Bulletin of the Iranian Mathematical Society 49(2023), Art.67, 25pp.

Quartic congruences and eta products

Zhi-Hong Sun
School of Mathematics and Statistics
Huaiyin Normal University
Huaian, Jiangsu 223300, P.R. China
Email: zhsun@hytc.edu.cn
URL: http://maths.hytc.edu.cn/szh1.htm

Dongxi Ye
School of Mathematics (Zhuhai)
Sun Yat-sen University
Zhuhai, Guangdong 519082, P.R. China
Email: yedx3@mail.sysu.edu.cn

Abstract

Let $a_{15}(n), a_{20}(n)$ and $a_{24}(n)$ be defined by

$$\begin{aligned}&q\prod_{k=1}^{\infty}(1-q^k)(1-q^{3k})(1-q^{5k})(1-q^{15k})=\sum_{n=1}^{\infty}a_{15}(n)q^n,\\&q\prod_{k=1}^{\infty}(1-q^{2k})^2(1-q^{10k})^2=\sum_{n=1}^{\infty}a_{20}(n)q^n,\\&q\prod_{k=1}^{\infty}(1-q^{2k})(1-q^{4k})(1-q^{6k})(1-q^{12k})=\sum_{n=1}^{\infty}a_{24}(n)q^n\quad(|q|<1),\end{aligned}$$

and let $p>3$ be a prime. In this paper, for $p\equiv 3 \pmod 4$ we reveal the connection between $a_{20}(p)$ and residue-counts of x^4-4x^2+4x modulo p as x runs over $0,1,\ldots,p-1$, and the connection between $a_{24}(p)$ and residue-counts of x^3+c/x modulo p as x runs over $1,2,\ldots,p-1$, where c is an integer not divisible by p. We also deduce the congruences for $a_{15}(p), a_{24}(p)$ modulo 16 and $a_{20}(p)$ modulo 4, and pose some analogous conjectures.

MSC(2020): 11A07, 11L10, 11E20, 11E25, 11F11, 11F20, 11F33, 11G20
Keywords: congruence; eta product; modular form; elliptic curve; quadratic form

1. Introduction

The Dedekind eta function $\eta(z)$ is given by

$$\eta(z)=q^{\frac{1}{24}}\prod_{n=1}^{\infty}\left(1-q^n\right)\quad\text{with}\quad q=e^{2\pi iz}.$$

It is shown by Martin and Ono [13] that there are only finitely many newforms of weight 2 in the form of eta products, which are summarized in the following table:

level	eta product
11	$\eta(z)^2\eta(11z)^2$
14	$\eta(z)\eta(2z)\eta(7z)\eta(14z)$
15	$\eta(z)\eta(3z)\eta(5z)\eta(15z)$
20	$\eta(2z)^2\eta(10z)^2$
24	$\eta(2z)\eta(4z)\eta(6z)\eta(12z)$
27	$\eta(3z)^2\eta(9z)^2$
32	$\eta(4z)^2\eta(8z)^2$
36	$\eta(6z)^4$
48	$\dfrac{\eta(4z)^4\eta(12z)^4}{\eta(2z)\eta(6z)\eta(8z)\eta(24z)}$
64	$\dfrac{\eta(8z)^8}{\eta(4z)^2\eta(16z)^2}$
80	$\dfrac{\eta(4z)^6\eta(20z)^6}{\eta(2z)^2\eta(8z)^2\eta(10z)^2\eta(40z)^2}$
144	$\dfrac{\eta(12z)^{12}}{\eta(6z)^4\eta(24z)^4}$

Now for each level N given in the table, we define $a_N(n)$ for $n \geq 1$ to be the n-th Fourier coefficient of the corresponding eta product. Let p be an odd prime with $p \nmid N$. In [13], for $N \in \{27, 32, 36, 64, 144\}$ Martin and Ono gave the values of $a_N(p)$ in terms of the representations of p by suitable binary quadratic forms.

For $a \in \mathbb{Z}$ and given positive integer m let $\left(\frac{a}{m}\right)$ denote the Legendre-Jacobi-Kronecker symbol. In [17], using a result due to Eichler the first author stated that for any prime $p \neq 2, 3, 11$,

$$a_{11}(p) = -\left(\frac{6}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x+38}{p}\right). \tag{1.1}$$

In this paper, we give formulas for $a_N(p)$ with $N \in \{14, 15, 20, 24, 48, 80\}$, where $p > 5$ is a prime. We first relate $a_N(p)$ with the sum $\sum_{x=0}^{p-1}\left(\frac{x^3+Ax+B}{p}\right)$ by using the Modularity Theorem, and then reveal the connections between $a_N(p)$ and quartic congruences modulo p for $N \in \{20, 24, 48, 80\}$ and $p \equiv 3 \pmod 4$.

Let $p > 3$ be a prime, $a, b \in \mathbb{Z}$ and $N_p(a, b)$ be the number of incongruent residues of $x^4 + ax^2 + bx$ modulo p as x runs over $0, 1, \ldots, p-1$. In [16], the first author related $N_p(a, b)$ with the numbers of points on certain elliptic curves over $\mathbb{F}_p$ (the field with p elements), and completely determined $N_p(a, b)$ for some special values of (a, b). Inspired by the work in [16], in this paper we find the connection between $a_{20}(p)$ and $N_p(-4, 4)$ for $p \equiv 3 \pmod 4$, and deduce a formula for $N_p(c)$, which is the number of incongruent residues of $x^3 + c/x$ modulo p as x runs over $1, 2, \ldots, p-1$, where c is an integer not divisible by p. It is surprising that $N_p(c)$ is in connection with $a_{24}(p)$ and $a_{48}(p)$, which is proved by using the first author's previous work on the numbers of solutions of quartic congruences modulo p. The main results of this paper are summarized as follows:

Theorem 1.1. *Let $p>3$ be a prime of the form $4k+3$ and*

$$\delta(p)=\begin{cases}0 & \text{if } p\equiv 7,23 \pmod{40},\\ 1 & \text{if } p\equiv 3,27,31,39 \pmod{40},\\ 2 & \text{if } p\equiv 11,19 \pmod{40}.\end{cases}$$

Then

$$a_{20}(p)=-a_{80}(p)=\frac{5p+1}{2}+2\delta(p)-4N_p(-4,4).$$

Theorem 1.2. *Let $p>3$ be a prime and $c\in\mathbb{Z}$ with $p\nmid c$. Then*

$$N_p(c)=\delta+\frac{1}{8}\Big(5p-3+\Big(\frac{-c}{p}\Big)a_{24}(p)-\big(1+(-1)^{\frac{p-1}{2}}\big)\\ \times\Big(\sum_{x=1}^{(p-1)/2}\Big(\frac{x}{p}\Big)\Big(3\Big(\frac{x^2-4c}{p}\Big)+\Big(\frac{16c-3x^2}{p}\Big)-\Big(\frac{x^2-4c}{p}\Big)\Big(\frac{16c-3x^2}{p}\Big)\Big)\Big)\Big),$$

where

$$\delta=\begin{cases}2 & \text{if } 8\mid p-5 \text{ and } 27c \text{ is a quartic residue of } p,\\ 1 & \text{if } 8\mid p-7 \text{ and } \Big(\frac{27c}{p}\Big)=1,\\ 0 & \text{otherwise.}\end{cases}\tag{1.2}$$

In particular, for $p\equiv 3\pmod 4$ we have

$$N_p(c)=\begin{cases}\frac{5p+5}{8}+\frac{1}{8}\Big(\frac{-c}{p}\Big)a_{24}(p) & \text{if } 8\mid p-7 \text{ and } \Big(\frac{3c}{p}\Big)=1,\\ \frac{5p-3}{8}+\frac{1}{8}\Big(\frac{-c}{p}\Big)a_{24}(p) & \text{otherwise.}\end{cases}\tag{1.3}$$

We also deduce the following congruences for $a_{15}(p), a_{24}(p), a_{48}(p)$ modulo 16 and $a_{14}(p), a_{20}(p), a_{80}(p)$ modulo 4, where $p>5$ is a prime. The proofs are based on Theorems 1.1 and 1.2, and some known results on the number of representations of p as a linear combination of four squares or triangular numbers.

Theorem 1.3. *Let $p>3$ be a prime. Then*

$$a_{24}(p)=(-1)^{\frac{p-1}{2}}a_{48}(p)\equiv\begin{cases}p+1 \pmod{16} & \text{if } p\equiv 1 \pmod{12},\\ 4-(p+1) \pmod{16} & \text{if } p\equiv 5 \pmod{12},\\ -(p+1) \pmod{16} & \text{if } p\equiv 11,19,23 \pmod{24},\\ 8-(p+1) \pmod{16} & \text{if } p\equiv 7 \pmod{24}.\end{cases}$$

Theorem 1.4. *Let p be a prime such that $p\neq 2,5$. Then*

$$a_{20}(p)\equiv a_{80}(p)\equiv\begin{cases}0 \pmod 4 & \text{if } p\equiv 11,19 \pmod{20},\\ 2 \pmod 4 & \text{if } p\not\equiv 11,19 \pmod{20}.\end{cases}$$

Theorem 1.5. *Let p be a prime such that $p\neq 2,7$. Then*

$$a_{14}(p)\equiv\begin{cases}2 \pmod 4 & \text{if } p\equiv 1 \pmod 8 \text{ or } p\equiv \pm 3,\pm 19,\pm 27 \pmod{56},\\ 0 \pmod 4 & \text{otherwise.}\end{cases}$$

Theorem 1.6. *Let p be a prime with $p > 5$. Then*

$$a_{15}(p) \equiv \begin{cases} p+1 \pmod{16} & \text{if } p \equiv 11, 19, 31, 59 \pmod{60}, \\ 8+5(p+1) \pmod{16} & \text{otherwise.} \end{cases}$$

We remark that Köhler [12] gave the congruence for $a_{24}(p)$ modulo 16 in the case $p \equiv 7 \pmod 8$, and Alaca, Alaca and Aygin [2] proved that for any prime $p > 11$,

$$a_{11}(p) \equiv p+1 \pmod 5,\ a_{14}(p) \equiv p+1 \pmod 6,\ a_{15}(p) \equiv p+1 \pmod 4,$$
$$a_{20}(p) \equiv p+1 \pmod 6,\ a_{24}(p) \equiv 0 \pmod 2.$$

For positive integers a, b, c, d and non-negative integer n let $N(a, b, c, d; n)$ be the number of representations of n by $ax^2 + by^2 + cz^2 + dw^2$, and let $t(a, b, c, d; n)$ be the number of representations of n by $a\frac{x(x+1)}{2} + b\frac{y(y+1)}{2} + c\frac{z(z+1)}{2} + d\frac{w(w+1)}{2}$, where $x, y, z, w \in \mathbb{Z}$. Then we have the following result.

