For Theorems 3 and 4, consider the conjugates of θ given by (2.3), where $\alpha \in \mathscr{A}([-2, 2])$ ($\mathscr{C} \in \mathscr{E}$), $\alpha \in \mathscr{A}\big((-\infty, -2] \cup [2, \infty)\big)$ ($\mathscr{C} = \mathscr{H}$), and $B \in S_{\mathscr{C}}$ ($\mathscr{C} = \mathscr{E}, \mathscr{H}$). Then all conjugates of $\frac{1}{2}\big(\alpha + (\alpha^2-4)^{1/2}\big)$ are on U for $\mathscr{C} = \mathscr{E}$, and real for $\mathscr{C} = \mathscr{H}$. Further all conjugates of $\big(\prod_{j=1}^{n} B_j\big)^{1/2}$ are of the form $B^{\pm 1/2}\cdot w$, where w is on U ($\mathscr{C} = \mathscr{E}$) and real ($\mathscr{C} = \mathscr{H}$). Thus the result follows from the parametrization (1.2) of $\mathscr{C}$.

It remains only to show that, given z^* on $\mathscr{C}(0, 1, B^k, 1)$, where $k = k(B)$ and $B^k \in S_{\mathscr{C}}$ ($\mathscr{C} = \mathscr{E}, \mathscr{H}$), then the zeros z of

$$z^* = T_k\left(\frac{(z-C)\,\varepsilon^{1/2}}{R}\right)$$

lie on $\mathscr{C}(C, R, B, \varepsilon)$, where $k = 1$ or 2 for $\mathscr{C} = \mathscr{H}$.

Let $z^* = (\varepsilon B)^{k/2} t + \big((\varepsilon B)^{k/2} t\big)^{-1}$, where $t > 0$ in the case $k = 2$, $\mathscr{C} = \mathscr{H}$. Then the k roots z_j are given by

$$\frac{(z_j - C)\,\varepsilon^{1/2}}{R} = \omega^j (\varepsilon B)^{1/2} t^{1/k} + \big(\omega^j (\varepsilon B)^{1/2} t^{1/k}\big)^{-1} \qquad (j = 0, \ldots, k-1)$$

where $\omega = \exp(2\pi i/k)$, so

$$z_j = C + R\big(\omega^j B^{1/2} t^{1/k} + (\omega^j B^{1/2} t^{1/k})^{-1}\big) \qquad (j = 0, \ldots, k-1).$$

For $\mathscr{C} = \mathscr{E}$, $\omega^j t^{1/k}$ is on U, and $\omega^j t^{1/k}$ is real for $\mathscr{C} = \mathscr{H}$. Thus we have a parametrization (1.2) for z_j, which proves the result.

8. We now prove Theorem 1. Suppose that we have a parabola $\mathscr{P}(C, F)$ with C having a conjugate $C' \neq C$. Then as we saw in the proof of Theorem 2, there are at most 8 possible values for the parameter of an algebraic number z_i with conjugate $z_{i'}$, both on $\mathscr{P}(C, F)$. Hence the sum of the degrees of all algebraic numbers lying with their conjugates on $\mathscr{P}(C, F)$ is at most 8.

A similar argument holds for $\mathscr{C} = \mathscr{E}, \mathscr{H}$, if C or R^2 is irrational, except that 8 is replaced by 24.

References

[1] V. Ennola, *Conjugate algebraic integers on a circle with irrational center*, Math. Z. 134 (1973), pp. 337–350.

[2] V. Ennola and C. J. Smyth, *Conjugate algebraic numbers on a circle*, Ann. Acad. Sci. Fennicae A I 582 (1974).

[3] — — *Conjugate algebraic numbers on circles*, Acta Arith. 29 (1976), pp. 147–157.

[4] R. M. Robinson, *Conjugate algebraic integers on a circle*, Math. Z. 110 (1969), pp. 41–51.

Received on 25.5.1979
and in revised form on 20.9.1979 (1162)

ACTA ARITHMETICA
XL (1982)

A new cubic character sum

by

A. R. Rajwade and J. C. Parnami (Chandigarh, India)

1. Introduction and the statement of the main result. For a polynomial $f(x)$ with integer coefficients, the character sum Σ_f is defined by $\sum_{x (\mathrm{mod}\, p)} (f(x)|p)$, where p is a prime and $(a|p)$ the Legendre symbol. If $f(x)$ is linear, then clearly $\Sigma_f = 0$ and it is well known that

$$\Sigma_{ax^2+bx+c} = \left(\frac{a}{p}\right)\begin{cases} -1 & \text{if } \ b^2-4ac \not\equiv 0 \pmod{p}, \\ p-1 & \text{if } \ b^2-4ac \equiv 0 \pmod{p}. \end{cases}$$

It is surprising that beyond this little is known even for cubics, except some estimates. It is therefore equally remarkable that the exact value of Σ_f is known for the following cubics:

(i) $x^3 + ax$,

(ii) $x(x^2 + 4ax + 2a^2)$,

(iii) $x^3 + a$, and

(iv) $x(x^2 + 21ax + 112a^2)$.

