PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 5, May 1995

ON THE SOLUTIONS OF THE EQUATION $x^m + y^m - z^m = 1$ IN A FINITE FIELD

WEN-FONG KE AND HUBERT KIECHLE

(Communicated by William Adams)

ABSTRACT. An explicit formula for the number of solutions of the equation in the title is given when a certain condition, depending only on m and the characteristic of the field, holds.

1. INTRODUCTION

Let $(F, +, \cdot)$ be the Galois field of order $q = p^s$, where p is a prime and $s > 0$. Let $k \geq 2$. We say that the ordered pair (q, k) is *circular* if $k|(q-1)$ and the subgroup $\Phi \leq F^* := F\backslash\{0\}$ of order k satisfies[1]

$$|\Phi a + b \cap \Phi c + d| \leq 2$$

for all $a, c \in F^*$, $b, d \in F$ with $\Phi a \neq \Phi c$ or $b \neq d$. Let (q, k) be circular and put $m = (q-1)/k$. Denote the number of solutions of the equation

$$x^m + y^m - z^m = 1$$

in F by N. Also, let N' be the number of solutions with $xyz \neq 0$. The main purpose of this paper is to prove

Theorem 1. *Let (q, k) be circular.*

(1) *If k is even, then*

$$N = \begin{cases} 3(k-1)m^3 + 6m^2 + 3m & \text{if } 6|k; \\ 3(k-1)m^3 + 3m^2 + 3m & \text{if } p = 3; \\ 3(k-1)m^3 + 3m & \text{otherwise}; \end{cases}$$

and $N' = 3(k-1)m^3$.

(2) *If k is odd, and if $(q, 2k)$ is also circular, then $N = (2k-1)m^3 + 2m$ and $N' = (2k-1)m^3$.*

Note that in case (1) N is the number of solutions of $x^m + y^m + z^m = 1$, too. In order to prove this theorem, we separate the solutions of the equation into two disjoint sets S and T:

$$T = \{(x, y, z) | x^m + y^m - z^m = 1, \ xyz = 0 \text{ or } 1 \in \{x^m, y^m\}\},$$
$$S = \{(x, y, z) | x^m + y^m - z^m = 1, \ (x, y, z) \notin T\}.$$

Received by the editors November 17, 1992 and, in revised form, August 10, 1993.
1991 *Mathematics Subject Classification.* Primary 11D41, 11T23.

[1] This definition has its origin in certain designs obtained from F and Φ. See [1, 2] for details.

We will compute $|S|$ in §2 as an application of results in [12]. The crucial step in §2 requires some knowledge of this paper and is therefore not self-contained. To find $|T|$, we essentially have to deal with problems in two variables, namely, to find

$$t_+ = |\{(x, y) | x^m + y^m = 1\}| \quad \text{and} \quad t_- = |\{(x, y) | x^m - y^m = 1\}|.$$

In §3 we will show

Theorem 2. *Let (q, k) be circular.*

(1) *If k is even, then*

$$t_+ = t_- = \begin{cases} 2m^2 + 2m & \text{if } 6|k; \\ m^2 + 2m & \text{if } p = 3; \\ 2m & \text{otherwise.} \end{cases}$$

(2) *If k is odd, and if $(q, 2k)$ is also circular, then $t_+ = 2m$ and $t_- = m$.*

This proof also uses results from [12].

In a more general setting Hua-Vandiver [7] as well as Weil [18] give formulas for the number of solutions involving Jacobi sums (see also [9, Chapter 8, Theorem 5] for a comprehensive exposition and [10] for more literature). However, these formulas are hard to evaluate for large m. Explicit and simple formulas are only known for certain special cases, namely when m is small [5, 13], when k is small [17, 13], or when $2|s$ and $m|(\sqrt{q}+1)$ ([14, 8, 6] and, more general, [19]).

In fact m is always large in the circular case. So, in a sense, we attack the problem from the top, while estimates derived from Hua-Vandiver's or Weil's theorems assume q to be large enough. This will be discussed in more detail in §4.

