

SOME IDENTITIES ON THE CHARACTER SUM CONTAINING $\mathbf{x}(\mathbf{x}-1)(\mathbf{x}-\lambda)$

MASATOSHI YAMAUCHI

Let F_p be the prime field of characteristic p (p : an odd prime), and put $F'_p = F_p - \{0, 1\}$. Then for $\lambda \in F'_p$ we define

$$a_p(\lambda) = - \sum_{x \in F_p} \left(\frac{x(x-1)(x-\lambda)}{p} \right),$$

where $\left(\frac{*}{p} \right)$ denotes the Legendre symbol, and consider the sum

$$S_m(\lambda) = \sum_{\lambda \in F'_p} a_p(\lambda)^m.$$

The purpose of this note is to prove the following:

THEOREM.

$$S_2(p) = p^2 - 2p - 3,$$

$$S_4(p) = 2p^3 - 4p^2 - 9p - 3 - b_p,$$

$$S_6(p) = 5p^4 - 10p^3 - 27p^2 - 15p - 3 - 5pb_p - 2c_p,$$

where b_p and c_p are obtained from

$$q \prod_{n=1}^{\infty} (1 - q^{2n})^{12} = \sum_{n=1}^{\infty} b_n q^n,$$

$$q \prod_{n=1}^{\infty} (1 - q^n)^8 (1 - q^{2n})^8 = \sum_{n=1}^{\infty} c_n q^n.$$

The sum $S_m(p)$ is analogous to the sum considered by Birch [1]. We note that b_p and c_p are the eigen-values of Hecke operators acting on the space of cusp forms of weight 6 or 8 respectively, with respect to the elliptic modular group $\Gamma_0(4)$ (or $\Gamma(2)$), and the meaning of the above theorem is that the eigen-value of Hecke operators of higher weight appears in the

Received August 10, 1970.

congruence zeta function of a certain variety which have been found by Sato firstly.

1. The proof of the theorem

1.1. For $\lambda \in \mathbb{F}'_p$, let E_λ be an elliptic curve defined by the affine coordinate as follows with identity element (∞, ∞) as an additive group.

$$E_\lambda: y^2 = x(x - 1)(x - \lambda),$$

then it is well known that the order $N_p(\lambda)$ of the group of \mathbb{F}_p -rational points is $N_p(\lambda) = 1 + p - a_p(\lambda)$ and since $(0, 0)$, $(1, 0)$, $(\lambda, 0)$ and (∞, ∞) are all points of order 2 on E_λ , which are rational over \mathbb{F}_p .

$$N_p(\lambda) \equiv 0 \pmod{4} \text{ or } a_p(\lambda) \equiv 1 + p \pmod{4}.$$

For a moment, take $\lambda' \in \overline{\mathbb{F}}_p$: the algebraic closure of \mathbb{F}_p , and define $S = \{\lambda' \in \mathbb{F}_p | E_{\lambda'} \text{ is a super-singular elliptic curve}\} = \{\lambda' \in \mathbb{F}_p | \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda'^i = 0\}$.

1.2. For $\lambda \in \mathbb{F}'_p - S$, the endomorphism ring $\mathcal{A}(E_\lambda) = \mathcal{O}_\lambda$ is an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{a_p(\lambda)^2 - 4p})$, and contains an order of discriminant $a_p(\lambda)^2 - 4p$, since $a_p(\lambda)$ is the trace of the p -th power endomorphism π_λ which satisfies the equation $X^2 - a_p(\lambda)X + p = 0$.

LEMMA. Assume the discriminant of \mathcal{O}_λ is $(a_p(\lambda)^2 - 4p)f^{-2}$ then $f \equiv \text{mod } 2$. Conversely, for an order \mathcal{O} of discriminant $(s^2 - 4p)f^{-2}$ with $s \equiv 1 + p \pmod{4}$ and $f \equiv 0 \pmod{2}$, there exists $\lambda \in \mathbb{F}'_p - S$ such that $\mathcal{A}(E_\lambda) = \mathcal{O}$.

Proof. Let $\lambda(z)$ be a modular function for the principal congruence subgroup $\Gamma(2)$ of level 2 defined by $\lambda(z) = (e_1 + 2e_3)(e_3 - e_1)^{-1}$ where $e_1 = \mathcal{P}\left(\frac{1}{2}; z, 1\right)$, $e_3 = \mathcal{P}\left(\frac{z}{2}; z, 1\right)$, and let τ be an element of imaginary quadratic field $K = \mathbb{Q}(\sqrt{s^2 - 4p})$ with $s \equiv p + 1 \pmod{4}$, and denote the discriminant $D(\tau)$ of τ by $D(\tau) = (s^2 - 4p)f^{-2}$, then $K(\lambda(\tau))$ generates a ring class field over K . There exists $\pi \in K$ such that $p = \pi \cdot \pi'$ (π' : the conjugate of π), and we see π decomposes completely in $K(\lambda(\tau))$ if and only if $f \equiv 0 \pmod{2}$, because the corresponding ideal group H for $K(\lambda(\tau))$ is $H = \{\alpha \in \mathcal{O}_0 | \alpha = 1 + 2\alpha + 2m\beta, a \in \mathbb{Z}, \beta \in \mathcal{O}_0\}$, where \mathcal{O}_0 is the maximal order in K and $s^2 - 4p = f^2 m^2 d$ (d : the discriminant of \mathcal{O}_0), and we see easily that $\pi \in H$ if and only if $f \equiv 0 \pmod{2}$. Let $E_{\lambda(\tau)}$ be an elliptic curve defined by $y^2 = x(x - 1)(x - \lambda(\tau))$,