Theorem 1.7. *Let p be a prime with $p \neq 2, 11$. Then*

$$N(1,1,11,11;p) = \frac{4}{5}(p+1) + \frac{16}{5}a_{11}(p),$$
$$t(1,1,11,11;p-3) = \frac{16}{5}(p+1) - \frac{16}{5}a_{11}(p)$$

and so

$$a_{11}(p) \equiv \begin{cases} 1 \pmod 2 & \text{if } 4p = x^2 + 11y^2 \text{ with } x, y \in \mathbb{Z} \text{ and } 2 \nmid y, \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

We remark that Evink and Helminck [8] proved that $a_{11}(p) \equiv 0 \pmod 2$ for any prime $p = x^2 + 11y^2 \neq 11$ by using class field theory. For any odd prime p, it is known that

$$N(1,1,6,6;p) = 2(p+1+a_{24}(p)) \quad \text{for} \quad p \neq 3, \tag{1.4}$$

$$N(1,1,5,5;p) = \frac{4}{3}(p+1) + \frac{8}{3}a_{20}(p) \quad \text{for} \quad p \neq 5, \tag{1.5}$$

$$N(1,1,7,7;p) = \frac{4}{3}(p+1) + \frac{8}{3}a_{14}(p) \quad \text{for} \quad p \neq 7, \tag{1.6}$$

$$N(1,3,5,15;p) = \frac{p+1}{2} + \frac{3}{2}a_{15}(p) \quad \text{for} \quad p \neq 3, 5. \tag{1.7}$$

Actually, the identities (1.4)-(1.7) can be found in [3, Theorem 1.12], [4, Theorem 7.1], [18, Lemma 2.10] and [1, Theorem 3.3], respectively.

This paper is organized as follows. In Section 2, for $N \in \{14, 15, 20, 24, 48, 80\}$ we give explicit formulas for $a_N(p)$ in terms of the sum $\sum_{x=0}^{p-1}\left(\frac{x^3+Ax+B}{p}\right)$ and prove Theorems 1.1 and 1.2, where p is an odd prime such that $p \nmid N$. In Section 3, we prove Theorem 1.3. In Section 4, we prove Theorems 1.4 and 1.5. In Section 5, we give the proof of Theorem 1.6. In Section 6, we prove Theorem 1.7. In Section 7, based on calculations by Maple we pose three conjectures on $a_{11}(p)$ modulo 4 and $a_{14}(p), a_{20}(p)$ modulo 8.

2. Formulas for $a_N(p)$ and proofs of Theorems 1.1 and 1.2

By numerical calculations, in [18] the first author found the following conjectural identities analogous to (1.1) for $a_N(p)$ with $N \in \{14, 15, 20, 24, 48, 80\}$, where p is an odd prime such that $p \nmid N$. This provides uniform formulas for $a_N(p)$ concerning newforms of weight 2 that are eta products.

Lemma 2.1 ([18, Conjecture 2.1]). *Let $p > 3$ be a prime. Then*

$$a_{14}(p) = -\left(\frac{-3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-75x-506}{p}\right),$$

$$a_{15}(p) = -\left(\frac{-3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3x-322}{p}\right),$$

$$a_{20}(p) = \left(\frac{-1}{p}\right)a_{80}(p) = -\left(\frac{-3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x-11}{p}\right),$$

$$a_{24}(p) = \left(\frac{-1}{p}\right)a_{48}(p) = -\left(\frac{-3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-39x-70}{p}\right).$$

Proof. Let $E : y^2 = f_E(x)$ denote an elliptic curve over $\mathbb{Q}$, and let $a_E(1) = 1$ and $a_E(p)$ be defined for prime p by $a_E(p) = p + 1 - |\{\text{projective points of } E \text{ over } \mathbb{F}_p\}|$. It is well known (see for example [16, p.221]) that for $p \geq 3$, $a_E(p) = -\sum_{x=0}^{p-1}\left(\frac{f_E(x)}{p}\right)$. By the Modularity Theorem (see for example [7, Theorem 8.8.1]), there is a normalized newform $g_E(z) = \sum_{n=1}^{\infty} a_{g_E}(n)q^n$ of weight 2 for $\Gamma_0(N_E)$, where N_E denotes the algebraic conductor of E, with trivial Nebentypus such that $a_{g_E}(p) = a_E(p)$ for all primes p, that is, $a_{g_E}(2) = a_E(2)$ and $a_{g_E}(p) = -\sum_{x=0}^{p-1}\left(\frac{f_E(x)}{p}\right)$ for $p \geq 3$. Now from this point on, let E be an elliptic curve defined by one of the cubic polynomials in Lemma 2.1. One can compute and show that

$$a_E(2) = \begin{cases} 1 & \text{for } E : y^2 = x^3-75x-506 \text{ and } E : y^2 = x^3-3x-322, \\ 0 & \text{otherwise,} \end{cases}$$

and with the aid of SAGE, one also has that

$$N_E = \begin{cases} 126 & \text{for } E : y^2 = x^3-75x-506, \\ 45 & \text{for } E : y^2 = x^3-3x-322, \\ 180 & \text{for } E : y^2 = x^3-12x-11, \\ 72 & \text{for } E : y^2 = x^3-39x-70, \end{cases}$$

and the dimensions of the space $S_2^{new}(N_E)$ of newforms of weight 2 for $\Gamma_0(N_E)$ are given by

$$\dim(S_2^{new}(N_E)) = \begin{cases} 2 & \text{for } E : y^2 = x^3-75x-506, \\ 1 & \text{otherwise.} \end{cases}$$

On the other hand, appealing to [5, Corollary 3.1], one can check that

$$\sum_{n=1}^{\infty}\left(\frac{-3}{n}\right)a_\ell(n)q^n \in \begin{cases} S_2^{new}(126) & \text{for } \ell = 14, \\ S_2^{new}(45) & \text{for } \ell = 15, \\ S_2^{new}(180) & \text{for } \ell = 20, \\ S_2^{new}(72) & \text{for } \ell = 24. \end{cases}$$

Therefore, for each pair

$$(E,\ell)\in\big\{(y^2=x^3-3x-322,15),\ (y^2=x^3-12x-11,20),\ (y^2=x^3-39x-70,24)\big\},$$

both $g_E(z)$ and $\sum_{n=1}^{\infty}\left(\frac{-3}{n}\right)a_\ell(n)q^n$ lie in the same one-dimensional vector space with constant terms 1, and thus, one has that for any prime $p\geq 3$, $\left(\frac{-3}{p}\right)a_\ell(p)=a_{g_E}(p)=-\sum_{x=0}^{p-1}\left(\frac{f_E(x)}{p}\right)$. By [10], Sturm's theorem states that the order of vanishing at $i\infty$ of a holomorphic modular form of weight k for $\Gamma_0(N)$ is bounded by $[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]\frac{k}{12}$. Now, for the case $(E,\ell)=(y^2=x^3-75x-506,14)$, one can check that $a_{g_E}(p)$ and $\left(\frac{-3}{p}\right)a_{14}(p)$ agree on primes p up to 47, and thus, the Fourier coefficients of $g_E(z)$ and $\sum_{n=1}^{\infty}\left(\frac{-3}{n}\right)a_{14}(n)q^n$ agree on n up to 48 (the Sturm's bound for $\Gamma_0(126)$), since they are both newforms whose Fourier coefficients are completely determined by prime places. As a result, one can conclude that $g_E(z)=\sum_{n=1}^{\infty}\left(\frac{-3}{n}\right)a_{14}(n)q^n$ by Sturm's theorem, and $\left(\frac{-3}{p}\right)a_{14}(p)=a_{g_E}(p)=-\sum_{x=0}^{p-1}\left(\frac{x^3-75x-506}{p}\right)$ for any prime $p\geq 3$.

The remaining equalities $\left(\frac{-1}{p}\right)a_{20}(p)=a_{80}(p)$ and $\left(\frac{-1}{p}\right)a_{24}(p)=a_{48}(p)$ follow from similar reasoning as follows. From [5, Corollary 3.1] one finds that $\sum_{n=1}^{\infty}\left(\frac{-1}{n}\right)a_{20}(n)q^n$ and $\sum_{n=1}^{\infty}\left(\frac{-1}{n}\right)a_{24}(n)q^n$ are newforms with trivial Nebentypus of weight 2 for $\Gamma_0(80)$ and $\Gamma_0(48)$, respectively, whose Sturm bounds are 24 and 8, respectively. Verifying that the Fourier coefficients of $\sum_{n=1}^{\infty}\left(\frac{-1}{n}\right)a_{20}(n)q^n$ and $\sum_{n=1}^{\infty}a_{80}(n)q^n$ hold for prime places up to 23, and the Fourier coefficients of $\sum_{n=1}^{\infty}\left(\frac{-1}{n}\right)a_{24}(n)q^n$ and $\sum_{n=1}^{\infty}a_{48}(n)q^n$ hold for prime places up to 7, and using Sturm's theorem one concludes that they are identical. The proof is now complete.