For bookkeeping, we shall have F and k fixed such that $k|(q-1)$ and let $m = (q-1)/k$. Further, let ζ be a primitive element of F, $\varphi = \zeta^m$, and $\Phi = \langle\varphi\rangle$. Thus, $|\Phi| = k$. Also, let Λ be the set of all mth roots of unity, i.e., $\Lambda = \langle\zeta^k\rangle$. The letters t_+ and t_- will keep their meaning, too.

2. Number of elements in S

For a triple $\mathbf{x} = (x, y, z) \in (F^*)^3$ such that $x^m + y^m - z^m = 1$, we define $b_\mathbf{x} = (x^m - 1)(\varphi - 1)^{-1} = (z^m - y^m)(\varphi - 1)^{-1}$. In the following, we set up a correspondence between S and the set of all $b_\mathbf{x}$, which then gives a way to count the number of elements in S.

(2.1) *If $\mathbf{x} = (x, y, z) \in S$, then $(\Phi + b_\mathbf{x}) \cap (\Phi + \varphi b_\mathbf{x}) = \{d, e\}$, where $d = x^m + b_\mathbf{x} = 1 + \varphi b_\mathbf{x}$ and $e = z^m + b_\mathbf{x} = y^m + \varphi b_\mathbf{x}$, and $d \neq e$.*

Proof. Let $x = \zeta^r$, $y = \zeta^s$, and $z = \zeta^t$. Then $x^m = \varphi^r$, $y^m = \varphi^s$, and $z^m = \varphi^t$, so $\{d, e\} \subseteq (\Phi + b_\mathbf{x}) \cap (\Phi + \varphi b_\mathbf{x})$. Since $\mathbf{x} \in S$, we have $y^m \neq 1$; therefore, $d \neq e$. □

(2.2) *Let $b \in F^*$. If $|(\Phi + b) \cap (\Phi + \varphi b)| = 2$, then $b \in \Phi b_\mathbf{x}$ for some $\mathbf{x} \in S$.*

Proof. Suppose $(\Phi+b)\cap(\Phi+\varphi b) = \{d, e\}$, $d \neq e$, where $d = \varphi^r + b = \varphi^u + \varphi b$ and $e = \varphi^t + b = \varphi^s + \varphi b$. Then we have

$$\varphi^r - \varphi^u = (\varphi - 1)b = \varphi^t - \varphi^s.$$

Thus,

$$\varphi^{r-u} + \varphi^{s-u} - \varphi^{t-u} = 1.$$

Let $\mathbf{x} = (x, y, z)$, where $x = \zeta^{r-u}$, $y = \zeta^{s-u}$, and $z = \zeta^{t-u}$. Then certainly $x^m + y^m - z^m = 1$ and $b = \varphi^u b_{\mathbf{x}}$. It remains to show that $\mathbf{x} \in S$. Of course, $0 \notin \{x, y, z\}$. If $x^m = 1$, then $\varphi^{r-u} = (\zeta^m)^{r-u} = (\zeta^{r-u})^m = 1$, and so $\varphi^r = \varphi^u$. But then $\varphi = 1$, a contradiction. Similarly, if $y^m = 1$, then $\varphi^s = \varphi^u$, and so $d = e$, a contradiction again. Therefore, $\mathbf{x} \in S$. This completes the proof. □

We now define an equivalence relation on S. Two elements $\mathbf{x} = (x, y, z)$, $\mathbf{x}' = (x', y', z') \in S$ are equivalent, denoted by $\mathbf{x} \sim \mathbf{x}'$, if there are $\lambda_1, \lambda_2, \lambda_3 \in \Lambda$ such that $x' = \lambda_1 x$, $y' = \lambda_2 y$, and $z' = \lambda_3 z$. It is easy to see that each equivalence class $[\mathbf{x}]$, $\mathbf{x} \in S$, has m^3 elements.

