Journal of the Indian Math. Soc.
Vol. 54 (1989) 125–132

SOME IDENTITIES INVOLVING CHARACTER SUMS AND THEIR APPLICATIONS

J.C. PARNAMI, M.K. AGRAWAL AND A.R. RAJWADE

[Received July 29, 1988; Revised November 19, 1988]

§ 1. The identities. It is well known [8], that if the two elliptic curves $y^2 = f(x)$ and $y^2 = g(x)$, defined over the integers $\mathbb{Z}$ are isogenous, then for all primes $p \neq 2, 3$ and not dividing the discriminant of either, the character sums $\sum_{x(\mathrm{mod}\ p)} (f(x)/p)$ and $\sum_{x(\mathrm{mod}\ p)} (g(x)/p)$ are equal, where $(\cdot/p)$ is the Legendre symbol.

In this paper, we use a theorem of Velu [10] to construct isogenies of degrees 2 and 3 from suitable elliptic curves and then apply the above remark to obtain some identities involving character sums. We then use these identities to evaluate certain character sums involving elliptic curves. We first give a statement of Velu's theorem:

THEOREM A (*Velu* [10]). *Let E be an elliptic curve given by the equation $y^2 = x^3 + ax^2 + bx + c$, defined over the rationals Q and let F be a finite subgroup of E. Let F_2 be the set of points of $F-\{I\}$ (I the identity of E) of order 2, R the set of points of $F-\{I\}-F_2$ such that*

$$F - \{I\} - F_2 = R \cup -R, \quad -R \cap R = \phi$$

and let $S = F_2 \cup R$. Let $t = \sum_{Q \in S} t_Q$, $w = \sum_{Q \in S} (u_Q + x_Q t_Q)$, where if $\phi(x, y)$ is written for $x^3 + ax^2 + bx + c - y^2$, then

$$g_Q^x = (\partial\phi/\partial x)_Q,\ g_Q^y = (\partial\phi/\partial y)_Q,\ u_Q = (g_Q^y)^2,$$

$$t_Q = \begin{cases} g_Q^x \text{ if } Q \in F_2, \\ 2g_Q^x \text{ if } Q \notin F_2, \end{cases}$$

where we write $Q = (x_Q, y_Q)$. Let E^* be the curve

$$y^2 = x^3 + ax^2 + (b - 5t)\,x + (c - 4at - 7w).$$

Then the map $f: E \to E^*$ *given by* $f: (x, y) \to (X, Y)$, *where*

$$X = x + \sum_{Q \in S} \left\{ \frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right\},$$

$$Y = y - \sum_{Q \in S} \left\{ \frac{2yu_Q}{(x - x_Q)^3} + \frac{t_Q(y - y_Q) - g_Q^x g_Q^y}{(x - x_Q)^2} \right\}$$

is an isogeny from E *to* E^* *with kernel* F. *Moreover if* f_1 *is any other isogeny from* E *to* E' *with kernel* $f_1 = f$, *then* E' *and* E^* *are birationally equivalent.*

The order of the kernel F is called the degree of the isogeny. The construction of the isogenies is affected as follows: Let

$$E: y^2 = x(x^2 + ax + b) \tag{1}$$

be an elliptic curve. We know that (0, 0) is a point of E of order 2. Let $F = \{I, (0, 0)\}$. By Theorem A, the curve

$$E^*: y^2 = x(x^2 - 2ax + (a^2 - 4b)) \tag{2}$$

is isogenous to (1), the isogeny having kernel F. Hence

$$\sum_{x (\mathrm{mod}\, p)} \left(\frac{x(x^2 + ax + b)}{p} \right) = \sum_{x (\mathrm{mod}\, p)} \left(\frac{x(x^2 - 2ax + (a^2 - 4b))}{p} \right) \tag{3}$$

for every prime $p \neq 2$, 3 and not dividing the discriminant $16b^2(a^2 - 4b)$. It is not difficult to see that (3) holds even for $p = 3$ and for primes $p > 3$ that divide the discriminant $16b^2(a^2 - 4b)$. For $p = 3$, a direct hand calculation gives the result. For $p > 3$ dividing the discriminant, either $p \mid b$ or $p \mid a^2 - 4b$. In the first case result follows on letting $x \to x - a$ in the left side of (3). In the second case, letting $x \to (x - 2a)/4$ gives the result. Hence we get

THEOREM 1. *For any odd prime* p *and integers* a, b, *the equation* (3) *holds.*

