Progress in Computer Science and Applied Logic, Vol. 20

Counting the Number of Points on Affine Diagonal Curves

Cunsheng Ding, David R. Kohel, and San Ling

Abstract. The number of points on affine diagonal curves $aX^m + bY^n = c$ over finite fields can be computed in terms of cyclotomic numbers. The approach of Berndt, Evans and Williams [1] is to express the number of points in terms of generalized Jacobi sums, then to relate the Jacobi sums $J_r(\chi^u, \chi^v)$ to cyclotomic numbers. In this article we present the direct elementary method for the number of points on the affine curves $aX^m + bY^n = c$ over finite fields in terms of cyclotomic numbers. This approach is applicable when explicit formulas are already known for cyclotomic numbers, and circumvents the use of Jacobi sums. It generalizes to the determination of the number of points on affine diagonal hypersurfaces of higher dimension. The curves for which this method applies includes examples of elliptic and hyperelliptic curves which are of interest for public-key cryptosystems, coding theory and the design and analysis of sequences.

1. Introduction

Public-key cryptosystems play an important role in information and system security [21]. Elliptic and hyperelliptic curves have been successfully employed to construct public-key cryptosystems [12, 13, 19, 20]. Counting the number of points on these curves is necessary for the construction of such cryptosystems [14, 18]. Curves have also important applications in sequences and coding theory [24, 25].

Let α be a generating element of $\mathrm{GF}(q)^*$, and let e be a positive divisor of $q-1$. The cyclotomic classes $C_i^{(e)}$ of order e are defined with respect to α as $C_i^{(e)} = \alpha^i C_0^{(e)}$ for $i = 0, \ldots, e-1$, where $C_0^{(e)} = \{\beta^e \mid \beta \in \mathrm{GF}(q)^*\}$ is the set of e-th residues in $\mathrm{GF}(q)$. The corresponding *cyclotomic numbers* of order e are defined by

$$(i,j)_e = \left|\left(C_i^{(e)} + 1\right) \cap C_j^{(e)}\right|, \quad 0 \le i, j \le e-1.$$

Cyclotomic numbers were introduced by Gauss [11, §358] in his treatment of the number of solutions (x, y) of

$$aX^3 \equiv bY^3 + 1 \pmod{p}.$$

In the course of his general study he also defines the *periods* [11, §343], which we now refer to as Gaussian periods. The study of relations, properties and formulas for cyclotomic numbers and Gaussian periods is referred to as *cyclotomy.*

Cyclotomy finds applications in Waring's problems [5], the construction of difference sets [26, 27, 29] and almost difference sets [3], coding theory [7, 8, 9, 16, 17], and cryptography [3]. Dickson [6] used cyclotomy to derive results on the number of solutions of the diagonal surfaces $aX^m + bY^m + cZ^m = d$.

The connection between the number of points on affine diagonal curves and cyclotomy is generally expressed in terms of the theory of Jacobi sums. Berndt et al. [1], for example, express the number of points on an affine diagonal curve $aX^m + bY^n = c$ in terms of cyclotomic numbers via a two step process. First the number of points is expressed in terms of generalized Jacobi sums, then they show that the collection of Jacobi sums $J_r(\chi^u, \chi^v)$ can be expressed in terms of cyclotomic numbers. In this paper we present the direct elementary method for the calculation of the number of points on the affine diagonal curves $aX^m + bY^n = c$ over finite fields in terms of cyclotomic numbers. This applies in particular when m and n divide an exponent e for which explicit formulas are known for cyclotomic numbers. If one of the exponents $m = 2$, and $n > 4$, then the corresponding curve is hyperelliptic, and when (m, n) is one of $(2, 3)$, $(2, 4)$, or $(3, 3)$, the curve is elliptic. In the latter cases the curves have complex multiplication, and the determination of the number of points over a finite field does not require any of the sophisticated methods of Schoof, Atkin, and Elkies (see [22, 23, 10]). This direct approach circumvents the need to compute or analyse Jacobi sums, and provides an effective means of computing the number of points on more general diagonal hypersurfaces in terms of cyclotomic numbers.

