Advances in Applied Mathematics 48(2012), 106-120

Constructing x^2 for primes $p = ax^2 + by^2$

Zhi-Hong Sun
School of Mathematical Sciences,
Huaiyin Normal University,
Huaian, Jiangsu 223001, P.R. China
E-mail: zhihongsun@yahoo.com
Homepage: http://www.hytc.edu.cn/xsjl/szh

Abstract

Let a and b be positive integers and let p be an odd prime such that $p = ax^2 + by^2$ for some integers x and y. Let $\lambda(a,b;n)$ be given by $q\prod_{k=1}^{\infty}(1-q^{ak})^3(1-q^{bk})^3 = \sum_{n=1}^{\infty}\lambda(a,b;n)q^n$. In this paper, using Jacobi's identity $\prod_{n=1}^{\infty}(1-q^n)^3 = \sum_{k=0}^{\infty}(-1)^k(2k+1)q^{\frac{k(k+1)}{2}}$, we construct x^2 in terms of $\lambda(a,b;n)$. For example, if $2 \nmid ab$ and $p \nmid ab(ab+1)$, then $(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(4ax^2-2p) = \lambda(a,b;((ab+1)p-a-b)/8+1)$. We also give formulas for $\lambda(1,3;n+1), \lambda(1,7;2n+1)$, $\lambda(3,5;2n+1)$ and $\lambda(1,15;4n+1)$.

MSC: Primary 11E16, Secondary 11E25
Keywords: Binary quadratic form; Jacobi's identity

1. Introduction

Let p be a prime of the form $4k+1$. The two squares theorem asserts that there are unique positive integers x and y such that $p = x^2 + y^2$ and $2 \nmid x$. Since Legendre and Gauss, there are several methods to construct x and y. For example, if we choose the sign of x so that $x \equiv 1 \pmod 4$, we then have

(1.1) (Gauss [3], 1825) $\quad 2x \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p$,

(1.2) (Jacobsthal [3], 1907) $\quad 2x = -\sum_{n=0}^{p-1}\left(\frac{n^3-4n}{p}\right)$,

(1.3) (Liouville [7], 1862) $\quad 6x = N(p = t^2+u^2+v^2+16w^2) - 3p - 3$,

(1.4) (Klein and Fricke [6], 1892) $\quad 4x^2 - 2p = [q^p]q\prod_{k=1}^{\infty}(1-q^{4k})^6$,

(1.5) (Sun [13], 2006) $\quad 2y = 5p + 3 - 8V_p(z^4 - 3z^2 + 2z)$ for $p \equiv 5 \pmod{12}$,

where $\left(\frac{a}{p}\right)$ is the Legendre-Jacobi-Kronecker symbol, $N(p = t^2+u^2+v^2+16w^2)$ is the number of integral solutions to $p = t^2+u^2+v^2+16w^2$, $[q^n]f(q)$ denotes the coefficient of

[1]The author is supported by the Natural Sciences Foundation of China (grant No. 10971078).

q^n in the power series expansion of $f(q)$, and $V_p(f(z))$ is the number of $c \in \{0,1,\ldots,p-1\}$ such that $f(z) \equiv c \pmod p$ is solvable. We note that (1.3) was conjectured by Liouville and proved by A. Alaca, S. Alaca, M. F. Lemire, and K. S. Williams ([1]).

Let $\mathbb{Z}$ and $\mathbb{N}$ denote the sets of integers and positive integers, respectively. For $a,b,n \in \mathbb{N}$ let $\lambda(a,b;n) \in \mathbb{Z}$ be given by

$$q\prod_{k=1}^{\infty}(1-q^{ak})^3(1-q^{bk})^3 = \sum_{n=1}^{\infty}\lambda(a,b;n)q^n \quad (|q|<1).$$

In his "lost" notebook, Ramanujan ([9]) conjectured that $\lambda(1,7;n)$ is multiplicative and

$$\sum_{\substack{n=1\\ 2\nmid n}}^{\infty}\frac{\lambda(1,7;n)}{n^s} = \frac{1}{1+7^{1-s}}\prod_{p\equiv 3,5,6 \pmod 7}\frac{1}{1-p^{2-2s}}\prod_{p\equiv 1,2,4 \pmod 7}\frac{1}{1-(4x^2-2p)p^{-s}+p^{2-2s}},$$

where $s>1$, p runs over all distinct primes and x^2 is given by $p = x^2+7y^2 \equiv 1,2,4 \pmod 7$. This was proved by Hecke ([5]). See also [10]. The above assertion of Ramanujan implies

$$\lambda(1,7;p) = 4x^2-2p \quad \text{for primes} \quad p = x^2+7y^2 \equiv 1,2,4 \pmod 7. \tag{1.6}$$

In his "lost" notebook, Ramanujan ([9]) also conjectured that $\lambda(4,4;n)$ is multiplicative. This was proved by Mordell ([8]) in 1917. It is easily seen that $\lambda(4,4;p) = \lambda(1,1;(p+3)/4)$ for $p \equiv 1 \pmod 4$. Thus, (1.4) is equivalent to

$$\lambda(1,1;(p+3)/4) = 4x^2-2p \quad \text{for primes} \quad p = x^2+y^2 \equiv 1 \pmod 4 \text{ with } 2\nmid x. \tag{1.7}$$

In 1985 Stienstra and Beukers ([11]) proved

$$\lambda(2,6;p) = 4x^2-2p \quad \text{for primes} \quad p = x^2+3y^2 \equiv 1 \pmod 3. \tag{1.8}$$

It is easily seen that $\lambda(2,6;p) = \lambda(1,3;(p+1)/2)$ for odd p.

In this paper, with the help of Jacobi's identity ([2])

$$\prod_{n=1}^{\infty}(1-q^n)^3 = \sum_{k=0}^{\infty}(-1)^k(2k+1)q^{\frac{k(k+1)}{2}} \quad (|q|<1), \tag{1.9}$$

we construct x^2 for primes $p = ax^2+by^2$. For example, if $a,b \in \mathbb{N}$, $2\nmid ab$ and p is an odd prime such that $p \nmid ab(ab+1)$ and $p = ax^2+by^2$ with $x,y \in \mathbb{Z}$, then

$$\begin{aligned}(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(4ax^2-2p) &= \lambda(a,b;n+1)\\ &= \sum_{k_1+2k_2+\cdots+nk_n=n}(-3)^{k_1+\cdots+k_n}\frac{(a\sigma(\frac{1}{a})+b\sigma(\frac{1}{b}))^{k_1}\cdots(a\sigma(\frac{n}{a})+b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!},\end{aligned} \tag{1.10}$$

where $n = ((ab+1)p-a-b)/8$ and

$$\sigma(m) = \begin{cases}\sum_{d\mid m} d & \text{if } m \in \mathbb{N},\\ 0 & \text{otherwise.}\end{cases} \tag{1.11}$$

This can be viewed as a vast generalization of (1.6)-(1.8). In this paper we also give formulas for $\lambda(1,3;n+1), \lambda(1,7;2n+1)$, $\lambda(3,5;2n+1)$ and $\lambda(1,15;4n+1)$.

