IJMMS 2003:19, 1175–1183
PII. S0161171203206256
http://ijmms.hindawi.com

ON THE SPECIAL SOLUTIONS OF AN EQUATION IN A FINITE FIELD

LI HAILONG and ZHANG WENPENG

Received 10 June 2002

The main purpose of this paper is to prove the following conclusion: let p be a prime large enough and let k be a fixed positive integer with $2k|p-1$. Then for any finite field F_p and any element $0 \neq c \in F_p$, there exist three generators x, y, and $z \in F_p$ such that $x^k y^k + y^k z^k + x^k z^k = c$.

2000 Mathematics Subject Classification: 11E12, 11T23.

1. Introduction. Let p be an odd prime, let k be a fixed positive integer with $2k|p-1$, and let F_p be the finite field with p elements. It is clear that there exists at least one generator of F_p, and the number of all generators of F_p is equal to $\phi(p-1)$, where $\phi(n)$ is Euler's function. The main purpose of this paper is to study the following two problems:

(A) for any element $0 \neq c \in F_p$ whether there exist three generators x, y, and $z \in F_p$ such that

$$x^k y^k + y^k z^k + x^k z^k = c; \tag{1.1}$$

(B) if (A) is true, let $N(c,k,p)$ denotes the number of all solutions of (1.1). What can be said about the asymptotic properties of $N(c,k,p)$?

In this paper, we use the estimates for general Gauss sums and the properties of Dirichlet characters to study the above two problems and prove the following main conclusion.

Theorem 1.1. *Let p be an odd prime and k a fixed positive integer with $2k|p-1$. Then for any element $0 \neq c \in F_p$, the asymptotic formula*

$$N(c,k,p) = \frac{\phi^3(p-1)}{p} + \theta \cdot \frac{\phi^3(p-1)}{(p-1)^3} \cdot p \cdot 8^{\omega(p-1)}, \tag{1.2}$$

where $|\theta| \leq 54k^4$ and $\omega(n)$ denotes the number of all distinct prime divisors of n.

From this theorem, we may immediately deduce the following corollary.

Corollary 1.2. *Let p be a prime large enough and k a fixed positive integer with $2k|p-1$. Then for any integer $1 \le c \le p-1$, there exist three primitive roots x, y, and z modulo p such that the congruence*

$$x^k y^k + y^k z^k + x^k z^k \equiv c \bmod p. \tag{1.3}$$

2. Some lemmas. In this section, we give several lemmas which are necessary in the proof of Theorem 1.1. First, we let

$$G(n,\chi,k;q) = G(n,\chi;q) = \sum_{a=1}^{q} \chi(a) e\left(\frac{na^k}{q}\right), \tag{2.1}$$

where χ denotes a Dirichlet character $\bmod q$, $e(y) = e^{2\pi i y}$. Then we have the following lemma.

Lemma 2.1. *Let p be an odd prime and k a positive integer with $k|p-1$. Then for any integer n with $p \nmid n$,*

$$|G(n,\chi,k;p)| \begin{cases} \le k\sqrt{p}, & \text{if } \chi^{(p-1)/k} = \chi_0, \\ = 0, & \text{otherwise}, \end{cases} \tag{2.2}$$

where χ_0 denotes the principal character $\bmod p$.

Proof. Let g be a fixed primitive root $\bmod p$, then for any integer n with $p \nmid n$, there exist two integers l and i such that $n \equiv g^{lk+i} \pmod p$, here $0 \le i < k$. If b runs through a complete residue system $\bmod p$, then $g^l b$ also runs through a complete residue system $\bmod p$, so that we have

$$\begin{aligned} |G(n,\chi,k;p)|^2 &= \sum_{a=1}^{p} \sum_{b=1}^{p} \chi(a\bar{b}) e\left(\frac{g^{lk+i}(a^k - b^k)}{p}\right) \\ &= \sum_{a=1}^{p} \sum_{b=1}^{p} \chi(a) e\left(\frac{g^i (g^l b)^k (a^k - 1)}{p}\right) \\ &= \sum_{a=1}^{p} \chi(a) \sum_{b=1}^{p} e\left(\frac{g^i b^k (a^k - 1)}{p}\right). \end{aligned} \tag{2.3}$$

Note the trigonometric identity

$$\sum_{a=1}^{q} e\left(\frac{ma}{q}\right) = \begin{cases} q, & \text{if } q|m, \\ 0, & \text{if } q \nmid m. \end{cases} \tag{2.4}$$