Proof of Theorem 1.1. From Lemma 2.1 and [16, (2.5) and Theorem 2.8] we deduce that

$$\begin{aligned}p+1-\left(\frac{p}{3}\right)a_{20}(p)&=p+1+\left(\frac{p}{3}\right)a_{80}(p)=p+1+\sum_{x=0}^{p-1}\left(\frac{x^3-12x-11}{p}\right)\\&=\begin{cases}4N_p(-4,4)-\dfrac{3p-1}{2}-2\delta(p) & \text{if } p\equiv 7 \pmod{12},\\ -4N_p(-4,4)+\dfrac{7p+3}{2}+2\delta(p) & \text{if } p\equiv 11 \pmod{12}.\end{cases}\end{aligned}$$

Hence the result follows.

Proof of Theorem 1.2. Set $\mathbb{Z}_p=\{0,1,\dots,p-1\}$, $\mathbb{Z}_p^*=\{1,2,\dots,p-1\}$ and

$$\delta_1=\begin{cases}1 & \text{if } x^4\equiv -c \pmod{p} \text{ is insolvable},\\ 0 & \text{if } x^4\equiv -c \pmod{p} \text{ is solvable}.\end{cases}$$

From [15, Lemma 5.1 and Remark 5.1], $x^4+bx+c\equiv 0 \pmod{p}$ is solvable when $p\nmid b$ and $p\mid(-27b^4+256c^3)$. Thus,

$$\begin{aligned}N_p(c)&=|\{b\in\mathbb{Z}_p:\ x^4+bx+c\equiv 0 \pmod{p} \text{ is solvable}\}|\\&=p-|\{b\in\mathbb{Z}_p:\ x^4+bx+c\equiv 0 \pmod{p} \text{ is insolvable}\}|\\&=p-\delta_1-|\{b\in\mathbb{Z}_p:\ p\nmid b \text{ and } x^4+bx+c\equiv 0 \pmod{p} \text{ is insolvable}\}|\\&=p-\delta_1-|\{b\in\mathbb{Z}_p:\ p\nmid b(-27b^4+256c^3)\\&\qquad\qquad \text{and } x^4+bx+c\equiv 0 \pmod{p} \text{ is insolvable}\}|.\end{aligned}$$

By [15, Theorem 5.8], for $p \nmid b(-27b^4+256c^3)$, the congruence $x^4+bx+c\equiv 0 \pmod p$ is insolvable if and only if there exists a quadratic non-residue y modulo p satisfying $y^3-4cy-b^2\equiv 0 \pmod p$. Hence, from the above we derive that

$$\begin{aligned} N_p(c) &= p-\delta_1-\big|\{b\in\mathbb{Z}_p:\ p\nmid b(-27b^4+256c^3),\ b^2\equiv y^3-4cy \pmod p \\ &\qquad\qquad \text{for some quadratic non-residue } y \text{ of } p\}\big| \\ &= p-\delta_1-\big|\{b\in\mathbb{Z}_p^*:\ b^2\equiv y^3-4cy \pmod p \text{ for some quadratic non-residue } y \text{ of } p\}\big| \\ &\quad +\big|\{b\in\mathbb{Z}_p^*:\ p\mid(-27b^4+256c^3),\ b^2\equiv y^3-4cy \pmod p \\ &\qquad\qquad \text{for some quadratic non-residue } y \text{ of } p\}\big|. \end{aligned}$$

When $p\nmid b$ and $p\mid(-27b^4+256c^3)$, it is clear that $\left(\frac{3c}{p}\right)=1$ and

$$y^3-4cy-b^2\equiv\Big(y-\frac{3b^2}{4c}\Big)\Big(y+\frac{3b^2}{8c}\Big)^2 \pmod p.$$

Since $\left(\frac{3b^2\cdot 4c}{p}\right)=\left(\frac{3c}{p}\right)=1$ and $\left(\frac{-3b^2\cdot 8c}{p}\right)=\left(\frac{-2}{p}\right)$, we see that

$$\begin{aligned} &\big|\{b\in\mathbb{Z}_p^*:\ p\mid(-27b^4+256c^3),\ b^2\equiv y^3-4cy \pmod p \\ &\qquad \text{for some quadratic non-residue } y \text{ of } p\}\big| \\ &=\Big|\Big\{b\in\mathbb{Z}_p^*:\ p\mid(-27b^4+256c^3),\ \Big(\frac{-2}{p}\Big)=-1\Big\}\Big| \\ &=\big|\{b\in\mathbb{Z}_p^*:\ (4c/b)^4\equiv 27c \pmod p,\ p\equiv 5,7 \pmod 8\}\big|=2\delta. \end{aligned}$$

Hence,

$$\begin{aligned} N_p(c)=p-\delta_1+2\delta-\Big|\Big\{b\in\mathbb{Z}_p^*:\ &y^3-4cy-b^2\equiv 0 \pmod p \\ &\text{for some } y\in\mathbb{Z} \text{ with } \Big(\frac{y}{p}\Big)=-1\Big\}\Big|. \end{aligned} \tag{2.1}$$

If $\left(\frac{y}{p}\right)=-1$, then $y(y^2-4c)\equiv b^2 \pmod p$ for some $b\in\mathbb{Z}_p^*$ if and only if $\left(\frac{y^2-4c}{p}\right)=-1$. If $y^3-4cy\equiv x^3-4cx \pmod p$ and $x\not\equiv y \pmod p$, then $x^2+xy+y^2\equiv 4c \pmod p$ and so $(2x+y)^2\equiv 16c-3y^2 \pmod p$. Now suppose $y\in\mathbb{Z}_p$, $\left(\frac{y}{p}\right)=-1$ and $\left(\frac{y^2-4c}{p}\right)=-1$. Then $y(y^2-4c)\equiv b^2 \pmod p$ for two values $b\in\mathbb{Z}_p^*$. If $3y^2\equiv 16c \pmod p$, then $\left(\frac{y^2-4c}{p}\right)=\left(\frac{y^2/4}{p}\right)=1$. This contradicts the assumption. If $\left(\frac{16c-3y^2}{p}\right)=-1$, then $(2x+y)^2\equiv 16c-3y^2 \pmod p$ is insolvable and so $y^3-4cy\not\equiv x^3-4cx \pmod p$ for any $x\not\equiv y \pmod p$. If $\left(\frac{16c-3y^2}{p}\right)=1$, from the above there exist two distinct numbers $y_1,y_2\in\mathbb{Z}_p$ such that $(2y_i+y)^2\equiv 16c-3y^2 \pmod p$ and so $y^3-4cy-(y_i^3-4cy_i)=\frac14(y-y_i)((2y_i+y)^2+3y^2-16c)\equiv 0 \pmod p$ for $i=1,2$. If $y\notin\{y_1,y_2\}$, then the congruence $x^3-4cx-b^2\equiv 0 \pmod p$ has three distinct solutions $x\equiv y,y_1,y_2 \pmod p$ and so $yy_1y_2\equiv b^2 \pmod p$. Since $\left(\frac{y}{p}\right)=-1$, we see that $\left(\frac{y_1y_2}{p}\right)=-1$ and so there is a unique $i\in\{1,2\}$ such that $\left(\frac{y_i}{p}\right)=-1$ and $\left(\frac{y_i^2-4c}{p}\right)=-1$. If $y\in\{y_1,y_2\}$, then $(2y+y)^2\equiv 16c-3y^2 \pmod p$ and so $3y^2\equiv 4c \pmod p$. Hence, $\left(\frac{y^2-4c}{p}\right)=\left(\frac{-2y^2}{p}\right)=\left(\frac{-2}{p}\right)$. Therefore, $\left(\frac{3c}{p}\right)=1$ and $\left(\frac{-2}{p}\right)=-1$. Note that $2y_1+y\equiv-(2y_2+y) \pmod p$. For $y=y_1$

we have $y_2 \equiv -2y \pmod p$ and so $\left(\frac{y_2}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{y}{p}\right) = -1 \cdot (-1) = 1$. By symmetry, for $y = y_2$ we have $\left(\frac{y_1}{p}\right) = 1$. Since $-4 = (1+\sqrt{-1})^4$, we see that the number of $y \in \mathbb{Z}_p$ such that $\left(\frac{y}{p}\right) = -1$ and $y^2 \equiv \frac{4}{3}c = \frac{(1+\sqrt{-1})^4}{3^4}(-27c) \pmod p$ is δ given in Theorem 1.2. This implies that

$$\left|\left\{y \in \mathbb{Z}_p :\ y \in \{y_1, y_2\},\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1,\ \left(\frac{16c-3y^2}{p}\right) = 1\right\}\right| = \delta.$$

Therefore,

$$\begin{aligned}
&\left|\left\{b \in \mathbb{Z}_p^* :\ y^3 - 4cy - b^2 \equiv 0 \pmod p \text{ for some } y \in \mathbb{Z} \text{ with } \left(\frac{y}{p}\right) = -1\right\}\right| \\
&= 2\left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = \left(\frac{16c-3y^2}{p}\right) = -1\right\}\right| \\
&\quad + 2\left|\left\{y \in \mathbb{Z}_p :\ y \in \{y_1, y_2\},\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1,\ \left(\frac{16c-3y^2}{p}\right) = 1\right\}\right| \\
&\quad + \left|\left\{y \in \mathbb{Z}_p :\ y \notin \{y_1, y_2\},\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1,\ \left(\frac{16c-3y^2}{p}\right) = 1\right\}\right| \\
&= 2\left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = \left(\frac{16c-3y^2}{p}\right) = -1\right\}\right| \\
&\quad + \left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1,\ \left(\frac{16c-3y^2}{p}\right) = 1\right\}\right| + \delta \\
&= \left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = \left(\frac{16c-3y^2}{p}\right) = -1\right\}\right| \\
&\quad + \left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1\right\}\right| + \delta.
\end{aligned}$$

This together with (2.1) yields

$$\begin{aligned}
N_p(c) = p - \delta_1 + \delta &- \left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1\right\}\right| \\
&- \left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = \left(\frac{16c-3y^2}{p}\right) = -1\right\}\right|.
\end{aligned} \tag{2.2}$$