2. Basic lemmas

A negative integer d with $d \equiv 0, 1 \pmod 4$ is called a discriminant. Let d be a discriminant. The conductor of d is the largest positive integer $f = f(d)$ such that $d/f^2 \equiv 0, 1 \pmod 4$. As usual we set $w(d) = 2, 4, 6$ according as $d < -4, d = -4$ or $d = -3$. For $a, b, c \in \mathbb{Z}$ we denote the equivalence class containing the form $ax^2 + bxy + cy^2$ by $[a, b, c]$. Let $H(d)$ be the form class group consisting of classes of primitive, integral binary quadratic forms of discriminant d. For more details concerning binary quadratic forms, see for example [4]. For $n \in \mathbb{N}$ and $[a, b, c] \in H(d)$, following [14] we define

$$R([a, b, c], n) = |\{\langle x, y\rangle \in \mathbb{Z} \times \mathbb{Z} : \ n = ax^2 + bxy + cy^2\}|.$$

It is known that $R([a, b, c], n) = R([a, -b, c], n)$. If $R([a, b, c], n) > 0$, we say that n is represented by $[a, b, c]$.

For $m, n \in \mathbb{N}$ let (m, n) denote the greatest common divisor of m and n.

Lemma 2.1 ([14, Lemma 5.2]). *Let $d < 0$ be a discriminant with conductor f. Let p be a prime and $K \in H(d)$.*

(i) *p is represented by some class in $H(d)$ if and only if $(\frac{d}{p}) = 0, 1$ and $p \nmid f$.*

(ii) *Suppose $p \mid d$ and $p \nmid f$. Then p is represented by exactly one class $A \in H(d)$, and $A = A^{-1}$. Moreover, $R(A, p) = w(d)$.*

(iii) *Suppose $(\frac{d}{p}) = 1$. Then p is represented by some class $A \in H(d)$, and*

$$R(K, p) = \begin{cases} 0 & \text{if } K \neq A, A^{-1}, \\ w(d) & \text{if } A \neq A^{-1} \text{ and } K \in \{A, A^{-1}\}, \\ 2w(d) & \text{if } K = A = A^{-1}. \end{cases}$$

Lemma 2.2 ([14, Theorem 7.1]). *Let d be a negative discriminant and $K \in H(d)$. If $n_1, n_2 \in \mathbb{N}$ and $(n_1, n_2) = 1$, then*

$$R(K, n_1 n_2) = \frac{1}{w(d)} \sum_{\substack{K_1 K_2 = K \\ K_1, K_2 \in H(d)}} R(K_1, n_1) R(K_2, n_2).$$

Lemma 2.3. *Let $a, b \in \mathbb{N}$ and let p be an odd prime such that $p \neq a, b$, $p \nmid ab + 1$ and $p = ax^2 + by^2$ with $x, y \in \mathbb{Z}$.*

(i) *If $ab+1$ is not a square, then $R([a, 0, b], (ab+1)p) = 8$ and all the integral solutions to the equation $(ab+1)p = aX^2 + bY^2$ are given by $\{x \pm by, ax \mp y\}, \{x \pm by, -(ax \mp y)\}, \{-(x \pm by), ax \mp y\}$ and $\{-(x \pm by), -(ax \mp y)\}$.*

(ii) *If $ab + 1 = m^2$ for $m \in \mathbb{N}$, then $R([a, 0, b], (ab + 1)p) = 12$ and all the integral solutions to the equation $(ab + 1)p = aX^2 + bY^2$ are given by $\{mx, \pm my\}, \{-mx, \pm my\}$, $\{x \pm by, ax \mp y\}, \{x \pm by, -(ax \mp y)\}, \{-(x \pm by), ax \mp y\}$ and $\{-(x \pm by), -(ax \mp y)\}$.*

Proof. Since $p \neq a, b$ and $p = ax^2 + by^2 < p^2$, we see that $p \nmid abxy$, $(a, b) = 1$ and $(\frac{-4ab}{p}) = (\frac{-aby^2}{p}) = (\frac{a^2x^2}{p}) = 1$. As $p \nmid ab + 1$ and $[1, 0, ab][a, 0, b] = [a, 0, b]$, by Lemmas 2.1 and 2.2 we have

$$\begin{aligned} R([a, 0, b], (ab + 1)p) &= \frac{1}{w(-4ab)} \sum_{\substack{AB=[a,0,b] \\ A,B \in H(-4ab)}} R(A, p) R(B, ab + 1) \\ &= \frac{R([a, 0, b], p) R([1, 0, ab], ab + 1)}{w(-4ab)} = 2R([1, 0, ab], ab + 1). \end{aligned}$$

If $ab+1$ is not a square and $ab+1 = X^2+abY^2$ for some $X, Y \in \mathbb{Z}$, we must have $X^2 = Y^2 = 1$ and so $R([1, 0, ab], ab + 1) = 4$. Hence $R([a, 0, b], (ab + 1)p) = 2R([1, 0, ab], ab + 1) = 8$. It is clear that

$$xy \neq 0 \quad \text{and} \quad (ab + 1)p = (ab + 1)(ax^2 + by^2) = a(x \pm by)^2 + b(ax \mp y)^2.$$

Thus, $\{x \pm by, ax \mp y\}, \{x \pm by, -(ax \mp y)\}, \{-(x \pm by), ax \mp y\}, \{-(x \pm by), -(ax \mp y)\}$ are the eight integral solutions to the equation $(ab + 1)p = aX^2 + bY^2$. This proves (i).

If $ab + 1 = m^2$ for $m \in \mathbb{N}$ and $ab + 1 = X^2 + abY^2$ for some $X, Y \in \mathbb{Z}$, we must have $Y \in \{0, \pm 1\}$ and so $R([1, 0, ab], ab+1) = 6$. Hence $R([a, 0, b], (ab+1)p) = 2R([1, 0, ab], ab+1) = 12$. Since $xy \neq 0$ and

$$(ab + 1)p = (ab + 1)(ax^2 + by^2) = a(mx)^2 + b(my)^2 = a(x \pm by)^2 + b(ax \mp y)^2,$$

we see that $\{mx, \pm my\}, \{-mx, \pm my\}, \{x \pm by, ax \mp y\}, \{x \pm by, -(ax \mp y)\}, \{-(x \pm by), ax \mp y\}, \{-(x \pm by), -(ax \mp y)\}$ are 12 integral solutions to the equation $(ab + 1)p = aX^2 + bY^2$. This proves (ii).