Proofs of (i) can be found in [2], [7], [12], [16], those of (ii) in [1], [17], [13], [4], [5], those of (iii) in [9], [10], [8], [18], and those of (iv) in [15]. The common feature of these four cubics is that the curve $y^2 = f(x)$ is simply the most general elliptic curve defined over the rationals with complex multiplication by, respectively, $\sqrt{-1}$, $\sqrt{-2}$, $\sqrt{-3}$, $\sqrt{-7}$. There are five other such elliptic curves and it is conjectured by E. Lehmer and R. J. Evans that in each of these cases Σ_f has an answer similar to the above four cases. Recently H. Stark has developed a method which evaluates these sums systematically. The exact statement of Stark's result (unpublished) is:

$\Sigma_{f_m(x)} = c$ where $f_m(x)$ is the corresponding elliptic curve and where $4p = c^2 + md^2$ with $\left(\frac{c}{m}\right) = 1$ if $m = 7$, $\left(\frac{6}{p}\right)$ if $m = 11$, $\left(\frac{2}{p}\right)$ if $m = 19, 43,$ 67, 163.

We gather from E. Lehmer that Stark's proof of this result is far from elementary.

There are a few $f(x)$ of degree > 3 for which Σ_f is known exactly. See [1], [11], [6], [19].

The object of this paper is to treat the case $m = 11$. We make use of the $\sqrt{-11}$ division points on the elliptic curve with complex multiplication by $\sqrt{-11}$. The calculation of these division points is the major difficulty in the proof. The rest is similar to the case treated in [15]. The relevant $f(x)$ in our case is given by

$$f(x) = x^3 - 33\cdot 32a^2x + 7\cdot 16\cdot 11^2a^3.$$

For this f we have (by letting $x \to 2ax$)

$$\Sigma_f = \left(\frac{2a}{p}\right)\sum_{x(\bmod p)}\left(\frac{x^3-8\cdot 33x+14\cdot 11^2}{p}\right) = \left(\frac{2a}{p}\right)\mathfrak{S}, \quad \text{say}.$$

Our aim is the following:

THEOREM 1. *We have*

$$\mathfrak{S} = \begin{cases} 0 & \text{if } p \equiv 2, 6, 7, 8, 10 \pmod{11}, \\ c & \text{otherwise, where } 4p = c^2 + 11d^2 \text{ with } c \\ & \text{determined uniquely by } (c|11) = (6|p). \end{cases}$$

2. The $\sqrt{-11}$ division points on $y^2 = f(x)$. Let

$$y^2 = f(x) = x^3 - 33\cdot 32a^2x + 11^2\cdot 7\cdot 16\cdot a^3 \tag{2.1}$$

be the general elliptic curve with complex multiplication by $\sqrt{-11}$. If (x, y) is a generic point on (2.1), then it is known that [14]

$$\frac{-1+\sqrt{-11}}{2}(x, y) = (X, Y),$$

where

$$X = \frac{-(5+\sqrt{-11})[x^3-4(11-\sqrt{-11})ax^2+}{18[x-2(11-\sqrt{-11})a]^2}$$
$$\frac{+88(11-7\sqrt{-11})a^2x-704(11-14\sqrt{-11})a^3]}{18[x-2(11-\sqrt{-11})a]^2},$$

$$Y = \frac{(4-\sqrt{-11})[x^3-6(11-\sqrt{-11})ax^2+}{27[x-2(11-\sqrt{-11})a]^3}$$
$$\frac{+88\cdot 3(3+\sqrt{-11})a^2x+11\cdot 64(11-6\sqrt{-11})a^3]y}{27[x-2(11-\sqrt{-11})a]^3}$$