For $p \equiv 1 \pmod 4$ it is well known that $x^2 \equiv -1 \pmod p$ is solvable and so $x^4 \equiv -4 = (1+\sqrt{-1})^4 \pmod p$ is solvable. Now, it is clear that

$$\begin{aligned}
&\sum_{y \in \mathbb{Z}_p} \left(1 - \left(\frac{y}{p}\right)\right)\left(1 - \left(\frac{y^2-4c}{p}\right)\right) \\
&= 4\left|\left\{y \in \mathbb{Z}_p :\ \left(\frac{y}{p}\right) = \left(\frac{y^2-4c}{p}\right) = -1\right\}\right| + 1 - \left(\frac{-4c}{p}\right) + \delta_2,
\end{aligned}$$

where

$$\delta_2 = \begin{cases} 2 & \text{if } 4 \mid p-3 \text{ and } \left(\frac{c}{p}\right) = 1, \\ 4 & \text{if } 4 \mid p-1,\ \left(\frac{c}{p}\right) = 1 \text{ and } -c \text{ is not a quartic residue of } p, \\ 0 & \text{otherwise.} \end{cases}$$

If $y^2 \equiv 4c \pmod p$, then $\left(\frac{16c-3y^2}{p}\right) = \left(\frac{4c}{p}\right) = 1$. If $3y^2 \equiv 16c \pmod p$, then $\left(\frac{y^2-4c}{p}\right) = \left(\frac{4c/3}{p}\right) = 1$. Thus,

$$\begin{aligned}
&\sum_{y\in\mathbb{Z}_p} \Big(1-\Big(\frac{y}{p}\Big)\Big)\Big(1-\Big(\frac{y^2-4c}{p}\Big)\Big)\Big(1-\Big(\frac{16c-3y^2}{p}\Big)\Big)\\
&= 8\Big|\Big\{y\in\mathbb{Z}_p:\ \Big(\frac{y}{p}\Big)=\Big(\frac{y^2-4c}{p}\Big)=\Big(\frac{16c-3y^2}{p}\Big)=-1\Big\}\Big|\\
&\quad + \Big(1-\Big(\frac{-4c}{p}\Big)\Big)\Big(1-\Big(\frac{16c}{p}\Big)\Big),\\
&= 8\Big|\Big\{y\in\mathbb{Z}_p:\ \Big(\frac{y}{p}\Big)=\Big(\frac{y^2-4c}{p}\Big)=\Big(\frac{16c-3y^2}{p}\Big)=-1\Big\}\Big| + (1+(-1)^{\frac{p-1}{2}})\Big(1-\Big(\frac{c}{p}\Big)\Big).
\end{aligned}$$

Now, from (2.2) we deduce that

$$\begin{aligned}
N_p(c) &= p-\delta_1+\delta+\frac{1}{4}\Big(1-\Big(\frac{-c}{p}\Big)+\delta_2\Big)-\frac{1}{4}\sum_{y\in\mathbb{Z}_p}\Big(1-\Big(\frac{y}{p}\Big)\Big)\Big(1-\Big(\frac{y^2-4c}{p}\Big)\Big)\\
&\quad+\frac{1}{8}\Big(1+(-1)^{\frac{p-1}{2}}\Big)\Big(1-\Big(\frac{c}{p}\Big)\Big)\\
&\quad-\frac{1}{8}\sum_{y\in\mathbb{Z}_p}\Big(1-\Big(\frac{y}{p}\Big)\Big)\Big(1-\Big(\frac{y^2-4c}{p}\Big)\Big)\Big(1-\Big(\frac{16c-3y^2}{p}\Big)\Big)\\
&= p+\delta-\delta_1+\frac{1}{4}\delta_2+\frac{1}{8}\Big(3+(-1)^{\frac{p-1}{2}}\Big)\Big(1-\Big(\frac{-c}{p}\Big)\Big)\\
&\quad-\frac{1}{8}\sum_{y\in\mathbb{Z}_p}\Big(1-\Big(\frac{y}{p}\Big)\Big)\Big(1-\Big(\frac{y^2-4c}{p}\Big)\Big)\Big(3-\Big(\frac{16c-3y^2}{p}\Big)\Big).
\end{aligned}$$

It is easy to see that $-\delta_1+\frac{\delta_2}{4}+\frac{1}{8}(3+(-1)^{\frac{p-1}{2}})\left(1-\left(\frac{-c}{p}\right)\right)=0$. Thus,

$$N_p(c) = p+\delta-\frac{1}{8}\sum_{y\in\mathbb{Z}_p}\Big(1-\Big(\frac{y}{p}\Big)\Big)\Big(1-\Big(\frac{y^2-4c}{p}\Big)\Big)\Big(3-\Big(\frac{16c-3y^2}{p}\Big)\Big). \tag{2.3}$$

By [6, Theorem 2.1.2], we have $\sum_{x=0}^{p-1}\left(\frac{x^2+mx+n}{p}\right) = -1$ for $m,n\in\mathbb{Z}$ with $m^2-4n \not\equiv 0 \pmod p$. Thus,

$$\sum_{y\in\mathbb{Z}_p}\Big(\frac{y^2-4c}{p}\Big)=-1,\ \sum_{y\in\mathbb{Z}_p}\Big(\frac{16c-3y^2}{p}\Big)=\Big(\frac{-3}{p}\Big)\sum_{y\in\mathbb{Z}_p}\Big(\frac{y^2-16c/3}{p}\Big)=-\Big(\frac{-3}{p}\Big). \tag{2.4}$$

By [6, ex.14, p.207],

$$\sum_{y\in\mathbb{Z}_p}\Big(\frac{y^2-4c}{p}\Big)\Big(\frac{y^2-16c/3}{p}\Big)=-1+\Big(\frac{-4c}{p}\Big)\sum_{n\in\mathbb{Z}_p}\Big(\frac{n(n+1)(n+\frac{4}{3})}{p}\Big).$$

Therefore,

$$\begin{aligned}
&\sum_{y\in\mathbb{Z}_p}\left(\frac{y^2-4c}{p}\right)\left(\frac{y^2-16c/3}{p}\right)\\
&= -1+\left(\frac{-c}{p}\right)\sum_{n\in\mathbb{Z}_p}\left(\frac{(n-\frac79)(n+\frac29)(n+\frac59)}{p}\right) = -1+\left(\frac{-c}{p}\right)\sum_{n\in\mathbb{Z}_p}\left(\frac{n^3-\frac{13}{27}n-\frac{70}{729}}{p}\right)\\
&= -1+\left(\frac{-c}{p}\right)\sum_{x\in\mathbb{Z}_p}\left(\frac{(\frac{x}{9})^3-\frac{13}{27}\cdot\frac{x}{9}-\frac{70}{729}}{p}\right)
\end{aligned}$$

and so

$$\sum_{y\in\mathbb{Z}_p}\left(\frac{y^2-4c}{p}\right)\left(\frac{y^2-16c/3}{p}\right) = -1+\left(\frac{-c}{p}\right)\sum_{x\in\mathbb{Z}_p}\left(\frac{x^3-39x-70}{p}\right). \tag{2.5}$$

Since $\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)=0$, from (2.4) and (2.5) we deduce that

$$\begin{aligned}
&\sum_{y\in\mathbb{Z}_p}\Big(1-\left(\frac{y}{p}\right)\Big)\Big(1-\left(\frac{y^2-4c}{p}\right)\Big)\Big(3-\left(\frac{16c-3y^2}{p}\right)\Big)\\
&= 3\sum_{y\in\mathbb{Z}_p}1-3\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)-3\sum_{y\in\mathbb{Z}_p}\left(\frac{y^2-4c}{p}\right)-\left(\frac{-3}{p}\right)\sum_{y\in\mathbb{Z}_p}\left(\frac{y^2-16c/3}{p}\right)\\
&\quad+\left(\frac{-3}{p}\right)\sum_{y\in\mathbb{Z}_p}\left(\frac{y^2-4c}{p}\right)\left(\frac{y^2-16c/3}{p}\right)\\
&\quad+\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)\Big(3\left(\frac{y^2-4c}{p}\right)+\left(\frac{16c-3y^2}{p}\right)\Big)-\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)\left(\frac{y^2-4c}{p}\right)\left(\frac{16c-3y^2}{p}\right)\\
&= 3p+3+\left(\frac{3c}{p}\right)\sum_{x\in\mathbb{Z}_p}\left(\frac{x^3-39x-70}{p}\right)\\
&\quad+\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)\Big(3\left(\frac{y^2-4c}{p}\right)+\left(\frac{16c-3y^2}{p}\right)-\left(\frac{y^2-4c}{p}\right)\left(\frac{16c-3y^2}{p}\right)\Big).
\end{aligned}$$

This together with (2.3) gives

$$\begin{aligned}
N_p(c) = p+\delta-\frac18\Big(&3p+3+\left(\frac{3c}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-39x-70}{p}\right)\\
&+\sum_{y=0}^{p-1}\left(\frac{y}{p}\right)\Big(3\left(\frac{y^2-4c}{p}\right)+\left(\frac{16c-3y^2}{p}\right)-\left(\frac{y^2-4c}{p}\right)\left(\frac{16c-3y^2}{p}\right)\Big)\Big).
\end{aligned}$$

Applying Lemma 2.1 and the fact that $\left(\frac{y}{p}\right)+\left(\frac{p-y}{p}\right)=(1+(-1)^{\frac{p-1}{2}})\left(\frac{y}{p}\right)$ we obtain

$$\begin{aligned} N_p(c) &= p+\delta-\frac{1}{8}\Big(3p+3-\Big(\frac{-c}{p}\Big)a_{24}(p)+\big(1+(-1)^{\frac{p-1}{2}}\big) \\ &\quad\times\Big(\sum_{y=1}^{(p-1)/2}\Big(\frac{y}{p}\Big)\Big(3\Big(\frac{y^2-4c}{p}\Big)+\Big(\frac{16c-3y^2}{p}\Big)-\Big(\frac{y^2-4c}{p}\Big)\Big(\frac{16c-3y^2}{p}\Big)\Big)\Big)\Big) \\ &= \delta+\frac{1}{8}\Big(5p-3+\Big(\frac{-c}{p}\Big)a_{24}(p)-\big(1+(-1)^{\frac{p-1}{2}}\big) \\ &\quad\times\Big(\sum_{y=1}^{(p-1)/2}\Big(\frac{y}{p}\Big)\Big(3\Big(\frac{y^2-4c}{p}\Big)+\Big(\frac{16c-3y^2}{p}\Big)-\Big(\frac{y^2-4c}{p}\Big)\Big(\frac{16c-3y^2}{p}\Big)\Big)\Big)\Big). \end{aligned}$$

For $p\equiv 3 \pmod 4$ we see that

$$\delta=\begin{cases} 1 & \text{if } 8\mid p-7 \text{ and } \Big(\frac{3c}{p}\Big)=1, \\ 0 & \text{otherwise} \end{cases}$$

and hence (1.3) follows. The proof is now complete.