Lemma 2.4. *Let $a, b \in \mathbb{N}$, $(a, b) = 1$ and let p be an odd prime such that $p \neq ab, ab + 1$ and $p = x^2 + aby^2$ with $x, y \in \mathbb{Z}$. Suppose $(a - 1)(b - 1) \neq 0$ or $a + b$ is not a square. Then $R([a, 0, b], (a + b)p) = 8$ and all the integral solutions to the equation $(a + b)p = aX^2 + bY^2$ are given by*

$$\{x \pm by, x \mp ay\}, \{x \pm by, -(x \mp ay)\}, \{-(x \pm by), x \mp ay\}, \{-(x \pm by), -(x \mp ay)\}.$$

Proof. Since $p \neq ab, ab + 1$, we see that $p = x^2 + aby^2 > 1 + ab \geq a + b$ and so $p \nmid a + b$. As $[1, 0, ab][a, 0, b] = [a, 0, b]$, by Lemmas 2.1 and 2.2 we have

$$\begin{aligned} R([a, 0, b], (a + b)p) &= \frac{1}{w(-4ab)} \sum_{\substack{AB=[a,0,b] \\ A,B \in H(-4ab)}} R(A, p)R(B, a + b) \\ &= \frac{1}{w(-4ab)} R([1, 0, ab], p)R([a, 0, b], a + b) = 2R([a, 0, b], a + b). \end{aligned}$$

If $a+b = aX^2+bY^2$ for some $X, Y \in \mathbb{Z}$, we must have $X^2 = Y^2 = 1$. Thus $R([a, 0, b], a+b) = 4$ and so $R([a, 0, b], (a + b)p) = 2R([a, 0, b], a + b) = 8$. It is clear that

$$xy \neq 0 \quad \text{and} \quad (a + b)p = (a + b)(x^2 + aby^2) = a(x \pm by)^2 + b(x \mp ay)^2.$$

Thus, $\{x \pm by, x \mp ay\}, \{x \pm by, -(x \mp ay)\}, \{-(x \pm by), x \mp ay\}, \{-(x \pm by), -(x \mp ay)\}$ are the eight integral solutions to the equation $(a + b)p = aX^2 + bY^2$. This completes the proof.

Lemma 2.5. *Let $a, b, n \in \mathbb{N}$. Then*

$$\sum_{\substack{x,y \in \mathbb{Z}, x \equiv y \equiv 1 \pmod 4 \\ ax^2+by^2=8n+a+b}} xy = \lambda(a, b; n + 1).$$

Proof. Using Jacobi's identity (1.9) we see that

$$\begin{aligned}
&q\prod_{n=1}^{\infty}(1-q^{an})^3(1-q^{bn})^3\\
&=q\Big(\sum_{k=0}^{\infty}(-1)^k(2k+1)q^{a\frac{k(k+1)}{2}}\Big)\Big(\sum_{m=0}^{\infty}(-1)^m(2m+1)q^{b\frac{m(m+1)}{2}}\Big)\\
&=\sum_{n=0}^{\infty}\sum_{\substack{k,m\ge 0\\ a\frac{k(k+1)}{2}+b\frac{m(m+1)}{2}=n}}(-1)^k(2k+1)\cdot(-1)^m(2m+1)q^{n+1}.
\end{aligned}$$

Thus,

$$\begin{aligned}
\lambda(a,b;n+1)&=\sum_{\substack{k,m\ge 0\\ a\frac{k(k+1)}{2}+b\frac{m(m+1)}{2}=n}}(-1)^k(2k+1)\cdot(-1)^m(2m+1)\\
&=\sum_{\substack{k,m\ge 0\\ a(2k+1)^2+b(2m+1)^2=8n+a+b}}(-1)^k(2k+1)\cdot(-1)^m(2m+1)\\
&=\sum_{\substack{x\equiv y\equiv 1 \pmod 4\\ ax^2+by^2=8n+a+b}}xy.
\end{aligned}$$

This proves the lemma.

Lemma 2.6. *Let $a,b\in\mathbb{N}$ with $(a,b)=1$ and $ab\equiv 1 \pmod 4$. Let p be an odd prime such that $R([a,0,b],2p)>0$. Then $R([a,0,b],2p)=2w(-4ab)$.*

Proof. Suppose that $2p=ax^2+by^2$ with $x,y\in\mathbb{Z}$. Since $2p<p^2$ we see that $p\nmid xy$. We claim that $p\nmid ab$. If $p\mid a$, then $p\mid by^2$ and so $p\mid b$. This contradicts the fact $(a,b)=1$. Hence $p\nmid a$. Similarly, we have $p\nmid b$. Since $-ab\equiv 3 \pmod 4$ we see that $2\nmid f(-4ab)$. Thus, by Lemma 2.1, there exists exactly one class $A\in H(-4ab)$ such that $R(A,2)>0$ and we have $A=A^{-1}$. Using Lemmas 2.1, 2.2 and the fact $R([a,0,b],2p)>0$ we see that $R([a,0,b],2p)=\frac{1}{w(-4ab)}R(A,2)R(A[a,0,b],p)=R(A[a,0,b],p)=2w(-4ab)$. This completes the proof.

Lemma 2.7. *Let $a,b\in\mathbb{N}$, $ab\equiv 3 \pmod 4$, $K\in H(-4ab)$ and $K=K^{-1}$. Let p be an odd prime such that $p\nmid ab$ and $R(K,4p)>0$. Then $R(K,4p)=2w(-ab)$.*

Proof. From Lemma 2.2 we have

$$2R(K,4p)=\sum_{\substack{AB=K\\ A,B\in H(-4ab)}}R(A,p)R(B,4)>0.$$

Since $2\mid f(-4ab)$, by [14, Theorem 5.3(i)] we have $R(B,4)=0$ or $w(-ab)$ for $B\in H(-4ab)$. Suppose $R(A,p)>0$ for $A\in H(-4ab)$. Then $(AK)^{-1}=K^{-1}A^{-1}=KA^{-1}=A^{-1}K$ and so $R(A^{-1}K,4)=R((AK)^{-1},4)=R(AK,4)$. From the above and Lemma 2.1 we see that

$$\begin{aligned}
&2R(K,4p)\\
&=\begin{cases}R(A,p)R(AK,4)=4\cdot w(-ab) & \text{if } A=A^{-1},\\ R(A,p)R(A^{-1}K,4)+R(A^{-1},p)R(AK,4)=2w(-ab)+2w(-ab) & \text{if } A\ne A^{-1}.\end{cases}
\end{aligned}$$

This yields the result.

If $\{a_n\}$ and $\{b_n\}$ are two sequences satisfying

$$a_1 = b_1 \quad \text{and} \quad b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 = n a_n \ (n = 2, 3, \ldots),$$

we say that (a_n, b_n) is a Newton-Euler pair as in [12]. For a rational number m let $\sigma(m)$ be given by (1.11). Now we state the following result.

Lemma 2.8 . *Let $a, b \in \mathbb{N}$. Then $(\lambda(a, b; n+1), -3(a\sigma(n/a) + b\sigma(n/b)))$ is a Newton-Euler pair. That is, for $n \in \mathbb{N}$,*

$$a\sigma(\frac{n}{a}) + b\sigma(\frac{n}{b}) + \sum_{k=1}^{n-1} \big(a\sigma(\frac{k}{a}) + b\sigma(\frac{k}{b})\big)\lambda(a, b; n+1-k) = -\frac{n}{3}\lambda(a, b; n+1).$$

Proof. Suppose that q is real and $|q| < 1$. As

$$1 - q^n = \prod_{r=0}^{n-1} \big(1 - \mathrm{e}^{2\pi i \frac{r}{n}} q\big),$$

we see that

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \lambda(a, b; n+1) q^n &= \prod_{k=1}^{\infty} \big(1 - q^{ak}\big)^3 \big(1 - q^{bk}\big)^3 \\ &= \prod_{k=1}^{\infty} \prod_{r=0}^{ak-1} \big(1 - \mathrm{e}^{2\pi i \frac{r}{ak}} q\big)^3 \prod_{s=0}^{bk-1} \big(1 - \mathrm{e}^{2\pi i \frac{s}{bk}} q\big)^3. \end{aligned}$$

Observe that

$$\begin{aligned} &\sum_{k=1}^{\infty} \Big\{ \sum_{r=0}^{ak-1} 3\Big(\mathrm{e}^{2\pi i \frac{r}{ak}}\Big)^n + \sum_{s=0}^{bk-1} 3\Big(\mathrm{e}^{2\pi i \frac{s}{bk}}\Big)^n \Big\} \\ &= 3 \sum_{\substack{k \in \mathbb{N} \\ ak \mid n}} ak + 3 \sum_{\substack{k \in \mathbb{N} \\ bk \mid n}} bk = 3a\sigma\big(\frac{n}{a}\big) + 3b\sigma\big(\frac{n}{b}\big). \end{aligned}$$

From the above and [12, Example 1] we deduce the result.