It follows that $\frac{-1-\sqrt{-11}}{2}(x, y) = (\bar{X}, \bar{Y})$. Subtracting, we get

$$\sqrt{-11}(x, y) = (X, Y) - (\bar{X}, \bar{Y}).$$

The $\sqrt{-11}$ division points on (2.1) are those (x, y) for which $\sqrt{-11}(x, y) = I$ the point at infinity, i.e. (x, y) for which $X = \bar{X}$ or $\operatorname{Im}(X) = 0$, i.e. the (x, y) for which the x-coordinate satisfies the equation

$$x^5 - 88ax^4 + 11\cdot 80a^2x^3 + 11^2\cdot 7\cdot 64a^3x^2 - 11^2\cdot 37\cdot 256a^4x + 11^2\cdot 1024\cdot 43a^5 = 0,$$

and if we let $x \to 4ax$ this equation becomes

$$x^5 - 22x^4 + 55x^3 + 7\cdot 11^2x^2 - 37\cdot 11^2x + 43\cdot 11^2 = 0. \tag{2.2}$$

If x_1, x_2, x_3, x_4, x_5 are the roots of (2.2), then the 10 proper $\sqrt{-11}$ division points are $(x_j, \pm y_j)$ $(j = 1, 2, 3, 4, 5)$.

We try, as solutions of this equation, numbers belonging to the maximal real subfield of $Q(\zeta)$ where $\zeta = e^{2\pi i/11}$. The reasons for expecting this are:

(i) Past experience with the other cases.

(ii) We want the answer in such a shape.

(iii) It may be possible to prove this by using general theory (of elliptic curves).

So let $\zeta_j = \zeta^j + \zeta^{-j}$ $(j = 1, 2, 3, 4, 5)$. These ζ_j are the roots of

$$\theta^5 + \theta^4 - 4\theta^3 - 3\theta^2 + 3\theta + 1 = 0. \tag{2.3}$$

If x_1 is a root of (2.2), then the other roots are the conjugates of x_1.

Let then

$$x_1 = a_1\zeta_1 + a_2\zeta_2 + a_3\zeta_3 + a_4\zeta_4 + a_5\zeta_5,$$

so that

$$x_2 = a_5\zeta_1 + a_1\zeta_2 + a_4\zeta_3 + a_2\zeta_4 + a_3\zeta_5,$$
$$x_3 = a_4\zeta_1 + a_3\zeta_2 + a_1\zeta_3 + a_5\zeta_4 + a_2\zeta_5,$$
$$x_4 = a_3\zeta_1 + a_5\zeta_2 + a_2\zeta_3 + a_1\zeta_4 + a_4\zeta_5,$$
$$x_5 = a_2\zeta_1 + a_4\zeta_2 + a_5\zeta_3 + a_3\zeta_4 + a_1\zeta_5 \quad (a_j \in \mathbf{Z}).$$

Then $\sum x_j = -a_1 - a_2 - a_3 - a_4 - a_5$. But by (2.2) $\sum x_j = 22$. Hence

$$-a_1 - a_2 - a_3 - a_4 - a_5 = 22. \tag{2.4}$$

Now work out the second elementary symmetric function $\sum x_i x_j$ of the x's. A straightforward calculation shows that this equals

$$\Big\{\sum_{i=1}^{5} a_i^2+\sum_{\substack{i,j=1,\ldots,5\\ i\neq j}} a_i a_j+ +(a_1a_3+a_1a_4+a_2a_3+a_2a_5+a_4a_5)\Big\}(\zeta_1\zeta_2+\zeta_1\zeta_5+\zeta_2\zeta_4+\zeta_3\zeta_4+\zeta_3\zeta_5)+$$
$$+\Big\{\sum_{i=1}^{5} a_i^2+\sum_{\substack{i,j=1,\ldots,5\\ i\neq j}} a_i a_j+ +(a_1a_2+a_1a_5+a_2a_4+a_3a_4+a_3a_5)\Big\}(\zeta_1\zeta_3+\zeta_1\zeta_4+\zeta_2\zeta_3+\zeta_2\zeta_4+\zeta_4\zeta_5)+$$
$$+\sum_{\substack{i,j=1,\ldots,5\\ i\neq j}} a_i a_j\Big(\sum_{j=1}^{5}\zeta_j^2\Big).$$

If we simplify this using (2.4), it boils down to $11\left(66-\frac{1}{2}\sum a_i^2\right)$. But again by (2.2) $\sum x_i x_j = 55$; hence

$$66-\tfrac{1}{2}\sum a_i^2 = 5. \tag{2.5}$$

Equations (2.4) and (2.5) are

$$\begin{aligned} a_1+a_2+a_3+a_4+a_5 &= -22,\\ a_1^2+a_2^2+a_3^2+a_4^2+a_5^2 &= 122. \end{aligned} \tag{2.6}$$

