right), \ln(5p)\right\}.$$

If m is even then we have

$$\begin{aligned}\#\mathscr{L}_m(c) &= \frac{1}{2}\sum_{a=1}^{p-1}\left(1-(-1)^{a+(ca^m)_p}\right) = \frac{p-1}{2} - \frac{1}{2}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p} \\ &= \frac{p-1}{2} - \frac{1}{4}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p} - \frac{1}{4}\sum_{a=1}^{p-1}(-1)^{p-a+(c(p-a)^m)_p} \\ &= \frac{p-1}{2} - \frac{1}{4}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p} + \frac{1}{4}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p} = \frac{p-1}{2}.\end{aligned}$$

In this paper, we consider the representation of elements of $\mathbb{Z}_p$ as the sum of a m-th Lehmer number and a k-th power residue in $\mathbb{Z}_p^*$. Let $\mathscr{R}_k(p)$ be the set of k-th power residues in $\mathbb{Z}_p^*$. Our question is, whether exists $l \in \mathscr{L}_m(c)$ and $r \in \mathscr{R}_k(p)$ such that

$$n = l + r \tag{2}$$

for any given element $n \in \mathbb{Z}_p$. Let $\mathscr{F}_{k,m}(n,p)$ denote the number of solutions of the equation (2). For any odd integer $q \geqslant 3$ define the positive number T_q by

$$T_q = \frac{2\sum_{j=1}^{(q-1)/2} \tan\left(\frac{\pi j}{q}\right)}{q \ln q}.$$

Then, we have the following results.

THEOREM 1. *Let $p > 3$ be a prime and let $m \geqslant 2$ be an integer. For any given element $n \in \mathbb{Z}_p$ and any positive integer $k \mid p-1$, we have*

$$\left|\mathscr{F}_{k,m}(n,p) - \frac{p-1}{2k}\right| < \frac{m}{2} T_p^2 \sqrt{p} \ln^2 p + 2.$$

COROLLARY 1. *Let p be a prime and let $m \geqslant 2$ be an integer. For any positive integer $k \mid (p-1)$, if $p > 4(km)^2\left(\ln(km) + 4\ln\ln(km) + 4\ln^{-1}(km)\right)^4$ then any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a m-th Lehmer number and a k-th power residue in $\mathbb{Z}_p$.*

In Section 4, we compute the exact values of $\mathscr{F}_{k,m}(n,p)$ for the pairs $(k,m) = (2,2),(2,3),(3,2),(3,3)$, for small values of p, obtaining the following corollaries and conjectures.

COROLLARY 2. *Any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a classical 2-th Lehmer number and a quadratic residue in $\mathbb{Z}_p$ for any prime $p > 5$.*

COROLLARY 3. *Any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a classical 2-th Lehmer number and a 3-th power residue in $\mathbb{Z}_p$ for any prime $p > 13$.*

CONJECTURE 1. Any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a classical 3-th Lehmer number and a quadratic residue in $\mathbb{Z}_p$ for any prime $p > 5$ except $p = 13$.

CONJECTURE 2. Any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a classical 3-th Lehmer number and a 3-th power residue in $\mathbb{Z}_p$ for any prime $p > 31$.

2. Some Lemmas

In this section, we give some lemmas for the proofs of the theorems.

LEMMA 1. *Let χ be any Dirichlet character modulo a prime p. Then, for a positive integer $m \geqslant 2$ and arbitrary integers n, r, s with $(rs, p) = 1$, we have*

$$\left| \sum_{x=1}^{p} \chi(x+n) \exp\left(\frac{rx + sx^m}{p}\right) \right| \leqslant m\sqrt{p}.$$

Proof. This is the application of (1.3) of Cochrane and Pinner [2]. □

LEMMA 2. *For any odd integer $q \geqslant 3$ we have*

$$\frac{2}{\pi}\left(1 + \frac{0.548}{\ln q}\right) < T_q < \frac{2}{\pi}\left(1 + \frac{1.549}{\ln q}\right).$$

In particular, if $q \geqslant 1637$, then $T_q^2 < \frac{1}{2}$.

