Binary quadratic forms and sums of triangular numbers

Zhi-Hong Sun(孙智宏)
Huaiyin Normal University
http://www.hytc.edu.cn/xsjl/szh

Notation: $\mathbb{Z}$—the set of integers, $\mathbb{N}$—the set of positive integers, $[x]$— the greatest integer not exceeding x, $(\frac{a}{m})$—the Legendre-Jacobi-Kronecker symbol, $\text{ord}_p m$—the nonnegative integer α such that $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$, (a,b)—the greatest common divisor of a and b, (a,b,c)—the form $ax^2+bxy+cy^2$, $[a,b,c]$—the equivalence class containing the form (a,b,c), $H(d)$—the form class group of discriminant d, $h(d)$—the class number of discriminant d, $R(K,n)$—the number of representations of n by the class K.

My papers on the topic:

[SW1] 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.

[SW2] Z.H. Sun and K.S. Williams, Ramanujan identities and Euler products for a type of Dirichlet series, Acta Arith. 122(2006), 349-393.

[S1] Z.H. Sun, The expansion of $\prod_{k=1}^{\infty}(1-q^{ak})(1-q^{bk})$, Acta Arith. 134(2008), 11-29.

[S2] Z.H. Sun, On the number of representations of n by $ax(x-1)/2+by(y-1)/2$, J. Number Theory 129(2009), 971-989.

[S3] Z.H. Sun, Binary quadratic forms and sums of triangular numbers, Acta Arith. 146(2011), 257-297.

[S4] Z.H. Sun, On the number of representations of n by $ax^2+by(y-1)/2$, $ax^2+by(3y-1)/2$ and $ax(x-1)/2+by(3y-1)/2$, Acta Arith. 147(2011), 81-100.

[S5] Z.H. Sun, Constructing x^2 for primes $p=ax^2+by^2$, Advan. in Appl. Math. 48(2012), 106-120.

§1. Basic concepts of binary quadratic forms

A nonsquare integer d with $d \equiv 0, 1 \pmod 4$ is called a **discriminant**. For $a, b, c \in \mathbb{Z}$, $ax^2 + bxy + cy^2 = (a, b, c)$ is called a binary quadratic form with discriminant $d = b^2 - 4ac$. If $\gcd(a, b, c) = 1$, we say that the form $(a, b, c) = ax^2 + bxy + cy^2$ is **primitive**.

Suppose $a, b, c \in \mathbb{Z}$, $a, c > 0$ and $d = b^2 - 4ac < 0$. If $-a < b \le a < c$ or $0 \le b \le a = c$, we say that (a, b, c) is a **reduced form**. The number of primitive reduced forms with discriminant $d < 0$ is called the **class number** of discriminant d. We denote it by $h(d)$.

Let $d < 0$ be a discriminant. It is well known that
$h(d) = 1 \iff d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$ (13 numbers),

and
$h(d)=2 \iff d=-15,-20,-24,-32,-35,-36,$
$-40,-48,-51,-52,-60,-64,-72,-75,-88,-91,$
$-99,-100,-112,-115,-123,-147,-148,-187,$
$-232,-235,-267,-403,-427.$ (29 numbers)

Let p be an odd prime. By the theory of binary quadratic forms, there are unique positive integers x and y such that

$$
\begin{aligned}
&p=4k+1=x^2+4y^2,\\
&p=8k+1,3=x^2+2y^2,\\
&p=3k+1=x^2+3y^2=(L^2+27M^2)/4,\\
&p=20k+1,9=x^2+5y^2,\\
&p=24k+1,7=x^2+6y^2,\\
&p=7k+1,2,4=x^2+7y^2,\\
&p=40k+1,9,11,19=x^2+10y^2,\\
&p=30k+1,19=x^2+15y^2.
\end{aligned}
$$

Let $ax^2+bxy+cy^2$ be a primitive reduced form with $h(b^2-4ac)=1$ or 2. By genus theory, those primes p represented by $ax^2+bxy+cy^2$ can be characterized by congruence conditions.