Lemma 2.9. *Let $a, b, n \in \mathbb{N}$. Then*

$$\begin{aligned} &\lambda(a, b; n+1) \\ &= \sum_{k_1 + 2k_2 + \cdots + nk_n = n} (-3)^{k_1 + \cdots + k_n} \frac{(a\sigma(\frac{1}{a}) + b\sigma(\frac{1}{b}))^{k_1} \cdots (a\sigma(\frac{n}{a}) + b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1} \cdot k_1! \cdots n^{k_n} \cdot k_n!}. \end{aligned}$$

Proof. This is immediate from Lemma 2.8 and [12, Theorem 2.2].

3. Constructing x^2 for primes $p = ax^2 + by^2$

Theorem 3.1. *Let $a,b\in\mathbb{N}$ with $2\nmid ab$. Let p be an odd prime such that $p\neq a,b$, $p\nmid ab+1$ and $p=ax^2+by^2$ with $x,y\in\mathbb{Z}$. Let $n=((ab+1)p-a-b)/8$. Then*

$$\begin{aligned}&(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(4ax^2-2p)\\&=\lambda(a,b;n+1)=\sum_{k_1+2k_2+\cdots+nk_n=n}(-3)^{k_1+\cdots+k_n}\frac{(a\sigma(\frac{1}{a})+b\sigma(\frac{1}{b}))^{k_1}\cdots(a\sigma(\frac{n}{a})+b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!}.\end{aligned}$$

Proof. Clearly $2\mid x$ or $2\mid y$. If $2\mid y$, then $p\equiv ax^2\equiv a\pmod 4$ and so $(ab+1)p\equiv(ab+1)a\equiv a+b\pmod 8$. If $2\mid x$, then $p\equiv by^2\equiv b\pmod 4$ and so $(ab+1)p\equiv(ab+1)b\equiv a+b\pmod 8$. Thus $n\in\mathbb{N}$. By Lemma 2.3, all the integral solutions $\{X,Y\}$ with $2\nmid XY$ to the equation $8n+a+b=(ab+1)p=aX^2+bY^2$ are given by $\{x\pm by,ax\mp y\}$, $\{x\pm by,-(ax\mp y)\}$, $\{-(x\pm by),ax\mp y\}$, $\{-(x\pm by),-(ax\mp y)\}$. Since $x\pm by\equiv(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(ax\mp y)\pmod 4$, applying Lemma 2.5 we have

$$\begin{aligned}\lambda(a,b;n+1)&=\sum_{\substack{X\equiv Y\equiv 1\pmod 4\\ aX^2+bY^2=8n+a+b}}XY\\&=(x+by)\cdot(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(ax-y)+(x-by)\cdot(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(ax+y)\\&=(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}2(ax^2-by^2)=(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(4ax^2-2p).\end{aligned}$$

This together with Lemma 2.9 yields the result.

Corollary 3.1. *Let p be a prime of the form $4k+1$ and so $p=x^2+y^2$ with $x,y\in\mathbb{Z}$ and $2\nmid x$. Let $n=(p-1)/4$. Then*

$$4x^2-2p=\sum_{k_1+2k_2+\cdots+nk_n=n}(-6)^{k_1+\cdots+k_n}\frac{\sigma(1)^{k_1}\cdots\sigma(n)^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!}.$$

Proof. Taking $a=b=1$ in Theorem 3.1 we obtain the result.

Corollary 3.2. *Suppose that $p\equiv 1,9\pmod{20}$ is a prime and so $p=x^2+5y^2$ for some $x,y\in\mathbb{Z}$. Let $n=3(p-1)/4$. Then*

$$\begin{aligned}&(-1)^{x-1}(4x^2-2p)=\lambda(1,5;(3p+1)/4)\\&=\sum_{k_1+2k_2+\cdots+nk_n=n}(-3)^{k_1+\cdots+k_n}\frac{(\sigma(1)+5\sigma(\frac{1}{5}))^{k_1}\cdots(\sigma(n)+5\sigma(\frac{n}{5}))^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!}.\end{aligned}$$

Proof. Taking $a=1$ and $b=5$ in Theorem 3.1 we obtain the result.

Theorem 3.2. *Let $a,b\in\mathbb{N}$ with $(a,b)=1$. Let p be an odd prime such that $p\neq ab,ab+1$ and $p=x^2+aby^2$ with $x,y\in\mathbb{Z}$. Let $n=(a+b)(p-1)/8$.*

(i) *If $2\nmid ab$, then*

$$\begin{aligned}&(-1)^{\frac{ab+1}{2}y}(4x^2-2p)=\lambda(a,b;n+1)\\&=\sum_{k_1+2k_2+\cdots+nk_n=n}(-3)^{k_1+\cdots+k_n}\frac{(a\sigma(\frac{1}{a})+b\sigma(\frac{1}{b}))^{k_1}\cdots(a\sigma(\frac{n}{a})+b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!}.\end{aligned}$$

(ii) *If $2\nmid a$, $2\mid b$, $8\nmid b$ and $8\mid p-1$, then*

$$(-1)^{\frac{y}{2}}(4x^2-2p)=\lambda(a,b;n+1)$$

$$= \sum_{k_1+2k_2+\cdots+nk_n=n} (-3)^{k_1+\cdots+k_n} \frac{(a\sigma(\frac{1}{a})+b\sigma(\frac{1}{b}))^{k_1}\cdots(a\sigma(\frac{n}{a})+b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1}\cdot k_1!\cdots n^{k_n}\cdot k_n!}.$$

Proof. If $(a-1)(b-1)\neq 0$ or $a+b$ is not a square, using Lemma 2.4 we see that $R([a,0,b],(a+b)p)=8$ and all the integral solutions to $(a+b)p=aX^2+bY^2$ are given by $\{x\pm by, x\mp ay\}, \{x\pm by, -(x\mp ay)\}, \{-(x\pm by), x\mp ay\}, \{-(x\pm by), -(x\mp ay)\}$. If $a=1$ and $b+1=m^2$ for $m\in\mathbb{N}$, using Lemma 2.3(ii) we see that $R([1,0,b],(b+1)p)=12$ and all the integral solutions to $(b+1)p=X^2+bY^2$ are given by $\{mx,\pm my\},\{-mx,\pm my\},\{x\pm by, x\mp y\},\{x\pm by,-(x\mp y)\},\{-(x\pm by),x\mp y\},\{-(x\pm by),-(x\mp y)\}$. If $b=1$ and $a+1=k^2$ for $k\in\mathbb{N}$, using Lemma 2.3(ii) we see that $R([a,0,1],(a+1)p)=12$ and all the integral solutions to $(a+1)p=aX^2+Y^2$ are given by $\{ky,\pm kx\},\{-ky,\pm kx\},\{x\pm y,x\mp ay\},\{x\pm y,-(x\mp ay)\},\{-(x\pm y),x\mp ay\},\{-(x\pm y),-(x\mp ay)\}$.