The latter equation here has only a finite number of solutions (in fact just 16 up to the sign in the a_j) but of these only 5 satisfy the first one. They are

$$\begin{aligned}(a_1, a_2, a_3, a_4, a_5) = (-8, -6, -3, -3, -2),\ (-8, -5,\\ -5, -2, -2),\ (-8, -5, -4, -4, -1),\\ (-7, -7, -4, -2, -2),\ (-6, -6, -5, -5, 0).\end{aligned} \tag{2.7}$$

Here in each case the a_j may be combined with the ζ_j in 120 ways, but without loss of generality we may take $x_1 = a_1\zeta_1 + 24$ other possibilities, so that each case has 24 subcases. These are far too many to be checked for solution by computation. We therefore work out the third elementary symmetric function $\sum x_i x_j x_k$ of the roots and equate it to $-7\cdot 11^2$ using our equation (2.2). The final result is the equation

$$\begin{aligned}-7\cdot 11^2 = 3\sum a_j^3 &+ 7(a_1a_2a_3+a_1a_3a_4+a_1a_4a_5+a_2a_3a_5+a_2a_4a_5)-\\ &-2\sum_{i\neq j} a_i^2 a_j - 15(a_1a_2a_4+a_1a_2a_5+a_1a_3a_5+a_2a_3a_4+\\ &+a_3a_4a_5)+11(a_1^2a_2+a_2^2a_4+a_3^2a_5+a_4^2a_3+a_5^2a_1).\end{aligned} \tag{2.8}$$

Here we have used the following results:

(i) $\sum \zeta_j^3 = -4$,
(ii) $\sum \zeta_i^2\zeta_j = -5$,
(iii) $\zeta_1^2\zeta_2 + 4$ conjugates $= 7$,
(iv) $\zeta_1^2\zeta_3 + 4$ conjugates $= -4$,
(v) $\zeta_1^2\zeta_4 + 4$ conjugates $= -4$,
(vi) $\zeta_1^2\zeta_5 + 4$ conjugates $= -4$,
(vii) $\sum \zeta_i\zeta_j\zeta_k = 3$,
(viii) $\zeta_1\zeta_2\zeta_3 + 4$ conjugates $= 7$,
(ix) $\zeta_1\zeta_2\zeta_4 + 4$ conjugates $= -4$.

Now use $\sum a_i^2 a_j = -4\cdot 11\cdot 61 - \sum a_j^3$ (obtained by using the identity $\sum a_j^2\cdot\sum a_j = \sum a_i a_j^2 + \sum a_j^3$) and $3\sum a_i a_j a_k = \sum a_j^3 - 22\cdot 59$ (obtained by cubing $a_1+a_2+a_3+a_4+a_5 = -22$), (2.8) gives the equation

$$\begin{aligned}-6(a_1a_2a_4+a_1a_2a_5+a_1a_3a_5+a_2a_3a_4+a_3a_4a_5)+11\cdot 79\\ = -2(a_1^3+a_2^3+a_3^3+a_4^3+a_5^3)-3(a_1^2a_2+a_2^2a_4+a_3^2a_5+a_4^2a_3+a_5^2a_1).\end{aligned} \tag{2.9}$$

Now try out in this the various permutations from the cases. This gives the following two solutions: $(a_1, a_2, a_3, a_4, a_5) = (-8, -5, -2, -5, -2)$ and $(-8, -2, -5, -5, -2)$. Of these the first one works right through. Hence we have the following

Proposition 1. *The 5 roots of (2.2) are* $x_1 = -8\zeta_1-5\zeta_2-2\zeta_3-5\zeta_4-2\zeta_5$ *and the 4 conjugates* x_2, x_3, x_4, x_5 *obtained by letting* $\zeta\to\zeta^j$ $(j = 2, 3, 4, 5)$ *in* x_1.

This then gives the following

Proposition 2. *The x-coordinates of the proper* $\sqrt{-11}$ *division points on* (2.1) *are*

$$X_1 = 4ax_1 = 4a[-8(\zeta+\zeta^{10})-5(\zeta^2+\zeta^9)-2(\zeta^3+\zeta^8)-5(\zeta^4+\zeta^7)-2(\zeta^5+\zeta^6)],$$

$$X_2 = 4ax_2 = 4a[-2(\zeta+\zeta^{10})-8(\zeta^2+\zeta^9)-5(\zeta^3+\zeta^8)-5(\zeta^4+\zeta^7)-2(\zeta^5+\zeta^6)],$$