Further, $g^i b^k$, $i = 0,\dots,k-1$; $b = 1,\dots,p$ runs through k complete residue systems mod p so that we have the identity

$$\begin{aligned}\sum_{i=0}^{k-1}|G(g^i,\chi,k;p)|^2 &= \sum_{a=1}^{p}\chi(a)\sum_{b=1}^{p}\sum_{i=0}^{k-1}e\left(\frac{g^ib^k(a^k-1)}{p}\right)\\ &= k\sum_{a=1}^{p-1}\chi(a)\sum_{b=1}^{p}e\left(\frac{b(a^k-1)}{p}\right)\\ &= kp\sum_{\substack{a=1\\ a^k\equiv 1(\operatorname{mod} p)}}^{p-1}\chi(a)\\ &= kp\left(1+\chi\left(g^{(p-1)/k}\right)+\cdots+\chi\left(g^{(k-1)(p-1)/k}\right)\right)\\ &= \begin{cases}k^2p, & \text{if } \chi^{(p-1)/k}=\chi_0,\\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{2.5}$$

From (2.5), we easily get the estimate

$$\begin{aligned}|G(n,\chi,k;p)| &\le \left(\sum_{i=0}^{k-1}|G(g^i,\chi,k;p)|^2\right)^{1/2}\\ &= \begin{cases}k\sqrt{p}, & \text{if } \chi^{(p-1)/k}=\chi_0,\\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{2.6}$$

This proves Lemma 2.1. □

Lemma 2.2. *Let p be an odd prime and let n be an integer. Then*

$$\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sideset{}{'}\sum_{a=1}^{k}e\left(\frac{a\operatorname{ind} n}{k}\right) = \begin{cases}\dfrac{p-1}{\phi(p-1)}, & \text{if } n \text{ is a primitive root of } p,\\ 0, & \text{otherwise,}\end{cases} \tag{2.7}$$

where $\operatorname{ind} n$ *denotes the index of* n *relative to some fixed primitive root of* p*,* $\mu(n)$ *is the Möbius function, and* $\sum_{a=1}^{\prime k}$ *denotes the summation over all* a *such that* $(a,k)=1$.

Proof. See [1, Proposition 2.2]. □

Lemma 2.3. *Let p be an odd prime, let k a fixed positive integer with $2k|p-1$, and let χ_1, χ_2, and χ_3 be three Dirichlet characters* mod p*. Then for any* *integer* u *with* $(u,p)=1$,

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^k+b^kc^k+c^ka^k)}{p}\right)\right| \le 8k^3p\sqrt{p}. \tag{2.8}$$

Proof. Let g be any fixed primitive root mod p, then, from the properties of primitive roots and reduced residue system mod p, we have

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^k+b^kc^k+c^ka^k)}{p}\right)\\
&\quad=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(c)\chi_1(a)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^kc^k+b^kc^k+c^{2k}a^k)}{p}\right)\\
&\quad=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(c)\chi_1(a)\overline{\chi_2}(c)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^k+b^k+c^{2k}a^k)}{p}\right)\\
&\quad=\sum_{b=1}^{p-1}\chi_2(b)e\left(\frac{ub^k}{p}\right)\\
&\qquad\times\sum_{a=1}^{p-1}\chi_1(a)e\left(\frac{ua^kb^k}{p}\right)\sum_{c=1}^{p-1}\chi_1(c)\overline{\chi_2}(c)\chi_3(c)e\left(\frac{ua^kc^{2k}}{p}\right).
\end{aligned}\tag{2.9}$$

Let h be a fixed quadratic nonresidue modulo p, then

$$\begin{aligned}
&\sum_{a=1}^{p-1}\chi_1(a)e\left(\frac{ua^kb^k}{p}\right)\sum_{c=1}^{p-1}\chi_1(c)\overline{\chi_2}(c)\chi_3(c)e\left(\frac{ua^kc^{2k}}{p}\right)\\
&\quad=\frac{1}{2}\sum_{s=1}^{p-1}\sum_{t=0}^{1}\chi_1(s^2h^t)e\left(\frac{us^{2k}h^{kt}b^k}{p}\right)\\
&\qquad\times\sum_{c=1}^{p-1}\chi_1(c)\overline{\chi_2}(c)\chi_3(c)e\left(\frac{us^{2k}h^{kt}c^{2k}}{p}\right)\\
&\quad=\frac{1}{2}\sum_{t=0}^{1}\chi_1(h^t)\sum_{s=1}^{p-1}\chi_1(s^2)\overline{\chi_1}(s)\chi_2(s)\overline{\chi_3}(s)e\left(\frac{uh^{kt}s^{2k}b^k}{p}\right)\\
&\qquad\times\sum_{c=1}^{p-1}\chi_1(c)\overline{\chi_2}(c)\chi_3(c)e\left(\frac{uh^{kt}c^{2k}}{p}\right)\\
&\quad=\frac{1}{2}\sum_{t=0}^{1}\chi_1(h^t)G(uh^{kt},\chi_1\overline{\chi_2}\chi_3,2k;p)\\
&\qquad\times\sum_{s=1}^{p-1}\chi_1(s)\chi_2(s)\overline{\chi_3}(s)e\left(\frac{uh^{kt}s^{2k}b^k}{p}\right).
\end{aligned}\tag{2.10}$$