Proof. See Lemma 1 of [3]. □

LEMMA 3. *Let χ be any Dirichlet character modulo a prime p. Then, for an integer $m \geqslant 2$ and arbitrary integers n, c with $p \nmid c$,*

$$\left| \sum_{x=1}^{p-1} (-1)^{x+(cx^m)_p} \chi(x+n) \right| \leqslant m T_p^2 \sqrt{p} \ln^2 p$$

holds.

Proof. Via the orthogonality of trigonometric sums as follows

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

we can write

$$\begin{aligned}
&\sum_{x=1}^{p-1} (-1)^{x+(cx^m)_p} \chi(x+n) \\
&= \frac{1}{p^2} \sum_{x=1}^{p-1} \chi(x+n) \sum_{h=1}^{p-1}\sum_{d=1}^{p-1} (-1)^{h+d} \sum_{r=1}^{p} \exp\left(\frac{r(x-h)}{p}\right) \sum_{s=1}^{p} \exp\left(\frac{s(cx^m-d)}{p}\right) \\
&= \frac{1}{p^2} \sum_{x=1}^{p} \chi(x+n) \sum_{h=1}^{p-1}\sum_{d=1}^{p-1} (-1)^{h+d} \sum_{r=1}^{p} \exp\left(\frac{r(x-h)}{p}\right) \sum_{s=1}^{p} \exp\left(\frac{s(cx^m-d)}{p}\right)
\end{aligned}$$

$$=\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left\{\sum_{x=1}^{p}\chi(x+n)\exp\left(\frac{rx+scx^m}{p}\right)\right\}$$
$$\times\left\{\sum_{h=1}^{p-1}(-1)^h\exp\left(\frac{-rh}{p}\right)\right\}\left\{\sum_{d=1}^{p-1}(-1)^d\exp\left(\frac{-sd}{p}\right)\right\}. \quad (3)$$

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 (3) and Lemma 1, we have

$$\begin{aligned}\left|\sum_{x=1}^{p}(-1)^{x+(cx^m)_p}\chi(x+n)\right| &=\frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{x=1}^{p}\chi(x+n)\exp\left(\frac{rx+scx^m}{p}\right)\right|\\ &\quad\times\left|\sum_{h=1}^{p-1}(-1)^h\exp\left(\frac{-rh}{p}\right)\right|\left|\sum_{d=1}^{p-1}(-1)^d\exp\left(\frac{-sd}{p}\right)\right|\\ &\leqslant\frac{m\sqrt{p}}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\frac{\sin\left(\frac{\pi r}{p}\right)}{\cos\left(\frac{\pi r}{p}\right)}\right|\left|\frac{\sin\left(\frac{\pi s}{p}\right)}{\cos\left(\frac{\pi s}{p}\right)}\right|\\ &\leqslant mT_p^2\sqrt{p}\ln^2 p.\end{aligned}$$

This proves Lemma 3. □

3. Proof of Theorem 1 and Corollary 1

We will use above lemmas to prove Theorem 1 and Corollary 1. Firstly, we make a simple transformation of $\mathscr{F}_{k,m}(n,p)$. In the process of proof, for convenience we let $\mathscr{L}=\mathscr{L}_m(c)$ and let $\mathscr{R}_k=\mathscr{R}_k(p)$. In fact, $|\mathscr{R}_k|=\frac{p-1}{k}$.

From the definition of $\mathscr{F}_{k,m}(n,p)$, we can write

$$\begin{aligned}\mathscr{F}_{k,m}(n,p)&=\sum_{\substack{a=1\\ a\in\mathscr{L}\\ a+b\equiv n(\bmod p)}}^{p-1}\sum_{\substack{b=1\\ b\in\mathscr{R}_k}}^{p-1}1\\ &=\frac{1}{p}\sum_{h=1}^{p}\exp\left(\frac{-nh}{p}\right)\sum_{\substack{a=1\\ a\in\mathscr{L}}}^{p-1}\exp\left(\frac{ah}{p}\right)\sum_{\substack{b=1\\ b\in\mathscr{R}_k}}^{p-1}\exp\left(\frac{bh}{p}\right)\end{aligned}$$

$$\begin{aligned}&=\frac{(p-1)^2}{2kp}+\frac{1}{p}\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\sum_{\substack{a=1\\a\in\mathscr{L}}}^{p-1}\exp\left(\frac{ah}{p}\right)\sum_{\substack{b=1\\b\in\mathscr{R}_k}}^{p-1}\exp\left(\frac{bh}{p}\right)\\&\quad-\frac{p-1}{2kp}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\\&=\frac{(p-1)^2}{2kp}+E(n,p).\end{aligned}\tag{4}$$