if $f \equiv 0 \pmod 2$, then, for a prime ideal $\mathfrak{P}|\pi$ in $K(\lambda(\tau))$, whose absolute norm is p , the reduction mod \mathfrak{P} of $E_{\lambda(\tau)}$ defines an elliptic curve $E_\lambda(\lambda \in \mathbf{F}'_p - S)$, by the isomorphism $\mathcal{O}_0/\mathfrak{P} \cong \mathbf{F}_p$ and $\mathcal{A}(E_{\lambda(\tau)}) = \mathcal{A}(E_\lambda)$, hence the discriminant of $\mathcal{A}(E_\lambda)$ is $(s^2 - 4p)f^{-2}$. If f is odd, the reduction mod \mathfrak{P} of $E_{\lambda(\tau)}$ does not define an elliptic curve $E_\lambda(\lambda \in \mathbf{F}'_p - S)$, since the degree of \mathfrak{P} is greater than 1 hence $\mathcal{O}_0/\mathfrak{P} \not\cong \mathbf{F}_p$. This completes the proof of the lemma.

1.3. For an order \mathcal{O} as the lemma in **1.2**, there are $6 \cdot \frac{h((s^2 - 4p)f^{-2})}{w((s^2 - 4p)f^{-2})}$ distinct $\lambda \in \mathbf{F}'_p - S$ such that $\mathcal{A}(E_\lambda) = \mathcal{O}$, For $\lambda^{\pm 1}, (1 - \lambda)^{\pm 1}, (\lambda^{-1}(\lambda - 1))^{\pm 1}$ give the same absolute invariant $j = 2^8(\lambda^2 - \lambda + 1)^3/\lambda^2(1 - \lambda)^2$, and for a fixed $j \in \mathbf{F}_p$ there exist precisely $h((s^2 - 4p)f^{-2})$ elliptic curves with the same endomorphism ring \mathcal{O} , where $h(D)$ and $w(D)$ denote the class number of an order \mathcal{O} of discriminant D and a half of the number of units in \mathcal{O} , respectively.

1.4. We see that

$$6 \cdot \frac{h(D)}{w(D)} = \begin{cases} 3h(4D) & , \text{ if } D \equiv 0 \pmod 4 \\ 2h(4D) & , \text{ if } D \equiv 5 \pmod 8 \\ 3h(4D) + 3h(D), & \text{ if } D \equiv 1 \pmod 8, \end{cases}$$

hence we obtain

$$6 \cdot \sum_1 \frac{h((s^2 - 4p)f^{-2})}{w((s^2 - 4p)f^{-2})} = \sum_2 \frac{\delta((s^2 - 4p)f^{-2})}{2} \left(1 + \left\{ \frac{(s^2 - 4p)f^{-2}}{2} \right\} \right) \times \left\{ \frac{(s^2 - 4p)f^{-2}}{2} \right\} h((s^2 - 4p)f^{-2}),$$

where \sum_1 runs over all s, f with $s \equiv p + 1 \pmod 4 \quad |s| < 2\sqrt{p}$ and with $f \equiv 0 \pmod 2 \quad f > 0$, \sum_2 runs over all s, f with $|s| < 2\sqrt{p}$ and with $(s^2 - 4p)^{-2} \equiv 0, 1 \pmod 4 \quad f > 0$, $\delta(D) = 2$ or 3 according as $D/4 \equiv 5 \pmod 8$ or not, and $\left\{ \frac{D}{2} \right\} = 1$ or $\left(\frac{D}{2} \right)$ according as $D/4 \equiv 0, 1 \pmod 4$ or not.

