Internat. J. Math. & Math. Sci.
Vol. 22, No. 1 (1999) 55–65
S 0161-1712⟨99⟩22055-8

q-SERIES, ELLIPTIC CURVES, AND ODD VALUES OF THE PARTITION FUNCTION

NICHOLAS ERIKSSON

(Received 28 January 1997)

ABSTRACT. Let $p(n)$ be the number of partitions of an integer n. Euler proved the following recurrence for $p(n)$:

$$p(n) = \sum_{k=1}^{\infty} (-1)^{k+1}\Big(p(n-\omega(k)) + p(n-\omega(-k))\Big), \qquad (*)$$

where $\omega(k) = (3k^2+k)/2$. In view of Euler's result, one sees that it is fairly easy to compute $p(n)$ very quickly. However, many questions remain open even regarding the parity of $p(n)$. In this paper, we use various facts about elliptic curves and q-series to construct, for every $i \geq 1$, finite sets M_i for which $p(n)$ is odd for an odd number of $n \in M_i$.

Keywords and phrases. The partition function, elliptic curves, q-series.

1991 Mathematics Subject Classification. 11P83.

1. The partition function. A partition of a nonnegative integer n is any non-increasing sequence of positive integers whose sum is n. Let $p(n)$ denote the number of partitions of n. Even though Euler's recurrence $(*)$ gives a method for computing $p(n)$, there are many open problems and conjectures regarding the overall behavior of the partition function. For instance, the following questions regard the parity of $p(n)$.

CONJECTURE 1.1 (Parkin-Shanks [5]). *The number of $n \leq x$ for which $p(n)$ is even is* $\sim (1/2)x$.

CONJECTURE 1.2 (Subbarao [7]). *In any arithmetic progression $r \pmod t$, there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even, and there are infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd.*

K. Ono [3] has recently proven most of this conjecture.

NEWMAN'S PROBLEM (Newman [2]). Exhibit an infinite sequence of integers $n_1 < n_2 < \cdots$ for which $p(n_i)$ is odd (resp., even).

Euler proved that the *generating* function for $p(n)$ was given by the infinite product

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}. \qquad (1.1)$$

Euler also discovered the identity

$$\prod_{n=1}^{\infty} (1-q^n) = \sum_{n=-\infty}^{\infty} (-1)^n q^{(3n^2+n)/2}. \qquad (1.2)$$

2. Elliptic curves. An elliptic curve over the rationals is a non-singular curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where the coefficients a_i are integers. Any curve of the above form is isomorphic to one, say E, of the form

$$E:\ y^2 = x^3 + ax^2 + bx + c, \tag{2.2}$$

with integers a, b, and c. The *discriminant* of E, denoted by $\Delta(E)$, is given by

$$\Delta(E) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \tag{2.3}$$

If p is prime, then let $GF(p)$ denote the finite field with p elements. If p is prime, then $\bar{E}_p$ is the *reduction* of E to $GF(p)$. If the reduction is smooth, then we say E has *good* reduction at p. Otherwise, E has *bad* reduction at p. If $p \nmid \Delta(E)$, then E has good reduction at p.

The Hasse-Weil L-function of E, denoted by $L(E,s)$, is obtained by examining the reductions $\bar{E}_p$. If p is a prime of good reduction, then define the integer $a(p)$ as

$$a(p) = p + 1 - N_p, \tag{2.4}$$

where N_p is the number of points of $\bar{E}_p$ rational over $GF(p)$, including the point at infinity. There are similar rules for those p with bad reduction. If p is prime and $k \geq 2$, then

$$a(p^k) = \begin{cases} a(p)\,a(p^{k-1}) - pa(p^{k-2}) & p \text{ good reduction,} \\ a(p)\,a(p^{k-1}) & p \text{ bad reduction.} \end{cases} \tag{2.5}$$

Furthermore, if $\gcd(n,m) = 1$, then

$$a(nm) = a(n)\,a(m). \tag{2.6}$$

The L-function is then given by

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}. \tag{2.7}$$

As a consequence of (2.5) and (2.6), we obtain:

Proposition 2.1. *Let E be an elliptic curve and let $L(E,s) = \sum_{n=1}^{\infty} (a(n)/n^s)$ be its Hasse-Weil function. Suppose that $n > 1$ is relatively prime to $2 \cdot \Delta(E)$ with prime factorization*

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}, \tag{2.8}$$

where

$$a(p_i) \equiv 0 \pmod 2 \quad \text{and} \quad a(q_j) \equiv 1 \pmod 2. \tag{2.9}$$

Then $a(n)$ is odd if and only if every $a_i \equiv 0 \pmod 2$ and every $b_j \not\equiv 2 \pmod 3$.

PROOF. By hypothesis, every p_i and q_j are odd primes all with good reduction. Then by (4), we find that for every $k \geq 2$,

$$\begin{aligned} a(p_i^k) &\equiv a(p_i^{k-2}) \pmod 2, \\ a(q_j^k) &\equiv a(q_j^{k-1}) + a(q_j^{k-2}) \pmod 2. \end{aligned} \tag{2.10}$$

It is easy to verify then that $a(p_i^k)$ is odd if and only if $k \equiv 0 \pmod 2$, and that $a(q_j^k)$ is odd if and only if $k \not\equiv 2 \pmod 3$. The result now follows easily from (2.6). □

EXAMPLE 2.1. In this example, let E denote the curve

$$E: y^2 = x^3 - x. \tag{2.11}$$

Since $\Delta(E) = 4$, E has good reduction at every prime $p \neq 2$. If $p = 5$, then $\bar{E}_p = \bar{E}_5$ is the collection of points $(x, y) \in GF(5) \times GF(5)$ satisfying the congruence

$$y^2 \equiv x^3 - x \pmod 5. \tag{2.12}$$

An easy computation verifies that the only such points are

$$(0,0),\ (1,0),\ (2,1),\ (2,4),\ (3,2),\ (3,3),\ (4,0),\ \infty. \tag{2.13}$$

So in this case $N_5 = 8$, and so $a(5) = 5 + 1 - 8 = -2$. In fact, the first few terms of $L(E, s)$ are

$$L(E, s) = 1 - \frac{2}{5^s} - \frac{3}{9^s} + \frac{6}{13^s} + \cdots. \tag{2.14}$$

The Taniyama-Shimura-Weil conjecture states that all elliptic curves over the rationals are modular. A curve is modular if its L-function corresponds to the Fourier expansion at infinity of a modular form. Specifically, if E is modular and $L(E, s) = \sum_{n=1}^{\infty} (a(n)/n^s)$, then

$$F_E(z) = \sum_{n=1}^{\infty} a(n) q^n \quad (q = e^{2\pi i z}) \tag{2.15}$$

is a *modular* form. For a number of explicit examples (see [1]), the form $F_E(z)$ is given as a product of Dedekind's η-function defined by

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n). \tag{2.16}$$

For example, take the η-product

$$F_E(z) = \eta^4(6z) = q \prod_{n=1}^{\infty} (1 - q^{6n})^4. \tag{2.17}$$

The coefficients of the L-function $L(E, s)$ of the elliptic curve $E: y^2 = x^3 + 1$ are the same as those in the Fourier expansion of $F_E(z)$.

3. q-series results. In this section, we give two theorems which do not depend on elliptic curves. They simply depend on q-series manipulations.

Theorem 3.1. *If $n=(2m+1)^2$, then an odd number of the values*

$$p\left(\frac{n-1}{4}-\left(\frac{a^2+a}{2}+6b^2+2b\right)\right) \tag{3.1}$$

are odd, where $a \geq 0$ and b are integers.