(2.3) *Let* $\mathbf{x}, \mathbf{x}' \in S$. *Then* $b_{\mathbf{x}} = b_{\mathbf{x}'}$ *if and only if* $\mathbf{x} \sim \mathbf{x}'$.

Proof. Let $\mathbf{x} = (x, y, z)$, $\mathbf{x}' = (x', y', z')$. First assume that $\mathbf{x} \sim \mathbf{x}'$ and let $\lambda \in \Lambda$ such that $x' = \lambda x$. Then, by definition,

$$\begin{aligned} b_{\mathbf{x}'} &= (x'^m - 1)(\varphi - 1)^{-1} = ((\lambda x)^m - 1)(\varphi - 1)^{-1} \\ &= (x^m - 1)(\varphi - 1)^{-1} = b_{\mathbf{x}}. \end{aligned}$$

Conversely, suppose $b_{\mathbf{x}} = b_{\mathbf{x}'}$. From (2.1), we have

$$\begin{aligned} (\Phi + b_{\mathbf{x}}) \cap (\Phi + \varphi b_{\mathbf{x}}) &= \{d, e\}, \\ (\Phi + b_{\mathbf{x}'}) \cap (\Phi + \varphi b_{\mathbf{x}'}) &= \{d', e'\}, \end{aligned}$$

where $d = x^m + b_{\mathbf{x}} = 1 + \varphi b_{\mathbf{x}}$, $e = z^m + b_{\mathbf{x}} = y^m + \varphi b_{\mathbf{x}}$, $d' = x'^m + b_{\mathbf{x}'} = 1 + \varphi b_{\mathbf{x}'}$, and $e' = z'^m + b_{\mathbf{x}'} = y'^m + \varphi b_{\mathbf{x}'}$. From $b_{\mathbf{x}} = b_{\mathbf{x}'}$ and circularity we derive $\{d, e\} = \{d', e'\}$. We conclude that $d = d'$ and $e = e'$, since otherwise $y'^m = 1$. Hence, $x^m = x'^m$, $y^m = y'^m$, and $z^m = z'^m$, and so $\mathbf{x} \sim \mathbf{x}'$. □

(2.4) *Let* (q, k) *be circular.*

(1) *If* k *is even, then* $|S| = m^3(k - 2)$.

(2) *If* k *is odd and* $(q, 2k)$ *is also circular, then* $S = \varnothing$.

Proof. Suppose $2|k$. From (4.6) and (4.7) of [12] together with (2.2), there are exactly $2(k/2 - 1) = k - 2$ different $b_{\mathbf{x}}$. By (2.3), each $b_{\mathbf{x}}$ corresponds to exactly one equivalence class $[\mathbf{x}]$ in $S/\sim$. Since each $[\mathbf{x}]$ has m^3 elements, we get $|S| = m^3(k - 2)$. This is (1).

Now, (2) follows from (2.2) and (2.3) together with [12, (4.9)]. □

Remarks. (1) from [12, (4.4)], it follows that if $\mathbf{x} = (x, y, z)$ runs through S, then x^m runs through all of $\Phi \backslash \{-1, 1\}$. Therefore all the $b_{\mathbf{x}}$ are easy to obtain. Using (2.1), one gets e, and then y^m and z^m. Thus, the problem of finding all the elements in S boils down to the problem of finding mth roots in F.

(2) The condition that (q, k) is circular cannot be dropped. For example, the pairs (11, 5), (13, 6), (43, 7), (31, 10) are not circular, and $|S|$ is, in each case, different from the value computed using the formula in the theorem.

However, the theorem is valid for the pairs (19, 6) and (71, 10), although they are not circular either. (See also the remarks in §4.)