Two forms (a, b, c) and (a', b', c') are **equivalent** ($(a, b, c) \sim (a', b', c')$) if and only if there exist integers α, β, γ and δ with $\alpha\delta - \beta\gamma = 1$ such that the substitution $x = \alpha X + \beta Y,\ y = \gamma X + \delta Y$ transforms (a, b, c) to (a', b', c'). The substitutions $x = Y,\ y = -X$ and $x = X + kY,\ y = Y$ imply

$$(a, b, c) \sim (c, -b, a) \sim (a, 2ak + b, ak^2 + bk + c).$$

We denote the **equivalence class** of (a, b, c) by $[a, b, c]$. If $(a, b, c) \sim (a', b', c')$, it is easy to see that $\gcd(a, b, c) = \gcd(a', b', c')$. Thus, (a, b, c) is primitive if and only if (a', b', c') is primitive. It is also known that equivalent forms have the same discriminant. The equivalence classes of primitive, integral, binary quadratic forms of discriminant d form a finite abelian group under Gaussian composition, called the **form class group**. We denote this group by $H(d)$ and its order is $h(d)$.

Lagrange: Every (primitive) form of discriminant $d < 0$ is equivalent to exactly one (primitive) reduced form of discriminant d.

Lagrange: If $(a,b,c) \sim (a',b',c')$, then n is represented by (a,b,c) if and only if n is represented by (a',b',c').

Gauss: If $(a,b,c) \sim (a',b',c')$, then

$$|\{(x,y) \in \mathbb{Z}^2 : n = ax^2 + bxy + cy^2\}|$$
$$= \{(x,y) \in \mathbb{Z}^2 : n = a'x^2 + b'xy + c'y^2\}|.$$

For $a,b,c \in \mathbb{Z}$ with $a,c > 0$ and $b^2 - 4ac < 0$ we define

$$R([a,b,c],n) = |\{(x,y) \in \mathbb{Z}^2 : n = ax^2 + bxy + cy^2\}|,$$
$$R'([a,b,c],n)$$
$$= |\{(x,y) \in \mathbb{Z}^2 : n = ax^2 + bxy + cy^2, (x,y) = 1\}|.$$

Since $[a,b,c]^{-1} = [a,-b,c]$, for $K \in H(d)$ we have $R(K,n) = R(K^{-1},n)$. If $R(K,n) > 0$, we say that n is represented by K.

Theorem 1.1. *Let d be a discriminant, $n \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}$ with $b^2 - 4ac = d$. Then*

$$R([a,b,c],n) = \sum_{m \in \mathbb{N}, m^2 | n} R'\Big([a,b,c], \frac{n}{m^2}\Big)$$

and

$$R'([a,b,c],n) = \sum_{m\in\mathbb{N}, m^2|n} \mu(m) R\Big([a,b,c], \frac{n}{m^2}\Big),$$

where $\mu(n)$ is the Möbius function.

§2. **Formulas for** $N(n,d)$

For a discriminant d the **conductor** of d is the largest positive integer $f = f(d)$ such that $d/f^2 \equiv 0, 1 \pmod 4$. If $f(d) = 1$, we say that d is a **fundamental discriminant**.

For discriminant $d < 0$ let

$$w(d) = \begin{cases} 2 & \text{if } d < -4, \\ 4 & \text{if } d = -4, \\ 6 & \text{if } d = -3. \end{cases}$$

For $n \in \mathbb{N}$ and discriminant $d < 0$ define

$$N(n,d) = \sum_{K\in H(d)} R(K,n).$$

Let $d < 0$ be a discriminant with conductor f. Let $d_0 = d/f^2$ and $n \in \mathbb{N}$. When $(n, d) = 1$, Dirichlet proved the following formula for $N(n, d)$:

$$N(n,d) = w(d) \sum_{k|n} \left(\frac{d_0}{k}\right). \tag{2.1}$$

In 1997 Kaplan and Williams showed that this is also true under the weaker condition $(n, f) = 1$. Taking $n = 1$ in (2.1) we find $N(1, d) = w(d)$.

Sun and Williams obtained the complete formula for $N(n, d)$, which improved the Huard-Kaplan-Williams formula.