Remark 2.1. Let p be a prime such that $p\equiv 1 \pmod 4$ and so $p=a^2+b^2$ with $a,b\in\mathbb{Z}$ and $a\equiv 3 \pmod 4$. Let m be an integer not divisible by p. From [6, Theorem 6.2.1] we deduce that

$$\sum_{x=1}^{(p-1)/2}\Big(\frac{x}{p}\Big)\Big(\frac{x^2+m}{p}\Big)=\begin{cases} \pm a & \text{if } m^{\frac{p-1}{4}}\equiv\pm 1 \pmod p, \\ \pm b & \text{if } m^{\frac{p-1}{4}}\equiv\pm\frac{b}{a} \pmod p. \end{cases}$$

Thus, the sums $\sum_{x=1}^{(p-1)/2}\big(\frac{x}{p}\big)\big(\frac{x^2-4c}{p}\big)$ and $\sum_{x=1}^{(p-1)/2}\big(\frac{x}{p}\big)\big(\frac{16c-3x^2}{p}\big)$ in Theorem 1.2 can be evaluated for $p\equiv 1 \pmod 4$.

3. Proof of Theorem 1.3

The purpose of this section is to prove the congruence for $a_{24}(p)$ modulo 16, where $p>3$ is a prime. From now on we use $[x]$ to denote the greatest integer not exceeding x, and let $\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$ and $\mathbb{Z}^4=\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. For $n=0,1,2,\dots$ let

$$\begin{aligned} r_2(n)&=\big|\{(x,y)\in\mathbb{Z}^2 \mid n=x^2+y^2\}\big|, \\ t_2(n)&=\Big|\Big\{(x,y)\in\mathbb{Z}^2 \;\Big|\; n=\frac{x(x+1)}{2}+\frac{y(y+1)}{2}\Big\}\Big|. \end{aligned}$$

For convenience we also define $r_2(n)=t_2(n)=0$ for $n\notin\{0,1,2,\dots\}$. It is well known that for $n=1,2,3,\dots$,

$$r_2(n)=4\sum_{d\mid n,2\nmid d}(-1)^{\frac{d-1}{2}},\quad t_2(n)=4\sum_{d\mid 4n+1}(-1)^{\frac{d-1}{2}}. \tag{3.1}$$

See for example [14, p.27] and [20, Theorem 4.3(iii)].

Lemma 3.1. *For $n = 1, 2, 3, \dots$ we have*

$$r_2(n) \equiv \begin{cases} 4 \pmod 8 & \text{if } n = m^2 \text{ or } 2m^2 \text{ for } m \in \mathbb{Z}, \\ 0 \pmod 8 & \text{otherwise,} \end{cases} \tag{3.2}$$

and for $n = 0, 1, 2, \dots$ we have

$$t_2(n) \equiv \begin{cases} 4 \pmod 8 & \text{if } 4n+1 \text{ is a square,} \\ 0 \pmod 8 & \text{if } 4n+1 \text{ is not a square.} \end{cases} \tag{3.3}$$

Proof. It is clear that $r_2(0) = 1$ and $t_2(0) = 4$. Now suppose that n is a positive integer and $n = 2^\alpha n_0 (2 \nmid n_0)$. From (3.1) we see that

$$\begin{aligned} r_2(n) =& r_2(n_0) = 4 \sum_{d \mid n_0} (-1)^{\frac{d-1}{2}} = 4 \sum_{\substack{d \mid n_0 \\ d^2 < n_0}} \Big((-1)^{\frac{d-1}{2}} + (-1)^{\frac{1}{2}(\frac{n_0}{d} - 1)} \Big) + 4 \sum_{\substack{d \mid n_0 \\ d^2 = n_0}} (-1)^{\frac{d-1}{2}} \\ &\equiv \begin{cases} 4 \pmod 8 & \text{if } n_0 \text{ is a square,} \\ 0 \pmod 8 & \text{if } n_0 \text{ is not a square,} \end{cases} \end{aligned}$$

which yields (3.2). On the other hand, from (3.1) we deduce that

$$\begin{aligned} t_2(n) &= 4 \sum_{\substack{d \mid 4n+1 \\ d^2 < 4n+1}} \Big((-1)^{\frac{d-1}{2}} + (-1)^{\frac{1}{2}(\frac{4n+1}{d} - 1)} \Big) + 4 \sum_{\substack{d \mid 4n+1 \\ d^2 = 4n+1}} (-1)^{\frac{d-1}{2}} \\ &\equiv \begin{cases} 0 \pmod 8 & \text{if } 4n+1 \text{ is not a square,} \\ 4 \pmod 8 & \text{if } 4n+1 \text{ is a square.} \end{cases} \end{aligned}$$

Thus, the lemma is proved.

Proof of Theorem 1.3. From Lemma 2.1, $a_{48}(p) = (-1)^{\frac{p-1}{2}} a_{24}(p)$. Since $x^3 - x^{-1} \equiv b \pmod p$ implies that $(p-x)^3 - (p-x)^{-1} \equiv p - b \pmod p$, and $x^3 - x^{-1} \equiv 0 \pmod p$ is clearly solvable, we see that $N_p(-1)$ is odd. Now, taking $c = -1$ in Theorem 1.2 we derive that

$$a_{24}(p) = \begin{cases} 8N_p(-1) - (5p+5) \equiv 8 - (p+1) \pmod{16} & \text{if } 24 \mid p - 7, \\ 8N_p(-1) - (5p-3) \equiv 8 - (5p-3) \equiv -(p+1) \pmod{16} & \text{otherwise.} \end{cases}$$

This proves the theorem in the case $p \equiv 3 \pmod 4$.

Now assume that $p \equiv 1 \pmod 4$. By [18, Theorem 4.15], $t(2, 2, 3, 3; (p-5)/4) = 2(p + 1 - a_{24}(p))$. Suppose $p = 12k + 1 \equiv 1 \pmod{12}$. Then

$$\begin{aligned} &t(2, 2, 3, 3; (p-5)/4) \\ &= \Big| \Big\{ (x, y, z, w) \in \mathbb{Z}^4 : \ 3k - 1 = 2\Big(\frac{x(x+1)}{2} + \frac{y(y+1)}{2} \Big) + 3\Big(\frac{z(z+1)}{2} + \frac{w(w+1)}{2} \Big) \Big\} \Big| \\ &= \sum_{n=0}^{[(3k-1)/2]} t_2(n) t_2\Big(\frac{3k - 1 - 2n}{3} \Big) = \sum_{s=0}^{[(k-1)/2]} t_2(3s+1) t_2(k - 1 - 2s). \end{aligned}$$

Since $4(3s+1) + 1 \equiv 2 \pmod 3$ we see that $4(3s+1)+1$ is not a square. By Lemma 3.1, $8 \mid t_2(3s+1)$ and $4 \mid t_2(k-1-2s)$. Hence

$$2(p + 1 - a_{24}(p)) = t(2, 2, 3, 3; (p-5)/4) = \sum_{s=0}^{[(k-1)/2]} t_2(3s+1) t_2(k-1-2s) \equiv 0 \pmod{32}.$$

It then follows that $a_{24}(p) \equiv p+1 \pmod{16}$.

Now assume that $p \equiv 5 \pmod{12}$. By [3, Theorem 1.12], $2(p+1+a_{24}(p)) = N(1,1,6,6;p)$. Also,

$$N(1,1,6,6;p) = r_2(0)r_2(p) + \sum_{n=1}^{(p-5)/6} r_2(n)r_2(p-6n) = 8 + \sum_{n=1}^{(p-5)/6} r_2(n)r_2(p-6n).$$

Since $p-6n \equiv 5 \pmod 6$ we see that $p-6n$ is not represented by x^2 and $2x^2$. Thus, $8 \mid r_2(p-6n)$, $4 \mid r_2(n)$ and so $32 \mid r_2(n)r_2(p-6n)$ for $n = 1, 2, \ldots, \frac{p-5}{6}$ by Lemma 3.1. It then follows that

$$2(p+1+a_{24}(p)) = N(1,1,6,6;p) \equiv 8 \pmod{32},$$

which yields $a_{24}(p) \equiv 4-(p+1) \pmod{16}$. This completes the proof.

The Eisenstein series of weight 2 is given by

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma(n)e^{2\pi inz}, \tag{3.4}$$

where $\sigma(n)$ is the sum of positive divisors of n. For any prime $p>3$, $p+1+a_{24}(p)$ can be viewed as the p-th coefficient of $\eta(2z)\eta(4z)\eta(6z)\ \eta(12z) - \frac{1}{24}E_2(z)$, and $\eta(2z)\eta(4z)\eta(6z)\eta(12z)$ and $E_2(z)$ are constituents of the space of holomorphic modular forms of weight 2 and level $\Gamma_0(24)$ with trivial Nebentypus, so one may speculate that $p+1+a_{24}(p)$ might be the p-th Fourier coefficient of another holomorphic modular form. In what follows, we list all the eta quotients that are holomorphic modular forms of weight 2 and level $\Gamma_0(24)$ with trivial Nebentypus and confirm this speculation.