3. The equations $x^m \pm y^m = 1$ and the number of elements in T

We remind the reader of the following notation

$$t_+ = |\{(x, y) | x^m + y^m = 1\}| \quad \text{and} \quad t_- = |\{(x, y) | x^m - y^m = 1\}|.$$

We will also have use for

$$t = |\Phi \cap \Phi + 1|.$$

The next theorem seems to be well known; essentials appear e.g. in [14; 4, Theorems 2 and 3]. However, we include a proof for completeness and due to the lack of a suitable reference.

(3.1) *$t_+ = tm^2 + 2m$ and*

$$t_- = \begin{cases} tm^2 + 2m & \text{if } 2|k; \\ tm^2 + m & \text{if } 2 \nmid k. \end{cases}$$

Proof. Assume $x, y \in F^*$. We have $x^m + y^m = 1$ if and only if $x^{-m} - (yx^{-1})^m = 1$. This shows

$$t' := |\{(x, y) | x^m + y^m = 1, xy \neq 0\}| = |\{(x, y) | x^m - y^m = 1, xy \neq 0\}|.$$

Since $x^m = y^m + 1$ puts $x^m \in \Phi \cap \Phi + 1$, and since there are m different $x \in F^*$ with $x^m = \varphi$ for any given $\varphi \in \Phi$, we find $t' = tm^2$.

The case $y = 0$ leads to the m solutions $(x, 0)$, $x \in \Lambda$. There exists $u \in F^*$ such that $u^m = -1$ if and only if $2|k$. Hence, if $x = 0$, there is no solution for $-y^m = 1$ in the case $2 \nmid k$, while all other cases have another m solutions $(0, y)$, $y \in u^{-1}\Lambda$. □

By circularity, we have $t \in \{0, 1, 2\}$. Using results of [12] we can say more.

(3.2) *Let (q, k) be circular.*
   (1) *Assume $2|k$; then $t = 1$ if and only if $2 \in \Phi$.*
   (2) *If $2 \nmid k$ and $(q, 2k)$ is also circular, then $t \in \{0, 1\}$.*

Proof. From both assumptions we have $2|(q-1)$; therefore, $p \neq 2$. Thus there is an $h \in F$ with $2h = 1$ ("$h = 1/2$"), and

$$t = |\Phi \cap \Phi + 1| = |\Phi + (-1)h \cap \Phi + h|.$$

(1) (4.3) and (4.4) of [12] applied to E_h^1 (notation from [12]) prove the assertion.

(2) Obviously, there is a subgroup Ψ of order $2k$ in F^*. Note that $\Phi \subset \Psi$. If $\Psi + (-1)h \cap \Psi + h = \{a, b\}$ and $a \in \Phi + h$, then we find from (4.4) of [12] that $b \notin \Phi + h$. From this the result follows. □

We are now in a position to compute t.

(3.3) *Let (q, k) be circular.*
   (1) *If $2|k$, then*

$$t = \begin{cases} 2 & \text{if } 6|k; \\ 1 & \text{if } \operatorname{char} F = 3; \\ 0 & \text{otherwise.} \end{cases}$$

   (2) *If $2 \nmid k$ and $(q, 2k)$ is also circular, then $t = 0$.*

The proof utilizes the following two lemmas.

Lemma A. *Assume* $2|k$, *then* $t = 1 \Leftrightarrow \operatorname{char} F = 3$. *In this case,* $\Phi \cap \Phi + 1 = \{-1\}$.

Proof. From (3.2.1) we know $t = 1 \Leftrightarrow 2 \in \Phi$. Let $t = 1$. To see that $\operatorname{char} F = 3$, we note that $-1 \in \Phi$. Thus we obtain

$$-1 = -2 + 1 \in \Phi \cap \Phi + 1$$

and

$$2 = 1 + 1 \in \Phi \cap \Phi + 1.$$

Therefore, $2 = -1$ in F or, equivalently, $\operatorname{char} F = 3$. Conversely, if $\operatorname{char} F = 3$, then $2 = -1 \in \Phi$ since $2|k$ by the hypothesis. This shows Lemma A. □

Lemma B. $t = 2 \Leftrightarrow 6|k$. *In this case,* $\Phi \cap \Phi + 1 = \{\gamma, \gamma^{-1}\}$ *with a primitive* 6th *root of unity* γ.