We first assume $2\nmid ab$. If $ab\equiv 1\pmod 4$, then $p=x^2+aby^2\equiv 1\pmod 4$ and so $(a+b)(p-1)\equiv 0\pmod 8$. If $ab\equiv 3\pmod 4$, then $4\mid a+b$ and so $8\mid (a+b)(p-1)$. Thus, we always have $8\mid (a+b)(p-1)$. It is easily seen that $x\pm by\equiv 1\pmod 2$ and $x\pm by\equiv (-1)^{\frac{ab+1}{2}y}(x\mp ay)\pmod 4$. Thus, applying the above and Lemma 2.5 we have

$$\begin{aligned}\lambda(a,b;n+1) &= \sum_{\substack{X\equiv Y\equiv 1 \pmod 4\\ aX^2+bY^2=8n+a+b}} XY\\ &= (x+by)\cdot(-1)^{\frac{ab+1}{2}y}(x-ay)+(x-by)\cdot(-1)^{\frac{ab+1}{2}y}(x+ay)\\ &= (-1)^{\frac{ab+1}{2}y}2(x^2-aby^2)=(-1)^{\frac{ab+1}{2}y}(4x^2-2p).\end{aligned}$$

This together with Lemma 2.9 proves (i).

Now we consider (ii). Since $2\nmid a$, $2\mid b$, $8\nmid b$ and $8\mid p-1$, we deduce $2\nmid x$, $8\mid by^2$ and so $2\mid y$. It is easily seen that $x\pm by\equiv 1\pmod 2$ and $x\pm by\equiv(-1)^{\frac{y}{2}}(x\mp ay)\pmod 4$. Thus, applying the above and Lemma 2.5 we have

$$\begin{aligned}\lambda(a,b;n+1) &= \sum_{\substack{X\equiv Y\equiv 1 \pmod 4\\ aX^2+bY^2=8n+a+b}} XY\\ &= (x+by)\cdot(-1)^{\frac{y}{2}}(x-ay)+(x-by)\cdot(-1)^{\frac{y}{2}}(x+ay)\\ &= (-1)^{\frac{y}{2}}2(x^2-aby^2)=(-1)^{\frac{y}{2}}(4x^2-2p).\end{aligned}$$

This together with Lemma 2.9 yields (ii). The proof is now complete.

Corollary 3.3. *Let $a,b\in\mathbb{N}$ with $2\nmid ab$ and $(a,b)=1$. Let p be an odd prime such that $p\neq ab, ab+1$ and $p=x^2+aby^2$ with $x,y\in\mathbb{Z}$. Then*

$$\lambda\Big(a,b;\frac{(a+b)(p-1)}{8}+1\Big)=\lambda\Big(1,ab;\frac{(ab+1)(p-1)}{8}+1\Big).$$

Proof. By Theorem 3.1 we have

$$(-1)^{\frac{1+ab}{2}(x+1)}(4x^2-2p)=\lambda\Big(1,ab;\frac{(ab+1)(p-1)}{8}+1\Big).$$

This together with Theorem 3.2(i) gives the result.

Corollary 3.4. *Suppose $a \in \mathbb{N}$ and $2 \nmid a$. Let p be an odd prime such that $p = x^2 + 16ay^2$ with $x, y \in \mathbb{Z}$. Then*

$$(-1)^y(4x^2 - 2p) = \lambda\Big(a, 4; \frac{(a+4)p - a + 4}{8}\Big).$$

Proof. Taking $b = 4$ and replacing y with $2y$ in Theorem 3.2(ii) we deduce the result.

Let p be an odd prime. From Theorem 3.2(ii) we deduce:

(3.1) $(-1)^{\frac{y}{2}}(4x^2 - 2p) = \lambda(1, 2; (3p+5)/8)$ for $p = x^2 + 2y^2 \equiv 1 \pmod 8$,
(3.2) $(-1)^{\frac{y}{2}}(4x^2 - 2p) = \lambda(1, 6; (7p+1)/8)$ for $p = x^2 + 6y^2 \equiv 1 \pmod{24}$,
(3.3) $(-1)^{\frac{y}{2}}(4x^2 - 2p) = \lambda(1, 10; (11p-3)/8)$ for $p = x^2 + 10y^2 \equiv 1, 9 \pmod{40}$,
(3.4) $(-1)^{\frac{y}{2}}(4x^2 - 2p) = \lambda(1, 12; (13p-5)/8)$ for $p = x^2 + 12y^2 \equiv 1 \pmod{24}$.

Theorem 3.3. *Let $a, b \in \mathbb{N}$, $2 \nmid a$, $2 \mid b$ and $8 \nmid b$. Let p be a prime such that $p \equiv a \pmod 8$, $p \neq a$, $p \nmid ab+1$ and $p = ax^2 + by^2$ with $x, y \in \mathbb{Z}$. Let $n = ((ab+1)p - a - b)/8$. Then*

$$\begin{aligned}&(-1)^{\frac{a-1}{2}+\frac{y}{2}}(4ax^2 - 2p) = (-1)^{\frac{a-1}{2}+\frac{y}{2}}(2p - 4by^2) = \lambda(a, b; n+1)\\ &= \sum_{k_1+2k_2+\cdots+nk_n=n} (-3)^{k_1+\cdots+k_n} \frac{(a\sigma(\frac{1}{a}) + b\sigma(\frac{1}{b}))^{k_1} \cdots (a\sigma(\frac{n}{a}) + b\sigma(\frac{n}{b}))^{k_n}}{1^{k_1} \cdot k_1! \cdots n^{k_n} \cdot k_n!}.\end{aligned}$$

Proof. Clearly we have $2 \nmid x$ and so $8 \mid by^2$. Since $8 \nmid b$ we must have $2 \mid y$. As $p \equiv a \pmod 8$ we have $(ab+1)p \equiv (1+ab)a \equiv a+b \pmod 8$. By Lemma 2.3, all the integral solutions $\{X, Y\}$ with $2 \nmid XY$ to the equation $8n + a + b = (ab+1)p = aX^2 + bY^2$ are given by $\{x \pm by, ax \mp y\}, \{x \pm by, -(ax \mp y)\}, \{-(x \pm by), ax \mp y\}, \{-(x \pm by), -(ax \mp y)\}$. Since x is odd, we may choose the sign of x so that $x \equiv 1 \pmod 4$. Then $x \pm by \equiv (-1)^{\frac{a-1}{2}+\frac{y}{2}}(ax \mp y) \equiv 1 \pmod 4$. Therefore, applying Lemma 2.5 we have

$$\begin{aligned}\lambda(a, b; n+1) &= \sum_{\substack{X \equiv Y \equiv 1 \pmod 4\\ aX^2+bY^2=8n+a+b}} XY\\ &= (x+by) \cdot (-1)^{\frac{a-1}{2}+\frac{y}{2}}(ax - y) + (x - by) \cdot (-1)^{\frac{a-1}{2}+\frac{y}{2}}(ax + y)\\ &= (-1)^{\frac{a-1}{2}+\frac{y}{2}} 2(ax^2 - by^2) = (-1)^{\frac{a-1}{2}+\frac{y}{2}}(4ax^2 - 2p)\\ &= (-1)^{\frac{a-1}{2}+\frac{y}{2}}(2p - 4by^2).\end{aligned}$$

This together with Lemma 2.9 proves the theorem.

