

Some Results and Problems on the Diophantine Equations

Sun Qi

(Institute of Math., Sichuan University, Chengdu)

1. On Diophantine equations  $x_1^{x_1} x_2^{x_2} \dots x_k^{x_k} = z^z$

Erdős asked for integer solutions of the equation

$$x^x y^y = z^z \quad (1)$$

with  $x > 1, y > 1$ . In 1940, Ko Chao<sup>[1]</sup> proved that when  $(x, y) = 1$ , equation (1) has no solutions in positive integers  $x > 1, y > 1, z > 1$  and when  $(x, y) \neq 1$ , equation (1) has infinitely many solutions

$$\begin{aligned} x &= 2^{2^{n+1}(2^n - n - 1) + 2n} (2^n - 1)^{2(2^n - 1)} \\ y &= 2^{2^{n+1}(2^n - n - 1)} (2^n - 1)^{2(2^n - 1) + 2} \\ z &= 2^{2^{n+1}(2^n - n - 1) + n + 1} (2^n - 1)^{2(2^n - 1) + 1} \end{aligned}$$

$n > 1$ , with  $4xy = z$ . Other solutions have not been found yet. Recently, Erdős pointed out that it is possible that these should be all the solutions of the equation (1).

In 1984, Uchiyama<sup>[(内山) [2]]</sup> proved that there can only be a finite number of solutions for any fixed value of  $Q = xy/z < \frac{1}{4}$ .

Anderson conjectured that the equation  $w^w x^x y^y = z^z$  has no solution with  $1 < w < x < y$ .

In 1964, Ko Chao and Sun Qi<sup>[3]</sup> proved the equation

$$\prod_{i=1}^k x_i^{x_i} = z^z, \quad x_i > 1, k \geq 2, i = 1, \dots, k,$$

has infinitely many solutions

$$\begin{aligned}
 x_1 &= k^{k^n(k^{n+1}-2n-k)+2n} (k^n-1)^{2(k^n-1)} \\
 x_2 &= k^{k^n(k^{n+1}-2n-k)} (k^n-1)^{2(k^n-1)+2} \\
 x_3 &= \dots = x_k = k^{k^n(k^{n+1}-2n-k)+n} (k^n-1)^{2(k^n-1)+1} \\
 z &= k^{k^n(k^{n+1}-2n-k)+n+1} (k^n-1)^{2(k^n-1)+1}
 \end{aligned}$$

of which the first one is  $x_1=3^{14}2^4$ ,  $x_2=3^{12}2^6$ ,  $x_3=3^{13}2^5$ ,  
 $z=3^{14}2^5$  for  $k=3$ . It gives a counter-example to Anderson's  
 Conjecture.

For  $2 \nmid xy$  are there any solutions of equation (1)? This  
 still remains unproved. For the equation  $x_1^{x_1} x_2^{x_2} x_3^{x_3} = z^z$  we asked  
 that are there any solution with  $1 < x_1 < x_2 < x_3$ ,  $2 \nmid x_1 x_2 x_3$ ?

## 2. Some exponential equations

Jesmanowicz conjectured that the diophantine equation

$$a^x + b^y = c^z$$

has no integer solution except  $x=y=z=2$ , where  $a, b, c$  satisfy  
 $a^2 + b^2 = c^2$ . Ko Chao<sup>[4]-[6]</sup> made a lot of investigations about  
 it in 1958-1965. Lu Wenduan<sup>[7]</sup>, Chen Jingrun<sup>[8]</sup> and Sun Qi<sup>[9]</sup>  
 also have studied this conjecture. For example, Lu proved  
 that if  $a=4n^2-1$ ,  $b=4n$ ,  $c=4n^2+1$ , then Jesmanowicz's con-  
 jecture is true.