2. Cyclotomy and Affine Diagonal Curves

In this section we use cyclotomic numbers to express the number of points on the curve

$$aX^m + bY^n = 1 \tag{1}$$

over $\mathrm{GF}(q)$, where a and b are in $\mathrm{GF}(q)^*$, in terms of the cyclotomic numbers of certain order. It is straightforward to see that when $m = n \,|\, q-1$, then the number of points (x, y) on (1) with $xy \neq 0$ is m^2 times a cyclotomic number.

Given a curve $aX^m + bY^n = c$, we first write $m = m_1 m_2$ and $n = n_1 n_2$, where $m_2 = \gcd(q-1, m)$ and $n_2 = \gcd(q-1, n)$. Then there exist integers r and s, relatively prime to $q-1$, such that $rm \equiv m_2 \bmod q-1$ and $sn \equiv n_2 \bmod q-1$. Since the maps $\alpha \mapsto \alpha^r$ and $\alpha \mapsto \alpha^s$ are automorphisms of $\mathrm{GF}(q)^*$ sending k-th residues to k-residues, the curve $aX^{mr} + bY^{ns} = 1$, or equivalently the curve $aX^{m_2} + bY^{n_2} = 1$, has the same number of points as the curve (1). We can thus reduce to the case that m and n both divide $q-1$. Henceforth, we assume that m and n divide $q-1$. We set e equal to the least common multiple of m and n, which clearly also divides $q-1$.

The genus of the curve (1) is known to be

$$\frac{(m-1)(n-1)-\gcd(m,n)+1}{2}.$$

For exponents (m,n) with $1 < m \leq n$, the curve has genus zero if and only if $(m,n) = (2,2)$ and has genus one if and only if (m,n) is in $\{(2,3),(2,4),(3,3)\}$. Of particular interest are the hyperelliptic curves, where $m = 2$ and $n > 4$.

As before, fix a primitive element α of GF(q), and define cyclotomic classes $C_i^{(m)}$ of order m. Now we consider the relation among the cyclotomic classes of orders m and e.

Lemma 2.1. *Suppose that $e = mr$. Then $C_j^{(m)}$ is the disjoint union of the r cyclotomic classes $C_{im+j}^{(e)}$ for $0 \leq i < r$.*

Proof. It is straightforward to see that $C_0^{(m)} = \bigcup_{i=0}^{r-1} C_{im}^{(e)}$. Hence $C_j^{(m)} = \alpha^j C_0^{(m)}$ has the form indicated. □

Let $N(a,b)$ denote the number of points on the curve (1), and define $\delta_m(c)$ to be the number of solutions of the equation $cX^m = 1$. It is clear that $\delta_m(c)$ equals m if c is an m-th residue and is zero otherwise.

Theorem 2.2. *Let r and s be the integers such that $e = mr = ns$, and define h and k to be integers such that $-a$ and b lie in $C_h^{(e)}$ and $C_k^{(e)}$, respectively. Then*

$$N(a,b) = \delta_m(a) + \delta_n(b) + mn \sum_{i=0}^{r-1} \sum_{j=0}^{s-1} (in+h, jm+k)_e.$$

Proof. It is clear that $N(a,b) - \delta_m(a) - \delta_n(b)$ is the number of points (x,y) on (1) such that $xy \neq 0$. Since x^m takes on each element of $C_0^{(m)}$ exactly m times as x ranges over GF(q)*, it follows that

$$\begin{aligned}
N(a,b) - \delta_m(a) - \delta_n(b) &= mn \Big| \big(-a\, C_0^{(m)} + 1 \big) \bigcap b\, C_0^{(n)} \Big| \\
&= mn \Big| \big(\bigcup_{i=0}^{s-1} -a\, C_{im}^{(e)} + 1 \big) \bigcap \big(\bigcup_{j=0}^{s-1} b\, C_{jn}^{(e)} \big) \Big| \\
&= mn \Big| \big(\bigcup_{i=0}^{r-1} C_{im+h}^{(e)} + 1 \big) \bigcap \big(\bigcup_{j=0}^{s-1} C_{jn+k}^{(e)} \big) \Big| \\
&= mn \sum_{i=0}^{r-1} \sum_{j=0}^{s-1} (im+h, jn+k)_e,
\end{aligned}$$

which completes the proof. □

In the next section we apply the theorem to the determination of the number of points on curves which have the form (1).