Next, we estimate the error term $E(n,p)$. Let χ_k denote a Dirichlet character modulo p with order k, we have

$$\begin{aligned}&E(n,p)\\&=\frac{1}{2p}\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\sum_{a=1}^{p-1}\left(1-(-1)^{a+(ca^m)_p}\right)\exp\left(\frac{ah}{p}\right)\sum_{\substack{b=1\\b\in\mathscr{R}_k}}^{p-1}\exp\left(\frac{bh}{p}\right)\\&\quad-\frac{p-1}{2kp}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\\&=\frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\sum_{a=1}^{p-1}\left(1-(-1)^{a+(ca^m)_p}\right)\exp\left(\frac{ah}{p}\right)\\&\quad\times\sum_{b=1}^{p-1}\left(1+\chi_k(b)+\chi_k^2(b)+\cdots+\chi_k^{k-1}(b)\right)\exp\left(\frac{bh}{p}\right)-\frac{p-1}{2kp}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\\&=-\frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-hn}{p}\right)\sum_{b=1}^{p-1}\sum_{i=1}^{k-1}\chi_k^i(b)\exp\left(\frac{bh}{p}\right)\\&\quad-\frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-hn}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+(cx^m)_p}\exp\left(\frac{ah}{p}\right)\sum_{b=1}^{p-1}\sum_{i=1}^{k-1}\chi_k^i(b)\exp\left(\frac{bh}{p}\right)\\&\quad+\frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-hn}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\exp\left(\frac{ah}{p}\right)\\&\quad+\frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-hn}{p}\right)-\frac{p-1}{2kp}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\\&:=-\Sigma_1-\Sigma_2+\Sigma_3+\Sigma_4-\Sigma_5.\end{aligned}\tag{5}$$

Now, we calculate each term in (5). For Σ_1, we have

$$\begin{aligned}|\Sigma_1|&=\frac{1}{2kp}\left|\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\sum_{b=1}^{p-1}\sum_{i=1}^{k-1}\chi_k^i(b)\exp\left(\frac{bh}{p}\right)\right|\\&=\frac{1}{2kp}\left|\sum_{i=1}^{k-1}\tau(\chi_k^i)\sum_{h=1}^{p-1}\overline{\chi}_k^i(h)\exp\left(\frac{-nh}{p}\right)\right|\end{aligned}$$

$$= \frac{1}{2kp}\left|\sum_{i=1}^{k-1}\chi_k^i(n)\tau(\chi_k^i)\overline{\tau}(\chi_k^i)\right|$$
$$\leqslant \frac{k-1}{2k}, \tag{6}$$

where $\tau(\chi_k^i)=\sum_{b=1}^{p-1}\chi_k^i(b)\exp\left(\frac{b}{p}\right)$ is Gauss sums and we know that $\tau(\chi_k^i)\overline{\tau}(\chi_k^i)=p$.

For Σ_2, we can write

$$\Sigma_2 = \frac{1}{2kp}\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\exp\left(\frac{ah}{p}\right)\sum_{b=1}^{p-1}\sum_{i=1}^{k-1}\chi_k^i(b)\exp\left(\frac{bh}{p}\right)$$
$$= \frac{1}{2kp}\sum_{h=1}^{p}\exp\left(\frac{(a+b-n)h}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\sum_{b=1}^{p-1}\sum_{i=1}^{k-1}\chi_k^i(b)$$
$$= \frac{1}{2k}\sum_{i=1}^{k-1}\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\chi_k^i(n-a).$$