For the Diophantine equation

$$a^x + b^y = c^z \quad (2)$$

where  $a, b, c$  are different primes. In 1958-1976, Nagell,  
 Makowski, Hadano, Uchiyama studied this equation. They gave  
 all the solution  $(x, y, z)$  for  $\max(a, b, c) \leq 17$ . In 1984, Sun Qi

and Zhou Xiaoming<sup>[10]</sup> gave all the nonnegative integral solutions of equation (2) for  $\max(a,b,c)=19$ . We proved also that the equation (2) has no solutions in non-negative integers  $x>1, y, z$ , if that  $a=2, b=p, c=q$ , where  $p \equiv 5 \pmod{8}$  or  $p \equiv 1 \pmod{8}$  and  $p=u^2+16v^2, 2 \nmid v$ , and  $q \equiv 3 \pmod{4}, q \equiv 2 \pmod{p}$ .

In 1985, for  $\max(a,b,c)=23$ ,<sup>it</sup> has been solved by Yang Xiaozuo.<sup>[11]</sup>

In 1987, for  $29 \leq \max(a,b,c) < 100$ ,<sup>it</sup> has been solved by Cao Zhenfu.<sup>[12]</sup>

Selfridge asks for what  $a$  and  $b$

$$2^a - 2^b \mid n^a - n^b, \quad (3)$$

is true for all  $n$ ?

Sun Qi and Zhang Mingzhi<sup>[13]</sup> proved that for  $0 \leq b < a$  if and only if  $(a,b)=(1,0), (2,1), (3,1), (4,2), (5,3), (5,1), (6,2), (7,3), (8,4), (8,2), (9,3), (14,2), (15,3), (16,4), (3)$  is true for all  $n$ .

### 3. Some diophantine equations which arise in the combinatorial theory and the theory of finite groups

Hall asked for the integer solution of the Diophantine equation

$$p^r + 2 = q^s \quad (4)$$

which arises in the combinatorial theory, where  $p, q$  are prime numbers. This includes that  $5^2 + 2 = 3^3$ , but we know no other case in which both  $r>1$  and  $s>1$ . Sun Qi and Zhou Xiaoming<sup>[14]</sup> studied the case  $p+2=q$  in (4). Cao Zhenfu<sup>[15]</sup> proved that when  $p+2=q$ , then the equation (4) has no solution for  $r>1, s>1$ .

Crescenzo<sup>[16]</sup> investigated the equation (5) below, which arise in the theory of finite groups.

$$p^m - 2q^n = \pm 1, \quad p, q \text{ primes, } m > 1, n > 1. \quad (5)$$

Crescenzo proved that with the exception of the relation  $(239)^2 - 2(13)^4 = -1$ , every solution of (5) has exponents  $m=n=2$ .

However, it should be noted that Crescenzo's theorem is wrong. Because the equation (5) has another solution  $p=3$ ,  $q=11$ ,  $m=5$ ,  $n=2$ .

For diophantine equation

$$3^m - 2q^n = 1, \quad m > 1, n > 1, q \text{ is an odd prime, } 2 \nmid m, \quad (6)$$

we conjectured that equation (6) has no solution except  $q=11$ ,  $m=5$ ,  $n=2$ .

For equation (6), the proof of following results are easy.

1) If  $2 \mid n$ , then the conjecture is true.

2) If the equation (6) has solution, then  $q \equiv 1 \pmod{12}$ .

3) If the equation (6) has solution then  $\left(\frac{q}{7}\right) = \left(\frac{q}{13}\right) = \left(\frac{q}{757}\right)$

$= 1$ , where  $\left(\frac{a}{q}\right)$  denotes legendre symbol.

Recently, Sun Qi studies further equations (7) and (8) below, which include (4) and (6) respectively.

For diophantine equation

$$a^m - kb^n = 2, \quad k > 0, 2 \nmid k, \quad (7)$$

and diophantine equation

$$a^m - lb^n = 1, \quad l > 0, \quad (8)$$

we proved the following results.