From (2.9) and (2.10), we have

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^k+b^kc^k+c^ka^k)}{p}\right)\\
&\quad=\frac{1}{2}\sum_{t=0}^{1}\chi_1(h^t)G(uh^{kt},\chi_1\overline{\chi_2}\chi_3,2k;p)\\
&\qquad\times\sum_{b=1}^{p-1}\chi_2(b)e\left(\frac{ub^k}{p}\right)\sum_{a=1}^{p-1}\chi_1(a)\chi_2(a)\overline{\chi_3}(a)e\left(\frac{uh^{kt}a^{2k}b^k}{p}\right)\\
&\quad=\frac{1}{4}\sum_{t=0}^{1}\chi_1(h^t)G(uh^{kt},\chi_1\overline{\chi_2}\chi_3,2k;p)\\
&\qquad\times\sum_{s=1}^{p-1}\sum_{r=0}^{1}\chi_2(s^2h^r)e\left(\frac{us^{2k}h^{rk}}{p}\right)\\
&\qquad\times\sum_{a=1}^{p-1}\chi_1(a)\chi_2(a)\overline{\chi_3}(a)e\left(\frac{uh^{kt}s^{2k}h^{rk}a^{2k}}{p}\right)\\
&\quad=\frac{1}{4}\sum_{r=0}^{1}\sum_{t=0}^{1}\chi_1(h^t)\chi_2(h^r)G(uh^{kt},\chi_1\overline{\chi_2}\chi_3,2k;p)\\
&\qquad\qquad\times G(uh^{rk},\overline{\chi_1}\chi_2\chi_3,2k;p)G(uh^{kt}h^{rk},\chi_1\chi_2\overline{\chi_3},2k;p).
\end{aligned}\tag{2.11}$$

Applying Lemma 2.1 to (2.11), we immediately get the estimate

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(c)e\left(\frac{u(a^kb^k+b^kc^k+c^ka^k)}{p}\right)\right|\le 8k^3p\sqrt{p}.\tag{2.12}$$

This proves Lemma 2.3. □

3. Proof of the Theorem 1.1. We only prove that Theorem 1.1 is true if F_p is a complete residue system modulo p, then, from the isomorphism properties of the finite field, we can deduce that Theorem 1.1 is true for any finite field F_p. Let p be an odd prime and $\mathcal{A}(p)=\mathcal{A}$ denotes the set of all primitive roots modulo p in the interval $[1,p-1]$, then, from the trigonometric identity (2.4) and Lemma 2.2, we have

$$\begin{aligned}
N(c,k,p)&=\sum_{\substack{u\in\mathcal{A}\\ u^kv^k+v^kw^k+u^kw^k\equiv c(p)}}\sum_{v\in\mathcal{A}}\sum_{w\in\mathcal{A}}1\\
&=\frac{\phi^3(p-1)}{p(p-1)^3}\sum_{j\mid p-1}\sum_{h\mid p-1}\sum_{l\mid p-1}\frac{\mu(j)}{\phi(j)}\frac{\mu(h)}{\phi(h)}\frac{\mu(l)}{\phi(l)}
\end{aligned}$$

$$
\begin{aligned}
&\times \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{d=1}^{l}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h} + \frac{d \operatorname{ind} w}{l}\right) \\
&\times \sum_{t=1}^{p} e\left(\frac{t(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \\
= &\frac{\phi^3(p-1)}{p(p-1)^3} \sum_{j|p-1} \sum_{h|p-1} \sum_{l|p-1} \frac{\mu(j)}{\phi(j)} \frac{\mu(h)}{\phi(h)} \frac{\mu(l)}{\phi(l)} \\
&\times \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{d=1}^{l}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h} + \frac{d \operatorname{ind} w}{l}\right) \\
&+ \frac{\phi^3(p-1)}{p(p-1)^3} \sum_{j|p-1} \sum_{h|p-1} \sum_{l|p-1} \frac{\mu(j)}{\phi(j)} \frac{\mu(h)}{\phi(h)} \frac{\mu(l)}{\phi(l)} \\
&\times \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{d=1}^{l}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h} + \frac{d \operatorname{ind} w}{l}\right) \\
&\times \sum_{t=1}^{p-1} e\left(\frac{t(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \\
\equiv &\frac{\phi^3(p-1)}{p(p-1)^3} [R_1 + R_2].
\end{aligned}
\tag{3.1}
$$