$$X_3 = 4ax_3 = 4a[-5(\zeta+\zeta^{10})-2(\zeta^2+\zeta^9)-8(\zeta^3+\zeta^8)-2(\zeta^4+\zeta^7)-5(\zeta^5+\zeta^6)],$$

$$X_4 = 4ax_4 = 4a[-2(\zeta+\zeta^{10})-2(\zeta^2+\zeta^9)-5(\zeta^3+\zeta^8)-8(\zeta^4+\zeta^7)-5(\zeta^5+\zeta^6)],$$

$$X_5 = 4ax_5 = 4a[-5(\zeta+\zeta^{10})-5(\zeta^2+\zeta^9)-2(\zeta^3+\zeta^8)-2(\zeta^4+\zeta^7)-8(\zeta^5+\zeta^6)].$$

Now substitute these x-coordinates in (2.1) and we get the corresponding y-coordinates as $Y_1 = 12a\sqrt{(-33a)}\{1+16\zeta_1+12\zeta_2+4\zeta_3+20\zeta_4+8\zeta_5\}^{1/2}$ and Y_2, Y_3, Y_4, Y_5 as conjugates. Here the $\{\}^{1/2}$ is inelegant – we expect it to lie in $\boldsymbol{Z}[\zeta]$. Trial and error is hopeless. We could give the final answer here, but the way it comes about is interesting and we mention it.

Let $X = 1+16\zeta_1+12\zeta_2+4\zeta_3+20\zeta_4+8\zeta_5$. We expect $X^{1/2}$ to belong to $\boldsymbol{Z}[\zeta]$. In case it does not, we still have the $\sqrt{-33}$ outside to fiddle with. It may be that $(-X)^{1/2}$ or $(\pm 3X)^{1/2}$ or $\pm(11X)^{1/2}$, etc. may lie in $\boldsymbol{Z}[\zeta]$. Trying for $X^{1/2}$ gives:

$$X+\lambda(1+\zeta_1+\zeta_2+\zeta_3+\zeta_4+\zeta_5) = (c_1\zeta_1+c_2\zeta_2+c_3\zeta_3+c_4\zeta_4+c_5\zeta_5)^2.$$

Equating coefficients, we get the following system of Diophantine equations:

$$\begin{array}{ll}
\text{(i)} & 2(c_1^2+c_2^2+c_3^2+c_4^2+c_5^2) = 1+\lambda,\\
\text{(ii)} & c_1^2+2(c_1c_3+c_2c_4+c_3c_5+c_4c_5) = 12+\lambda,\\
\text{(iii)} & c_2^2+2(c_1c_3+c_1c_5+c_2c_5+c_3c_4) = 20+\lambda,\\
\text{(iv)} & c_3^2+2(c_1c_4+c_1c_5+c_2c_3+c_2c_4) = 8+\lambda,\\
\text{(v)} & c_4^2+2(c_1c_2+c_1c_4+c_2c_5+c_3c_5) = 4+\lambda,\\
\text{(vi)} & c_5^2+2(c_1c_2+c_2c_3+c_3c_4+c_4c_5) = 16+\lambda.
\end{array}$$

Here (i) implies that λ is odd $= 1+2d$. Then (ii), ..., (vi) imply that, respectively, c_1, c_2, c_3, c_4, c_5 are odd, so that $c_j^2 \equiv 1 \pmod 8$, and then (i) gives $1+1+2d \equiv 2\cdot 5 \pmod 8$, i.e. $d = 4\mu$, say. Thus $\lambda = 1+8\mu$ and all c_j are odd. We now subtract equations (ii), ..., (vi) from equation (i) and get the following set of equations:

$$\begin{aligned}
&(c_1-c_3)^2+(c_3-c_5)^2+(c_4-c_5)^2+(c_2-c_4)^2+c_2^2 = -11,\\
&(c_1-c_3)^2+(c_1-c_5)^2+(c_2-c_5)^2+(c_3-c_4)^2+c_4^2 = -19,\\
(2.10)\quad &(c_1-c_4)^2+(c_1-c_5)^2+(c_2-c_3)^2+(c_2-c_4)^2+c_5^2 = -7,\\
&(c_1-c_2)^2+(c_1-c_4)^2+(c_2-c_5)^2+(c_3-c_5)^2+c_3^2 = -3,\\
&(c_1-c_2)^2+(c_2-c_3)^2+(c_3-c_4)^2+(c_4-c_5)^2+c_1^2 = -15,
\end{aligned}$$

which is clearly impossible for $c_j \in \boldsymbol{Z}$. So now we introduce the various factors in X and try. It turns out that $\sqrt{-11}$ works. Indeed, the system (2.10) is simply replaced by one with the right-hand sides multiplied by -11. Trial and error now gives the following solution:

$$c_1 = 7,\quad c_2 = 7,\quad c_3 = 3,\quad c_4 = 11,\quad c_5 = 5.$$

Since there is a unique solution (up to the sign), this gives

$$-11X = (7\zeta_1+7\zeta_2+3\zeta_3+11\zeta_4+5\zeta_5)^2.$$

This may be directly checked.