1) If the equation (7) has positive integer solution  $a_1, b_1, m_1, n_1$ , with  $2 \nmid m_1, n_1, m_1 > 1, n_1 > 1$ , then  $\frac{a_1^{m_1} + kb_1^{n_1}}{2} + a_1^{\frac{m_1-1}{2}} b_1^{\frac{n_1-1}{2}} \sqrt{ka_1 b_1}$  is the fundamental solution of the Pell's equation  $x^2 - ka_1 b_1 y^2 = 1$ .

2) If the equation (8) has positive integer solution  $a_2, b_2, m_2, n_2$ , with  $2 \nmid m_2 n_2, m_2 > 1, n_2 > 1$ , then  $a_2^{m_2} + \lambda b_2^{n_2} + 2a_2^{\frac{m_2-1}{2}} b_2^{\frac{n_2-1}{2}}$   $\sqrt{\lambda a_2 b_2}$  is the fundamental solution of the Pell's equation  $x^2 - \lambda a_2 b_2 y^2 = 1$ .

From above results, we proved that equation (7) has no positive integer solution  $a_1, b_1, m_1, n_1$ ,  $2 \nmid m_1 n_1, m_1 > 1, n_1 > 1$ , if that  $a_1 = kb_1 t^2 + 2$  or  $b_1 = ka_1 t^2 + 2$ , etc. For the equation (8), we proved similar results also. If  $q = pt^2 + 2$ , where  $p, q$  denote odd prime numbers, then equation  $q^m = p^n + 2$  has no integer solution  $m, n$  with  $m > 1, n > 1, 2 \nmid mn$ .

We proved also the following result.

If  $q = 6s^2 + 1$ , then the equation (6) has no solution.

#### 4. Some Cubic equations and Quartic equations

From the well known identity

$$(x+1)^3 + (x-1)^3 - 2x^3 = 6x,$$

Mordell suggested that perhaps most of the numbers can be expressed as  $x^3 + y^3 + 2z^3$  with integers  $x, y, z$ . In 1936, Ko Chao [18] gave the decompositions into four cubes in this form for  $n \leq 100$  except the numbers 76, 99.

For the diophantine equations  $x^3 + y^3 + 2z^3 = 76$  and  $x^3 + y^3 + 2z^3 = 99$ , we asked that are there any integral solution  $x, y, z$ ? This still remains unproved.

A interesting equation is

$$x^3 + y^3 + z^3 = n \tag{9}$$

When  $n=3$ , there are solutions given by  $(x,y,z)=(1,1,1)$ ,  $(4,4,-5)$ ,  $(4,-5,4)$ ,  $(-5,4,4)$ . In 1984, Scarowsky and Boyarsky proved that the equation (9) has no new solutions were found for  $|m| \leq 50000$ , where  $x+y+z=3m$ ,  $m \in \mathbb{Z}$ . In 1985, Cassels proved that any integral solution of the equation (9) has  $x \equiv y \equiv z \pmod{9}$ . Recently, Sun Qi<sup>[19]</sup> proved that if  $n=9a^3$ , where  $a$  is not divisible by primes of the form  $6k+1$ , then any integral solution of the equation  $x^3+y^3+z^3=9a^3$  satisfies  $9 \mid \frac{xyz}{d^3}$ , where  $(x,y,z)=d$ . If  $n=3a^3$ ,  $3 \nmid a$ , then any integral solution of the equation  $x^3+y^3+z^3=3a^3$  satisfies  $\frac{x}{d} \equiv \frac{y}{d} \equiv \frac{z}{d} \pmod{9}$ .

Ljunggren proved that if  $D > 2$  be a square-free integer which is not divisible by primes of the form  $6n+1$ , then equations

$$x^3 \pm 1 = Dy^2 \quad (10)$$

have ~~has~~ at most one solution in positive integers  $x, y$ . In 1981, Ko Chao and Sun Qi<sup>[20],[21]</sup> proved that the only solution in integers of the equations (10) is  $x=1, y=0$ . In 1975-1981, Ko Chao and Sun Qi<sup>[22]-[26]</sup> studied the equation

$$x^4 - Dy^2 = 1, \quad D > 1, \quad \mu(D) \neq 0. \quad (11)$$

We They proved that 1) If  $D \equiv 3 \pmod{8}$ ,  $\xi = x_0 + y_0 \sqrt{D}$  is the fundamental solution of the equation  $x^2 - Dy^2 = 1$  and if  $x_0 \equiv 0 \pmod{2}$ , then the equation (11) has no solutions in positive integers  $x, y$ . 2) If  $D=2p$ ,  $p$  is an odd prime number, then the equation (11) has no positive integral solutions except  $p=3, x=7, y=20$ . 3) If  $D$  is not divisible by primes of the form