Proof. Consider the η-product

$$\eta^2(4z)\eta^2(8z)=\sum_{n=1}^{\infty} a(n)q^n = q\prod_{n=1}^{\infty}(1-q^{4n})^2(1-q^{8n})^2. \tag{3.2}$$

Factor this as

$$\eta^2(4z)\eta^2(8z)=\eta^3(8z)\frac{\eta^2(4z)}{\eta(8z)}. \tag{3.3}$$

Recall the following identity due to Jacobi.

$$\prod_{n=1}^{\infty}(1-q^n)^3=\sum_{a=0}^{\infty}(-1)^a(2a+1)q^{(a^2+a)/2}. \tag{3.4}$$

Using this identity and another well known identity, we obtain

$$\eta^3(8z)=\sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(2n+1)^2} \tag{3.5}$$

and

$$\frac{\eta^2(4z)}{\eta(8z)}=1+2\sum_{n=1}^{\infty}(-1)^n q^{4n^2}, \tag{3.6}$$

so,

$$\begin{aligned}\eta^3(8z)\frac{\eta^2(4z)}{\eta(8z)} &= \left(\sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(2n+1)^2}\right)\cdot\left(1+2\sum_{n=1}^{\infty}(-1)^n q^{4n^2}\right)\\ &\equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2.\end{aligned} \tag{3.7}$$

So,

$$\eta^2(4z)\eta^2(8z)\equiv q+q^9+q^{25}+q^{49}+\cdots \pmod 2. \tag{3.8}$$

Because $\prod_{n=1}^{\infty}(1/(1-q^n))$ is the generating function for the partition function, we find that

$$q\left(\sum_{n=0}^{\infty}p(n)q^{4n}\right)\cdot\prod_{n=1}^{\infty}(1-q^{4n})^3\cdot\prod_{n=1}^{\infty}(1-q^{8n})^2=\eta^2(4z)\eta^2(8z). \tag{3.9}$$

Using Jacobi's identity, (1.2) and the fact that $(1-q^{8n})^2 \equiv (1-q^{16n}) \pmod 2$, this becomes

$$\left(\sum_{n=0}^{\infty} p(n)q^{4n+1}\right) \cdot \left(\sum_{a=0}^{\infty} q^{2a^2+2a}\right) \cdot \left(\sum_{b=-\infty}^{\infty} q^{24b^2+8b}\right) \equiv \eta^2(4z)\eta^2(8z) \pmod 2. \tag{3.10}$$

Therefore, we find that

$$\sum_{n=1}^{\infty} a(n)q^n \equiv \left(\sum_{n=0}^{\infty} p(n)q^{4n+1}\right) \cdot \left(\sum_{a\geq 0,\, b\in\mathbb{Z}} q^{2a^2+2a+24b^2+8b}\right) \pmod 2. \tag{3.11}$$

Therefore, it is easy to check that

$$a(n) \equiv \sum_{a\geq 0,\, b\in\mathbb{Z}} p\left(\frac{n-1}{4} - \left(\frac{a^2+a}{2} + 6b^2 + 2b\right)\right) \pmod 2. \tag{3.12}$$

The theorem now follows immediately. □

Theorem 3.2. *If $n = (6m+1)^2$, then an odd number of the values*

$$p\left(\frac{n-1}{6} - \left(\frac{a^2+a}{2} + 3b^2 + b\right)\right) \tag{3.13}$$

are odd, where $a \geq 0$ and b are integers.

Proof. Consider the η-product

$$\eta^4(6z) = \prod_{n=0}^{\infty} (1-q^{6n})^4. \tag{3.14}$$

Since $\eta^4(6z) \equiv \eta(24z) \pmod 2$, we can use (1.2) to give us

$$\eta(24z) = \sum_{n=-\infty}^{\infty} (-1)^n q^{36n^2+12n+1} \equiv \sum_{n=-\infty}^{\infty} q^{(6n+1)^2} \pmod 2. \tag{3.15}$$

Thus, $\eta^4(6z) \equiv 1 + q^{25} + q^{49} + q^{121} + q^{169} + \cdots \pmod 2$. Because $\prod_{n=1}^{\infty} (1/(1-q^n))$ is the generating function for the partition function, we find that

$$q\left(\sum_{n=0}^{\infty} p(n)q^{6n}\right) \cdot \prod_{n=1}^{\infty} (1-q^{6n})^3 \cdot \prod_{n=1}^{\infty} (1-q^{6n})^2 = \eta^4(6z). \tag{3.16}$$