Proposition 3.1. *Let*

$$f_1(z) = \frac{\eta(2z)^3\eta(3z)^6\eta(8z)^2\eta(12z)^{15}}{\eta(z)^2\eta(4z)^5\eta(6z)^9\eta(24z)^6}, \quad f_2(z) = \frac{\eta(2z)^2\eta(3z)^6\eta(8z)^4\eta(12z)^8}{\eta(z)^2\eta(4z)^4\eta(6z)^6\eta(24z)^4},$$
$$f_3(z) = \frac{\eta(3z)^6\eta(4z)^5\eta(12z)^5}{\eta(z)^2\eta(2z)\eta(6z)^5\eta(8z)^2\eta(24z)^2}, \quad f_4(z) = \frac{\eta(2z)\eta(3z)^6\eta(8z)\eta(12z)^6}{\eta(z)^2\eta(4z)^2\eta(6z)^3\eta(24z)^3},$$
$$f_5(z) = \frac{\eta(2z)^5\eta(3z)^2\eta(8z)\eta(12z)^{18}}{\eta(z)^2\eta(4z)^4\eta(6z)^9\eta(24z)^7}, \quad f_6(z) = \frac{\eta(2z)^4\eta(3z)^2\eta(8z)^3\eta(12z)^{11}}{\eta(z)^2\eta(4z)^3\eta(6z)^6\eta(24z)^5},$$
$$f_7(z) = \frac{\eta(2z)\eta(3z)^2\eta(4z)^6\eta(12z)^8}{\eta(z)^2\eta(6z)^5\eta(8z)^3\eta(24z)^3}, \quad f_8(z) = \frac{\eta(2z)^3\eta(3z)^2\eta(12z)^9}{\eta(z)^2\eta(4z)\eta(6z)^3\eta(24z)^4},$$
$$f_9(z) = \frac{\eta(2z)^5\eta(3z)^6\eta(8z)\eta(12z)^8}{\eta(z)^2\eta(4z)^4\eta(6z)^7\eta(24z)^3}, \quad f_{10}(z) = \frac{\eta(2z)^7\eta(8z)^2\eta(12z)^{13}}{\eta(z)^2\eta(3z)^2\eta(4z)^7\eta(6z)\eta(24z)^6},$$
$$f_{11}(z) = \frac{\eta(2z)^6\eta(6z)^2\eta(8z)^4\eta(12z)^6}{\eta(z)^2\eta(3z)^2\eta(4z)^6\eta(24z)^4}, \quad f_{12}(z) = \frac{\eta(2z)^3\eta(4z)^3\eta(6z)^3\eta(12z)^3}{\eta(z)^2\eta(3z)^2\eta(8z)^2\eta(24z)^2},$$
$$f_{13}(z) = \frac{\eta(2z)^5\eta(6z)^5\eta(8z)\eta(12z)^4}{\eta(z)^2\eta(3z)^2\eta(4z)^4\eta(24z)^3}, \quad f_{14}(z) = \frac{\eta(2z)^7\eta(3z)^2\eta(12z)^{11}}{\eta(z)^2\eta(4z)^3\eta(6z)^7\eta(24z)^4},$$
$$f_{15}(z) = \frac{\eta(2z)^9\eta(6z)\eta(8z)\eta(12z)^6}{\eta(z)^2\eta(3z)^2\eta(4z)^6\eta(24z)^3}.$$

Then one has that

$$\begin{aligned}
f_1(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{48}E_2(2z) + \frac{5}{72}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad - \frac{7}{48}E_2(6z) - \frac{1}{24}E_2(8z) + \frac{1}{144}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_2(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{24}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad - \frac{5}{72}E_2(6z) - \frac{1}{24}E_2(8z) - \frac{1}{48}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_3(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) - \frac{1}{16}E_2(2z) - \frac{1}{24}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad + \frac{23}{144}E_2(6z) - \frac{1}{24}E_2(8z) - \frac{5}{48}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_4(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) - \frac{1}{48}E_2(2z) + \frac{1}{72}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad + \frac{1}{144}E_2(6z) - \frac{1}{24}E_2(8z) - \frac{7}{144}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_5(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{16}E_2(2z) + \frac{5}{72}E_2(3z) - \frac{1}{48}E_2(4z) \\
&\quad - \frac{23}{144}E_2(6z) + \frac{5}{144}E_2(12z) + \frac{1}{18}E_2(24z), \\
f_6(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{24}E_2(2z) + \frac{1}{24}E_2(3z) - \frac{1}{12}E_2(6z) \\
&\quad - \frac{1}{48}E_2(8z) + \frac{1}{16}E_2(24z), \\
f_7(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) - \frac{1}{48}E_2(2z) - \frac{1}{24}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad + \frac{7}{48}E_2(6z) - \frac{1}{12}E_2(8z) - \frac{5}{48}E_2(12z) + \frac{1}{12}E_2(24z), \\
f_8(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{48}E_2(2z) + \frac{1}{72}E_2(3z) + \frac{1}{48}E_2(4z) \\
&\quad - \frac{1}{144}E_2(6z) - \frac{1}{24}E_2(8z) - \frac{5}{144}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_9(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{16}E_2(2z) + \frac{1}{8}E_2(3z) + \frac{1}{16}E_2(4z) \\
&\quad - \frac{43}{144}E_2(6z) - \frac{1}{24}E_2(8z) + \frac{1}{16}E_2(12z) + \frac{5}{72}E_2(24z), \\
f_{10}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{5}{48}E_2(2z) + \frac{5}{72}E_2(3z) - \frac{3}{16}E_2(4z) \\
&\quad - \frac{1}{16}E_2(6z) + \frac{1}{24}E_2(8z) + \frac{5}{144}E_2(12z) + \frac{1}{24}E_2(24z), \\
f_{11}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{12}E_2(2z) + \frac{1}{24}E_2(3z) - \frac{7}{48}E_2(4z) \\
&\quad - \frac{1}{24}E_2(6z) + \frac{1}{24}E_2(8z) + \frac{1}{48}E_2(12z) + \frac{1}{24}E_2(24z), \\
f_{12}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{48}E_2(2z) - \frac{1}{24}E_2(3z) - \frac{1}{48}E_2(4z) \\
&\quad + \frac{1}{48}E_2(6z) + \frac{1}{24}E_2(8z) - \frac{1}{48}E_2(12z) + \frac{1}{24}E_2(24z),
\end{aligned}$$

$$\begin{aligned}
f_{13}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{1}{16}E_2(2z) + \frac{1}{72}E_2(3z) - \frac{5}{48}E_2(4z)\\
&\quad - \frac{1}{48}E_2(6z) + \frac{1}{24}E_2(8z) + \frac{1}{144}E_2(12z) + \frac{1}{24}E_2(24z),\\
f_{14}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{5}{48}E_2(2z) + \frac{1}{8}E_2(3z) - \frac{1}{16}E_2(4z)\\
&\quad - \frac{5}{16}E_2(6z) + \frac{1}{24}E_2(8z) + \frac{5}{48}E_2(12z) + \frac{1}{24}E_2(24z),\\
f_{15}(z) &= \eta(2z)\eta(4z)\eta(6z)\eta(12z) - \frac{1}{24}E_2(z) + \frac{7}{48}E_2(2z) + \frac{1}{8}E_2(3z) - \frac{13}{48}E_2(4z)\\
&\quad - \frac{5}{48}E_2(6z) + \frac{1}{24}E_2(8z) + \frac{1}{16}E_2(12z) + \frac{1}{24}E_2(24z).
\end{aligned}$$

Proof. These follow from the facts that $f_i(z)$ are all holomorphic modular forms of weight 2 and level $\Gamma_0(24)$ with trivial Nebentypus by [9], and $\eta(2z)\eta(4z)\eta(6z)\eta(12z)$ and $E_2(z) - tE_2(tz)$ for $t|24$ form a basis for the vector space of such holomorphic modular forms by [7, Chapter 4].

Corollary 3.1. *For $i = 1, \ldots, 15$, let $f_i(z)$ be defined as in Proposition 3.1, and write $f_i(z) = \sum_{n=0}^{\infty} b_i(n)e^{2\pi inz}$. Then for any prime $p > 3$, one has that $b_i(p) = a_{24}(p) + p + 1$ for $i = 1, \ldots, 15$.*

Proof. These follow from equating the p-th coefficients on both sides of the identities of Proposition 3.1. For example, equating the p-th coefficients on both sides of the equation associated with $f_1(z)$, one deduces that $b_1(p) = a_{24}(p) + \sigma(p) = a_{24}(p) + p + 1$.

Remark 3.1 From Proposition 3.1 we deduce Corollary 3.1. Combining Corollary 3.1 with Theorem 1.3 yields the congruences for $b_i(p)$ modulo 16, where $p > 3$ is a prime and $i \in \{1, 2, \ldots, 15\}$.

4. Proofs of Theorems 1.4 and 1.5

Proof of Theorem 1.4. We first assume that $p \equiv 3 \pmod 4$. By Theorem 1.1,

$$\begin{aligned}
a_{20}(p) = -a_{80}(p) \equiv \frac{5p+1}{2} + 2\delta(p) &\equiv \begin{cases} \dfrac{p+1}{2} \pmod 4 & \text{if } p \equiv 3, 27, 31, 39 \pmod{40},\\ \dfrac{p-3}{2} \pmod 4 & \text{if } p \equiv 7, 11, 19, 23 \pmod{40}, \end{cases}\\
&\equiv \begin{cases} 0 \pmod 4 & \text{if } p \equiv 11, 19 \pmod{20},\\ 2 \pmod 4 & \text{if } p \equiv 3, 7 \pmod{20}. \end{cases}
\end{aligned}$$

Now assume that $p \equiv 1 \pmod 4$. By [21, Theorem 4.2],

$$t\Big(1, 1, 5, 5; \frac{p-3}{2}\Big) = \frac{8}{3}(p+1) - \frac{8}{3}a_{20}(p). \tag{4.1}$$

On the other hand,

$$t\Big(1, 1, 5, 5; \frac{p-3}{2}\Big) = \sum_{n=0}^{[(p-3)/10]} t_2(n)t_2\Big(\frac{p-3}{2} - 5n\Big). \tag{4.2}$$

If $4n+1$ is a square, then n is even and so $4\big(\frac{p-3}{2} - 5n\big) + 1 \equiv 5 \pmod 8$. Thus $4\big(\frac{p-3}{2} - 5n\big) + 1$ is not a square. By (3.3), we have $4 \mid t_2(n)$, $8 \mid t_2(\frac{p-3}{2} - 5n)$ and so $32 \mid t_2(n)t_2(\frac{p-3}{2} - 5n)$.

