Distribution of the difference of an integer and its m-th power mod n

Zhefeng Xu (zfxu@nwu.edu.cn)

School of Mathematics, Northwest University

Oct. 13, 2015

Outline

1. Integer and its inverse modulo n
2. D. H. Lehmer problem
3. Integer and its m-th power modulo n

1. Integer and its inverses modulo n

✠ Let $n \geq 3$ be an integer and $0 < a < n$ be an integer with $(a, n) = 1$. We know that there is an unique integer b with $1 \leq b < n$ such that $ab \equiv 1 \pmod{n}$. Integer b, denoted by $\overline{a}$, is called the inverse of a modulo n.

✠ A variety of distribution properties of integers and their inverses modulo n were studied by many authors.

1. Integer and its inverses modulo n

Professor Zhang was the first person to explicitly study the difference of an integer and its inverse mod n.

Theorem 1.1. Wenpeng Zhang, 1995.

For any fixed integer $k \geq 1$

$$\sum_{a=1}^{n}{}' (a - \overline{a})^{2k} = \frac{\phi(n) n^{2k}}{(2k+1)(k+1)} + O\left(4^k n^{\frac{4k+1}{2}} d^2(n) \ln^2 n\right),$$

here $\sum_{a=1}^{n}{}'$ denotes the summation over a from 1 to n with $(a, n) = 1$, $\phi(n)$ is the Euler function and $d(n)$ is the divisor function. □

1. Integer and its inverses modulo n

In fact, for any positive integer c with $(c,n)=1$), let

$$M(n,k,c)=\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv c \bmod n}}^{n}\sideset{}{'}\sum_{b=1}^{n}(a-b)^{2k},$$

Zhang's method gave a same asymptotic formula for $M(n,k,c)$:

$$M(n,k,c)=\frac{\phi(n)n^{2k}}{(2k+1)(k+1)}+O\left(4^k n^{\frac{4k+1}{2}}d^2(n)\ln^2 n\right). \tag{1.1}$$

In 2003, Zhang defined

$$E(c,n)=M(n,1,c)-\frac{1}{6}\phi(n)n^2-\frac{1}{3}n\prod_{p|n}(1-p)$$

and studied the mean square value of the error term $E(c,n)$.

1. Integer and its inverses modulo n

Zhang's following result showed the fact that the error term in (1.1) is the best possible:

Theorem 1.2. Wenpeng Zhang, 2003.

For any integer $n > 2$, there holds

$$\sum_{c=1}^{n}{}' E^2(c,n) = \frac{5}{36}n^3\phi^3(n)\prod_{p^\alpha \| n}\frac{\frac{(p+1)^3}{p(p^2+1)} - \frac{1}{p^{3\alpha-1}}}{1+\frac{1}{p}+\frac{1}{p^2}} + O\left(n^5\exp\left(\frac{4\ln n}{\ln\ln n}\right)\right).$$

- Especially, if $n = p$ is an odd prime,

$$\sum_{c=1}^{p-1} E^2(c,p) = \frac{5}{36}p^6 + O\left(n^5\exp\left(\frac{4\ln p}{\ln\ln p}\right)\right).$$

1. Integer and its inverses modulo n

In 1994, Professor Andrew Granville asked Zhang wether there is a distribution function for $|a-\overline{a}|$. For any constant $0<\delta\leq 1$, Zhang defined

$$S(n,\delta)=\#\{a:1\leq a\leq n,(a,n)=1,|a-\overline{a}|\leq \delta n\}.$$

Theorem 1.3. Wenpeng Zhang, 1996.

There holds an asymptotic formula for $S(n,\delta)$ as follows:

$$S(n,\delta)=\delta(2-\delta)\phi(n)+O\left(n^{\frac{1}{2}}d^2(n)\ln^3 n\right).$$

♠ This asymptotic formula yields, for any positive real number $0<\delta\leq 1$

$$\lim\frac{\#\{a:1\leq a\leq n,(a,n)=1,|a-\overline{a}|\leq \delta n\}}{\phi(n)}=\delta(2-\delta).$$

1. Integer and its inverses modulo n

Mizan R. Khan and I. E. Shparlinski, 2003.