3. Examples and Computations

Theorem 2.2 shows that the number of points on curves of form (1) can be calculated when cyclotomic numbers of order e are known. We now do some specific computations to illustrate this idea.

Example 3.1. We consider the genus one curve

$$aX^2 + bY^4 = 1,$$

over GF(q), where $q \equiv 1 \bmod 4$. By definition $\delta_2(a) = 2$ if $a \in C_0^{(4)} \cup C_2^{(4)}$, and $\delta_2(a) = 0$ otherwise. Similarly $\delta_4(b) = 4$ if $b \in C_0^{(4)}$, and $\delta_4(b) = 0$ otherwise. To calculate the number of points on this curve, we apply the known formulas for the cyclotomic numbers of order 4.

It has been proven [26] that the 16 possible cyclotomic numbers $(h,k)_4$ are determined by the decomposition $q = u^2 + 4v^2$, where $u \equiv 1 \bmod 4$ and the sign of v is dependent on the choice of the primitive root used to define the cyclotomic classes. There are at most five distinct cyclotomic numbers of order 4. The relations of these numbers are given in Table 1, and the values A, B, C, D and E are given by Table 2.

$h\backslash k$	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

when $q \equiv 1 \bmod 8$

$h\backslash k$	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

when $q \equiv 5 \bmod 8$

TABLE 1. The relations of the cyclotomic numbers of order 4.

	$q \equiv 1 \bmod 8$	$q \equiv 5 \bmod 8$
$16A$	$q - 11 - 6u$	$q - 7 + 2u$
$16B$	$q - 3 + 2u + 8v$	$q + 1 + 2u - 8v$
$16C$	$q - 3 + 2u$	$q + 1 - 6u$
$16D$	$q - 3 + 2u - 8v$	$q + 1 + 2u + 8v$
$16E$	$q + 1 - 2u$	$q - 3 - 2u$

TABLE 2. The values of the cyclotomic numbers of order 4.

Let $(-a,b) \in C_h^{(2)} \times C_k^{(4)}$. From Theorem 2.2 and the tables of cyclotomic numbers and their relations, it follows that the number of points $N(a,b)$ on the curves $aX^2 + bY^4 = 1$ are those given by Table 3. □

(h,k)	$q \equiv 1 \bmod 8$	$q \equiv 5 \bmod 8$
$(0,0)$	$q-1-2u$	$q-1+2u$
$(0,1)$	$q+1+4v$	$q+1-4v$
$(0,2)$	$q-1+2u$	$q-1-2u$
$(0,3)$	$q+1-4v$	$q+1+4v$
$(1,0)$	$q+1+2u$	$q+1-2u$
$(1,1)$	$q-1-4v$	$q-1+4v$
$(1,2)$	$q+1-2u$	$q+1+2u$
$(1,3)$	$q-1+4v$	$q-1-4v$

TABLE 3. The number of points on $aX^2 + bY^4 = 1$.

Remark 3.2. Since the genus of the curve is one, the number of points of the projective model $\mathcal{C} : aX^2Z^2 + bY^4 = Z^4$ of the curve of Example 3.1 must satisfy the Hasse bound

$$||\mathcal{C}(\mathrm{GF}(q))| - q - 1| \leq 2\lfloor\sqrt{q}\rfloor.$$

If $u = 1$ or $v = \pm 1$ remains fixed, then for $q = u^2 + 4v^2$ sufficiently large, one verifies from Table 3 that there exist curves $\mathcal{C}$ of this form attaining the maximal possible points for this genus.

Example 3.3. We consider the genus 2 hyperelliptic curve

$$X^2 = Y^6 + 1.$$

over $\mathrm{GF}(q)$, where $q \equiv 7 \bmod 12$. In the notation of Theorem 2.2 we have $m = 2$, $n = 6$, $e = 6$, and $a = -b = 1$, so find $\delta_2(a) = 2$ and $\delta_6(b) = 0$. To calculate the number of points on this curve, we apply known formulas for cyclotomic numbers of order 6 (see [26]). The relations of these numbers are given in Table 4.

$h\backslash k$	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	E	C	I
2	H	J	G	F	I	B
3	A	G	H	A	G	H
4	G	F	I	B	H	J
5	H	I	E	C	I	G

TABLE 4. The relations of the cyclotomic numbers of order 6.