First, we estimate the main term R_1. Note (2.4) and $\sum_{a=1}^{p-1} \chi(a) = 0$ (χ is a non-principal character modulo p), from the definition of Dirichlet characters, we have

$$
\begin{aligned}
R_1 = &(p-1)^3 + 3(p-1)^2 \sum_{\substack{j|p-1 \\ j>1}} \frac{\mu(j)}{\phi(j)} \sum_{a=1}^{j}{}' \sum_{u=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j}\right) \\
&+ 3(p-1) \sum_{\substack{j|p-1 \\ j>1}} \sum_{\substack{h|p-1 \\ h>1}} \frac{\mu(j)}{\phi(j)} \frac{\mu(h)}{\phi(h)} \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h}\right) \\
&+ \sum_{\substack{j|p-1 \\ j>1}} \sum_{\substack{h|p-1 \\ h>1}} \sum_{\substack{l|p-1 \\ l>1}} \frac{\mu(j)}{\phi(j)} \frac{\mu(h)}{\phi(h)} \frac{\mu(l)}{\phi(l)} \\
&\times \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{d=1}^{l}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h} + \frac{d \operatorname{ind} w}{l}\right) \\
= &(p-1)^3 + 3(p-1)^2 \sum_{\substack{j|p-1 \\ j>1}} \frac{\mu(j)}{\phi(j)} \sum_{a=1}^{j}{}' \sum_{u=1}^{p-1} \chi(u;a,j) \\
&+ 3(p-1) \sum_{\substack{j|p-1 \\ j>1}} \sum_{\substack{h|p-1 \\ h>1}} \frac{\mu(j)}{\phi(j)} \frac{\mu(h)}{\phi(h)} \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{v=1}^{p-1} \chi(v;b,h) \sum_{u=1}^{p-1} \chi(u;a,j)
\end{aligned}
$$

$$+\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{l|p-1\\l>1}}\frac{\mu(j)}{\phi(j)}\frac{\mu(h)}{\phi(h)}\frac{\mu(l)}{\phi(l)}$$

$$\times\sum_{a=1}^{j}{}'\sum_{b=1}^{h}{}'\sum_{d=1}^{l}{}'\sum_{v=1}^{p-1}\chi(v;b,h)\sum_{u=1}^{p-1}\chi(u;a,j)\sum_{w=1}^{p-1}\chi(w;d,l), \tag{3.2}$$

where $\chi(u;a,j) = e(a\operatorname{ind}u/j)$, $\chi(v;b,h) = e(b\operatorname{ind}v/h)$, and $\chi(w;d,l) = e(d\operatorname{ind}w/l)$ are three Dirichlet characters $\operatorname{mod}p$. Since $j > 1$, $h > 1$, $l > 1$, and $(b,h) = (a,j) = (d,l) = 1$, the characters $\chi(u;a,j)$, $\chi(v;b,h)$, and $\chi(w;d,l)$ are three primitive characters $\operatorname{mod}p$. Therefore, we have

$$\sum_{u=1}^{p-1}\chi(u;a,j)=\sum_{v=1}^{p-1}\chi(v;b,h)=\sum_{w=1}^{p-1}\chi(w;d,l)=0. \tag{3.3}$$

From these identities and (3.2), we immediately get the main term

$$R_1 = (p-1)^3. \tag{3.4}$$

In order to estimate the error term R_2 in (3.1), first we separate R_2 into four parts. That is,

$$R_2=\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\sum_{w=1}^{p-1}\sum_{t=1}^{p-1}e\left(\frac{t(u^kv^k+v^kw^k+w^ku^k-c)}{p}\right)$$

$$+3\sum_{\substack{j|p-1\\j>1}}\frac{\mu(j)}{\phi(j)}\sum_{a=1}^{j}{}'\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\sum_{w=1}^{p-1}e\left(\frac{a\operatorname{ind}u}{j}\right)$$

$$\times\sum_{t=1}^{p-1}e\left(\frac{t(u^kv^k+v^kw^k+w^ku^k-c)}{p}\right)$$

$$+3\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{h|p-1\\h>1}}\frac{\mu(j)}{\phi(j)}\frac{\mu(h)}{\phi(h)}\sum_{a=1}^{j}{}'\sum_{b=1}^{h}{}'\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\sum_{w=1}^{p-1}e\left(\frac{a\operatorname{ind}u}{j}+\frac{b\operatorname{ind}v}{h}\right)$$