✠ They defined the maximal difference between an integer and its inverse

$$M(n) = \max\{|a - \overline{a}| : 1 \leq a \leq n, (a, n) = 1\},$$

and proved

$$n - M(n) = o\left(n^{\frac{3}{4}+\epsilon}\right)$$

for any $\epsilon > 0$. □

2. D. H. Lehmer problem

Let $n > 2$ be an odd integer and c be an integer coprime to n. For each integer a with $1 \leq b < n$, there is a unique integer b with $1 \leq c < n$ such that $ab \equiv c \pmod{n}$. Let $M(c, n)$ denote the number of solutions of the congruence equation $ab \equiv c \bmod n$ with $1 \leq a,\ b < n$ such that a, b are of opposite parity. D. H. Lehmer posed the problem to find $N(1, p)$ or at least to say something non-trivial about it, see problem F12 of Guy's book "Unsolved problems in number theory". About the D. H. Lehmer problem, Wenpeng Zhang proved:

Theorem 2.1. Wenpeng Zhang, 1992.

For any odd prime p, there holds

$$M(1, p) = \frac{1}{2}p + O\left(p^{\frac{1}{2}} \ln^2 p\right)$$

□

and

2. D. H. Lehmer problem

Theorem 2.2. Wenpeng Zhang, 1994.

For any odd integer $n > 2$, there holds

$$M(1,n) = \frac{\phi(n)}{2} + O\left(n^{\frac{1}{2}} d^2(n) \ln^2 n\right).$$

□

Let $E(c,n) = M(c,n) - \frac{\phi(n)}{2}$, the following result illustrate that the estimate for $E(c,n)$ in Theorem 2.1 and Theorem 2.2 are the best possible:

Theorem 2.3. Wenpeng Zhang, Zongben Xu and Yuan Yi, 2003.

For any odd integer $n > 2$, there holds

$$\sum_{c=1}^{n}{}' E^2(c,n) = \frac{3}{4}\phi^2(n) \prod_{p^\alpha \| n} \frac{\frac{(p+1)^3}{p(p^2+1)} - \frac{1}{p^{3\alpha-1}}}{1+\frac{1}{p}+\frac{1}{p^2}} + O\left(n \exp\left(\frac{4\ln n}{\ln\ln n}\right)\right).$$

□

2. D. H. Lehmer problem

Denote by $M_{\frac{1}{2}}(a,p)$ the number of pairs of integers b,c with $bc \equiv a(\mod p)$, $1 \leq b,c \leq \frac{p-1}{2}$ and with b,c having different parity. The methods of Theorem 2.1 give also the formula:

$$M_{\frac{1}{2}}(1,p) = \frac{1}{8}(p-1) + O\left(p^{\frac{1}{2}}\ln^2 p\right).$$

For any fixed positive integer a with $(a,p)=1$, let

$$E_{\frac{1}{2}}(a,p) = M_{\frac{1}{2}}(1,p) - \frac{1}{8}(p-1).$$

Zhefeng Xu and Wenpeng Zhang studied the mean value of $E_{\frac{1}{2}}(a,p)$ and obtained the following results:

Theorem 2.4. Zhefeng Xu and Wenpeng Zhang, 2006.

- For any odd prime p, there holds

$$\sum_{a=1}^{p-1} E_{\frac{1}{2}}^2(a,p) = \frac{9}{64}p^2 + O\left(p^{1+\epsilon}\right),$$

Theorem 2.5. Zhefeng Xu and Wenpeng Zhang, 2008.

Let p be an odd prime and s be an integer with $0 \le s < \frac{\ln p}{\ln 2}$. Then we have the asymptotic formulae

$$\sum_{a<\frac{p}{4}}\sum_{d<\frac{p}{4}} E(4ad,p) = \frac{-3}{8}p^2 + O(p^{1+\epsilon}),$$

$$\sum_{a<\frac{p}{4}}\sum_{d<\frac{p}{4}} E(8ad,p) = \frac{-3}{4}p^2 + O(p^{1+\epsilon}),$$

$$\sum_{a<\frac{p}{4}}\sum_{d<\frac{p}{4}} E(16ad,p) = \frac{-3}{8}p^2 + O(p^{1+\epsilon})$$

and

$$\sum_{a<\frac{p}{4}}\sum_{d<\frac{p}{4}} E(2^s ad,p) = O_s(p^{1+\epsilon}) \quad \text{if} \quad s \neq 2,3,4.$$

2. D. H. Lehmer problem

From the method of proving Theorem 2.5, one know the main term of the mean value

$$\sum_{a<\frac{p}{4}}\sum_{d<\frac{p}{4}} E(2^s ad, p)$$

is zero when $s \neq 2, 3, 4$. That is to say, the factors $4, 8, 16$ in Theorem 2.5 are necessary. Otherwise, the main term can't be obtained by the method in the proof Theorem 2.5.

- For D. H. Lehmer problem over shorter interval, define

$$M(N, c; p) = \sum_{\substack{a=1 \\ ab\equiv c \bmod p \\ 2\nmid(a+b)}}^{N}\sum_{b=1}^{p-1} 1,$$

where N is a positive integer with $N \leq p-1$.