We have proved the following

PROPOSITION 3. *The y-coordinates of the $\sqrt{-11}$ division points on* (2.1) *are*

$$Y_1 = 12a(3a)^{1/2}[7(\zeta+\zeta^{10})+7(\zeta^2+\zeta^9)+3(\zeta^3+\zeta^8)+11(\zeta^4+\zeta^7)+5(\zeta^5+\zeta^6)],$$

$$Y_2 = 12a(3a)^{1/2}[5(\zeta+\zeta^{10})+7(\zeta^2+\zeta^9)+11(\zeta^3+\zeta^8)+7(\zeta^4+\zeta^7)+3(\zeta^5+\zeta^6)],$$

$$Y_3 = 12a(3a)^{1/2}[11(\zeta+\zeta^{10})+3(\zeta^2+\zeta^9)+7(\zeta^3+\zeta^8)+5(\zeta^4+\zeta^7)+7(\zeta^5+\zeta^6)],$$

$$Y_4 = 12a(3a)^{1/2}[3(\zeta+\zeta^{10})+5(\zeta^2+\zeta^9)+7(\zeta^3+\zeta^8)+7(\zeta^4+\zeta^7)+11(\zeta^5+\zeta^6)],$$

$$Y_5 = 12a(3a)^{1/2}[7(\zeta+\zeta^{10})+11(\zeta^2+\zeta^9)+5(\zeta^3+\zeta^8)+3(\zeta^4+\zeta^7)+7(\zeta^5+\zeta^6)],$$

Now let $\boldsymbol{P}$ be the $\sqrt{-11}$ division point (X_1, Y_1). Then the remaining 9 proper $\sqrt{-11}$ division points are $-\boldsymbol{P}$, $\pm 2\boldsymbol{P}$, $\pm 3\boldsymbol{P}$, $\pm 4\boldsymbol{P}$, $\pm 5\boldsymbol{P}$. We further need to know which is which. A simple calculation involving addition of points on (2.1) finally gives the following

THEOREM 2. *Let X_j and Y_j $(j = 1, 2, 3, 4, 5)$ be as found in Propositions* 2 *and* 3. *Then the proper $\sqrt{-11}$ division points* (10 *in number*) *on the elliptic curve* (2.1) *are $(X_j, \pm Y_j)$. If $\boldsymbol{P}$ is the point (X_1, Y_1), then $2\boldsymbol{P} = (X_4, -Y_4)$, $3\boldsymbol{P} = (X_2, Y_2)$, $4\boldsymbol{P} = (X_5, Y_5)$, $5\boldsymbol{P} = (X_3, Y_3)$, and of course for any point (x, y) one has $-(x, y) = (x, -y)$.*

3. Proof of Theorem 1. Let N_p be the number of points on the projective curve

$$y^2 = x^3-33\cdot 32z^2x+11^2\cdot 7\cdot 16z^3$$

in the finite field of p elements. First of all, N_p is equal to 1 plus the number of solutions of the congruence

(3.1) $$y^2 \equiv x^3 - 33\cdot 32a^2x + 11^2\cdot 7\cdot 16a^3 \pmod p$$

(the 1 coming from the point at infinity)

$$= 1 + \sum \{1 + (y^2/p)\} = p + 1 + (2a|p)\mathfrak{S}$$

(the $\mathfrak{S}$ mentioned in Theorem 1).