If $4n+1$ is not a square, then $8 \mid t_2(n)$, $4 \mid t_2(\frac{p-3}{2}-5n)$ and so $32 \mid t_2(n)t_2(\frac{p-3}{2}-5n)$ by (3.3). Hence, from (4.1) and (4.2) we deduce that

$$\frac{8}{3}(p+1)-\frac{8}{3}a_{20}(p)=t\Big(1,1,5,5;\frac{p-3}{2}\Big)=\sum_{n=0}^{[(p-3)/10]}t_2(n)t_2\Big(\frac{p-3}{2}-5n\Big)\equiv 0 \pmod{32},$$

which yields $a_{20}(p)\equiv p+1\equiv 2 \pmod 4$. To complete the proof, we note that $a_{20}(p)=(-1)^{\frac{p-1}{2}}a_{80}(p)$ by Lemma 2.1.

Remark 4.1 Let $p>5$ be a prime, and let $\#E_p(y^2=x^3-12x-11)$ be the number of points on the elliptic curve $y^2=x^3-12x-11$ over $\mathbb{F}_p$. In [11], Kim, Koo and Park proved the first author's conjecture:

$$\#E_p(y^2=x^3-12x-11)\equiv\begin{cases}6 \pmod{12} & \text{if } p\equiv 3,7 \pmod{20},\\ 0 \pmod{12} & \text{otherwise.}\end{cases}$$

This together with Lemma 2.1 yields the congruence for $a_{20}(p)$ modulo 12.

Proof of Theorem 1.5. By [18, Lemma 2.10], $N(1,1,7,7;p)=\frac{4}{3}(p+1)+\frac{8}{3}a_{14}(p)$. By (3.2), for $n=1,2,\ldots,[\frac{p}{7}]$,

$$r_2(n)r_2(p-7n)\equiv\begin{cases}16 \pmod{32} & \text{if } n \text{ and } p-7n \text{ are represented by } x^2 \text{ or } 2x^2,\\ 0 \pmod{32} & \text{otherwise.}\end{cases}$$

Since $r_2(0)=1$ and $r_2(p)=4(1+(-1)^{\frac{p-1}{2}})$, we derive that

$$\begin{aligned}&\frac{4}{3}(p+1)+\frac{8}{3}a_{14}(p)-4(1+(-1)^{\frac{p-1}{2}})\\ &\equiv N(1,1,7,7;p)-r_2(p)=\sum_{n=1}^{[p/7]}r_2(n)r_2(p-7n)\\ &\equiv\begin{cases}16 \pmod{32} & \text{if } p \text{ is only represented by one form in } \{x^2+7y^2,x^2+14y^2,2x^2+7y^2\},\\ 0 \pmod{32} & \text{otherwise.}\end{cases}\end{aligned}$$

It is well known (see for example [19, Corollary 4.2 and Theorem 11.2]) that

$$\begin{aligned}&p=x^2+7y^2\ (x,y\in\mathbb{Z}) \iff p\equiv 1,9,11 \pmod{14},\\ &p=x^2+14y^2 \text{ or } 2x^2+7y^2\ (x,y\in\mathbb{Z}) \iff p\equiv 1,9,15,23,25,39 \pmod{56}.\end{aligned}$$

Thus,

$$\frac{4}{3}(p+1)+\frac{8}{3}a_{14}(p)-4(1+(-1)^{\frac{p-1}{2}})\equiv\begin{cases}16 \pmod{32} & \text{if } p\equiv 11,29,37,43,51,53 \pmod{56},\\ 0 \pmod{32} & \text{otherwise.}\end{cases}$$

That is,

$$\frac{p+1}{2}+a_{14}(p)+\frac{1}{2}(1+(-1)^{\frac{p-1}{2}})\equiv\begin{cases}2 \pmod 4 & \text{if } p\equiv 11,29,37,43,51,53 \pmod{56},\\ 0 \pmod 4 & \text{otherwise,}\end{cases}$$

which yields the result.

5. Proof of Theorem 1.6

For any non-negative integer n, let T_n be the number of integral solutions to the equation $n = x^2 + 3y^2$. Then clearly $T_0 = 1$. By [19, Theorem 4.1], for $n = 1, 2, 3, \ldots$ we have

$$T_n = \begin{cases} 6\sum\limits_{k\mid\frac{n}{4}} \left(\dfrac{-3}{k}\right) & \text{if } 4 \mid n, \\ 2\sum\limits_{k\mid n} \left(\dfrac{-3}{k}\right) & \text{if } 2 \nmid n, \\ 0 & \text{if } 4 \mid n-2. \end{cases}$$

Thus $T_{3m} = T_m$ for $m = 1, 2, 3, \ldots$. If m is a positive integer such that $3 \nmid m$, then clearly

$$\sum_{k\mid m} \left(\frac{-3}{k}\right) = \sum_{\substack{k\mid m\\ k^2<m}} \left(\left(\frac{-3}{k}\right) + \left(\frac{-3}{m/k}\right)\right) + \sum_{\substack{k\mid m\\ k^2=m}} \left(\frac{-3}{k}\right) \equiv \begin{cases} 1 \pmod 2 & \text{if } m \text{ is a square,} \\ 0 \pmod 2 & \text{otherwise} \end{cases}$$

and so

$$T_m \equiv \begin{cases} 2 \pmod 4 & \text{if } m \text{ is a square,} \\ 0 \pmod 4 & \text{if } m \text{ is not a square.} \end{cases}$$

Hence, for $n = 1, 2, 3, \ldots$ we have

$$T_n \equiv \begin{cases} 2 \pmod 4 & \text{if } n = x^2 \text{ or } 3x^2 \text{ for } x \in \mathbb{Z}, \\ 0 \pmod 4 & \text{otherwise} \end{cases}$$

and so

$$T_nT_{p-5n} \equiv \begin{cases} 4 \pmod 8 & \text{if } n \text{ and } p-5n \text{ are represented by } x^2 \text{ or } 3x^2, \\ 0 \pmod 8 & \text{otherwise.} \end{cases}$$

Note that $T_0 = 1$ and $T_p = 2\left(1 + \left(\frac{p}{3}\right)\right)$. It then follows that

$$\begin{aligned} &N(1,3,5,15;p) \\ &= \left|\left\{(x,y,z,w) \in \mathbb{Z}^4 : \ p = x^2+3y^2+5(z^2+3w^2)\right\}\right| = \sum_{n=0}^{[(p-1)/5]} T_nT_{p-5n} \\ &\equiv \begin{cases} T_0T_p + 4 \equiv 2\left(\left(\dfrac{p}{3}\right) - 1\right) \pmod 8 \\ \qquad \text{if } p \text{ is only represented by one form in } \{x^2+5y^2, x^2+15y^2, 3x^2+5y^2\}, \\ T_0T_p + 4 + 4 \equiv 2\left(\left(\dfrac{p}{3}\right) + 1\right) \pmod 8 \\ \qquad \text{if } p \text{ is represented by } x^2+5y^2 \text{ and } x^2+15y^2, \\ T_0T_p = 2\left(\left(\dfrac{p}{3}\right) + 1\right) \pmod 8 \\ \qquad \text{if } p \text{ is not represented by any form in } \{x^2+5y^2, x^2+15y^2, 3x^2+5y^2\}. \end{cases} \end{aligned}$$

It is well known (see [6] or [19]) that

$$\begin{aligned} p = x^2+5y^2 &\iff p \equiv 1, 9 \pmod{20}, \\ p = x^2+15y^2 &\iff p \equiv 1, 19 \pmod{30}, \\ p = 3x^2+5y^2 &\iff p \equiv 17, 23 \pmod{30}. \end{aligned}$$

Thus,

$$N(1,3,5,15;p) \equiv \begin{cases} 2\left(\left(\frac{p}{3}\right)-1\right) \equiv 4 \pmod 8 & \text{if } p \equiv 29, 41 \pmod{60}, \\ 2\left(\left(\frac{p}{3}\right)-1\right) \equiv 0 \pmod 8 & \text{if } p \equiv 19, 31 \pmod{60}, \\ 2\left(\left(\frac{p}{3}\right)-1\right) \equiv 4 \pmod 8 & \text{if } p \equiv 17, 23 \pmod{30}, \\ 2\left(\left(\frac{p}{3}\right)+1\right) \equiv 4 \pmod 8 & \text{if } p \equiv 1, 49 \pmod{60}, \\ 2\left(\left(\frac{p}{3}\right)+1\right) \equiv 4 \pmod 8 & \text{if } p \equiv 7, 13 \pmod{30}, \\ 2\left(\left(\frac{p}{3}\right)+1\right) \equiv 0 \pmod 8 & \text{if } p \equiv 11, 59 \pmod{60}. \end{cases}$$

Now applying (1.7) gives

$$\begin{aligned} a_{15}(p) &= \frac{1}{3}(2N(1,3,5,15;p) - p - 1) \\ &\equiv \begin{cases} \frac{1}{3}(-p-1) \equiv p+1 \pmod{16} & \text{if } p \equiv 11, 19, 31, 59 \pmod{60}, \\ \frac{1}{3}(8-p-1) \equiv 8 + 5(p+1) \pmod{16} & \text{otherwise.} \end{cases} \end{aligned}$$

This proves Theorem 1.6.