$4n+1$ , then the equation (11) has no positive integral solutions. In 1979 and 1981, Ko Chao and Sun Qi<sup>[27]-[29]</sup> also studied the equations  $x^2 - Dy^4 = 1$ ,  $x^4 + 4 = Dy^2$  and  $x^3 \pm 8 = Dy^2$ .

For equation  $6y^2 = x(x+1)(2x+1)$  Mordell asked if there was an elementary proof. In 1985, Ma Degang<sup>[30]</sup> have answered the Mordell's question.

In 1942, Ljunggren ~~has~~ showed that the only solutions of  $x^2 = 2y^4 - 1$  in positive integers are (1,1) and (239,13) but his proof is difficult. Mordell asks if it is possible to find a simple or elementary proof. This still remains ~~un~~proved.

In 1967, Bumby proved that the diophantine equation

$$2y^2 = 3x^4 - 1 \quad (12)$$

has only integer solutions  $x = \pm 1, \pm 3$ . The proof depends upon an application of the (law quadratic reciprocity) in the quadratic fields  $\mathbb{Q}(\sqrt{-2})$ .

In 1979, Bremner proved that the diophantine equation

$$3x^4 - 4y^4 - 2x^2 + 12y^2 - 9 = 0 \quad (13)$$

only positive integer solutions  $x=1, y=1$ , and  $x=3, y=3$ . The proof depends upon an application of the Skolem's p-adic method.

We asks if it is possible to find an elementary proof for the equation (12) or the equation (13).

5. The equation  $\frac{1}{x_1} \dots \frac{1}{x_s} \pm \frac{1}{x_1 \dots x_s} = 1$ . Znām problem.  
S-problem.

For the equation

$$\sum_{i=1}^s \frac{1}{x_i} - \frac{1}{x_1 \dots x_s} = 1, \quad 0 < x_1 < \dots < x_s, \quad (14)$$

in 1964, Ko Chao and Sun Qi<sup>[31]</sup> gave all solutions for  $s=5$  and  $s=6$ .

Let  $\Omega(s)$  be the number of positive integral solutions of the equation (14). In 1978, Sun Qi<sup>[32]</sup> proved that when  $s \geq 4$ , then  $\Omega(s) < \Omega(s+1)$ .

In 1978, Janák and Shula gave eighteen solutions of the system of congruences

$$x_1 \dots x_{i-1} x_{i+1} \dots x_n + 1 \equiv 0 \pmod{x_i}, \quad x_i > 1, \quad i=1, \dots, n, \quad n > 1, \quad (15)$$

for  $n=7$ . Let  $H(n)$  be the number of solutions of the system of congruences (15). In 1983, Sun Qi<sup>[33]</sup> proved that if  $n \geq 4$ , then  $H(n) < H(n+1)$ . As a corollary one obtains: If  $n \geq 7$ , then  $H(n) \geq n+11$ .

In 1972, Znām asked whether for every positive integer  $n > 1$  there exist integers  $x_i > 1$  ( $i=1, \dots, n$ ) such that  $x_i$  is a proper divisor of the numbers  $x_1 \dots x_{i-1} x_{i+1} \dots x_n + 1$  for every  $i$ . In 1983, Sun Qi<sup>[34]</sup> proved that let  $Z(n)$  be the number of solutions of the Znām problem with  $1 < x_1 < \dots < x_n$ , we have  $Z(n) \geq \Omega(n) - \Omega(n-1) > 0$ , when  $n \geq 5$ . Hence the problem of Znām is completely solved. It is difficult to prove  $Z(n+1) > Z(n)$ , when  $n \geq 5$ .