Theorem 2.1 ([SW1, 2006]). *Let d be a discriminant with conductor f. Let $d_0 = d/f^2$ and $n \in \mathbb{N}$. If (n, f^2) is not a square, then $N(n,d) = 0$. If $(n, f^2) = m^2$ for $m \in \mathbb{N}$, then*

$$\frac{N(n,d)}{w(d)} = m \prod_{p|m} \left(1 - \frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\right) \cdot \sum_{k|\frac{n}{m^2}} \left(\frac{d_0}{k}\right)$$

$$= \prod_{(\frac{d_0}{p})=-1} \frac{1 + (-1)^{\mathrm{ord}_p n}}{2}$$

$$\times\, m \prod_{p|m} \left(1 - \frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\right)$$

$$\times \prod_{(\frac{d_0}{p})=1} \left(1 + \mathrm{ord}_p \frac{n}{m^2}\right),$$

where in the products p runs over all distinct primes.

When $h(d) = 1$,

$$N(n,d) = \begin{cases} R([1,0,-\frac{d}{4}],n) & \text{if } 2 \mid d, \\ R([1,1,\frac{1-d}{4}],n) & \text{if } 2 \nmid d. \end{cases}$$

Example 2.1: $d = -28$, $f = 2$, $d_0 = -7$, $h(d) = 1$,

$$\begin{aligned} R([1,0,7],n) &= N(n,-28) \\ &= \begin{cases} 0 & \text{if } 4 \mid n-2, \\ 2\sum_{k|n}(\frac{-7}{k}) & \text{if } 2 \nmid n, \\ 2\sum_{k|\frac{n}{4}}(\frac{-7}{k}) & \text{if } 4 \mid n. \end{cases} \end{aligned}$$

If for any $n_1, n_2 \in \mathbb{N}$ with $(n_1, n_2) = 1$, we have $f(n_1 n_2) = f(n_1)f(n_2)$, we say that $f(n)$ is a multiplicative function.

Theorem 2.2 ([SW1, 2006]). *Let d be a discriminant. Then $N(n,d)/w(d)$ is a multiplicative function of $n \in \mathbb{N}$.*

Theorem 2.3 ([SW1]). *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let s be a complex number with $Re(s) > 1$. Then the Dirichlet series $\sum_{n=1}^{\infty} \frac{N(n,d)/w(d)}{n^s}$ converges absolutely and*

$$\sum_{n=1}^{\infty} \frac{N(n,d)/w(d)}{n^s}$$

$$= \prod_{p|f} \left(\frac{1 - p^{\alpha_p(1-2s)}}{1 - p^{1-2s}} + \frac{p^{\alpha_p(1-2s)}(1 - \frac{1}{p}(\frac{d_0}{p}))}{(1 - p^{-s})(1 - (\frac{d_0}{p})p^{-s})} \right)$$

$$\times \prod_{p \nmid f} \frac{1}{(1 - p^{-s})(1 - (\frac{d_0}{p})p^{-s})},$$

where p runs over all primes and $\alpha_p = \mathrm{ord}_p f$.

Example 2.2:

$$\sum_{n=1}^{\infty} \frac{\frac{1}{2}R([1,0,7],n)}{n^s}$$
$$= \frac{1-2^{1-s}+2^{1-2s}}{(1-2^{-s})^2} \cdot \frac{1}{1-7^{-s}}$$
$$\times \prod_{p\equiv 1,9,11 \pmod{14}} \frac{1}{(1-p^{-s})^2}$$
$$\times \prod_{p\equiv 3,5,13 \pmod{14}} \frac{1}{1-p^{-2s}},$$

where p runs over all primes satisfying the condition under the product.

§3. Formulas for $R(K,p^t)$ and $R'(K,p^t)$

Theorem 3.1 ([SW1]. *Let d be a discriminant with conductor f, and let p be a prime such that $p \nmid f$. Let t be a nonnegative integer and $K \in H(d)$. Let I be the identity in $H(d)$.*

(i) If $(\frac{d}{p}) = -1$, then

$$R(K, p^t) = \begin{cases} w(d) & \text{if } 2 \mid t \text{ and } K = I, \\ 0 & \text{otherwise.} \end{cases} .$$

(ii) If $p \mid d$, then

$$R(K, p^t)$$
$$= \begin{cases} w(d) & \text{if } 2 \mid t \text{ and } K = I, \\ & \quad \text{or if } 2 \nmid t \text{ and } p \text{ is represented by } K, \\ 0 & \text{otherwise.} \end{cases}$$