As examples, taking $a = 3, 5$ and $b = 2$ in Theorem 3.3 we have:

(3.5) $(-1)^{\frac{y}{2}}(8y^2 - 2p) = \lambda(2, 3; (7p+3)/8)$ for $p = 3x^2 + 2y^2 \equiv 11 \pmod{24}$,
(3.6) $(-1)^{\frac{y}{2}}(2p - 8y^2) = \lambda(2, 5; (11p+1)/8)$ for $p = 5x^2 + 2y^2 \equiv 13, 37 \pmod{40}$.

Corollary 3.5. *Let $a, b \in \mathbb{N}$ with $2 \nmid a$, $2 \mid b$, $8 \nmid b$ and $(a, b) = 1$. Let $p \equiv 1 \pmod 8$ be a prime such that $p \neq ab, ab+1$ and $p = x^2 + aby^2$ with $x, y \in \mathbb{Z}$. Then*

$$\lambda\Big(a, b; \frac{(a+b)(p-1)}{8} + 1\Big) = \lambda\Big(1, ab; \frac{(ab+1)(p-1)}{8} + 1\Big).$$

Proof. By Theorem 3.3 we have

$$(-1)^{\frac{y}{2}}(4x^2-2p)=\lambda\Big(1,ab;\frac{(ab+1)(p-1)}{8}+1\Big).$$

This together with Theorem 3.2(ii) gives the result.

4. Constructing xy for primes $p = ax^2 + by^2$

Theorem 4.1. *Let $a,b\in\mathbb{N}$, $8\nmid a$, $8\nmid b$ and $n\in\{0,1,2,\dots\}$. Let p be an odd prime such that $p=8n+a+b=ax^2+by^2$ with $x,y\in\mathbb{Z}$ and $x\equiv y \pmod 4$. Then*

$$xy=\lambda(a,b;n+1)\quad\textit{and}\quad 2ax^2-p=\pm\sqrt{p^2-4ab\lambda(a,b;n+1)^2}.$$

Proof. It is clear that $(a,b)=1$. Let $x,y\in\mathbb{Z}$ be such that $p=8n+a+b=ax^2+by^2$. When $2\mid x$, we have $2\nmid y$, $a\equiv 8n+a=ax^2+by^2-b\equiv ax^2\equiv 0,4a \pmod 8$ and so $8\mid a$. When $2\mid y$, we have $2\nmid x$, $b\equiv 8n+b=ax^2+by^2-a\equiv by^2\equiv 0,4b \pmod 8$ and so $8\mid b$. As $8\nmid a$ and $8\nmid b$, we see that $2\nmid xy$. Suppose $x\equiv y\equiv 1 \pmod 4$. Then x and y are unique by Lemma 2.1. Now applying Lemma 2.5 we obtain $xy=\lambda(a,b;n+1)$.

Set $\lambda=\lambda(a,b;n+1)$. Then $x^2(p-ax^2)=bx^2y^2=b\lambda^2$ and so $ax^4-px^2+b\lambda^2=0$. Thus, $x^2=(p\pm\sqrt{p^2-4ab\lambda^2})/(2a)$. This completes the proof.

For example, if $p=8n+3$ is a prime and so $p=x^2+2y^2$ with $x\equiv y \pmod 4$, then $xy=\lambda(1,2;n+1)$ and $2x^2-p=\pm\sqrt{p^2-8\lambda(1,2;n+1)^2}$.

Theorem 4.2. *Let $a,b\in\mathbb{N}$ with $(a,b)=1$, $ab>1$ and $ab\equiv 1 \pmod 4$. Let p be an odd prime and $2p=8n+a+b=ax^2+by^2$ with $n\in\{0,1,2,\dots\}$, $x,y\in\mathbb{Z}$ and $4\mid x-y$. Then*

$$xy=\lambda(a,b;n+1)\quad\textit{and}\quad ax^2=p\pm\sqrt{p^2-ab\lambda(a,b;n+1)^2}.$$

Proof. Let $x,y\in\mathbb{Z}$ be such that $2p=8n+a+b=ax^2+by^2$. Then clearly $2\nmid xy$. Suppose $x\equiv y\equiv 1 \pmod 4$. Then x and y are unique by Lemma 2.6. Now applying Lemma 2.5 we obtain $xy=\lambda$, where $\lambda=\lambda(a,b;n+1)$. Thus, $x^2(2p-ax^2)=bx^2y^2=b\lambda^2$ and so $ax^4-2px^2+b\lambda^2=0$. Hence, $x^2=(p\pm\sqrt{p^2-ab\lambda^2})/a$. This completes the proof.

For example, if $p=4n+3\equiv 3,7 \pmod{20}$ is a prime and so $2p=x^2+5y^2$ with $x\equiv y \pmod 4$, then $xy=\lambda(1,5;n+1)$ and $x^2-p=\pm\sqrt{p^2-5\lambda(1,5;n+1)^2}$.

Theorem 4.3. *Let $a,b\in\mathbb{N}$, $2\nmid ab$, $ab\neq 3$, $a+b\equiv 4 \pmod 8$. Let p be an odd prime such that $p\nmid ab$ and $4p=ax^2+by^2$ with $x,y\in\mathbb{Z}$ and $x\equiv y\equiv 1 \pmod 4$. Then*

$$xy=\lambda\quad\textit{and}\quad ax^2=2p\pm\sqrt{4p^2-ab\lambda^2},$$

where $\lambda=\lambda(a,b;\frac12(p-\frac{a+b}{4})+1)$.

Proof. Clearly $(a,b)=1$ and $ab\equiv 3 \pmod 4$. From Lemma 2.7 we know that x and y are unique. Set $n=\frac12(p-\frac{a+b}{4})$. Then $8n+a+b=4p$. By Lemma 2.5 we have $xy=\lambda$ and so $x^2y^2=\lambda^2$. Thus $x^2(4p-ax^2)=b\lambda^2$ and so $ax^4-4px^2+b\lambda^2=0$. Hence $x^2=\frac{4p\pm\sqrt{16p^2-4ab\lambda^2}}{2a}=\frac{2p\pm\sqrt{4p^2-ab\lambda^2}}{a}$. This completes the proof.

For example, if $p\neq 11$ is an odd prime and $4p=x^2+11y^2$ with $x\equiv y\equiv 1 \pmod 4$, then $xy=\lambda$ and $x^2=2p\pm\sqrt{4p^2-11\lambda^2}$, where $\lambda=\lambda(1,11;(p-1)/2)$.

5. Evaluation of $\lambda(1,3;n), \lambda(1,7;2n+1)$ and $\lambda(3,5;2n+1)$

For $n\in\mathbb{N}$, in [6, Vol.2] Klein and Fricke showed that

$$\lambda(1,1;n+1)=\sum_{\substack{x,y\in\mathbb{Z},x\equiv 1\pmod 4\\ x^2+y^2=4n+1}}(x^2-y^2). \tag{5.1}$$

See also [8]. In the section we evaluate $\lambda(1,3;n), \lambda(1,7;2n+1)$ and $\lambda(3,5;2n+1)$.