2. D. H. Lehmer problem

In 1993, Zhiyong Zheng proved that

$$M(N,c;p)=\frac{1}{2}N+O\left(p^{\frac{1}{2}}\ln^2 p\right).$$

Denote

$$E(N,c;p)=M(N,c;p)-\frac{1}{2}N,$$

Yaming Lu and Yuan Yi studied the mean square value of $E(N,c;p)$.

Theorem 2.6 Yaming Lu and Yuan Yi, 2011.

For any positive integer $N\leq p-1$, there holds

$$\begin{aligned}\sum_{c=1}^{p-1}E^2(N,c;p) &= \left(\frac{1}{4}+\frac{4}{9\zeta(3)}\sum_{k=1}^{\infty}\frac{1}{(2k+1)^2}\sum_{a=0}^{k}\frac{1}{2a+1}\right)pN\\ &\quad +O\left(p\ln^2 N+N^2p^{\epsilon}\right).\end{aligned}$$

2. D. H. Lehmer problem

✠ It is clear that Theorem 2.6 is nontrivial if $p^{\epsilon} < N < p^{1-\epsilon}$, thus it is not a generalization of Theorem 2.3 when $n = p$.

✠ Many scholars generalized the D. H. Lehmer problem from other directions.

♠ In 2001, C. Cobeli and A. Zaharescu generalized the Lehmer problem to a more general irreducible curve defined mod p and instead of the parity conditions on the coordinates by some more general congruence conditions.

♠ In 2009 and 2011, Yaming Lu, Ping Xi and Yuan Yi generalized the condition $2 \nmid a + b$ to the condition $k \nmid (a + b)$ and $(a + b, k) = l$ for any positive integer k and l with $l|k$.

2. D. H. Lehmer problem

♠ In 2006, E. Alkan, F. Stan and A. Zaharescu generalized the classical Lehmer problem to high-dimensional Lehmer problem and studied the distribution of the so-called Lehmer-k tuples.

♠ In 2009, I. E. Shparlinski improved the results of E. Alkan etc., and studied the distribution of the Lehmer-k tuples in more general boxes.

♠ In 2013, Zhefeng Xu and Tianping Zhang studied the high-dimensional D. H. Lehmer problem over incomplete intervals.

2. D. H. Lehmer problem

Let k be a positive integer and n a nonnegative integer, $0 < \lambda_1, \cdots, \lambda_{k+1} \leq 1$ be real numbers and $\mathbf{w} = (\lambda_1, \lambda_2, \cdots, \lambda_{k+1})$. Let $q \geq \max\left\{\left[\frac{1}{\lambda_i}\right] : 1 \leq i \leq k+1\right\}$ be a positive integer, and a an integer coprime to q. A natural problem is to calculate the number of $(b_1, \cdots, b_k)$ with $b_1 \cdots b_k c \equiv a \pmod{q}$, $1 \leq b_i \leq \lambda_i q (i = 1, \cdots, k)$, $1 \leq c \leq \lambda_{k+1} q$ and $2 \nmid (b_1 + \cdots + b_k + c)$. Define

$$N(a, k, \mathbf{w}, q, n) = \sum_{\substack{b_1=1 \\ b_1 \cdots b_k c \equiv a (\mod q) \\ 2 \nmid (b_1 + \cdots + b_k + c)}}^{[\lambda_1 q]}{}' \cdots \sum_{b_k=1}^{[\lambda_k q]}{}' \sum_{c=1}^{[\lambda_{k+1} q]}{}' (b_1 \cdots b_k - c)^{2n}.$$

2. D. H. Lehmer problem

Let k be a positive integer and n a nonnegative integer, $0 < \lambda_1, \cdots, \lambda_{k+1} \leq 1$ be real numbers and $\mathbf{w} = (\lambda_1, \lambda_2, \cdots, \lambda_{k+1})$. Let $q \geq \max\left\{\left[\frac{1}{\lambda_i}\right] : 1 \leq i \leq k+1\right\}$ be a positive integer, and a an integer coprime to q. A natural problem is to calculate the number of $(b_1, \cdots, b_k)$ with $b_1 \cdots b_k c \equiv a \pmod{q}$, $1 \leq b_i \leq \lambda_i q (i = 1, \cdots, k), 1 \leq c \leq \lambda_{k+1} q$ and $2 \nmid (b_1 + \cdots + b_k + c)$. Define

$$N(a, k, \mathbf{w}, q, n) = \sum_{b_1=1}^{[\lambda_1 q]}{}' \cdots \sum_{b_k=1}^{[\lambda_k q]}{}' \sum_{\substack{c=1 \\ b_1 \cdots b_k c \equiv a (\mod q) \\ 2 \nmid (b_1 + \cdots + b_k + c)}}^{[\lambda_{k+1} q]}{}' (b_1 \cdots b_k - c)^{2n}.$$

2. D. H. Lehmer problem

By using the properties of trigonometric sum and the estimates of n-dimensional Kloosterman sum, they proved an asymptotic formula for $N(a,k,\mathbf{w},q,n)$ as follows:

Theorem 2.7. Zhefeng Xu and Tianping Zhang, 2013.