Remarks: 1. A particular case of Theorem 1 (with $a = -4$, $b = 2$) was proved by Williams [12]. His proof can be generalized to realise Theorem 1 as follows:

$$\sum_{x=0}^{p-1} \left(\frac{x(x^2 + ax + b)}{p} \right) = \sum_{x=1}^{p-1} \left(\frac{x + b/x + a}{p} \right)$$

$$= \sum_{X} \left(\frac{X + a}{p} \right) \left\{ 1 + \left(\frac{X^2 - 4b}{p} \right) \right\}$$

where

$$X = (x + b/x)$$

$$= \sum_{X(\mathrm{mod}\ p)} \left(\frac{X(X^2 - 2aX + a^2 - 4b)}{p}\right)$$

as required.

2. The transformation of Remark 1 is precisely the same as that in Velu's theorem in the present particular case.

So much for the isogeny of degree 2.

Next let E: $y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve with $c \neq 0$. Then $P = (0, \sqrt{c})$ is a point of E of order 3 if and only if $b^2 = 4ac$. When this is so, we see, by Velu's theorem that the curve

$$E^*\colon\ y^2 = x^3 + ax^2 - 9bx - (27c + 8ab)$$

is isogenous to E, the kernel of the isogeny being $\{I, \pm P\}$. It follows that

$$\sum_{x(\mathrm{mod}\ p)} \left(\frac{x^3 + ax^2 + bx + c}{p}\right) = \sum_{x(\mathrm{mod}\ p)} \left(\frac{x^3 + ax^2 - 9bx - (27c + 8ab)}{p}\right) \qquad x(\mathrm{mod} \tag{4}$$

for primes $p \neq 2, 3$ and not dividing the discriminant $8(b^3 - 54\,c^2)$ of E. Here again we shall show that (4) holds for $p = 3$ and for primes $p > 3$ that divide the discriminant $8(b^3 - 54c^2)$. For $p = 3$ a direct hand calculation gives the result. So let $p(> 3)$ be a prime that divides the discriminant. We have

(i) $b^3 \equiv 54c^2 \pmod{p}$, and

(ii) $b^2 \equiv 4ac$ (by hypothesis).

These give

$$27b \equiv 8a^3 \text{ and } 27^2 c \equiv 16a^3. \tag{5}$$

Now let $x \to (3x - 8a)/27$ in the left hand side of (4) and using (5) we get the right hand side. Hence we have

THEOREM 2. *For any odd prime p and integers a, b, c satisfying $b^2 = 4ac$, the equation* (4) *holds.*

§ 2. **Applications.** As our first application, we look at elliptic curves with complex multiplication. In addition to the nine elliptic curves E_m

defined over the rationals Q, with End E_m equal to the full ring of integers of $Q(\sqrt{-m})$, $m = 1, 2, 3, 7, 11, 19, 43, 67, 163$, there are exactly four other curves, defined over Q, whose endomorphism rings are proper subrings of the full ring. They are C_j: $y^2 = f_j(x)$ $(j = 1, 2, 3, 4)$, where

$$f_1(x) = x^3 - 6x^2 + x \quad \text{with End } C_1 = \mathbb{Z}[2i],$$

$$f_2(x) = x^3 + 6x^2 - 3x \quad \text{with End } C_2 = \mathbb{Z}[\sqrt{-3}],$$

$$f_3(x) = x^3 - 42x^2 - 7x \quad \text{with End } C_3 = \mathbb{Z}[\sqrt{-7}],$$

$$f_4(x) = x^3 - 120x + 506 \text{ with End } C_4 = \mathbb{Z}\left[\frac{3(-1+\sqrt{-3})}{2}\right].$$

We wish to evaluate the character sums $\sum_{x(p)} (f_j(x)/p)$.

COROLLATY 1. *The character sum* $\sum (f_1(x)/p)$

$$= \begin{cases} 2a \text{ if } p \equiv 1(4),\ p = a^2 + b^2,\ a \equiv 2 + \left(\frac{2}{p}\right) (\text{mod } 4), \\ 0 \quad \text{if } p \equiv 3(4). \end{cases}$$

Proof.

$$\sum\left(\frac{f_1(x)}{p}\right) = \sum\left(\frac{x^3 - 6x^2 + x}{p}\right) = \sum\left(\frac{x^3 + 12x^2 + 32x}{p}\right)$$

(by Theorem 1)

$$= \sum\left(\frac{x^3 + 3x^2 + 2x}{p}\right) \quad (\text{by letting } x \to 4x)$$

$$= \sum\left(\frac{x(x+1)(x+2)}{p}\right) = \sum\left(\frac{x^3 - x}{p}\right)$$

(by letting $x \to x - 1$).