Lemma 5.1. *Let $a,b,n\in\mathbb{N}$ with $2\nmid ab$. Then*

$$\sum_{\substack{x,y\in\mathbb{Z},x+ay\equiv 1\pmod 4\\ x^2+aby^2=2n+1}}(x+ay)(x-by)=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+aby^2=2n+1}}(x^2-aby^2).$$

Proof. If $x,y\in\mathbb{Z}$ and $x^2+aby^2=2n+1$, then clearly $x+ay$ is odd. Since $(x+ay)(x-by)=(-x+a(-y))(-x-b(-y))$, we see that

$$\begin{aligned}&\sum_{\substack{x,y\in\mathbb{Z},x+ay\equiv 1\pmod 4\\ x^2+aby^2=2n+1}}(x+ay)(x-by)\\
&=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+aby^2=2n+1}}(x+ay)(x-by)=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+aby^2=2n+1}}(x^2-aby^2+(a-b)xy)\\
&=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+aby^2=2n+1}}(x^2-aby^2).\end{aligned}$$

This proves the lemma.

Theorem 5.1. *Let $n\in\mathbb{N}$. Then*

$$\lambda(1,3;n+1)=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+3y^2=2n+1}}(x^2-3y^2),$$

$$\lambda(1,7;2n+1)=\frac12\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+7y^2=2n+1}}(x^2-7y^2).$$

Proof. From Lemma 2.5 we have

$$\lambda(1,3;n+1)=\sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1\pmod 4\\ X^2+3Y^2=8n+4}}XY.$$

As $H(-12)=\{[1,0,3]\}$, by Lemma 2.2 we have

$$R([1,0,3],8n+4)=\frac12R([1,0,3],4)R([1,0,3],2n+1)=3R([1,0,3],2n+1).$$

Thus, if $R([1,0,3],2n+1)=0$, then $R([1,0,3],8n+4)=0$ and so $\lambda(1,3;n+1)=0$. Hence the result is true in this case. Now assume that $2n+1=x^2+3y^2$ with $x,y\in\mathbb{Z}$. Then

$8n+4=4(x^2+3y^2)=(x+3y)^2+3(x-y)^2$. As $R([1,0,3],8n+4)=3R([1,0,3],2n+1)$ we see that all the integral solutions to the equation $8n+4=X^2+3Y^2$ are given by $\{2x,2y\},\{x+3y,x-y\},\{x+3y,-(x-y)\}$, where $\{x,y\}$ runs over all integral solutions to the equation $2n+1=x^2+3y^2$. Hence, using Lemmas 2.5, 5.1 and the fact $x+3y\equiv x-y \pmod 4$ we deduce

$$\begin{aligned}\lambda(1,3;n+1)&=\sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ X^2+3Y^2=8n+4}} XY=\sum_{\substack{x,y\in\mathbb{Z},x+3y\equiv 1 \pmod 4\\ x^2+3y^2=2n+1}}(x+3y)(x-y)\\ &=\frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+3y^2=2n+1}}(x^2-3y^2).\end{aligned}$$

Now we consider the formula for $\lambda(1,7;2n+1)$. By Lemma 2.5 we have

$$\lambda(1,7;2n+1)=\sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ X^2+7Y^2=16n+8}} XY.$$

As $H(-28)=\{[1,0,7]\}$, by Lemma 2.2 we have

$$R([1,0,7],16n+8)=\frac{1}{2}R([1,0,7],8)R([1,0,7],2n+1)=2R([1,0,7],2n+1).$$

Thus, if $R([1,0,7],2n+1)=0$, then $R([1,0,7],8(2n+1))=0$ and so $\lambda(1,7;2n+1)=0$. Hence the result is true in this case. Now assume that $2n+1=x^2+7y^2$ with $x,y\in\mathbb{Z}$. Then $16n+8=8(x^2+7y^2)=(x+7y)^2+7(x-y)^2$. As $R([1,0,7],16n+8)=2R([1,0,7],2n+1)$ we see that all the integral solutions to the equation $16n+8=X^2+7Y^2$ are given by $\{x+7y,x-y\},\{x+7y,-(x-y)\}$, where $\{x,y\}$ runs over all integral solutions to the equation $2n+1=x^2+7y^2$. Hence, using Lemmas 2.5, 5.1 and the fact $x+7y\equiv x-y \pmod 4$ we deduce

$$\begin{aligned}\lambda(1,7;2n+1)&=\sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ X^2+7Y^2=16n+8}} XY=\sum_{\substack{x,y\in\mathbb{Z},x+7y\equiv 1 \pmod 4\\ x^2+7y^2=2n+1}}(x+7y)(x-y)\\ &=\frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+7y^2=2n+1}}(x^2-7y^2).\end{aligned}$$

This completes the proof.

Theorem 5.2. *For $n\in\mathbb{N}$ we have*

$$\lambda(1,15;4n+1)=\lambda(3,5;2n+1)=\frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+15y^2=2n+1}}(x^2-15y^2).$$

Proof. It is clear that

$$R([3,0,5],8)=4,\ R([1,0,15],8)=0,\ R([1,0,15],16)=6 \quad\text{and}\quad R([3,0,5],16)=0.$$

As $H(-60)=\{[1,0,15],[3,0,5]\}$, by Lemma 2.2 and the above we have

$$2R([3,0,5],8(2n+1))$$

$$= R([3,0,5],8)R([1,0,15],2n+1) + R([1,0,15],8)R([3,0,5],2n+1)$$
$$= 4R([1,0,15],2n+1)$$

and

$$\begin{aligned}&2R([1,0,15],16(2n+1))\\ &= R([1,0,15],16)R([1,0,15],2n+1) + R([3,0,5],16)R([3,0,5],2n+1)\\ &= 6R([1,0,15],2n+1).\end{aligned}$$

From Lemma 2.5 we have

$$\lambda(1,15;4n+1) = \sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ X^2+15Y^2=16(2n+1)}} XY, \quad \lambda(3,5;2n+1) = \sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ 3X^2+5Y^2=8(2n+1)}} XY.$$

Thus, if $R([1,0,15],2n+1) = 0$, then $R([1,0,15],16(2n+1)) = R([3,0,5],8(2n+1)) = 0$ and so $\lambda(1,15;4n+1) = \lambda(3,5;2n+1) = 0$. Hence the result is true in this case.