For $a,k,\mathbf{w},q,n$ defined as above, there holds

$$N(a,k,\mathbf{w},q,n)=C(k,\mathbf{w},n)\phi^k(q)q^{2kn}+O\left(4^{n\varepsilon_k}q^{(2n+1)k-\frac{1}{2}}d^2(q)\ln^2 q\right),$$

where

$$C(k,\mathbf{w},n)=\begin{cases}\dfrac{(\lambda_1\cdots\lambda_k)^{2n+1}\lambda_{k+1}}{2(2n+1)^k}, & \text{if } k\geq 2;\\ \dfrac{\lambda_1^{2n+2}+\lambda_2^{2n+2}-(\lambda_1-\lambda_2)^{2n+2}}{4(n+1)(2n+1)}, & \text{if } k=1\end{cases}$$

and $\varepsilon_k=\frac{1}{2}\left(1-(-1)^{\left[\frac{1}{k}\right]}\right)$. □

2. D. H. Lehmer problem

By using the properties of trigonometric sum and the estimates of n-dimensional Kloosterman sum, we proved an asymptotic formula for $N(a,k,\mathbf{w},q,n)$ as follows:

Theorem 2.7. Zhefeng Xu and Tianping Zhang, 2013.

For $a,k,\mathbf{w},q,n$ defined as above, there holds

$$N(a,k,\mathbf{w},q,n)=C(k,\mathbf{w},n)\phi^k(q)q^{2kn}+O\left(4^{n\varepsilon_k}q^{(2n+1)k-\frac{1}{2}}d^2(q)\ln^2 q\right),$$

where

$$C(k,\mathbf{w},n)=\begin{cases}\dfrac{(\lambda_1\cdots\lambda_k)^{2n+1}\lambda_{k+1}}{2(2n+1)^k}, & \text{if } k\geq 2;\\ \dfrac{\lambda_1^{2n+2}+\lambda_2^{2n+2}-(\lambda_1-\lambda_2)^{2n+2}}{4(n+1)(2n+1)}, & \text{if } k=1\end{cases}$$

and $\varepsilon_k=\frac{1}{2}\left(1-(-1)^{\left[\frac{1}{k}\right]}\right)$. □

2. D. H. Lehmer problem

Taking $n = 0$ and $\mathbf{w} = \mathbf{1/2} = (\frac{1}{2}, \frac{1}{2}, \cdots, \frac{1}{2})$ in Theorem 2.7, we can get the following result about the high-dimensional D. H. Lehmer problem over half intervals:

Corollary 2.8.

For any nonnegative integer n,

$$N(a, k, \mathbf{1/2}, q, 0) = \frac{\phi^k(q)}{2^{k+2}} + O\left(q^{k-\frac{1}{2}} d^2(q) \ln q\right).$$

□

✠ By using the method of character sums and the properties of Dirichlet L-functions, the power of q in the error term in Corollary 2.8 can be improved from $k - \frac{1}{2}$ to $\frac{k}{2}$ in the case $2 \nmid q$. Let $N_{\frac{1}{2}}(a, k, q)$ denotes $N(a, k, \mathbf{w}, q, 0)$ for the case $\mathbf{w} = \left(\frac{1}{2}, \frac{1}{2}, \cdots, \frac{1}{2}\right)$.

Theorem 2.9. Zhefeng Xu and Tianping Zhang, 2013.

Let $q > 2$ be an odd integer and a coprime to q. Then for any positive integer k with $(q, k(k+1)) = 1$, we have the asymptotic formula

$$N_{\frac{1}{2}}(a, k, q) = \frac{\phi^k(q)}{2^{k+2}} + O\left(2^{k^2+3k+2} q^{\frac{k}{2}} d(q) (2^{k+2}k)^{\omega(q)} \ln^{k+1} q\right).$$

□

We also showed the error term in Theorem 2.9 is close to the best possible by studying the mean square value of the error term for the case $q = p^\alpha$. For $m > 0$, the error term in Theorem 2.7 is not the best possible.