In 1985, Sun Qi and Cao Zhenfu<sup>[35]</sup> studied the equation

$$\sum_{i=1}^s \frac{1}{x_i} - \frac{1}{x_1 \dots x_s} = 1, \quad 0 < x_1 \dots < x_s. \quad (16)$$

Let  $A(s)$  be the number of solutions of the equation (16).

**We** **They** proved that if  $t \geq 9$ , then  $A(t+1) \geq \Omega(t) + \Omega(t-1) + 6$ .

For  $s=6$ , we gave that there are 17 solutions of equation

(16) in all. I conjecture that if  $n \geq 3$ , then  $A(n+1) > A(n)$ .



In 1984, Sun Qi and Cao Zhenfu<sup>[36]</sup> proved that  $\Omega(s+1) \geq \Omega(s)+3$ , when  $s \geq 10$ . From this result, we also have  $Z(s) \geq 3$  and  $H(s) \geq 3s-9$ , when  $s \geq 10$ .

In 1986, Sun Qi and Cao Zhenfu<sup>[37]</sup> proved the following theorems.

1) If  $s \geq 2$ , then  $Z(s) = H(s) - H(s-1)$ .

2) If  $s \geq 10$ , then  $\Omega(s+1) \geq \Omega(s)+5$ .

3) If  $s \geq 11$ , then  $Z(s) \geq 5$ .

For  $Z(s)$ , we conjecture that if  $s \geq 4$ , then

$$Z(s+1) > Z(s).$$

In 1984, Sun Qi posed such a problem that, for each integer  $n > 1$ , if there are  $n$  integers  $x_i > 1$  ( $i=1, \dots, n$ ) such that each  $x_i$  is a proper <sup>divisor</sup> of integer  $x_1 \dots x_{i-1} \wedge x_{i+1} \dots x_n - 1$ . We call the problem as  $\mathfrak{S}$ -problem for simplicity. For each integer  $n > 1$ , we use the symbol  $X(n)$  to express the number of solutions to  $\mathfrak{S}$ -problem for the case of  $n$  integers. Recently, Li-Shuguang<sup>[38]</sup> proved that if  $n \geq 4$ , then  $X(n) > 0$  and if  $n=2, 3$ , then  $X(n)=0$ . Thus, the  $\mathfrak{S}$ -problem is solved. Is this true that  $X(n+1) > X(n)$  for  $n \geq 4$ ?

6. The equation  $\sum_{i=1}^n \frac{y_i}{d_i} \equiv 0 \pmod{1}$ . Diophantine equation over Finite fields.

Let  $d_1, \dots, d_n$  be fixed positive integers. It is well-known that the number  $I(d_1, \dots, d_n)$  of solutions of the equation

$$\frac{y_1}{d_1} + \frac{y_2}{d_2} + \dots + \frac{y_n}{d_n} \equiv 0 \pmod{1}, \quad y_i \text{ integers,}$$

$$1 \leq y_i < d_i \quad (i=1, \dots, n) \quad (17)$$

play an important role in the study of diagonal equations over finite fields.

In 1948 and in 1949, Hua and Vandiver, <sup>[39],[40]</sup> Furtado, Weil at about the same time proved the following results. If  $N$  denote the number of solutions of the equation

$$\sum_{i=1}^n a_i x_i^{d_i} = 0, \quad \text{where } d_i \mid q-1$$

$$(i=1, \dots, n) \tag{18}$$

over finite field  $F$ , then

$$|N - q^{n-1}| \leq I(d_1, \dots, d_n) (q-1) q^{\frac{n-2}{2}} \tag{19}$$

Hence the value of  $I(d_1, \dots, d_n)$  heavily affects the estimate of the number  $N$  of solutions of the equation (18).