For $q \equiv 7 \bmod 12$, the 36 cyclotomic numbers are functions of a representation $q = u^2 + 3v^2$, where $u \equiv 1 \bmod 3$ and the sign of v is dependent on the choice of primitive root used to define the cyclotomic classes.

Let α be the primitive element of $\mathrm{GF}(q)$ employed to define the cyclotomic classes of order 6, and let $2 = \alpha^m$. The values of the 10 basic constants are given in Table 5. By Theorem 2.2 and the above cyclotomic numbers of order 6, we find

	$m \equiv 0 \bmod 3$	$m \equiv 1 \bmod 3$	$m \equiv 2 \bmod 3$
$36A$	$q-11-8u$	$q-11-2u$	$q-11-2u$
$36B$	$q+1-2u+12v$	$q+1-2u-12v$	$q+1+4u$
$36C$	$q+1-2u+12v$	$q+1-8u+12v$	$q+1-2u+12v$
$36D$	$q+1+16u$	$q+1+10u+12v$	$q+1+10u-12v$
$36E$	$q+1-2u-12v$	$q+1-2u-12v$	$q+1-8u-12v$
$36F$	$q+1-2u-12v$	$q+1+4u$	$q+1-2u+12v$
$36G$	$q-5+4u+6v$	$q-5+4u+6v$	$q-5-2u+6v$
$36H$	$q-5+4u-6v$	$q-5-2u-6v$	$q-5+4u-6v$
$36I$	$q+1-2u$	$q+1+4u$	$q+1+4u$
$36J$	$q+1-2u$	$q+1-8u+12v$	$q+1-8u-12v$

TABLE 5. The values of the cyclotomic numbers of order 6.

$$\begin{aligned} N(1,-1) &= 2+12\sum_{i=0}^{2}(0,2i+3)_6 \\ &= 2+12(E+A+C) = q-1-4u \end{aligned}$$

for the number of points on the curve $X^2 = Y^6+1$. □

Let $F(X)$ and $G(X)$ be permutation polynomials for GF(q). Then Theorem 2.2 also applies to curves of the form

$$aF(X)^m + bG(Y)^n = 1.$$

We indicate in the next example how this can be applied to point counting on curves of a more exotic form.

Example 3.4. Let q be of the form $30t+7$. Then $5X^5+5cX^3+c^2X$ is a permutation polynomial of GF(q) [15, p. 352]. Let $F(X) = 5X^5+5X^3+X$ and $G(Y) = 5Y^5-5Y^3+Y$. Then both $F(X)$ and $G(Y)$ are permutation polynomials of GF(q). Then the number of points on the curve

$$\begin{aligned} &125X^{15}+375X^{13}+450X^{11}+275X^9+90X^7+15X^5+X^3+ \\ &25Y^{10}-50Y^8+35Y^6-10Y^4+Y^2 = 1 \end{aligned}$$

can be computed with the help of cyclotomic numbers of order 6. □

It should be noted that in each of the above examples a specific equation was treated. With a minimal amount of additional work, by Theorem 2.2 the complete set of cyclotomic numbers $(i,j)_{m,n}$ of *mixed order* m,n could be determined, reducing the formulas for cyclotomic numbers of order e to explicit mixed order formulas for all divisors m,n of e.

4. Generalization

The concepts of cyclotomic numbers have natural generalizations to higher dimensions, and for many fixed exponents and dimensions it is possible to find explicit formulas for these values. This permits a cyclotomic approach to the study of general diagonal hypersurfaces

$$a_1X_1^{e_1} + a_2X_2^{e_2} + \cdots + a_nX_n^{e_n} = 1 \tag{2}$$

over $\mathrm{GF}(q)^n$. In fact these equations are *quotients* of the hypersurface

$$a_1Z_1^e + a_2Z_2^e + \cdots + a_nZ_n^e = 1, \tag{3}$$

where e_i divides e for each i, by the map $(z_1, \ldots, z_n) \longmapsto (z_1^{e/e_1}, \ldots, z_n^{e/e_n})$. There exist other quotients, and it is an interesting problem to determine the number of points on these general quotients.