From Lemma 3, we also have

$$|\Sigma_2| \leqslant \frac{1}{2k}\sum_{i=1}^{k-1}\left|\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\chi_k^i(n-a)\right|$$
$$\leqslant \frac{1}{2k}\sum_{i=1}^{k-1}\left|\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\chi_k^i(a-n)\right|$$
$$\leqslant \frac{m(k-1)}{2k}T_p^2\sqrt{p}\ln^2 p, \tag{7}$$

and

$$|\Sigma_3| = \frac{1}{2kp}\left|\sum_{h=1}^{p}\exp\left(\frac{(a-n)h}{p}\right)\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p} - \sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\right|$$
$$\leqslant \frac{1}{2k}\left|(-1)^{n+(cn^m)_p}\right| + \frac{1}{2kp}\left|\sum_{a=1}^{p-1}(-1)^{a+(ca^m)_p}\right|$$
$$< \frac{1}{k}, \tag{8}$$

$$|\Sigma_4| = \frac{1}{2kp}\left|\sum_{h=1}^{p-1}\exp\left(\frac{-nh}{p}\right)\right| < \frac{1}{2k}. \tag{9}$$

Let χ be the principal character in Lemma 3, we also have

$$|\Sigma_5| < \frac{p-1}{2kp}\left|\sum_{\substack{a=1\\a\neq n}}^{p-1}(-1)^{a+(ca^m)_p}\right| + \frac{1}{2k} < \frac{m}{2k}T_p^2\sqrt{p}\ln^2 p + \frac{1}{2k}. \tag{10}$$

So, combining (5)-(9) we have

$$|E(n,p)| < \frac{m}{2} T_p^2 \sqrt{p} \ln^2 p + 2. \tag{11}$$

From (4) and (11), we immediately get

$$\left| \mathscr{F}_{k,m}(n,p) - \frac{p-1}{2k} \right| < \frac{m}{2} T_p^2 \sqrt{p} \ln^2 p + 2.$$

This completes the proof of Theorem 1.

For Corollary 1 we also have a brief proof. If $\mathscr{F}_{k,m}(n,p) > 0$ then any given element n of $\mathbb{Z}_p$ can be represented as sum of a m-th Lehmer number and a k-th power residue in $\mathbb{Z}_p$. Such is the case if $p > kmT_p^2 \sqrt{p} \ln^2 p + 4k + 1$. By Lemma 2 and computation, it suffices to have $p > 4(km)^2 \left(\ln(km) + 4\ln\ln(km) + 4\ln^{-1}(km)\right)^4$.

4. Numerical calculation

Using the numerical calculation method, the values of $\mathscr{F}_{k,m}(n,p)$ are respectively calculated for different prime p, when (k,m) is $(2,2)$, $(2,3)$, $(3,2)$, and $(3,3)$. The calculation results are showed in Table 1.

Table 1: *Elements $\mathbb{Z}_p$ which cannot be represented in for different (k,m)*

(k,m)	calculational upper of p	the p corresponding to $\mathbb{Z}_p$ in which some elements cannot be represented	which $n \in \mathbb{Z}_p$ cannot be represented
(2,2)	65536	3	1,2
		5	1
(2,3)	65536	3	1,2,3
		5	5
		13	3,10,13
(3,2)	331776	3	2
		7	1,3
		13	1
(3,3)	100000	3	1,2,3
		7	7
		13	1,2,5,8,11,12
		19	19
		31	2,12,19,29,31

Consider first the case $(k,m) = (2,2)$. Corollary 1 yields $\mathscr{F}_{2,2}(n,p) > 0$, for any prime $p > 61967$. For $p < 61967 < 2^{16}$ computer computations show that $\mathscr{F}_{2,2}(n,p) > 0$ for all $p \geqslant 7$. For $p = 3$ we found that the values 1 and 2 cannot be represented as such a sum, while for $p = 5$, the value 1 cannot be represented.

For $(k,m) = (3,2)$. Corollary 1 yields $\mathscr{F}_{3,2}(n,p) > 0$, for any prime $p > 235163$. For $p < 235163 < 331776$ computer computations show that $\mathscr{F}_{3,2}(n,p) > 0$ for all

$p > 13$. For $p = 7$ we found that the values 1 and 3 cannot be represented as such a sum, while for $p = 13$, the value 1 cannot be represented. For $\mathscr{F}_{2,3}(n,p)$, for $p < 2^{16}$ computer computations show that $\mathscr{F}_{2,3}(n,p) > 0$ for all $p > 13$, and for $\mathscr{F}_{3,3}(n,p)$, for $p < 10^5$ computer computations show that $\mathscr{F}_{3,3}(n,p) > 0$ for all $p > 31$. The prime p and the unrepresentable elements in $\mathbb{Z}_p$ are also showed in Table 1.