2. D. H. Lehmer problem

In 2015, to improve the related results in Theorem 2.7, Tianping Zhang and Zhefeng Xu studied a more general mean value. Let $a, k, \mathbf{w}, q, n$ defined as above, for positive integer t with $t \leq k$, define

$$N(a,k+1,t,\mathbf{w},q,m) = \sideset{}{'}\sum_{b_1=1}^{[\lambda_1 q]}\sideset{}{'}\sum_{b_2=1}^{[\lambda_2 q]}\cdots\sideset{}{'}\sum_{b_{k+1}=1}^{[\lambda_{k+1} q]}(b_1\cdots b_t - b_{t+1}\cdots b_{k+1})^m.$$

$$b_1 b_2 \cdots b_{k+1} \equiv a \pmod{q}$$

$$2 \nmid (b_1 + b_2 + \cdots + b_{k+1})$$

Theorem 2.10. Tianping Zhang and Zhefeng Xu, 2015.

For any positive integer m, we have the asymptotic formulae

$$\begin{aligned} & N(a,k+1,t,\mathbf{w},q,m) \\ = & \begin{cases} A\phi^k(q)q^{mt}+O\left(q^{mt+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t>\frac{k+1}{2}, \\ B\phi^k(q)q^{m(k-t+1)}+O\left(q^{m(k-t+1)+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t<\frac{k+1}{2}, \\ D\phi^k(q)q^{mt}+O\left(2^m q^{mt+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t=\frac{k+1}{2}, \end{cases} \end{aligned}$$

where

$$A=\frac{(\lambda_1\cdots\lambda_t)^{m+1}(\lambda_{t+1}\cdots\lambda_{k+1})}{2(m+1)^t},$$

$$B=\frac{(-1)^m(\lambda_1\cdots\lambda_t)(\lambda_{t+1}\cdots\lambda_{k+1})^{m+1}}{2(m+1)^{k-t+1}},$$

$$D=\sum_{j=0}^{m}C_m^j(-1)^j\frac{(\lambda_1\cdots\lambda_t)^{m-j+1}(\lambda_{t+1}\cdots\lambda_{k+1})^{j+1}}{2((m-j+1)(j+1))^{\frac{k+1}{2}}}.$$

Theorem 2.10. Tianping Zhang and Zhefeng Xu, 2015.

For any positive integer m, we have the asymptotic formulae

$$\begin{aligned} & N(a,k+1,t,\mathbf{w},q,m) \\ = & \begin{cases} A\phi^k(q)q^{mt}+O\left(q^{mt+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t>\frac{k+1}{2}, \\ B\phi^k(q)q^{m(k-t+1)}+O\left(q^{m(k-t+1)+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t<\frac{k+1}{2}, \\ D\phi^k(q)q^{mt}+O\left(2^m q^{mt+k-\frac{1}{2}}d^2(q)\ln q\right), & \text{if} \quad t=\frac{k+1}{2}, \end{cases} \end{aligned}$$

where

$$A=\frac{(\lambda_1\cdots\lambda_t)^{m+1}(\lambda_{t+1}\cdots\lambda_{k+1})}{2(m+1)^t},$$

$$B=\frac{(-1)^m(\lambda_1\cdots\lambda_t)(\lambda_{t+1}\cdots\lambda_{k+1})^{m+1}}{2(m+1)^{k-t+1}},$$

$$D=\sum_{j=0}^{m}C_m^j(-1)^j\frac{(\lambda_1\cdots\lambda_t)^{m-j+1}(\lambda_{t+1}\cdots\lambda_{k+1})^{j+1}}{2((m-j+1)(j+1))^{\frac{k+1}{2}}}.$$

2. D. H. Lehmer problem

Suppose there exist at least one j with $1 \le j \le k+1$ such that $\lambda_j = 1$, some stronger error terms can be obtained for $N(a, k+1, t, \mathbf{w}, q, m)$

Theorem 2.11. Tianping Zhang and Zhefeng Xu, 2015.

For any nonnegative integer m, we have

$$\begin{aligned} & N(a, k+1, t, \mathbf{w}, q, m) \\ = \ & \frac{1}{2} \prod_{u=1}^{t} \sigma_m(\lambda_u, q) \prod_{\substack{v=t+1 \\ v \neq j}}^{k+1} \sigma_0(\lambda_v, q) + O\left(q^{2k+(m-2)t+1}\right) \\ & + O\left(q^{mt+\frac{k}{2}} d_{k+1}(q) \ln^{k+1} q\right) \qquad \text{if} \qquad \frac{k+1}{2} < t < j, \end{aligned}$$

$$
\begin{aligned}
& N(a, k+1, t, \mathbf{w}, q, m) \\
= \quad & \frac{(-1)^m}{2} \prod_{\substack{u=1 \\ u \neq j}}^{t} \sigma_0(\lambda_u, q) \prod_{v=t+1}^{k+1} \sigma_m(\lambda_v, q) + O\left(q^{m(k-t+1)+\frac{k}{2}}\right) \\
& + O\left(q^{m(k-t+1)+2t-1}\right) \qquad \text{if} \qquad j < t < \frac{k+1}{2},
\end{aligned}
$$