To illustrate how the number of solutions of the general diagonal hypersurface (2) is determined by cyclotomic numbers, we consider the special case

$$X_1^2 + X_2^4 + X_3^2 + X_4^4 = 1 \tag{4}$$

over the field $\mathrm{GF}(q)$, where $q \equiv 1 \bmod 4$.

We denote the number of points on $X^2+Y^4 = a$ by $N(a)$. Then $N(0) = 2q-1$, and otherwise, when $a \in C_k^{(4)}$, it follows from the computation in Example 3.3 that $N(a)$ is given by

k	$q \equiv 1 \bmod 8$	$q \equiv 5 \bmod 8$
0	$q-1+2u$	$q-1-2u$
1	$q-1-4v$	$q-1+4v$
2	$q-1-2u$	$q-1+2u$
3	$q-1+4v$	$q-1-4v$

where $q = u^2 + 4v^2$. Let $h = (q-1)/2 \bmod 4$ so that $C_h^{(4)}$ is the cyclotomic class of -1. Then the number N of points on the hypersurface (4) is given by

$$\begin{aligned}
N &= \sum_{a \in \mathrm{GF}(q)} N(a)N(1-a) \\
&= 2N(0)N(1) + \sum_{i=0}^{3}\sum_{j=0}^{3} |C_i^{(4)} \cap (1 - C_j^{(4)})| N(\alpha^i)N(\alpha^j) \\
&= 2N(0)N(1) + \sum_{i=0}^{3}\sum_{j=0}^{3} |C_{i+h}^{(4)} \cap (C_j^{(4)} - 1)| N(\alpha^i)N(\alpha^j) \\
&= 2N(0)N(1) + \sum_{i=0}^{3}\sum_{j=0}^{3} (i+h, j)_4 N(\alpha^i)N(\alpha^j).
\end{aligned}$$

From this formula, we find that when $q \equiv 1 \bmod 8$ we have

$$N = q^3 - q(4u+1) - 2(u^3 + u^2 + 4uv^2 + 4v^2),$$

for the number of points on the hypersurface (4). For example, when $q = 17$, we have $N = 4760$. When $q \equiv 5 \bmod 8$, we derive a similar formula. □

The approach given in Berndt et al. [1] requires the computation of generalized Jacobi sums $J_r(\chi_1^{n_1}, \chi_2^{n_2}, \chi_3^{n_3}, \chi_4^{n_4})$. This example shows, for small exponents e, how the approach through cyclotomic numbers suffices to compute points on general diagonal hypersurfaces.

5. Concluding Remarks

The classical approach to the study of point counting on curves over finite fields is to express the number of points in terms of character sums. The number of points on the curve (1) and more generally the diagonal hypersurface (2), can be expressed in terms of Jacobi or Gaussian sums (see [15, Section 6.3] and [1]). In 1934 Davenport and Hasse [4] gave theoretical characterizations of these sums, which is the foundation for most of the present-day explicit formulas for cyclotomic numbers. Via a more computationally sophisticated algorithm, Buhler and Koblitz [2] recently showed, at least for prime exponents e, that it is possible to apply this characterization directly to compute the number of points on certain hyperelliptic curves of the form (1) in polynomial time. In contrast, the present approach makes use of elementary formulas with simple implementation, to treat the same hyperelliptic curves.

The use of elliptic curves has become central to public-key cryptography in the last years, and considerable attention has been given to the subject of hyperelliptic curves in cryptography. Beyond the examples of elliptic and hyperelliptic curves for which the present method can be applied, the general class of diagonal curves may be of future interest for cryptosystems because of their rich structure and amenability to rapid point counting algorithms. In addition, curves of the form (1) with relative small exponents may be useful in constructing error correcting codes and sequences. Detailed information about curves and their applications in coding theory, sequences and cryptography can be found in [24, 25].

Acknowledgments: The authors thank the reviewer for helpful comments that improved the presentation of this paper.

References

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums,* John Wiley & Sons, Inc., 1998.

[2] J. Buhler and N. Koblitz, *Lattice basis reduction, Jacobi sums, and hyperelliptic cryptosystems*, Bull. Austral. Math. Soc., **58** (1998), 147–154.