For the case  $d_1=d_2=\dots=d_n$ , it is proved that  $I(d, \dots, d) = \frac{d-1}{d} ((d-1)^{n-1} + (-1)^n)$ . For the more general case  $d_1 \mid d_2 \dots d_n \mid d_n$ , in 1986, Sun Qi, Wan Daqing, Ma Degang <sup>[4]</sup> proved that

$$I(d_1, \dots, d_n) = \prod_{j=1}^{n-1} (d_j - 1) - \prod_{j=1}^{n-2} (d_j - 1) \dots + (-1)^{n-1} (d_2 - 1)(d_1 - 1) + (-1)^n (d_1 - 1).$$

A complicated formula for  $I(d_1, \dots, d_n)$  was obtained independently by Lide and Niederreiter, Stanly, and us <sup>[42]</sup> with different methods. The formula can be stated as follows

$$I(d_1, \dots, d_n) = (-1)^n + \sum_{r=1}^n (-1)^{(n-r)} \sum_{1 \leq i_1 < \dots < i_r \leq n} \frac{d_{i_1} \dots d_{i_r}}{\text{lcm}[d_{i_1}, \dots, d_{i_r}]}.$$

Form (19), it is interesting to determine when  $I(d_1, \dots, d_n) = 0$ , for if  $I(d_1, \dots, d_n) = 0$ , then (18) has exactly  $q^{n-1}$  solutions. Some partial results have been obtained by Joly. In 1985, Sun Qi and Wan Daqing <sup>[43]</sup> proved following theorem: Let  $n > 2$ , then (17) has no solutions if and only if one of the

following conditions holds. 1) For some  $d_i, (d_i, \frac{d_1 \cdots d_n}{d_i}) = 1$   
 or 2) If  $d_{i_1}, \dots, d_{i_k} (1 \leq i_1 < \dots < i_k \leq n)$  is the set of all  
 even integers among  $\{d_1, \dots, d_n\}$ , then  $2 \nmid k, \frac{d_{i_1}}{2}, \dots, \frac{d_{i_k}}{2}$  are  
 pairwise prime, and  $d_{i_j}$  is prime to any odd number in  $\{d_1, \dots,$   
 $d_n\} (j=1, \dots, k)$  if  $k < n$ .

Recently, Sun Qi<sup>[44]</sup> have proved the following theorems.

Theorem 1. Suppose  $GF(p)$  is a finite field, where  $p$  is  
 an odd prime number,  $\{u, v, \theta\} \subset GF(p), uv \neq 0$ , if

$$p > \sqrt{p} (2^{\omega(p-1)} - 1)^2 + \sqrt{p} - (\sqrt{p} - 3) \frac{(p-1)}{\varphi(p-1)} - 1,$$

then there are two primitive roots  $\alpha$  and  $\beta$  in  $GF(p)$  such that  
 $u\alpha + v\beta = \theta$ , where  $\mu$  is Mobius function,  $\varphi$  is Euler's totient  
 function,  $\omega(p-1)$  denotes the number of distinct prime factors  
 of  $p-1$ .

Theorem 2. If  $p > 2^{60}$ , then there are two primitive roots  
 $\alpha$  and  $\beta$  such that  $u\alpha + v\beta = \theta$ .

Theorem 3. If  $p > 3$ , and

$$p > \sqrt{p} (2^{\omega(p-1)} - 1)^2 - (\sqrt{p} - 1) \left( \frac{(p-1)}{\varphi(p-1)} - 1 \right),$$

then there are two primitive roots  $\alpha$  and  $\beta$  such that  $\alpha - \beta = 1$ .

Vegh asks whether, for all primes  $p > 61$ , every integer  
 can be expressed as the difference of two primitive roots of  
 $p$ .

From theorem 2, we easily deduce the following corollary.

Corollary. If  $p > 2^{60}$ , then every integer can be expres-  
 sed as the difference of two primitive roots of  $p$ .

We can extend theorems 1-3 to  $GF(p^n)$  ( $n > 1$ ) without dif-  
 ficulty. For example, we have the following theorem.