Since $(1-q^{6n})^2 \equiv (1-q^{12n}) \pmod 2$, we can use (3.4) and (1.2) to get

$$\left(\sum_{n=0}^{\infty} p(n)q^{6n+1}\right) \cdot \left(\sum_{a=0}^{\infty} q^{3a^2+3a}\right) \cdot \left(\sum_{b=-\infty}^{\infty} q^{18b^2+6b}\right) \equiv \eta^4(6z) \pmod 2. \tag{3.17}$$

Therefore, we find that

$$\sum_{n=1}^{\infty} a(n)q^n \equiv \left(\sum_{n=0}^{\infty} p(n)q^{6n+1}\right) \cdot \left(\sum_{a\geq 0,\, b\in\mathbb{Z}} q^{3a^2+3a+18b^2+6b}\right) \pmod 2. \tag{3.18}$$

Therefore, it is easy to check that

$$a(n) \equiv \sum_{a \geq 0,\, b \in \mathbb{Z}} p\left(\frac{n-1}{6} - \left(\frac{a^2+a}{2} + 3b^2 + b\right)\right) \pmod 2. \tag{3.19}$$

The theorem now follows immediately. □

Example 3.1. Here, we illustrate an example of Theorem 3.2. If $m = 1$, then $n = (6m+1)^2 = 49$. We must find pairs (a,b) with $a \geq 0$ and b integers such that

$$\frac{n-1}{6} = 8 \geq \left(\frac{a^2+a}{2} + 3b^2 + b\right). \tag{3.20}$$

These pairs are: $(0,0)$ $(0,-1)$ $(0,1)$ $(1,0)$ $(1,-1)$ $(1,1)$ $(2,0)$ $(2,-1)$ $(2,1)$ $(3,0)$ $(3,-1)$. Theorem 3.2 tells us that an odd number of the following values are odd:

$$\begin{aligned} &p(8) = 22, \quad p(6) = 11, \quad p(4) = 5, \quad p(7) = 15, \quad p(5) = 7, \quad p(3) = 3, \\ &p(5) = 7, \quad p(3) = 3, \quad p(1) = 1, \quad p(2) = 2, \quad p(0) = 1. \end{aligned} \tag{3.21}$$

Nine of the eleven are indeed odd.

Group law for elliptic curves. If E is an elliptic curve, $E:\ y^2 = x^3 + ax^2 + bx + c$, the point at infinity is taken to be its identity element O, and $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points on E, then $P + Q := (x_3, y_3)$, where

$$x_3 = \lambda^2 - a - x_1 - x_2 \tag{3.22}$$

and

$$y_3 = \lambda x_3 + y_1 - \lambda x_1. \tag{3.23}$$

If $P = Q$, then

$$\lambda = \frac{3x^2 + 2ax + b}{2y}, \tag{3.24}$$

otherwise

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{3.25}$$

The question of finding points of order two on a curve is the same as that of finding all the points such that $P + P = O$ but $P \neq O$. It is easily seen from the above that this is satisfied only when $y = 0$.

Fundamental theorem. *If E is an elliptic curve and p is a prime of good reduction, then $\bar{E}_p$ with the point at infinity is a finite abelian group.*

Theorem 3.3. *Let E be the elliptic curve*

$$E:\ y^2 = x^3 + ax^2 + bx + c, \tag{3.26}$$

and $L(E,s) = \sum_{n=1}^{\infty} (a(n)/n^s)$ its Hasse-Weil function. If the odd prime p has good reduction, then $a(p)$ is odd if and only if $x^3 + ax^2 + bx + c \equiv 0 \pmod p$ has no solution.