[3] T. Cusick, C. Ding, and A. Renvall, *Stream ciphers and number theory*, North-Holland Mathematical Library, Elsevier/North-Holland, 1998

[4] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math., **172** (1934), 115–182.

[5] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391–424, and 463–474.

[6] L. E. Dickson, *Congruences involving only e-th powers,* Acta Arith., **1** (1936), 161–167.

[7] C. Ding and T. Helleseth, *New generalized cyclotomy and its applications,* Finite Fields and Their Applications, **4** (1998), 140–166.

[8] C. Ding and T. Helleseth, *Generalized cyclotomic codes of length* $p_1^{e1} \cdots p_t^{et}$, IEEE Trans. Information Theory, **45(2)** (1999), 467–474.

[9] C. Ding and V. Pless, *Cyclotomy and duadic codes of prime lengths,* IEEE Trans. Information Theory, **45(2)** (1999), 453–466.

[10] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in: Computational Perspectives on Number Theory, A conference in honor of A.O.L. Atkin, 1998.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801. English translation, Yale, New Haven, 1966.

[12] N. Koblitz, *Elliptic curve cryptosystems,* Math. Comp., **48** (1987), 203–209.

[13] N. Koblitz, *Hyperelliptic curve cryptosystems,* J. Cryptology, **1** (1989), 139–150.

[14] N. Koblitz, *CM curves with good cryptographic properties,* Advances in Cryptology — Proc. Crypto'91, Lecture Notes in Comput. Sci., Vol. 576, Springer-Verlag, Berlin, 1992, 279–287.

[15] R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley, 1983; Second edition, Cambridge University Press, 1997.

[16] F. J. MacWilliams, *Cyclotomic numbers, coding theory and orthogonal polynomials,* Discrete Mathematics, **3** (1972), 133–151.

[17] R. J. McEliece and H. Rumsey, Jr., *Euler products, cyclotomy, and coding,* J. of Number Theory, **4** (1972), 302–311.

[18] A. J. Menezes, S. A. Vanstone, and R. J. Zuccherato, *Counting points on elliptic curves over* F_{2^m}, Math. Comp., **60** (1993), 407–420.

[19] V. Miller, *Uses of elliptic curves in cryptography,* Advances in Cryptology–Proc. Crypto'85, Lecture Notes in Comp. Sci., Vol. 218, Springer-Verlag, Berlin, 1986, 417–426.

[20] T. Okamoto and K. Sakurai, *Efficient algorithms for the construction of hyperelliptic cryptosystems,* Advances in cryptology – Proc. Crypto'91, Lecture in Comput. Sci., Vol. 576. Springer-Verlag, Berlin, 1991, 267–278.

[21] A. Salomaa, *Public-key cryptography,* 2nd Ed., Springer-Verlag, 1996.

[22] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp., **44** (1985), 483–494.

[23] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux., **7** (1995), 219–254.

[24] I. E. Shparlinski, *Computational and algorithmic problems in finite fields,* Mathematics and Its Applications, **88** (1992), Kluwer Academic Publishers, Boston, London.

[25] I. E. Shparlinski, *Finite fields: theory and computation – the meeting point of number theory, computer science, coding theory and cryptography,* Mathematics and Its Applications, **477** (1999), Kluwer Academic Publishers, Boston, London.

[26] T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, 1967.

[27] T. Storer, *Cyclotomies and difference sets modulo a product of two distinct odd primes*, Michigan Math. J., **14** (1967), 117–127.

[28] A. L. Whiteman, *The cyclotomic numbers of order twelve,* Acta Arith., **6** (1960), 53–76.

[29] A. L. Whiteman, *A family of difference sets*, Illinois J. Math., **6** (1962), 107–121.

Cunsheng Ding
Department of Computer Science
National University of Singapore
S16, Room 05-08, 3 Science Drive 2
Singapore 117543
E-mail address: dingcs@comp.nus.edu.sg

David R. Kohel
School of Mathematics and Statistics
Carslaw Building, F7, University of Sydney
Sydney, NSW 2006, Australia
E-mail address: kohel@maths.usyd.edu.au

San Ling
Department of Mathematics
National University of Singapore
2 Science Drive 2, Singapore 117543
E-mail address: matlings@nus.edu.sg