1.5. Now we shall prove the theorem. First

$$\begin{aligned} S_2(p) &= \sum_{x, y, \lambda \in \mathbf{F}_p} \left(\frac{x(x - 1)(x - \lambda)}{p} \right) \left(\frac{y(y - 1)(y - \lambda)}{p} \right) - 2 \\ &= \sum_{x, y \in \mathbf{F}_p} \left(\frac{x(x - 1)y(y - 1)}{p} \right) \cdot \sum_{\lambda \in \mathbf{F}_p} \left(\frac{(\lambda - x)(\lambda - y)}{p} \right) - 2. \end{aligned}$$

By decomposing the above sum into two parts with $x = y$ and $x \neq y$, we see easily $S_2(p) = p^2 - 2p - 3$. As for the sum $S_4(p)$,

$$S_4(p) = \sum_{\lambda \in \mathbf{F}'_p} a_p(\lambda)^4 = \frac{1}{2} \sum_{|s| < 2\sqrt{p}} s^4 \cdot \sum_{\mathcal{N}_0(E_\lambda) = \mathbf{Q}(\sqrt{s^2 - 4p})} \cdot 1$$

$$= \frac{1}{2} \sum_{|s| < 2\sqrt{p}} s^4 \cdot \sum_2 \frac{\delta(D)}{2} \cdot \left(1 + \left\{\frac{D}{2}\right\}\right) \left\{\frac{D}{2}\right\} h(D)$$

where the sum \sum' denotes the number of elliptic curves E_λ for which the discriminant of $\mathcal{N}(E_\lambda)$ is $(s^2 - 4p)f^{-2}$, and other notations are the same as in 1.4 with $D = (s^2 - 4p)f^{-2}$. By the trace formula of Hecke operators for $\Gamma_0(4)$ obtained in [3], we see

$$b_p = -\frac{1}{2} \sum_2 \frac{\delta(D)}{2} \left(1 + \left\{\frac{D}{2}\right\}\right) \left\{\frac{D}{2}\right\} h(D) \cdot \frac{\rho^5 - \rho'^5}{\rho - \rho'} - 3,$$

where ρ, ρ' are the roots of $x^2 - sx + p = 0$.

Hence $\frac{\rho^5 - \rho'^5}{\rho - \rho'} = s^4 - 3ps^2 + p^2$.

Therefore

$$S_4(p) = -b_p - 3 + 3pS_2(p) - p^2(p \sim 2)$$

$$= 2p^3 - 4p^2 - 9p - 3 - b_p.$$

For the sum $S_6(p)$, this can be proved similarly so we may omit it. Hence this completes our proof of the theorem.

2. Some corollaries

2.1 For the set S defined in 1.1, $\#S = \frac{p-1}{2}$, ($\#$ denotes the cardinality of the set) and we know $S \cap \mathbf{F}'_p = \{\lambda \in \mathbf{F}'_p | a_p(\lambda) = 0\}$.

COROLLARY 1.

$$\#(S \cap \mathbf{F}'_p) = \begin{cases} 0 & , \text{ if } p \equiv 1 \pmod{4} \\ 3h(-p), & \text{ if } p \equiv 3 \pmod{4}, \end{cases}$$

where $h(-p)$ denotes the class number of $\mathbf{Q}(\sqrt{-p})$.

Proof. By 1.3 and 1.4, we obtain

$$\#(\mathbf{F}'_p - S) = \frac{1}{2} \sum_{s \neq 0} \frac{\delta(D)}{2} \left(1 + \left\{\frac{D}{2}\right\}\right) \left\{\frac{D}{2}\right\} h(D),$$

hence $p - 2 = \#\mathbf{F}'_p = \frac{1}{2} \sum_{s \neq 0} \frac{\delta(D)}{2} \left(1 + \left\{\frac{D}{2}\right\}\right) \left\{\frac{D}{2}\right\} h(D) + \#(S \cap \mathbf{F}'_p)$ and by

the trace formula of Hecke operators for $\Gamma_0(4)$ with weight 2, we have

$$p - 2 = \frac{1}{2} \sum_{s \neq 0} \frac{\delta(D)}{2} \left(1 + \left\{ \frac{D}{2} \right\} \right) \left\{ \frac{D}{2} \right\} h(D) + h',$$

where

$$h' = \begin{cases} 0 & , \text{ if } p \equiv 1 \pmod{4} \\ \frac{3}{2} h(-4p) + \frac{3}{2} h(-p) = 3h(-p), & \text{ if } p \equiv 7 \pmod{8} \\ h(-4p) = 3h(-p) & , \text{ if } p \equiv 3 \pmod{8}. \end{cases}$$

This completes the proof.

2.2 By **1.1**, $a_p(\lambda) \equiv 1 + p \pmod{4}$, hence $a_p(\lambda)^4 \equiv (1 + p)^4 \pmod{2^8}$ therefore $S_4(p) \equiv (p-2)(p+1)^4 \pmod{2^8}$. According to our theorem for $S_4(p)$, b_p satisfies the following congruence property;

COROLLARY 2.

$$-b_p \equiv p^5 + 1 + 2p(p^3 + 1) - 4p^2(p + 1) \pmod{2^8}$$

or in other words,

$$b_p \equiv p^5 + 1 \pmod{2^8}.$$

REFERENCES

[1] B.J. Birch, How the number of points of elliptic curves over a fixed prime field varies, J. London Math. Soc., 43 (1968), 57-60.
 [2] ———, Weber's class invariants, Mathematika, 16 (1969), 283-294.
 [3] M. Yamauchi, On the trace of Hecke operators for certain modular groups, to appear.

*Mathematical Institute
 Nagoya University*