(iii) Suppose $(\frac{d}{p}) = 1$ so that p is only represented by some class A and the inverse A^{-1} in $H(d)$. Let m be the order of A in $H(d)$. If K is not a power of A, then $R(K, p^t) = 0$. If $k, t_0 \in \{0, 1, \ldots, m-1\}$ with $t_0 \equiv t \pmod{m}$, then

$$R(A^k,p^t)$$
$$= \begin{cases} 0 & \text{if } 2 \mid m \text{ and } 2 \nmid k-t, \\ w(d)\Big(\Big[\dfrac{t}{m/(2,m)}\Big]+1\Big) & \text{if } t_0 \in S_{k,m}, \\ w(d)\Big[\dfrac{t}{m/(2,m)}\Big] & \text{otherwise,} \end{cases}$$

where

$$S_{k,m} = \begin{cases} \{r \mid k \le r < m,\ 2 \mid k-r\} \\ \quad \cup\{r \mid m-k \le r < m,\ 2 \nmid k-r\} \\ \qquad\qquad\qquad \text{if } 2 \nmid m, \\ \{r \mid \min\{k,m-k\} \le r < \dfrac{m}{2},\ 2 \mid k-r\} \\ \quad \cup\{r \mid \max\{k,m-k\} \le r < m,\ 2 \mid k-r\} \\ \qquad\qquad\qquad \text{if } 2 \mid m. \end{cases}$$

Theorem 3.2 ([SW1]). *Let d be a discriminant with conductor f. Let $K \in H(d)$ and $t \in \mathbb{N}$. Let p be a prime such that $p \nmid f$.*

(i) *If $(\frac{d}{p}) = -1$, then $R'(K,p^t) = 0$.*

(ii) If $(\frac{d}{p}) = 0$, then p is represented by unique $A \in H(d)$ and we have

$$R'(K, p^t) = \begin{cases} w(d) & \text{if } t = 1 \text{ and } K = A, \\ 0 & \text{otherwise.} \end{cases}$$

(iii) If $(\frac{d}{p}) = 1$, then p is represented by some $A \in H(d)$ and we have

$$R'(K, p^t) \\ = \begin{cases} 0 & \text{if } K \neq A^t, A^{-t}, \\ w(d) & \text{if } K \in \{A^t, A^{-t}\} \text{ and } A^t \neq A^{-t}, \\ 2w(d) & \text{if } K = A^t = A^{-t}. \end{cases}$$

Theorem 3.3 ([SW1]) Let d be a discriminant with conductor f. Let p be a prime such that $(\frac{d}{p}) = 0, 1$ and $p \nmid f$. Then p is represented by some class $A \in H(d)$. For $t \in \mathbb{N}$ and $K \in H(d)$ we have

$$R(K, p^{t+1}) + R(K, p^{t-1}) = R(AK, p^t) + R(A^{-1}K, p^t).$$

§4. Multiplicative functions involving $R(K, n)$

Theorem 4.1 ([SW1]). *Let d be a discriminant. If $n_1, n_2, \ldots, n_r (r \geq 2)$ are pairwise prime positive integers and $K \in H(d)$, then*

$$R(K, n_1 n_2 \cdots n_r) = \frac{1}{w(d)^{r-1}} \sum_{K_1 K_2 \cdots K_r = K} R(K_1, n_1) \cdots R(K_r, n_r)$$

and

$$R'(K, n_1 n_2 \cdots n_r) = \frac{1}{w(d)^{r-1}} \sum_{K_1 K_2 \cdots K_r = K} R'(K_1, n_1) \cdots R'(K_r, n_r),$$

where the summations are taken over all $K_1, \ldots, K_r \in H(d)$ such that $K_1 K_2 \cdots K_r = K$.