$$\times\sum_{t=1}^{p-1}e\left(\frac{t(u^kv^k+v^kw^k+w^ku^k-c)}{p}\right)$$

$$+\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{l|p-1\\l>1}}\frac{\mu(j)}{\phi(j)}\frac{\mu(h)}{\phi(h)}\frac{\mu(l)}{\phi(l)}$$

$$
\begin{aligned}
&\times \sum_{a=1}^{j}{}' \sum_{b=1}^{h}{}' \sum_{d=1}^{l}{}' \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j} + \frac{b \operatorname{ind} v}{h} \frac{d \operatorname{ind} w}{l}\right) \\
&\times \sum_{t=1}^{p-1} e\left(\frac{t(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \\
\equiv\ & R_{21} + R_{22} + R_{23} + R_{24}.
\end{aligned}
\tag{3.5}
$$

Let g be any fixed primitive root mod p. Then note that $2k|p-1$, from the properties of primitive roots and reduced residue system mod p, we have

$$
\begin{aligned}
R_{21} &= \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} \sum_{t=1}^{p-1} e\left(\frac{t(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \\
&= \frac{1}{2k} \sum_{s=0}^{p-2} \sum_{t=0}^{2k-1} \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{g^{2ks+t}(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \\
&= \frac{1}{2k} \sum_{t=0}^{2k-1} \sum_{s=0}^{p-2} e\left(\frac{-c g^t g^{2ks}}{p}\right) \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{g^t g^{2ks}(u^k v^k + v^k w^k + w^k u^k)}{p}\right) \\
&= \frac{1}{2k} \sum_{t=0}^{2k-1} \sum_{a=1}^{p-1} e\left(\frac{-c g^t a^{2k}}{p}\right) \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{g^t(u^k v^k + v^k w^k + w^k u^k)}{p}\right).
\end{aligned}
\tag{3.6}
$$

Applying Lemmas 2.1 and 2.3 to (3.6), we immediately get

$$
|R_{21}| \le 16k^4 p^2. \tag{3.7}
$$

Using the same method of proving (3.7) and Lemma 2.3, and noting the identity $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$, we can also get

$$
\left| \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \sum_{w=1}^{p-1} e\left(\frac{a \operatorname{ind} u}{j}\right) \sum_{t=1}^{p-1} e\left(\frac{t(u^k v^k + v^k w^k + w^k u^k - c)}{p}\right) \right| \le 16k^4 p^2 \tag{3.8}
$$

or

$$
\begin{gathered}
|R_{22}| \le 48k^4 p^2 \cdot 2^{\omega(p-1)}, \qquad |R_{23}| \le 48k^4 p^2 \cdot 4^{\omega(p-1)}, \\
|R_{24}| \le 16k^4 p^2 \cdot 8^{\omega(p-1)}.
\end{gathered}
\tag{3.9}
$$

From (3.5), (3.7), and (3.9), and noting that $\omega(p-1) \ge 1$, we get

$$
|R_2| \le 54k^4 p^2 \cdot 8^{\omega(p-1)}. \tag{3.10}
$$

Combining (3.1), (3.4), and (3.10), we obtain

$$N(c,k,p)=\frac{\phi^3(p-1)}{p}+\theta\cdot\frac{\phi^3(p-1)}{(p-1)^3}\cdot p\cdot 8^{\omega(p-1)}, \tag{3.11}$$

where $|\theta|\le 54k^4$. This completes the proof of Theorem 1.1.

Note 3.1. Using the similar method of proving Theorem 1.1, we can also get the asymptotic formula

$$N(0,k,p)=\frac{\phi^3(p-1)}{p}+\theta_1\cdot\frac{\phi^3(p-1)}{(p-1)^2}\cdot\sqrt{p}\cdot 4^{\omega(p-1)}, \tag{3.12}$$

where $|\theta_1|\le k^3$.

Acknowledgment. This work was supported by the National Science Foundation (NSF) and Province Natural Science Foundation (PNSF) of China.

References

[1] W. Narkiewicz, *Classical Problems in Number Theory*, Monografie Matematyczne, vol. 62, Państwowe Wydawnictwo Naukowe (PWN-Polish Scientific Publishers), Warsaw, 1986.

Li Hailong: Department of Mathematics, Weinan Teacher's College, Weinan, Shaanxi, China

E-mail address: lihailong@163.com

Zhang Wenpeng: Research Center for Basic Science, Xi'an Jiaotong University, Xi'an, Shaanxi, China

E-mail address: wpzhang@nwu.edu.cn