Proof. By definition, $a(p) = p+1-N_p$, where N_p is the number of rational points of E over $GF(p)$. Since p is an odd prime, we find that $a(p)$ is odd if and only if

$$N_p \equiv 1 \pmod{2}. \tag{3.27}$$

The elliptic curve $\bar{E}_p$ is a finite abelian group with N_p elements, so Lagrange's theorem states that N_p is a multiple of the order of each of the individual points. Thus, asking when N_p is odd is the same as asking for which $\bar{E}_p$ are there no points of order two. A point of order 2 on an elliptic curve is one whose y-coordinate is zero. Thus, N_p and, consequently, $a(p)$ is odd if the equation $y^2 \equiv x^3+ax^2+bx+c \equiv 0 \pmod{p}$ has no solution for which $y = 0$. □

Theorem 3.4. *Let $p_1 < p_2 < \cdots$ be the primes for which*

$$x^3-4x^2-160x-1264 \equiv 0 \pmod{p_i} \tag{3.28}$$

have solutions in GF (p_i) and let $q_1 < q_2 < \cdots$ be the primes for which

$$x^3-4x^2-160x-1264 \equiv 0 \pmod{q_j} \tag{3.29}$$

has no solutions in GF (q_j). Suppose that $n > 1$ is relatively prime to 2378 and that it has the factorization

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}. \tag{3.30}$$

If every $a_i \equiv 0 \pmod{2}$ and every $b_j \not\equiv 2 \pmod{3}$, then an odd number of the values

$$p\left(n-1-\left(\frac{a^2+a}{2}+33b^2+11b\right)\right) \tag{3.31}$$

are odd, where $a \geq 0$ and b are integers.

Proof. In [1], it is proved that if E is the curve

$$E:\ y^2 = x^3-4x^2-160x-1264, \tag{3.32}$$

then its Hasse-Weil function $L(E,s) = \sum_{n=1}^{\infty} (a(n)/n^s)$ has the property that its coefficients $a(n)$ are given by

$$\eta^2(z)\eta^2(11z) = q\prod_{n=1}^{\infty} (1-q^n)^2(1-q^{11n})^2. \tag{3.33}$$

However, since $(1-q^{11n})^2 \equiv (1-q^{22n}) \pmod{2}$, we find that

$$\sum_{n=1}^{\infty} a(n)q^n \equiv q\prod_{n=1}^{\infty} (1-q^n)^2(1-q^{22n}) \pmod{2}. \tag{3.34}$$

Therefore, we find by (1.1) that

$$\left(\sum_{n=0}^{\infty} p(n)q^{n+1}\right)\prod_{n=1}^{\infty} (1-q^n)^3 \prod_{n=1}^{\infty} (1-q^{22n}) \equiv \sum_{n=1}^{\infty} a(n)q^n \pmod{2}. \tag{3.35}$$

But by Jacobi's identity (3.4) and Euler's identity (1.2), this reduces to

$$\left(\sum_{n=0}^{\infty} p(n)q^{n+1}\right)\cdot\left(\sum_{a=0}^{\infty} q^{(a^2+a)/2}\right)\cdot\left(\sum_{n=-\infty}^{\infty} q^{33b^2+11b}\right) \equiv \sum_{n=1}^{\infty} a(n)q^n \pmod 2. \quad (3.36)$$

Therefore, it turns out that

$$a(n) \equiv \sum_{a\geq 0,\, b\in\mathbb{Z}} p\left(n-1-\left(\frac{a^2+a}{2}+33b^2+11b\right)\right) \pmod 2. \quad (3.37)$$

The result now follows immediately from Theorem 3.3 and Proposition 2.1. □

Example 3.2. It is easy to show that there is no solution to the equation

$$x^3-4x^2-160x-1264 \equiv 0 \pmod{p_i} \quad (3.38)$$

for the primes 3 and 5. So by (2.6), $n = 15$ is a suitable choice to illustrate Theorem 3.4. We must, therefore, find all pairs (a,b) with $a \geq 0$ and $b \in \mathbb{Z}$ such that $14 \geq (\frac{a^2+a}{2} + 33b^2+11b)$. These pairs are: $(0,0)$ $(1,0)$ $(2,0)$ $(3,0)$ $(4,0)$. So by Theorem 3.4, an odd number of the following

$$p(14) = 135, \quad p(13) = 101, \quad p(11) = 56, \quad p(8) = 22, \quad p(4) = 5 \quad (3.39)$$

are odd.