Example 4.1 If $(n_1, n_2) = 1$ and $K \in H(d)$, then

$$R(K, n_1 n_2) = \frac{1}{w(d)} \sum_{A \in H(d)} R(A, n_1) R(A^{-1} K, n_2).$$

Definition 4.1. *Let d be a discriminant and $n \in \mathbb{N}$. Let $H(d) = \{A_1^{k_1} \cdots \ A_r^{k_r} \mid 0 \le k_1 < h_1, \ldots, 0 \le k_r < h_r\}$ with $h_1 \cdots h_r = h(d)$. For $K = A_1^{k_1} \cdots A_r^{k_r} \in H(d)$ and $M = A_1^{m_1} \cdots A_r^{m_r} \in H(d)$ we define*

$$[K, M] = \frac{k_1 m_1}{h_1} + \cdots + \frac{k_r m_r}{h_r}$$

and

$$F(M, n) = \frac{1}{w(d)} \sum_{K \in H(d)} \cos 2\pi [K, M] \cdot R(K, n).$$

Theorem 4.2. *Let d be a discriminant and $n \in \mathbb{N}$.*

(i) *If $M \in H(d)$, then $F(M, n)$ is a multiplicative function of n.*

(ii) *If $K \in H(d)$, then*

$$R(K, n) = \frac{w(d)}{h(d)} \sum_{M \in H(d)} \cos 2\pi [K, M] \cdot F(M, n).$$

Theorem 4.3 ([SW1]). *Let d be a discriminant such that $H(d)$ is cyclic and $2 \leq h(d) \leq 6$ ($h(d) \in \{2,3,5,6\}$ implies $H(d)$ is cyclic). Let I be the principal class in $H(d)$. Let A be a generator of $H(d)$ and $n \in \mathbb{N}$. Recall that $w(d) = 1$ or 2 according as $d > 0$ or $d < 0$.*

(i) *If $h(d) = 2, 3$, then $F(A,n) = (R(I,n) - R(A,n))/w(d)$ is a multiplicative function of n.*

(ii) *If $h(d) = 4$, then*

$$F(A,n) = (R(I,n) - R(A^2,n))/w(d),$$
$$F(A^2,n) = (R(I,n) + R(A^2,n) - 2R(A,n))/w(d)$$

are multiplicative functions of n.

(iii) If $h(d) = 5$, then

$$F(A,n)$$
$$= (R(I,n) + \frac{\sqrt{5}-1}{2}R(A,n) - \frac{\sqrt{5}+1}{2}R(A^2,n))\Big/w(d),$$
$$F(A^2,n)$$
$$= (R(I,n) - \frac{\sqrt{5}+1}{2}R(A,n) + \frac{\sqrt{5}-1}{2}R(A^2,n))\Big/w(d)$$

are multiplicative functions of n.

(iv) If $h(d) = 6$, then

$$F(A,n)$$
$$= (R(I,n) + R(A,n) - R(A^2,n) - R(A^3,n))/w(d),$$
$$F(A^2,n)$$
$$= (R(I,n) - R(A,n) - R(A^2,n) + R(A^3,n))/w(d),$$
$$F(A^3,n)$$
$$= (R(I,n) - 2R(A,n) + 2R(A^2,n) - R(A^3,n))/w(d)$$

are multiplicative functions of n.

§5. Formulas for $F(A,p^t)$ when $h(d)=2,3,4$

For $K \in H(d)$ define $R(K) = \{n \in \mathbb{N} : \ R(K,n) > 0\}$. Thus, $n \in R(K)$ if and only if $R(K,n) > 0$.

Theorem 5.1 Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $h(d) = 2$ and $H(d) = \{I, A\}$ with $A^2 = I$. For $n \in \mathbb{N}$ let $F(A,n) = \frac{1}{w(d)}(R(I,n) - R(A,n))$. Let p be a prime and let t be a nonnegative integer. If $p \nmid f$, then

$$F(A,p^t) = \begin{cases} \dfrac{1}{2}(1+(-1)^t) & \text{if } (\frac{d_0}{p}) = -1, \\ 1 & \text{if } p \mid d_0 \text{ and } p \in R(I), \\ (-1)^t & \text{if } p \mid d_0 \text{ and } p \in R(A), \\ t+1 & \text{if } p \nmid d_0 \text{ and } p \in R(I), \\ (-1)^t(t+1) & \text{if } p \nmid d_0 \text{ and } p \in R(A). \end{cases}$$

Theorem 5.2 Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $h(d) = 3$ and $H(d) = \{I, A, A^2\}$ with $A^3 = I$. For $n \in \mathbb{N}$ let $F(A,n) = \frac{1}{w(d)}(R(I,n) - R(A,n))$. Let p be a prime and let t be a nonnegative integer.