Proof. Suppose $6|k$. There is $\gamma \in \Phi$ of order 6, thus γ is a primitive 6th root of unity, hence $\gamma^2 - \gamma + 1 = 0$. This implies

$$\gamma = \gamma^2 + 1 \in \Phi \cap \Phi + 1.$$

Also, we have

$$\gamma^5 = \gamma^4\gamma = \gamma^4(\gamma^2 + 1) = \gamma^4 + 1 \in \Phi \cap \Phi + 1.$$

Since $\gamma \neq \gamma^5$, we conclude that $t \geq 2$. By circularity we have $t = 2$.

For the converse, assume $t = 2$. Then $2|k$ by (3.2.2). Suppose

$$\varphi^s = \varphi^r + 1 \in \Phi \cap \Phi + 1,$$

where $s, t \in \mathbf{N}$. Then

$$-\varphi^r = -\varphi^s + 1 \in \Phi \cap \Phi + 1.$$

If $\varphi^s = -\varphi^r$, we have

$$\varphi^{s-r} = -1 \quad \text{and} \quad \varphi^{s-r} = \varphi^{-r} + 1,$$

which puts $2 = -\varphi^{-r} \in \Phi$, contracting Lemma A. So $\varphi^s \neq -\varphi^r$. From $\varphi^{s-r} = \varphi^{-r} + 1$ and circularity we must have $\varphi^{s-r} = -\varphi^r$, because $\varphi^{s-r} = \varphi^s$ leads to the contradiction $2 \in \Phi$ as before. Hence

$$\varphi^{2r} = -\varphi^s.$$

This means $-\varphi^r = \varphi^{2r} + 1$; therefore, $(\varphi^r)^3 = 1$ and $\varphi^r \neq 1$. Now we can conclude $3|k$ and so $6|k$. This completes the proof for Lemma B. □

Proof of (3.3). (1) follows directly from Lemma A and Lemma B.

(2) As in the proof of (3.2.2), we will need the subgroup Ψ of F^* of order $2k$. Notice that $\Phi \subset \Psi$. In case $|\Psi \cap \Psi + 1| = 2$, we find from Lemma B that $\Phi \cap \Phi + 1 = \varnothing$ because Φ does not contain a primitive 6th root of unity, i.e., an element of order 6.

The case $|\Psi \cap \Psi + 1| = 1$ implies $\Psi \cap \Psi + 1 = \{-1\}$ by Lemma A, but -1 is not in Φ, so $t = 0$ in this case. If $\Psi \cap \Psi + 1 = \varnothing$, then $\Phi \cap \Phi + 1 = \varnothing$. Since $(q, 2k)$ is circular, we have covered all the cases and have always found $t = 0$. □

The proof of Theorem 2 comes directly from (3.1) and (3.3).

To employ (3.1) in the proof of Theorem 1, we decompose T into the disjoint subsets

$$T_0 = \{(x, y, z) \in T | xyz = 0\}$$

and

$$T_1 = \{(x, y, z) \in T | 1 \in \{x^m, y^m\}, xyz \neq 0\} = T \backslash T_0.$$

(3.4) $|T_1| = (2k-1)m^3$.

Proof. If $x^m = 1$, then we are left with $y^m - z^m = 0$, which has $m(q-1)$ solutions (each $y \in F^*$ gives m z's). Similarly, we find $m(q-1)$ solutions in the case $y^m = 1$. If $x^m = y^m = 1$, then we have $z^m = 1$. Thus, we conclude that

$$|T_1| = 2m^2(q-1) - m^3 = m^3(2k-1).$$

since the m^3 triples (x, y, z), $x, y, z \in \Lambda$, have been counted twice. □

Finding $|T_0|$ can be reduced to the problem discussed in (3.1).