But by a well-known theorem of Deuring [3] we have

$$N_p = \begin{cases} p+1 & \text{if } p \text{ is not a norm from } Q(\sqrt{-11}) \text{ to } Q, \\ p+1-\pi-\bar{\pi} & \text{if } p = \operatorname{Norm}(\pi) = \pi\bar{\pi}. \end{cases}$$

Let $\pi = (c + d\sqrt{-11})/2$, $c \equiv d \pmod 2$. Then $p = \pi\bar{\pi} = (c^2 + 11d^2)/4$, i.e. $4p = c^2 + 11d^2$ and $\pi + \bar{\pi} = c$. Hence Deuring's theorem gives

(3.2) $$N_p = \begin{cases} p+1 & \text{if } p \equiv 2, 6, 7, 8, 10 \pmod{11}, \\ p+1-c & \text{otherwise, where } 4p = c^2 + 11d^2. \end{cases}$$

Equating (3.1) and (3.2) gives

(3.3) $$\mathfrak{S} = \begin{cases} 0 & \text{if } p \equiv 2, 6, 7, 8, 10 \pmod{11}, \\ -(2a|p)\cdot c & \text{otherwise, i.e. if } p \equiv 1, 3, 4, 5, 9 \pmod{11} \\ & \text{where } 4p = c^2 + 11d^2. \end{cases}$$

Here the problem is the sign of c, i.e. the normalization of π and $\bar{\pi}$. Deuring's theorem also tells us that the correct sign $+\pi$ or $-\pi$ is that for which multiplication of points of (2.1) by the π with the correct sign has the same effect as has the Frobenius automorphism

$$f_p : (x, y) \to (x^p, y^p) \pmod p.$$

We try the action of the Frobenius map on the $\sqrt{-11}$ division points. We look at each of the 5 cases $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ in turn.

Case 1. $p \equiv 1 \pmod{11}$. Let $\boldsymbol{P} = (X_1, Y_1)$. Then $f_p(\boldsymbol{P}) = (X_1^p, Y_1^p) = (X_1, (3a|p)Y_1) = (3a|p)(X_1, Y_1)$. But $f_p(\boldsymbol{P}) = \pi\boldsymbol{P}$ by the very definition of π with the correct sign. Hence $(\pi - (3a|p))\boldsymbol{P} = \boldsymbol{I}$. But $\boldsymbol{P}$ is a proper $\sqrt{-11}$ division point. It follows that $\pi \equiv (3a|p) \pmod{\sqrt{-11}}$, i.e.

$$c + d\sqrt{-11} \equiv 2(3a|p) \pmod{\sqrt{-11}}, \quad \text{i.e.} \quad c \equiv 2(3a|p) \pmod{11}.$$

Case 2. $p \equiv 3 \pmod{11}$. Again let $\boldsymbol{P} = (X_1, Y_1)$. Then $f_p(\boldsymbol{P}) = (X_1^p, Y_1^p) = (X_3, (3a|p)Y_3) = (3a|p)(X_3, Y_3) = (3a|p)5\boldsymbol{P}$ (see Theorem 2). Hence as above $\pi \equiv 5(3a|p) \pmod{\sqrt{-11}}$ giving $c \equiv 10(3a|p) \pmod{11}$.

Case 3. $p \equiv 4 \pmod{11}$. Here $c \equiv 7(3a|p) \pmod{11}$ similarly.

Case 4. $p \equiv 5 \pmod{11}$. Here $c \equiv 8(3a|p) \pmod{11}$.

Case 5. $p \equiv 9 \pmod{11}$. Here $c \equiv 6(3a|p) \pmod{11}$, i.e.

$$-(2a|p)c \equiv (6|p)\cdot \begin{cases} 9 \\ 1 \\ 4 \\ 3 \\ 5 \end{cases} \pmod{11} \quad \text{according as} \quad p \equiv \begin{cases} 1 \\ 3 \\ 4 \\ 5 \\ 9 \end{cases} \pmod{11}.$$

Hence by (3.3)

$$\mathfrak{S} = \begin{cases} 0 & \text{if } p \equiv 2, 6, 7, 8, 10 \pmod{11}, \\ c & \text{otherwise where } 4p = c^2 + 11d^2, \end{cases}$$

with

$$c \equiv (6|p)\cdot \begin{cases} 9 \\ 1 \\ 4 \\ 3 \\ 5 \end{cases} \pmod{11} \quad \text{according as} \quad p \equiv \begin{cases} 1 \\ 3 \\ 4 \\ 5 \\ 9 \end{cases} \pmod{11},$$

i.e. $(c|11) = (6|p)$. This completes the proof of Theorem 1.

References

[1] B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. 99 (1961), pp. 241–245.

[2] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, Crelle 172 (1934), pp. 151–182.

[3] M. Deuring, *Die Typen den Multiplikatorenrings Elliptische Funktionen Körper*, Abh. Math. Sem. Univ. Hamburg, 14 (1941), pp. 197–272.

[4] R. E. Guidici, J. B. Muskat, and S. F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. 171 (1972), pp. 317–347.