Theorem 4. If  $p^n > 2^{60}$ , then there are two primitive roots

$\alpha$  and  $\beta$  in  $GF(p^n)$  such that  $u\alpha + v\beta = \theta$ , where  $\{u, v, \theta\} \subset GF(p^n)$ ,  $uv\theta \neq 0$ .

In order to prove our theorems we need the following lemmas.

Lemma 1. Let  $\chi$  and  $\lambda$  be characters of  $GF(p)$ , and set

$$J_{u,v}(\chi, \lambda, \theta) = \sum_{\substack{u\ell + v m = \theta \\ \ell, m \in GF(p)}} \chi(\ell)\lambda(m), \text{ then}$$

$$|J_{u,v}(\chi, \lambda, \theta)| = \begin{cases} \sqrt{p}, & \text{if } \chi\lambda \neq \chi_0. \\ 1, & \text{if } \chi\lambda = \chi_0. \end{cases}$$

where  $\chi_0$  denotes the trivial character of  $GF(p)$ .

Lemma 2. If  $\delta > 1$ ,  $\eta > 1$ ,  $\delta | p-1$ ,  $\eta | p-1$ ,  $(a, \delta) = (b, \eta) = 1$ ,  $1 \leq a \leq \delta$ ,  $1 \leq b \leq \eta$ , then  $\chi_{a(p-1)/\delta}$ ,  $\chi_{b(p-1)/\eta}$  are not equal to  $\chi_0$ , and  $\chi_{a(p-1)/\delta} \chi_{b(p-1)/\eta} = \chi_0$  if  $\frac{a}{\delta} + \frac{b}{\eta} \equiv 0 \pmod{1}$ ,  $\chi_{a(p-1)/\delta} \chi_{b(p-1)/\eta} \neq \chi_0$ , if  $\frac{a}{\delta} + \frac{b}{\eta} \not\equiv 1 \pmod{1}$ .

Lemma 3. Let  $n \in GF(p)$ ,  $n \neq 0$ , then

$$\sum_{k|p-1} \frac{\mu(k)}{\varphi(k)} \sum_{\substack{a=1 \\ (a,k)=1}}^k e^{\frac{2\pi i a \text{ind} n}{k}} = \begin{cases} 0, & \text{if } n \text{ is not a primitive root,} \\ \frac{p-1}{\varphi(p-1)}, & \text{if } n \text{ is a primitive root,} \end{cases}$$

Lemma 4.

$$\sum_{\delta|p-1} \frac{|\mu(\delta)|}{\varphi(\delta)} = \frac{p-1}{\varphi(p-1)}.$$

A natural problem is that, is the result above true to primitive roots modulo  $p^l$  ( $l \geq 2$ , the  $p$  is an odd prime)? The problem is solved in [45]. Sun Qi and Li Shuguang have proved the following theorem.

Theorem. Let  $p$  be an odd prime and integer  $l \geq 2$ . When  $p > 2^{6l}$ , there exist at least  $(p-2)p^{l-2}$  pairs of primitive roots

$\alpha$  and  $\beta$  modulo  $p^l$  such that

$$a\alpha + b\beta \equiv c \pmod{p^l}.$$

Recently, Sun Qi, <sup>[46]</sup> have proved the following theorem.

Theorem Let  $p$  be an odd prime and  $h \in \text{GF}(p)$ ,  $h \neq 0$ .

If  $m \geq 3$ , then there is a primitive root  $g$  in  $\text{GF}(p^m)$  such that

$$g + g^p + \dots + g^{p^{m-1}} = h$$

except  $m=3$ ,  $p=11$ .

For  $m=3$ ,  $p=11$ , the problem above still remains unproved.