Now assume that $2n+1 = x^2+15y^2$ with $x,y \in \mathbb{Z}$. Then $16(2n+1) = (4x)^2+15(4y)^2 = (x+15y)^2+15(x-y)^2$ and $8(2n+1) = 3(x+5y)^2+5(x-3y)^2$. Since $R([3,0,5],8(2n+1)) = 2R([1,0,15],2n+1)$ and $R([1,0,15],16(2n+1)) = 3R([1,0,15],2n+1)$, we see that all the integral solutions to the equation $3X^2+5Y^2 = 8(2n+1)$ are given by $\{x+5y, \pm(x-3y)\}$, and all the integral solutions to the equation $X^2+15Y^2 = 16(2n+1)$ are given by $\{4x,4y\}$ and $\{x+15y, \pm(x-y)\}$, where $\{x,y\}$ runs over all integral solutions to the equation $2n+1 = x^2+15y^2$. As $x+5y \equiv x-3y \equiv \pm 1 \pmod 4$ and $x+15y \equiv x-y \equiv \pm 1 \pmod 4$, from the above and Lemma 5.1 we deduce

$$\begin{aligned}\lambda(1,15;4n+1) &= \sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ X^2+15Y^2=16(2n+1)}} XY = \sum_{\substack{x,y\in\mathbb{Z},x+15y\equiv 1 \pmod 4\\ x^2+15y^2=2n+1}} (x+15y)(x-y)\\ &= \frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+15y^2=2n+1}} (x^2-15y^2)\end{aligned}$$

and

$$\begin{aligned}\lambda(3,5;2n+1) &= \sum_{\substack{X,Y\in\mathbb{Z},X\equiv Y\equiv 1 \pmod 4\\ 3X^2+5Y^2=8(2n+1)}} XY = \sum_{\substack{x,y\in\mathbb{Z},x+5y\equiv 1 \pmod 4\\ x^2+15y^2=2n+1}} (x+5y)(x-3y)\\ &= \frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+15y^2=2n+1}} (x^2-15y^2).\end{aligned}$$

This proves the theorem.

Theorem 5.3. *Let $p > 5$ be a prime. Then*

$$\lambda(3,5;p)=\begin{cases}0 & \text{if } p\not\equiv 1,19 \pmod{30},\\ 4x^2-2p & \text{if } p\equiv 1,19 \pmod{30} \text{ and so } p=x^2+15y^2 (x,y\in\mathbb{Z}),\end{cases}$$

$$\lambda(3,5;2p)=\begin{cases}0 & \text{if } p\not\equiv 17,23 \pmod{30},\\ 2p-12x^2 & \text{if } p\equiv 17,23 \pmod{30} \text{ and so } p=3x^2+5y^2 (x,y\in\mathbb{Z}),\end{cases}$$

$$\lambda(3,5;3p)=\begin{cases}0 & \text{if } p\not\equiv 17,23 \pmod{30},\\ 36x^2-6p & \text{if } p\equiv 17,23 \pmod{30} \text{ and so } p=3x^2+5y^2 (x,y\in\mathbb{Z}),\end{cases}$$

$$\lambda(3,5;5p)=\begin{cases}0 & \text{if } p\not\equiv 17,23 \pmod{30},\\ 10p-60x^2 & \text{if } p\equiv 17,23 \pmod{30} \text{ and so } p=3x^2+5y^2 (x,y\in\mathbb{Z}).\end{cases}$$

Proof. If $p \equiv 1, 19 \pmod{30}$, then $p = x^2 + 15y^2$ for some positive integers x and y (see [14, Table 9.1]). By Lemma 2.1, x and y are unique. From Theorem 5.2 we have

$$\lambda(3,5;p)=\frac{1}{2}\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+15y^2=p}}(x^2-15y^2)=2(x^2-15y^2)=4x^2-2p.$$

If $p \not\equiv 1, 19 \pmod{30}$, then p is not represented by x^2+15y^2. Thus, by Theorem 5.2 we have $\lambda(3, 5; p) = 0$.

If $p \equiv 17, 23 \pmod{30}$, then $p = 3x^2 + 5y^2$ with $x, y \in \mathbb{Z}$ (see [14, Table 9.1]). Taking $a = 3$ and $b = 5$ in Theorem 3.1 we obtain $\lambda(3, 5; 2p) = 2p - 12x^2$. If $p \not\equiv 17, 23 \pmod{30}$, as $R([3, 0, 5], 16) = R([3, 0, 5], p) = 0$, using Lemma 2.2 we see that $2R([3, 0, 5], 16p) = R([3, 0, 5], 16)R([1, 0, 15], p) + R([1, 0, 15], 16)R([3, 0, 5], p) = 0$. Thus, appealing to Lemma 2.5 we have $\lambda(3, 5; 2p) = 0$.

Let $b \in \{3, 5\}$. By Theorem 5.2 we have

$$\lambda(3,5;bp)=\frac{1}{2}\sum_{\substack{X,Y\in\mathbb{Z}\\ X^2+15Y^2=bp}}(X^2-15Y^2).$$

As $H(-60) = \{[1, 0, 15], [3, 0, 5]\}$, $R([1, 0, 15], b) = 0$ and $R([3, 0, 5], b) = 2$, using Lemma 2.2 we see that

$$\begin{aligned}R([1,0,15],bp)&=\frac{1}{2}(R([1,0,15],b)R([1,0,15],p)+R([3,0,5],b)R([3,0,5],p))\\ &=R([3,0,5],p).\end{aligned}$$

If $p \not\equiv 17, 23 \pmod{30}$, then $R([1, 0, 15], bp) = R([3, 0, 5], p) = 0$ and so $\lambda(3, 5; bp) = 0$. If $p \equiv 17, 23 \pmod{30}$, then there are unique positive integers x and y such that $p = 3x^2 + 5y^2$. As $R([1, 0, 15], bp) = R([3, 0, 5], p) = 4$, we see that all the integral solutions to $3p = X^2+15Y^2$ are given by $\{\pm 3x, \pm y\}$, and all the integral solutions to $5p = X^2 + 15Y^2$ are given by $\{\pm 5y, \pm x\}$. Thus,

$$\lambda(3,5;3p)=\frac{1}{2}\sum_{\substack{X,Y\in\mathbb{Z}\\ X^2+15Y^2=3p}}(X^2-15Y^2)=2((3x)^2-15y^2)=36x^2-6p$$

and

$$\lambda(3,5;5p)=\frac{1}{2}\sum_{\substack{X,Y\in\mathbb{Z}\\ X^2+15Y^2=5p}}(X^2-15Y^2)=2((5y)^2-15x^2)=10p-60x^2.$$

This completes the proof.

References

[1] A. Alaca, S. Alaca, M. F. Lemire, K. S. Williams, Jacobi's identity and representations of integers by certain quaternary quadratic forms, Int. J. Mod. Math. 2(2007) 143-176.

[2] G.E. Andrews, R. Askey, R. Roy, Special Functions, Cambridge Univ. Press, UK, 1999, p.500

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

[4] D.A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Wiley, New York, Chichester, 1989.

[5] E. Hecke, Mathematische Werke, Vandenhocck and Ruprecht, 1959.

[6] F. Klein, R. Fricke, Vorlesungen uber die Theorie der elliptischen Modulfunktionen, (Vols. 1, 2), Teubner, Leipzig, 1892.

[7] J. Liouville, Sur la forme $x^2 + y^2 + z^2 + 16t^2$, J. Math. Pures Appl. 7(1862) 165-168.

[8] L.J. Mordell, On Mr Ramanujan's empirical expansions of modular functions, Proc. Cambridge Philos. Soc. 19(1917) 117-124.

[9] S. Ramanujan, The Lost Notebook and Other Unpublished Papers, Narosa, New Delhi, 1988.

[10] S.S. Rangachari, Ramanujan and Dirichlet series with Euler products, Proc. Indian. Acad. Sci. (Math. Sci.) 91(1982) 1-15.

[11] J. Stienstra, F. Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, Math. Ann. 271(1985) 269-304.

[12] Z.H. Sun, On the properties of Newton-Euler pairs, J. Number Theory 114(2005) 88-123.

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

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