[5] P. A. Leonard and K. S. Williams, *Jacobi sums and a theorem of Brewer*, Rocky Mountain J. of Maths. 5 (1975), pp. 301–308, *Erratum*, 6 (1976), p. 501.

[6] — *Evaluation of certain Jacobsthal sums*, Bolletino U.M.I. (5) 15-B (1978), pp. 717–723.

[7] B. Morlaye, *Démonstration elementaire d'un théorème de Davenport et Hasse*, L'Enseignement Math. 18 (1972), pp. 269–276.

[8] L. D. Olson, *Conductors of elliptic curves*, J. of Number Theory 8 (1976), pp. 397–414.

[9] A. R. Rajwade, *Arithmetic on curves with complex multiplication by the Eisenstein integers*, Proc. Camb. Phil. Soc. 65 (1969), pp. 59–73.

[10] — *On rational primes p congruent to* 1 *(mod 3 or 5)*, ibid. 66 (1969), pp. 61–70.

[11] — *On the congruence* $y^2 \equiv x^5 - a \pmod p$, ibid. 74 (1973), pp. 473–475.

[12] — *A note on the number of solutions* N_p *of the congruence* $y^2 \equiv x^3 - Dx \pmod p$, ibid. 67 (1970), pp. 603–605.

[13] A. R. Rajwade, *Certain classical congruences via elliptic curves*, J. London Math. Soc. 8 (1974), pp. 60–62.
[14] — *Some formulae for elliptic curves with complex multiplication*, Indian J. of Pure and Applied Maths. 8 (1977), pp. 379–387.
[15] — *The Diophantine equation* $y^2 = x(x^2+21Dx+112D^2)$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Australian Math. Soc. 24 (1977), pp. 286–295.
[16] Surjit Singh and A. R. Rajwade, *The number of solutions of the congruence* $y^2 \equiv x^4 - a \pmod p$, L'Enseignement Math. 20 (1974), pp. 265–273.
[17] A. L. Whiteman, *A theorem of Brewer on character sums*, Duke Math. J. 30 (1963), pp. 545–552.
[18] K. S. Williams, *Note on a cubic character sum*, Aequationes Mathematicae 12 (1975), pp. 229–231.
[19] — *Evaluation of character sums connected with elliptic curves*, Proc. Amer. Math. Soc. 73 (1979), pp. 291–299.

DEPARTMENT OF MATHEMATICS
PANJAB UNIVERSITY
Chandigarh, India

Received on 27. 7. 1979
and in revised form on 29. 11. 1979 (1171)

ACTA ARITHMETICA
XL (1982)

Новые оценки коротких тригонометрических сумм

Ян Мозер (Братислава)

Профессор А. А. Карацуба поместил в книге [1], стр. 89, в качестве примера, следующую теорему: *для справедливости гипотезы Линделёфа необходимо и достаточно выполнение следующего условия*

$$\sum_{1\leqslant n\leqslant x} n^{it} = O(\sqrt{x}|t|^{\varepsilon}), \quad 0 < x < |t|, \ \varepsilon > 0. \tag{1}$$

Первая (нетривиальная) часть этой теоремы является новым результатом в теории дзета-функции Римана.

Предлагаемая работа посвящена анализу дальнейших возможностей кроющихся в этом направлении.

1. Пусть ([5], стр. 383)

$$\vartheta(t) = -\frac{1}{2}t\ln\pi + \operatorname{Im}\ln\Gamma\left(\frac{1}{4}+\frac{1}{2}it\right) = \frac{1}{2}t\ln\frac{t}{2\pi} - \frac{1}{2}t - \frac{1}{8}\pi + O\left(\frac{1}{t}\right). \tag{2}$$

Исходя из приближенного функционального уравнения ([5], стр. 82, 85)

$$\zeta(s) = \sum_{n\leqslant x}\frac{1}{n^s} + \chi(s)\sum_{n\leqslant y}\frac{1}{n^{1-s}} + O(x^{-\sigma}) + O(t^{1/2-\sigma}y^{\sigma-1}), \tag{3}$$

где ([5], стр. 81)

$$\chi(s) = \frac{2^{s-1}\pi^s}{\Gamma(s)\cos(\pi s/2)} = \left(\frac{2\pi}{t}\right)^{\sigma+it-1/2} e^{i(t+\pi/4)}\left\{1+O\left(\frac{1}{t}\right)\right\}, \tag{4}$$

и

$$s = \sigma+it, \quad 0\leqslant\sigma\leqslant 1, \quad 2\pi xy = t, \quad x > h > 0, \quad y > h > 0, \tag{5}$$

покажем, что имеет место