□

and

$$
\begin{aligned}
& N(a,k+1,t,\mathbf{w},q,m) \\
= \quad & \frac{1}{2}\left(\prod_{u=1}^{\frac{k+1}{2}}\sigma_m(\lambda_u,q)\prod_{\substack{v=\frac{k+3}{2}\\ v\neq j}}^{k+1}\sigma_0(\lambda_v,q)-\phi^k(q)q^{\frac{m(k+1)}{2}}\right) \\
& +O\left(2^m q^{\frac{m(k+1)}{2}+k-\frac{1}{2}}d^2(q)\ln q\right) \qquad \text{if} \qquad t=\frac{k+1}{2}<j,
\end{aligned}
$$

where $\sigma_m(\lambda_l,q)=\sum_{a=1}^{[\lambda_l q]}{}' a^m=\frac{u^{m+1}}{m+1}\frac{\phi(q)}{q}+O\left(u^m 2^{\omega(q)}\right)$. □

3. Integer and its m-th power mod n

In this section, we consider a similar problem which concerned the distribution of the difference between an integer and its m-th power modulo n over incomplete intervals, where $m \geq 2$ be an integer.
Let λ, δ be any real numbers with $0 < \lambda, \delta \leq 1$. For any integer a, denote by $(a)_n$ the integer b with $1 \leq b \leq n$ such that $b \equiv a \pmod{n}$. Define

$$S_{m,n,\lambda,\delta} = \{a : 1 \leq a \leq \lambda n, (a,n) = 1, |a - (a^m)_n| \leq \delta n\}.$$

Under this symbol, Theorem 1.3 can be written as

$$\#S_{\phi(n)-1,n,1,\delta} = \delta(2-\delta)\phi(n) + O\left(n^{\frac{1}{2}} d^2(n) \ln^3 n\right).$$

For any nonnegative real number k, we studied asymptotic distribution for the quantity

$$\sum_{a \in S_{m,n,\lambda,\delta}} |a - (a^m)_n|^k.$$

3. Integer and its m-th power mod n

Theorem 3.1. Zhefeng Xu, 2013.

Let λ, δ, n, m, k be defined as above and P the parallelogram with vertices $(0, -\delta)$, $(\lambda, \lambda - \delta)$, $(\lambda, \lambda + \delta)$ and $(0, \delta)$, then we have the asymptotic formula

$$\begin{aligned} & \frac{1}{\phi(n)} \sum_{a \in S_{m,n,\lambda,\delta}} \left| \frac{a - (a^m)_n}{n} \right|^k \\ = & \iint\limits_{P \bigcap [0,1]^2} |x - y|^k dx dy + O_{\delta,\lambda,k} \left(\frac{m^{\omega(n)+\frac{1}{2}} \sqrt{n} d(n) \ln^3 n}{\phi(n)} \right), \end{aligned}$$

where $\omega(n)$ denotes the number of different prime factors of n. □

Remark 3.2.

In fact, one can easily get the exact value of the double integration in our theorem as follows

$$\iint\limits_{P\bigcap[0,1]^2} |x-y|^k dxdy$$

$$= \begin{cases} \left(\frac{2\lambda}{k+1}-\frac{\delta}{k+2}\right)\delta^{k+1}, & \text{if } \lambda+\delta\leq 1 \text{ and } \delta<\lambda\ ; \\ \frac{(k+2)\lambda\delta^{k+1}+\lambda^{k+2}}{(k+1)(k+2)}, & \text{if } \lambda+\delta\leq 1 \text{ and } \delta\geq\lambda; \\ \frac{(k+2)(1+\lambda)\delta^{k+1}-2(k+1)\delta^{k+2}-(1-\lambda)^{k+2}}{(k+1)(k+2)}, & \text{if } \lambda+\delta>1 \text{ and } \delta<\lambda; \\ \frac{(k+2)\delta^{k+1}-(k+1)\delta^{k+2}+\lambda^{k+2}-(1-\lambda)^{k+2}}{(k+1)(k+2)}, & \text{if } \lambda+\delta>1 \text{ and } \delta\geq\lambda. \end{cases}$$

3. Integer and its m-th power mod n

As an example, we take $m = 2$, $\lambda = 1$, $k = 1$ and $n = p$ a prime. Then we get a distribution formula for the difference between an integer and its square modulo p as following

Corollary 3.3.