(3.5)

$$|T_0| = \begin{cases} 3t_+ - 3m & \textit{if } 2|k; \\ 2t_- + t_+ - 2m & \textit{if } 2 \nmid k. \end{cases}$$

Proof. Let

$$T_x = \{(0, y, z) | y^m - z^m = 1\}, \quad T_y = \{(x, 0, z) | x^m - z^m = 1\},$$

$$T_z = \{(x, y, 0) | x^m + y^m = 1\}.$$

Then

$$t_+ = |T_z| \quad \text{and} \quad t_- = |T_x| = |T_y|.$$

If $2|k$, then $t_+ = t_-$ by (3.1). Note that $T_0 = T_x \cup T_y \cup T_z$.

Since $T_x \cap T_y = \{(0, 0, z) | z^m = -1\}$, it follows that

$$|T_x \cap T_y| = \begin{cases} m & \text{if } 2|k; \\ 0 & \text{if } 2 \nmid k. \end{cases}$$

Obviously, we have $|T_x \cap T_z| = |T_y \cap T_z| = m$ and $T_x \cap T_y \cap T_z = \varnothing$. Now the assertion follows easily. □

Putting these results together, we find

$$(3.6) \qquad |T| = \begin{cases} (2k-1)m^3 + 3tm^2 + 3m & \text{if } 2|k; \\ (2k-1)m^3 + 3tm^2 + 2m & \text{if } 2 \nmid k. \end{cases} \quad \square$$

Proof of Theorem 1. Since $N = |S| + |T|$ and $N' = |S| + |T_1|$ in both cases, the result is an easy consequence of (2.4), (3.6), (3.4), and (3.3). □

4. The exponents

It is easy to see that the condition $m|(q-1)$ puts no real restriction to the problem; see [10, (1.2.3)] for details.[2]

By a previous remark, the condition that (q, k) is circular plays a crucial role in our argument. In this case, k cannot be too large. In fact, Clay shows

[2]The argument given in [13] is incorrect.

that $k \leq (3+\sqrt{4q-7})/2$ in [2, (5.6)]. From this we derive the following lower bound for m.

$$m \geq \frac{q-1}{q-4} \cdot \frac{\sqrt{4q-7}-3}{2} > \frac{\sqrt{4q-7}-3}{2}. \tag{4.1}$$

Proof. As mentioned above we have

$$\frac{q-1}{m} \leq \frac{\sqrt{4q-7}+3}{2}$$

and so

$$m \geq \frac{2(q-1)}{\sqrt{4q-7}+3} = \frac{q-1}{q-4} \cdot \frac{\sqrt{4q-7}-3}{2}.$$

Since $(q-1)/(q-4) > 1$, the second inequality is clear. □

Remarks. (1) Clay's bound is reached if (and only if) $q = p^{2s}$, $s > 0$; then the bound is $p^s + 1$, and $(q, p^s + 1)$ is always circular (cf. [2, (5.7), and (5.9)]). From [3, (1.3)] one can derive that

$$m \geq \frac{\sqrt{4q-3}-1}{2}$$

if Clay's bound is not reached for circular (q, k).

(2) Modisett shows that the circularity of (q, k), once $k|(q-1)$, depends only on p, and not on s in $q = p^s$. Furthermore, for any $k \geq 2$, there are only finitely many p's (!) such that (q, k) is not circular (cf. [2, (5.31); 16]). Last but not least, Modisett gives an algorithm to find the exceptional p's for any given k. For a list of exceptional primes when $k \leq 10$ see [2, §5, p. 73] or [16].

(3) Modisett's algorithm may be modified (and is then quicker) to determine whether or not a given pair (q, k) is circular. If $k|p-1$ for a prime p, [11] gives a fairly quick algorithm to determine the circularity of (p, k), which is substantially different from Modisett's.