6. Proof of Theorem 1.7

It is known (see [7, Chapter 4]) that the generating function of $N(1,1,11,11;n)$ is a holomorphic modular form of weight 2 and level $\Gamma_0(44)$. Using Sturm's theorem [10], one can verify that

$$\begin{aligned} \sum_{n=0}^{\infty} N(1,1,11,11;n)e^{2\pi i n z} = &-\frac{1}{30}E_2(z) + \frac{1}{15}E_2(2z) - \frac{2}{15}E_2(4z) + \frac{11}{30}E_2(11z) \\ &- \frac{11}{15}E_2(22z) + \frac{22}{15}E_2(44z) + \frac{16}{5}\eta(z)^2\eta(11z)^2 \\ &+ \frac{48}{5}\eta(2z)^2\eta(22z)^2 + \frac{64}{5}\eta(4z)^2\eta(44z)^2, \end{aligned}$$

where $E_2(z)$ is given by (3.4). Equating the p-th coefficients on both sides yields the identity

$$N(1,1,11,11;p) = \frac{4}{5}(p+1) + \frac{16}{5}a_{11}(p).$$

Also, equating the $2p$-th and $4p$-th coefficients on both sides gives

$$\begin{aligned} N(1,1,11,11;2p) &= \frac{4}{5}(p+1) + \frac{16}{5}a_{11}(2p) + \frac{48}{5}a_{11}(p), \\ N(1,1,11,11;4p) &= 4(p+1) + \frac{16}{5}a_{11}(4p) + \frac{48}{5}a_{11}(2p) + \frac{64}{5}a_{11}(p). \end{aligned}$$

On the other hand, by [18, Corollary 4.4], one has that

$$t(1,1,11,11;p-3) = N(1,1,11,11;4p) - N(1,1,11,11;2p).$$

Combining the above three identities gives

$$t(1,1,11,11;p-3)=\frac{16}{5}(p+1)+\frac{16}{5}a_{11}(p)+\frac{32}{5}a_{11}(2p)+\frac{16}{5}a_{11}(4p).$$

Since $a_{11}(2)=-2$, $a_{11}(4)=2$ and $a_{11}(n)$ is multiplicative, we get

$$t(1,1,11,11;p-3)=\frac{16}{5}(p+1)+\Big(\frac{16}{5}-\frac{64}{5}+\frac{32}{5}\Big)a_{11}(p)=\frac{16}{5}(p+1)-\frac{16}{5}a_{11}(p).$$

By (3.3), for $n=0,1,\ldots,[\frac{p-3}{11}]$,

$$\begin{aligned} t_2(n)t_2(p-3-11n)&\equiv\begin{cases}16 \pmod{32} & \text{if } 4n+1 \text{ and } 4(p-3-11n)+1 \text{ are squares,}\\ 0 \pmod{32} & \text{otherwise}\end{cases}\\ &\equiv\begin{cases}16 \pmod{32} & \text{if } 4p=x^2+11y^2 \text{ with } x,y\in\mathbb{Z} \text{ and } y^2=4n+1,\\ 0 \pmod{32} & \text{otherwise.}\end{cases}\end{aligned}$$

Thus,

$$\begin{aligned}\frac{16}{5}(p+1)-\frac{16}{5}a_{11}(p)=t(1,1,11,11;p-3)&=\sum_{n=0}^{[(p-3)/11]}t_2(n)t_2(p-3-11n)\\ &\equiv\begin{cases}16 \pmod{32} & \text{if } 4p=x^2+11y^2 \text{ with } x,y\in\mathbb{Z} \text{ and } 2\nmid y,\\ 0 \pmod{32} & \text{otherwise.}\end{cases}\end{aligned}$$

This yields the remaining result.

7. Three conjectures

In light of Theorems 1.3–1.7, some computational experiment leads to the following conjectures.

Conjecture 7.1. *Let p be a prime with $p>5$.*

(i) *If $p\equiv 1,9 \pmod{20}$ and so $p=x^2+25y^2$ for some $x,y\in\mathbb{Z}$, then*

$$p+1+a_{20}(p)\equiv\begin{cases}0 \pmod 8 & \text{if } 20\mid p-1 \text{ and } 2\mid x, \text{ or if } 20\mid p-9 \text{ and } 2\mid y,\\ 4 \pmod 8 & \text{if } 20\mid p-1 \text{ and } 2\mid y, \text{ or if } 20\mid p-9 \text{ and } 2\mid x.\end{cases}$$

(ii) *If $p\not\equiv 1,9 \pmod{20}$, then*

$$p+1+a_{20}(p)\equiv\begin{cases}0 \pmod 8 & \text{if } p\equiv 13,19,37,39 \pmod{40},\\ 2 \pmod 8 & \text{if } p\equiv 3,7 \pmod{40},\\ 4 \pmod 8 & \text{if } p\equiv 11,17,31,33 \pmod{40},\\ 6 \pmod 8 & \text{if } p\equiv 23,27 \pmod{40}.\end{cases}$$

Conjecture 7.2. *Let p be a prime such that $p\equiv 1,3,4,5,9 \pmod{11}$ and so $4p=x^2+11y^2$ for some integers x and y. Then*

$$p+1+a_{11}(p)\equiv\begin{cases}0 \pmod 4 & \text{if } x\equiv 0 \pmod 2,\\ \left(\frac{x}{11}\right) \pmod 4 & \text{if } x\equiv p \pmod 4.\end{cases}$$

Conjecture 7.3. *Let p be an odd prime with $p \neq 7$.*

(i) *Suppose that $p \equiv 1, 2, 4 \pmod 7$ and so $p = x^2 + 7y^2$ for some integers x and y. Then*

$$p + 1 + a_{14}(p) \equiv \begin{cases} 2(1 + (-1)^{\frac{p-1}{8} + \frac{y}{4}}) \pmod 8 & \text{if } p \equiv 1 \pmod 8, \\ 2\left(1 - (-1)^{\frac{p-3}{8} + \frac{(x-1)^2-1}{8}} \left(\frac{x}{7}\right)\right) \pmod 8 & \text{if } p \equiv 3 \pmod 8, \\ 2\left(1 - (-1)^{\frac{1}{2}(x - (\frac{x}{7}))}\right) \pmod 8 & \text{if } p \equiv 5 \pmod 8, \\ 0 \pmod 8 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

(ii) *Suppose that $p \equiv 3, 5, 6 \pmod 7$. If $p \equiv 1 \pmod 8$ and so $p = x^2 + 16y^2$ for some $x, y \in \mathbb{Z}$, then $p + 1 + a_{14}(p) \equiv 2(1 + (-1)^y) \pmod 8$.*

Competing Interests

The authors declare no conflicts of interest regarding the publication of this paper.

Acknowledgements

The authors thank the anonymous referees for their useful comments and suggestions. In particular, one referee suggests adding Corollary 3.1, and another referee suggests considering the congruences for $a_{14}(p)$ and $a_{15}(p)$, where $p > 7$ is a prime.

Zhi-Hong Sun was supported by the National Natural Science Foundation of China (grant No. 12271200). Dongxi Ye was supported by the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2023A1515010298) and the Fundamental Research Funds for the Central Universities, Sun Yat-sen University (Grant No. 22qntd2901).

References

[1] A. Alaca, *Representations by quaternary quadratic forms with coefficients* $1, 3, 5$ *or* 15, Integers **18**(2018), A12, 14pp.

[2] A. Alaca, S. Alaca, and Z.S. Aygin, *Eta quotients, Eisenstein series and elliptic curves*, Integers **18**(2018), A85, 12pp.

[3] A. Alaca, S. Alaca, M.F. Lemire and K.S. Williams, *Nineteen quaternary quadratic forms*, Acta Arith. **130**(2007), 277-310.

[4] A. Alaca, S. Alaca and K.S. Williams, *On the quaternary forms $x^2 + y^2 + z^2 + 5t^2$, $x^2 + y^2 + 5z^2 + 5t^2$ and $x^2 + 5y^2 + 5z^2 + 5t^2$*, J. Algebra Number Theory Appl. **9**(2007), 37-53.

[5] A.O.L. Atkin and W.-C. Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), 221-243.

[6] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[7] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer, New York, 2005.

[8] T. Evink and P.A. Helminck, *Tribonacci numbers and primes of the form $p = x^2 + 11y^2$*, Math. Slovaca **69**(2019), 521-532.

[9] T. Honda and I. Miyawaki, *Zeta-functions of elliptic curves of 2-power conductor*, J. Math. Soc. Japan **26**(1974), 362-373.

[10] L.J. Kilford, *Modular Forms: A Classical and Computational Introduction*, London: Imperial College Press, 2008, p.236.

[11] D. Kim, J.K. Koo and Y.K. Park, *On the elliptic curves modulo p,* J. Number Theory **128**(2008), 945-953.

[12] G. Köhler, *On two of Liouville's quaternary forms*, Arch. Math. **54**(1990), 465-473.

[13] Y. Martin and K. Ono, *Eta-quotients and elliptic curves,* Proc. Amer. Math. Soc. **125** (1997), 3169-3176.

[14] C.J. Moreno and S.S. Wagstaff, Jr., *Sums of Squares of Integers*, Chapman & Hall/CRC, Boca Raton, London, New York, 2006.

[15] Z.H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102**(2003), 41-89.

[16] Z.H. Sun, *On the number of incongruent residues of $x^4 + ax^2 + bx$ modulo p*, J. Number Theory **119**(2006), 210-241.

[17] Z.H. Sun, *Legendre polynomials and supercongruences*, Acta Arith. **159**(2013), 169-200.

[18] Z.H. Sun, *The number of representations of n as a linear combination of triangular numbers*, Int. J. Number Theory **15**(2019), 1191-1218.

[19] Z.H. Sun and K. S. Williams, *On the number of representations of n by $ax^2+bxy+cy^2$*, Acta Arith. **122** (2006), 101-171.

[20] Z.H. Sun and K. S. Williams, *Ramanujan identities and Euler products for a type of Dirichlet series*, Acta Arith. **122** (2006), 349-393.

[21] M. Wang and Z.H. Sun, *On the number of representations of n as a linear combination of four triangular numbers II*, Int. J. Number Theory **13**(2017), 593-617.