Let $\delta \in (0, 1]$ be real constant and $p > \left[\frac{1}{\delta}\right]$ a prime. Then we have the asymptotic formula

$$\sum_{a \in S_{2,p,1,\delta}} |a - (a^2)_n| = \left(\delta^2 - \frac{2\delta^3}{3}\right) p^2 + O_\delta\left(p^{\frac{3}{2}} \ln^3 p\right).$$

3. Integer and its m-th power mod n

Specially, taking $k = 0$ in Theorem 3.1, we get an asymptotic formula for the cardinality of $S_{m,n,\lambda,\delta}$ in following

Corollary 3.4.

$$\#S_{m,n,\lambda,\delta} = \phi(n)A_{P\bigcap[0,1]^2} + O_{\delta,\lambda}\left(m^{\omega(n)+\frac{1}{2}}n^{\frac{1}{2}}d(n)\ln^3 n\right),$$

where $A_{P\bigcap[0,1]^2}$ denotes the area of $P\bigcap[0,1]^2$, and one can easily get

$$A_{P\bigcap[0,1]^2} = \begin{cases} 2\lambda\delta - \frac{\delta^2}{2}, & \text{if } \lambda+\delta \leq 1 \text{ and } \delta < \lambda\ ; \\ \lambda\delta + \frac{\lambda^2}{2}, & \text{if } \lambda+\delta \leq 1 \text{ and } \delta \geq \lambda; \\ (1+\lambda)\delta - \delta^2 - \frac{(1-\lambda)^2}{2}, & \text{if } \lambda+\delta > 1 \text{ and } \delta < \lambda; \\ \delta+\lambda - \frac{\delta^2+1}{2}, & \text{if } \lambda+\delta > 1 \text{ and } \delta \geq \lambda. \end{cases}$$

3. Integer and its m-th power mod n

The following corollary gives some limit formulas:

Corollary 3.5.

Let ϵ be any positive constant. Then for $m^{\omega(n)+\frac{1}{2}} \ll n^{\frac{1}{2}-\epsilon}$, we have the limits

$$\lim_{n\to\infty} \frac{\#\{a : 1 \le a \le \lambda n, (a,n) = 1, |a - (a^m)_n| \le \delta n\}}{\phi(n)} = A_{P\bigcap[0,1]^2}.$$

For the special case $\lambda = 1$, there holds

$$\lim_{n\to\infty} \frac{\#\{a : 1 \le a < n, (a,n) = 1, |a - (a^m)_n| < \delta n\}}{\phi(n)} = \delta(2-\delta).$$

3. Integer and its m-th power mod n

Note.

Our Theorem 3.1 is nontrivial for $m^{\omega(n)+\frac{1}{2}} \ll n^{\frac{1}{2}-\epsilon}$, here ϵ denotes a arbitrary small positive number. So one can not obtain a corresponding result for the case $m = \phi(n) - 1$ from Theorem 3.1 due to an upper bound estimation of the two-term exponential sum,

$$\left| \sum_{\substack{x=1 \\ p \nmid x}}^{p^\alpha} e\left(\frac{ax^m + bx}{p^\alpha}\right) \right| \leq \begin{cases} mp^{\frac{\alpha}{2}+\frac{1}{2}}, & \text{if } m = p > 2, \alpha \geq 3 \text{ and } p \| b; \\ mp^{\frac{\alpha}{2}}, & \text{otherwise} \end{cases}$$

with $p \nmid (a, b)$ and $\alpha \geq 1$, which was used in the proof of Theorem 3.1. To improve the error term, we need a better bound for the two-term exponential sums. Of course, one can get a corresponding result for the case $m = \phi(n) - 1$ by using the bound for Kloosterman sums.

3. Integer and its m-th power mod n

✠ In 2011, for any integer m, J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner studied a general Lehmer problem about the parity of an integer and its m-th power modulo an odd prime p. Let E and O be 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 any integer c with $p \nmid c$ they defined

$$N_m(c) = \#\{x \in E : cx^m \in O\}$$

and

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

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

and

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

Theorem 3.6. J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner, 2011.