#### References

- [1] Ko Chao, Journal of the Chinese Math. Soc., 2(1940), 205-207.
- [2] Uchiyama, S., Tr. Mat. Inst. Steklova, 163(1984), 237-243.
- [3] Ko Chao, Sun Qi, Acta Sci. of Sichuan Univ., 2(1964), 5-9.
- [4] Ko Chao, Acta Sci. of Sichuan Univ., 1(1958), 73-80.
- [5] Ko Chao, *ibid.*, 2(1958), 81-90.
- [6] Ko Chao, *ibid.*, 3(1959), 25-34.
- [7] Lu Wenduan, <sup>*ibid.*</sup> 2(1959), 39-41.
- [8] Chen Jingrun, *ibid.*, 2(1962), 19-25.
- [9] Ko Chao, Sun Qi, *ibid.*, 3(1964), 1-12.
- [10] Sun Qi, Zhou Xiaoming, Kexue Tongbao, 9(1984), 1272.
- [11] Yang Xiaozuo, Acta Sci. of Sichuan Univ., 4(1985), 151-158.

- [12] Cao Zhenfu (to appear).
- [13] Sun Qi, Zhang Mingzhi, *proc. AMS*, 2(1985), 218-220.
- [14] See [10].
- [15] Cao Zhenfu, *Nature Journal*, 6(1985), 476-477.
- [16] Crescenzo, P., *Adv. Math.* 17(1975), 25-29.
- [17] Sun Qi (to appear).
- [18] Ko Chao, *Journal of the London Math. Soc.* 11(1936), 218-219.
- [19] Sun Qi, *Kexue Tongbao*, 17(1987), 1285-1287.
- [20] Ko Chao, Sun Qi, *Sci. Sin.*, 12(1981), 1453-1457.
- [21] Ko Chao, Sun Qi, *Acta. Sci. of Sichuan Univ.*, 2(1981), 1-6.
- [22] Ko Chao, Sun Qi, *Acta Math. Sinica*, 6(1980), 922-926.
- [23] Ko Chao, Sun Qi, *Chinese Annals of Math.*, 1(1980), 83-89.
- [24] Ko Chao, Sun Qi, *Kexue Tongbao*, 16(1979), 721-723.
- [25] Ko Chao, Sun Qi, *Acta Sci. of Sichuan Univ.*, 3(1980), 37-44.
- [26] Ko Chao, Sun Qi, *ibid.*, 2(1984), 1-3.
- [27] Ko Chao, Sun Qi, *Chinese Annals of Math.*, 2(1981), 491-496.
- [28] Ko Chao, Sun Qi, *Acta Sci. of Sichuan Univ.*, 4(1979), 1-4.
- [29] Ko Chao, Sun Qi, *ibid.*, 4(1981), 1-5.
- [30] Ma Degang, *ibid.*, 4(1985), 107-116.
- [31] Ko Chao, Sun Qi, *Acta Sci. of Sichuan Univ.*, 1(1964), 13-22.

- [32] Sun Qi, *ibid.*, 2-3(1978), 15-17.
- [33] Sun Qi, *Kexue Tongbao*, 4(1983), 446-447.
- [34] Sun Qi, *ibid.*, 11(1983), 1564.
- [35] Sun Qi, Cao Zhenfu, *ibid.*, 5(1985), 700.
- [36] Sun Qi, Cao Zhenfu,
- [37] Sun Qi, Cao Zhenfu, *Advances in Math.* 3(1986), 329-331.
- [38] Li Shuguang (to appear).
- [39] Hua, L. K., Vandiver, H. S., *Proc. Nat. Acad. Sci. U.S.A.*, 34(1948), 258-263.
- [40] Hua, L. K., Vandiver, H. S., *ibid.*, 35(1948), 94-99.
- [41] Sun Qi, Wan Daqing, Ma Degang, *Chinese Annals of Math.*, 2(1986), 232-236.
- [42] See [37].
- [43] Sun Qi, Wan Daqing, *Proc. AMS*, 2(1987).
- [44] Sun Qi, *Advances in Mathematics*, 2(1987), 213-215.
- [45] Sun Qi, Li Shuguang (to appear).
- [46] Sun Qi (to appear).

Han Wenbao