Theorem 3.5. *Let $p_1 < p_2 < \cdots$ be the primes for which*

$$x^3+x^2+72x-368 \equiv 0 \pmod{p_i} \quad (3.40)$$

have solutions in GF (p_i) and $q_1 < q_2 < \cdots$ the primes for which

$$x^3+x^2+72x-368 \equiv 0 \pmod{q_j} \quad (3.41)$$

has no solutions in GF (q_j). Suppose that $n > 1$ is relatively prime to 14 and that its prime factorization is

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}. \quad (3.42)$$

If every $a_i \equiv 0 \pmod 2$ and every $b_j \not\equiv 2 \pmod 3$, then an odd number of the values

$$p\left(n-1-\left(\frac{7a^2+7a}{2}+6b^2+2b\right)\right) \quad (3.43)$$

are odd, where $a \geq 0$ and b are integers.

Proof. In [1], it is proved that if E is the curve

$$E:\ y^2 = x^3+x^2+72x-368, \quad (3.44)$$

then its Hasse-Weil function $L(E,s) = \sum_{n=1}^{\infty} (a(n)/n^s)$ has the property that its coefficients $a(n)$ are given by

$$\eta(z)\eta(2z)\eta(7z)\eta(14z) = q \prod_{n=1}^{\infty} (1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n}). \tag{3.45}$$

Using Euler's identity (1.2), Jacobi's identity (3.4), and the fact that $(1-q^{2n}) \equiv (1-q^n)^2 \pmod 2$, the theorem follows in a manner similar to that of Theorem 3.4. □

Theorem 3.6. *Let $p_1 < p_2 < \cdots$ be the primes for which*

$$x^3 + x^2 + 4x + 4 \equiv 0 \pmod{p_i} \tag{3.46}$$

have solutions in GF (p_i) and $q_1 < q_2 < \cdots$ the primes for which

$$x^3 + x^2 + 4x + 4 \equiv 0 \pmod{q_j} \tag{3.47}$$

has no solutions in GF (q_j). Suppose that $n > 1$ is relatively prime to 10 and that its prime factorization is

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}. \tag{3.48}$$

If every $a_i \equiv 0 \pmod 2$ and every $b_j \not\equiv 2 \pmod 3$, then an odd number of the values

$$p\left(\frac{n-1}{2} - \left(a^2 + a + 30b^2 + 10b\right)\right), \tag{3.49}$$

are odd, where $a \geq 0$ and b are integers.

Proof. If E is the curve

$$E: y^2 = x^3 + x^2 + 4x + 4, \tag{3.50}$$

then in [1], it was proved that the coefficients $a(n)$ of its Hasse-Weil function $L(E,s) = \sum_{n=1}^{\infty} (a(n)/n^s)$ are given by

$$\eta^2(2z)\eta^2(10z) = q \prod_{n=1}^{\infty} (1-q^{2n})^2(1-q^{10n})^2. \tag{3.51}$$

The proof follows in a manner similar to Theorem 3.4. □

Theorem 3.7. *Let $p_1 < p_2 < \cdots$ be the primes for which*

$$x^3 - x^2 - 4x + 4 \equiv 0 \pmod{p_i} \tag{3.52}$$

have solutions in GF (p_i) and $q_1 < q_2 < \cdots$ the primes for which

$$x^3 - x^2 - 4x + 4 \equiv 0 \pmod{q_j} \tag{3.53}$$

has no solutions in GF (q_j). Suppose that $n > 1$ is relatively prime to 6 and that its prime factorization is