Now this last character sum is known ([1], [2], [4], [9]), since $y^2 = x^3 - x$ is the elliptic curve E_1 mentioned above. This completes the proof.

COROLLARY 2. *The character sum*

$$\sum(f_3(x)/p) = \begin{cases} 2a \text{ if } p \equiv 1(3),\ p = a^2 + 3b^2,\ a \equiv -1(3), \\ 0 \quad \text{if } p \equiv 2(3). \end{cases}$$

Proof.

$$\sum(f_2(x)/p) = \sum\left(\frac{x^3+6x^2-3x}{p}\right) = \sum\left(\frac{x^3-12x^2+48x}{p}\right)$$

(by Theorem 1)

$$= \sum\left(\frac{x^3-3x^2+3x}{p}\right) \text{ (by letting } x \to 4x)$$

$$= \sum\left(\frac{x^3+1}{p}\right) \text{ (by letting } x \to x+1).$$

Here $y^2 = x^3 + 1$ is the elliptic curve E_3 and so the above sum is known (see [5], [6]). This completes the proof.

COROLLARY 3. *The character sum*

$$\sum(f_3(x)/p) = \begin{cases} 2c \text{ if } (p/7) = 1,\ p = c^2 + 7d^2,\ (c/7) = -1, \\ 0 \quad \text{if } (p/7) = -1. \end{cases}$$

Proof.

$$\sum(f_3(x)/p) = \sum\left(\frac{x^3-42x^2-7x}{p}\right) = \sum\left(\frac{x^3+84x^2+179x}{p}\right)$$

(by Theorem 1)

$$= \sum\left(\frac{x^3+21x^2+112x}{p}\right) \text{ (by letting } x \to 4x).$$

Here $y^2 = x^3 + 21x^2 + 112x$ is the curve E_7 and so the above sum is known (see [7]). This completes the proof.

COROLLARY 4. *The character sum*

$$\sum(f_4(x)/p) = \begin{cases} a \text{ if } p \equiv 1(3),\ 4p = a^2 + 27b^2,\ (a/3) = (2/p), \\ 0 \text{ if } p \equiv 2(3). \end{cases}$$

Proof.

$$\sum(f_4(x)/p) = \sum\left(\frac{x^3-120x+506}{p}\right) = \sum\left(\frac{x^3+18x^2-12x+2}{p}\right)$$

(by letting $x \to x+6$)

$$= \sum\left(\frac{x^3+18x^2+108x+1674}{p}\right) \text{ (by Theorem 2)}$$

$$= \sum\left(\frac{x^3+1458}{p}\right) \text{ (by letting } x \to x-6\text{)}$$

$$= \sum\left(\frac{x^3+2}{p}\right) \text{ (by letting } x \to 9x\text{).}$$

This last equation also holds for $p = 3$ clearly. Here $y^2 = x^3 + 2$ is just E_9 and so this last sum is known This completes the proof.

Williams [11]), using different techniques, has also obtained certain identities and he remarks (on page 297 of [11]) that these identities can be used to evalute $\sum(f_j(x)/p)$, $j = 1, 2, 3$.

It is also interesting to evaluate these sums $\sum(f_j(x)/p)$ directly using the relevant division points and then applying the Frobenius automorphism. Poulakis [3] evaluates $\sum (f_2(x)/p)$ using this very procedure.

As further applications we now obtain some more identities by applying theorem 2 to character sums of the type $\sum\left(\frac{x^3+ax^2+bx}{p}\right)$.

For an arbitrary integer $k \neq 0$, we have

$$\sum\left(\frac{x^3+ax^2+bx}{p}\right) = \sum\left(\frac{(x+k)^3+a(x+k)^2+b(x+k)}{p}\right)$$

$$= \sum\left(\frac{x^3+Ax^2+Bx+C}{p}\right),$$

where $A = 3k + a$, $B = 3k^2 + 2ak + b$, $C = k^3 + ak^2 + bk$, so that $B^2 = 4AC$ if and only if $3k^4 + 4ak^3 + 66k^2 - b^2 = 0$, i.e. if and only if $(6k + a)^2 - a^2 = 3(b/k - 3k)^2$ i.e. if and only if $k \mid b$ and $u = 6k + a$, $v = b/k - 3k$ satisfy the Pellian equation