For any odd prime p and positive integer $m \ge 2$, there holds

$$\left| N_m(c) - \frac{p}{4} \right| \le \frac{1}{\pi} \Phi'(m) \min\left\{ \ln\left(\frac{356p}{\Phi'(m)}\right), \ln(5p) \right\}$$

and

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

□

Distribution of the difference of an integer and its m-th power mod n

✠ Now we consider the integer and its m-th power modulo n which are of opposite parity. We call this kind of integer the generalized D. H. Lehmer number. Our main purpose is to study the asymptotic properties of the higher power mean of difference between a generalized D. H. Lehmer number and its m-th power modulo n. Let $\lambda \in (0, 1]$ be any real constant, $n > \left[\frac{1}{\lambda}\right]$ and $m \geq 2$ be integers. For any nonnegative integer k, define

$$\Xi_k(\lambda, m; n) = \sideset{}{'}\sum_{\substack{a=1 \\ 2\nmid\left(a+(a^m)_n\right)}}^{[\lambda n]} \left|a - (a^m)_n\right|^k.$$

Distribution of the difference of an integer and its m-th power mod n

By using the similar methods as proving Theorem 3.1, we proved the following result:

Theorem 3.7. Zhefeng Xu, 2015.

Let λ, n, m defined as above. For any fixed nonnegative integer k, we have the asymptotic formula

$$\begin{aligned}\Xi_k(\lambda, m; n) &= \left(1+\lambda^{k+2}-(1-\lambda)^{k+2}\right)\frac{\phi(n)n^k}{(2k+2)(k+2)} \\ &\quad +O_{\lambda,k}\left(n^{k+\frac{1}{2}}m^{\omega(n)+\frac{1}{2}}d(n)\ln^2 n\right).\end{aligned}$$

□

Distribution of the difference of an integer and its m-th power mod n

Taking $\lambda = 1$, we get the following

Corollary 3.8.

For any fixed nonnegative integer k, we have the asymptotic formula

$$\begin{aligned} & \sum_{\substack{a=1 \\ 2\nmid\left(a+(a^m)_n\right)}}^{n}{}' \left|a-(a^m)_n\right|^k \\ = \ & \frac{\phi(n)n^k}{(k+1)(k+2)} + O_k\left(n^{k+\frac{1}{2}} m^{\omega(n)++\frac{1}{2}} d(n)\ln^2 n\right). \end{aligned}$$

Distribution of the difference of an integer and its m-th power mod n

For concise, taking $k = 1$, $n = p$ an odd prime, and $\lambda = \frac{1}{2}$, we can get the following result:

Corollary 3.9.

For any odd prime p and integer $m \geq 2$, we have

$$\sum_{\substack{a=1 \\ 2\nmid\left(a+(a^m)_p\right)}}^{\frac{p-1}{2}}{}' \left|a - (a^m)_p\right| = \frac{p^2}{12} + O\left((mp)^{\frac{3}{2}} \ln^2 p\right).$$

Distribution of the difference of an integer and its m-th power mod n

Taking $k = 0$ in Theorem 1, we can get following distribution of the number of the generalized D. H. Lehmer number in the interval $[1, [\lambda n]]$:

Corollary 3.10.

Let ϵ be any positive constant. Then for $m^{\omega(n)+\frac{1}{2}} \ll n^{\frac{1}{2}-\epsilon}$, we have the limits

$$\begin{aligned} & \lim_{n\to\infty} \frac{\#\{a : 1 \le a \le \lambda n, (a,n) = 1, 2 \nmid (a + (a^m)_n)\}}{\phi(n)} \\ = \quad & \frac{1}{4}\left(1 + \lambda^2 - (1-\lambda)^2\right). \end{aligned}$$

Distribution of the difference of an integer and its m-th power mod n

Because Theorem 3.7 is nontrivial for $m^{\omega(n)} \ll n^{\frac{1}{2}-\epsilon}$, so we can not obtain the corresponding result for the case $m = \phi(n) - 1$, the case of the classical D. H. Lehmer number, from Theorem 3.7 directly. For the case $m = \phi(n) - 1$, by using the same method of proving Theorem 3.7 and the estimation for Kloosterman sum

$$\left| \sum_{x=1}^{n}{}' e\left(\frac{a\overline{x} + bx}{n}\right) \right| \leq n^{\frac{1}{2}} d(n)(a, b, n)^{\frac{1}{2}},$$

we can get the following result:

Distribution of the difference of an integer and its m-th power mod n

Theorem 3.11. Zhefeng Xu , 2015.

For any real constants $\lambda \in (0,1]$, let $n > \left[\frac{1}{\lambda}\right]$ be an odd integer. Then for any fixed nonnegative integer k, there holds

$$\sum_{\substack{a=1 \\ 2\nmid(a+\overline{a})}}^{[\lambda n]}{}' |a-\overline{a}|^k = \left(1+\lambda^{k+2}-(1-\lambda)^{k+2}\right)\frac{\phi(n)n^k}{(2k+2)(k+2)}$$

$$+O_{\lambda,k}\left(n^{k+\frac{1}{2}}d^2(n)\ln^2 n\right).$$

Thank you!