Limited by computing power, we have not verified all the prime p for $\mathscr{F}_{k,m}(n,p)$ and the larger k and m. However, from the existing calculation results, we found that, except for very few small numbers, all elements in the residue class ring modulo a given prime p can be represented as sum of sum of a classical m-th Lehmer number and a k-th power residue in $\mathbb{Z}_p$, this gives us room to continue our efforts in theory or calculation.

Algorithm 1 *calculate the k-th power residue $\mathscr{R}_k(p)$ for a prime p and a given k*

Input: Given prime p and k, an empty set $\mathscr{R}_k(p)$;
Output: $\mathscr{R}_k(p)$.

for $n = 0, \cdots, p-1$ **do**
  $b \equiv n^k \bmod p$;
  if $b \notin \mathscr{R}_k(p)$ **then**
    $\mathscr{R}_k(p) = \mathscr{R}_k(p) \cup \{b\}$;
  end if
end for

Algorithm 2 *verify if each element in $\mathbb{Z}_p$ can be represented as sum of a classical m-th Lehmer number and a k-th power residue in $\mathbb{Z}_p$.*

Input: Given prime p and k, m. Calculate the set $\mathscr{R}_k(p)$ using Algorithm 1;
Output: S.

for $i = 1 : length(\mathscr{R}_k(p))$ **do**
  $a \equiv n - B(i) \bmod p$;
  $temp = a^m \bmod p$;
  if $a + temp$ cannot divide by 2 **then**
    put n into set S;
  end if
end for

Analysis of algorithm time complexity: For a given prime p, algorithm 2 includes two-layer cycle, the outer cycle needs p cycles, and the inner needs $(p-1)/k$ which is the number of k-th power residues modulo p, so the total number of cycles is about $p(p-1)/k$.

Inside the cycle, execute statement include three times of modulo operation, one subtraction and one addition, module operation is actually a division operation, so algorithm 2 needs $3p(p-1)/k$ times division, $2p(p-1)/k$ times addition, the complexity is $O(N^2)$. For a larger prime number, the algorithm would take a lot of time.

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 (11971381, 12371007) and

Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No. 22JSY007).

REFERENCES

[1] J. BOURGAIN, T. COCHRANE, J. PAULHUS, AND C. PINNER, *On the parity of kth powers mod p: A generalization of a problem of Lehmer*, Acta Arith., **147** (2011) 173–203.

[2] T. COCHRANE, C. PINNER, *Using Stepanov's method for exponential sums involving rational functions*, J. Number Theory, **116** (2006) 270–292.

[3] S. D. COHEN AND T. TRUDGAIN, *Lehmer numbers and primitive roots modulo a prime*, J. Number Theory, **203** (2019) 68–91.

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

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

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

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

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

[9] Z. F. XU, *Distribution of the difference of an integer and its m-th power mod n over incomplete intervals*, J. Number Theory, **133** (2013) 4200–4223.

[10] W. P. ZHANG, *On a problem of D. H. Lehmer and its generalization*, Compositio Math., **86** (1993) 307–316.

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

(Received October 17, 2023)

Yongli Su
School of Mathematics, Northwest University
Xi'an, China
e-mail: su_yongli@163.com

Jiankang Wang
School of Mathematics, Northwest University
Xi'an, China
and
Research Center for Number Theory and Its Applications
Northwest University
Xi'an, China
e-mail: wangjiankang@stumail.nwu.edu.cn

Bo Zhang
School of Mathematics, Northwest University
Xi'an, China
e-mail: bobozhang000@163.com

Zhefeng Xu
School of Mathematics, Northwest University
Xi'an, China
and
Research Center for Number Theory and Its Applications
Northwest University
Xi'an, China
e-mail: zfxu@nwu.edu.cn