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}. \tag{3.54}$$

If every $a_i \equiv 0 \pmod 2$ *and every* $b_j \not\equiv 2 \pmod 3$, *then an odd number of the values*

$$p\left(\frac{n-1}{2} - \left(3a^2+3a+12b^2+4b\right)\right) \tag{3.55}$$

are odd, where $a \geq 0$ *and* b *are integers.*

Proof. If E is the curve

$$E:\ y^2 = x^3 - x^2 - 4x + 4, \tag{3.56}$$

then in [1], it was proved that the coefficients $a(n)$ of its Hasse-Weil function $L(E,s) = \sum_{n=1}^{\infty}(a(n)/n^s)$ are given by

$$\eta(2)\eta(4z)\eta(6z)\eta(12z) = q\prod_{n=1}^{\infty}(1-q^{2n})(1-q^{4n})(1-q^{6n})(1-q^{12n}). \tag{3.57}$$

The proof follows in a manner similar to Theorem 3.4. □

Theorem 3.8. *Let* $p_1 < p_2 < \cdots$ *be the primes for which*

$$x^3 - 432 \equiv 0 \pmod{p_i} \tag{3.58}$$

have solutions in GF (p_i) *and* q_j *are the primes for which*

$$x^3 - 432 \equiv 0 \pmod{q_j} \tag{3.59}$$

has no solutions in GF (q_j). *Suppose that* $n > 1$ *is relatively prime to 6 and that its prime factorization is*

$$n = \prod_i p_i^{a_i} \prod_j q_j^{b_j}. \tag{3.60}$$

If every $a_i \equiv 0 \pmod 2$ *and every* $b_j \not\equiv 2 \pmod 3$, *then an odd number of the values*

$$p\left(\frac{n-1}{3} - \left(\frac{3a^2+3a}{2} + 27b^2 + 9b\right)\right) \tag{3.61}$$

are odd, where $a \geq 0$ *and* b *are integers.*

Proof. If E is the curve

$$E:\ y^2 = x^3 - 432, \tag{3.62}$$

then in [1], it was proved that the coefficients $a(n)$ of its Hasse-Weil function $L(E,s) = \sum_{n=1}^{\infty}(a(n)/n^s)$ are given by

$$\eta^2(3z)\eta^2(9z) = q\prod_{n=1}^{\infty}(1-q^{3n})^2(1-q^{9n})^2. \tag{3.63}$$

The proof follows in a manner similar to Theorem 3.4. □

Also, realize that the curves in Theorems 3.4, 3.5, and 3.8 were all changed from the form they are normally shown into the form $y^2 = x^3 + ax^2 + bx + c$ by a simple change of variables to ease the job of finding points of order two.

Acknowledgements. I am a high school student and this is a revised version of my paper from the Westinghouse Science Talent Search. I would like to thank Ken Ono for his great help in suggesting this idea as well as helping me throughout the way. His many suggestions vastly improved the form and content of this paper. Also, thanks are due to George McRae and Dick Lane for help with using $\mathcal{AMS}$-TEX and finding references. Jim Cusker has provided much support and encouragement for me to pursue mathematical research projects over the last three years in his Advanced Problems in Science class.

References

[1] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc. **125** (1997), no. 11, 3169–3176. MR 97m:11057. Zbl 970.60471.

[2] M. Newman, *Periodicity modulo m and divisibility properties of the partition function*, Trans. Amer. Math. Soc. **97** (1960), 225–236. MR 22#6778. Zbl 106.03903.

[3] K. Ono, *Parity of the partition function in arithmetic progressions*, J. Reine Angew. Math. **472** (1996), 1–15. MR 97e:11131. Zbl 835.11038.

[4] ———, *Odd values of the partition function*, Discrete Math. **169** (1997), no. 1-3, 263–268. CMP 97 13. Zbl 970.40475.

[5] T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466–480. MR 37#2711. Zbl 149.28501.

[6] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 93g:11003. Zbl 752.14034.

[7] M. V. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851–854. MR 34#1293. Zbl 173.01803.

Eriksson: 2401 S. Hills Dr. Missoula, MT 59803, USA
E-mail address: eriksson@mit.edu