In [7, Theorem II] Hua and Vandiver give the following bound

$$\frac{(q-1)^3}{q} - q^{-1/2}(1 + (m-1)\sqrt{q})^3 \leq N' \quad \text{(our notation)}.$$

To make sure that N' is not 0, we need

$$q^{-1/2}(1 + (m-1)\sqrt{q})^3 < \frac{(q-1)^3}{q}.$$

This implies

$$1 + (m-1)\sqrt{q} < \frac{q-1}{q^{1/6}}$$

and

$$m < \frac{q-1}{q^{2/3}} - \frac{1}{q^{1/2}} + 1 < q^{1/3} + 1.$$

The inequality $m < q^{1/3} + 1$ follows from [18], too. Putting in our lower bound for m given in (4.1), we find

$$\sqrt{q - 7/4} - 3/2 < q^{1/3} + 1;$$

thus

$$q - \frac{7}{4} < \left(q^{1/3} + \frac{5}{2}\right)^2 = (q^{1/3})^2 + 5q^{1/3} + \frac{25}{4},$$

and so

$$q < (q^{1/3})^2 + 5q^{1/3} + 8.$$

This is only possible for $q < 36$. So for $q \geq 37$ and $2|k$ our theorem shows the existence of solutions outside T in the circular case, while the estimates of Hua and Vandiver as well as Weil do not work.

Acknowledgment

The authors wish to express their gratitude to Professor James R. Clay for his continuous encouragement. The second author also thanks the Alexander von Humboldt Foundation, who sponsored him by a Feodor Lynen Fellowship.

References

1. J. R. Clay, *Circular block designs from planar near rings*, Ann. Discrete Math. **37** (1988), 95–106.
2. ——, *Nearrings: geneses and applications*, Oxford Univ. Press, Oxford, 1992.
3. J. R. Clay and H. Kiechle, *Linear codes from planar near rings and Möbius planes*, Algebras Groups Geom. **10** (1993), 333–344.
4. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
5. ——, *Congruences involving only e-th powers*, Acta Arith. **1** (1936), 161–167.
6. O. B. Faircloth, *On the number of solutions of some general types of equations in a finite field*, Canad. J. Math. **4** (1952), 343–351.
7. L.-K. Hua and H. S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 94–99.
8. ——, *On the number of solutions of some trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 477–481.
9. K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, second ed., Springer-Verlag, Berlin, Heidelberg, and New York, 1990.
10. J. -R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseign. Math. (2) **19** (1973), 1–117.
11. W.-F. Ke, *Structures of circular planar nearings*, Ph.D. dissertaton, Univ. Arizona, Tucson, 1992.
12. W.-F. Ke and H. Kiechle, *Combinatorial properties of ring generated circular planar nearings* (submitted).
13. D. H. Lehmer, *The number of solutions of a certain congruence involving the sum of like powers*, Utilitas Math. **39** (1991), 65–89.
14. H. H. Mitchell, *On the congruence $cx^\lambda + 1 \equiv dy^\lambda$ in a Galois field*, Ann. of Math. (2) **18** (1917), 120–131.
15. M. C. Modisett, *A characterization of the circularity of certain balanced incomplete block designs*, Ph.D. dissertation, Univ. Arizona, Tucson, 1988.
16. ——, *A characterizatin of the circularity of balanced incomplete block designs*, Utilitas Math. **35** (1989), 83–94.
17. Q. Sun, *The diagonal equation over a finite field F_p*, Sichuan Daxue Xuebao **26** (1989), 159–162. (Chinese)

18. A. Weil, *Number of solutions of equations in a finite field*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

19. J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. Number Theory **42** (1992), 247–257.

DEPARTMENT OF MATHEMATICS, NATIONAL CHENG KUNG UNIVERSITY, TAINAN, TAIWAN 70101, REPUBLIC OF CHINA

MATHEMATISCHES INSTITUT, TECHNISCHE UNIVERSITÄT MÜNCHEN, D-80290 MÜNCHEN, GERMANY

E-mail address: `kiechle@mathematik.tu-muenchen.de`