$$u^2 - 3v^2 = a^2. \tag{5}$$

Thus for a solution (u, v) of (5), satisfying $u \equiv a \pmod 6$, $k = (u-a)/6$, $b = k(v + 3k)$, $B^2 = 4AC$. Let $d = ((u-a)/6, (u+a)/2)$. Then $u^2 - a^2 = 3v^2$ gives

$$\left.\begin{aligned} u - a &= 6\lambda s^2 \\ u + a &= 2\lambda t^2 \\ v &= 2\lambda st \end{aligned}\right\} \tag{6}$$

for some integers λ, s, t (with $\lambda = \pm d$) and conversely for each value of λ, s, t, the Pellian equation (5) is satisfied by the quantities u, a, v defined by (6). Hence

$$\sum\left(\frac{x^3+ax^2+bx}{p}\right)$$

$$= \sum\left(\frac{x^3+\lambda(t^2-3s^2)x^2+\lambda^2s^3(3s+2t)x}{p}\right)$$

$$= \sum\left(\frac{x^3+\lambda t^2x^2+2\lambda^2s^2t(s+t)x+\lambda^3s^4(s+t)^2}{p}\right)$$

(on letting $x \to x+k$)

$$= \sum\left(\frac{x^3+\lambda t^2x^2-18\lambda^2s^2t(s+t)x-\lambda^3(27s^4(s+t)^2+16s^2t^2(s+t))}{p}\right)$$

(by Theorem 2)

$$= \sum\left(\frac{x^3+\lambda(9s^2+12st+t^2)x^2+\lambda^2s(3s+2t)^2x}{p}\right)$$

(on letting $x \to x+\lambda(3s^2+4st)$.

In particular, for $s=1$, $\lambda=-1$, we get the following

THEOREM 3. *For any integer t and odd prime p we have*

$$\sum_{x(\mathrm{mod}\ p)}\left(\frac{x(x^3-(t^2-3)x+(2t+3))}{p}\right)$$

$$= \sum_{x(\mathrm{mod}\ p)}\left(\frac{x(x^3-(t^2+12t+9)x+(2t+3)^2)}{p}\right).$$

For $t=-2$, this gives

$$\sum_{x(\mathrm{mod}\ p)}\left(\frac{x(x^2-x-1)}{p}\right) = \sum_{x(\mathrm{mod}\ p)}\left(\frac{x(x^2+11x-1)}{p}\right).$$

We gather from E. Lehmer, that an 'elementary' proof of this is desirable.

REFERENCES

1. DAVENPORT, H. and H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, Crelle, 172 (1935), 151–182.

2. MORLAYE, B., Demonstration elementaire d'un theoreme de Davenport el Hasse, *L'* Enseignement Mathemetique, 8 (1972), 269–276.

3. POULAKIS, D., Evaluation d'une somme cubique de caracteres, J. Number theory, 27 (1987), 41–45.

4. RAJWADE, A.R., A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - Dx \pmod{p}$, Proc. Camb. Soc., 67 (1970), 603–605.

5. ————————, Arithmetic on curves with complex multiplication by the Eisenstein integers, Proc. Camb. Phil. Soc., 65 (1969), 59–73.

6. ————————, On rational primes p congruent to 1 mod (3 or 5), Proc. Camb. Phil. Soc., 66 (1969), 61–70.

7. ————————, The diophantine equation $y^2 = x(x^2 + 21Dx + 112D^2)$ and the conjectures of Birch and Swinnerton-Dyer J. Australian Maths. Soc., 24 (1977), 286–295.

8. CASSELS, J.W.S., Diophantine equations with a special reference to Elliptic curves, J.L.M.S., 41 (1966), 193–291.

9. SINGH, SURJIT AND A.R. RAJWADE, The number of solutions of the congruence $y^2 \equiv x^4 - a \pmod{p}$, L' Enseignement Mathematique, 20 (1974), 265–273.

10. VELU, J., Isogenies entre courbes elliptiques, C.R. Acad. Paris, (1971), 238–241.

11. WILLIAMS, K.S., Finite transformations formulae involving the Legendre symbol, Pacific J. Maths., 34(1970), 559–568.

12. ————————, Note on Brewer's character sum, Proc. Amer. Math. Soc., 71 (1978), 153–154.

Department of Mathematics
Panjab University
Chandigarh -160014, India