If $p \nmid f$, then

$$F(A,p^t) = \begin{cases} 1 & \text{if } p \mid d_0, \\ \frac{1}{2}(1+(-1)^t) & \text{if } (\frac{d_0}{p}) = -1, \\ t+1 & \text{if } p \nmid d_0 \text{ and } p \in R(I), \\ -1 & \text{if } p \in R(A) \text{ and } 3 \mid t-1, \\ 0 & \text{if } p \in R(A) \text{ and } 3 \mid t-2, \\ 1 & \text{if } p \in R(A) \text{ and } 3 \mid t. \end{cases}$$

Theorem 5.3 Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $h(d) = 4$ and $H(d) = \{I, A, A^2, A^3\}$ with $A^4 = I$. Let $F(A,n) = \frac{1}{w(d)}(R(I,n) - R(A^2,n))$ and $F(A^2,n) = \frac{1}{w(d)}(R(I,n) + R(A^2,n) - 2R(A,n))$ for $n \in \mathbb{N}$. Let p be a prime such that $p \nmid f$ and let t be a nonnegative integer. Then

$$F(A,p^t) = \begin{cases} \dfrac{1+(-1)^t}{2} & \text{if } (\frac{d_0}{p}) = -1, \\ 1 & \text{if } p \mid d_0 \text{ and } p \in R(I), \\ t+1 & \text{if } p \nmid d_0 \text{ and } p \in R(I), \\ (-1)^t & \text{if } p \mid d_0 \text{ and } p \in R(A^2), \\ (-1)^t(t+1) & \text{if } p \nmid d_0 \text{ and } p \in R(A^2), \\ (-1)^{t/2} & \text{if } p \in R(A) \text{ and } 2 \mid t, \\ 0 & \text{if } p \in R(A) \text{ and } 2 \nmid t \end{cases}$$

and

$$F(A^2,p^t) = \begin{cases} \dfrac{1+(-1)^t}{2} & \text{if } (\frac{d_0}{p}) = -1, \\ 1 & \text{if } p \mid d_0, \\ t+1 & \text{if } p \nmid d_0 \text{ and } p \in R(I) \cup R(A^2), \\ (-1)^t(t+1) & \text{if } p \in R(A). \end{cases}$$

§6. **The method of determining** $R(K,n)$

If $n = p_1^{t_1} \cdots p_r^{t_r}$ is the standard factorization of n, then for $K \in H(d)$,

$$F(K,n) = F(K,p_1^{t_1}) \cdots F(K,p_r^{t_r}).$$

Hence, by Theorems 5.1-5.3 we can determine $R(K,n)$ for $K \in H(d)$, where $H(d)$ is cyclic and $h(d) = 2,3,4$.

Let d be a discriminant. If $H(d) = \{I, A\}$, then

$$\begin{cases} R(I,n) + R(A,n) = N(n,d), \\ R(I,n) - R(A,n) = w(d)F(A,n) \end{cases}$$

and so

$$R(I,n) = \frac{1}{2}(N(n,d) + w(d)F(A,n)),$$
$$R(A,n) = \frac{1}{2}(N(n,d) - w(d)F(A,n)).$$

If $H(d) = \{I, A, A^2\}$, then $R(A^2,n) = R(A^{-1},n) = R(A,n)$. We have

$$\begin{cases} R(I,n) + 2R(A,n) = N(n,d), \\ R(I,n) - R(A,n) = w(d)F(A,n) \end{cases}$$

and so

$$R(I,n) = \frac{1}{3}(N(n,d) + 2w(d)F(A,n)),$$
$$R(A,n) = \frac{1}{3}(N(n,d) - w(d)F(A,n)).$$

Similarly, if $H(d) = \{I, A, A^2, A^3\}$, then

$$R(I,n) = (F(I,n) + 2F(A,n) + F(A^2,n))w(d)/4,$$
$$R(A,n) = R(A^3,n) = (F(I,n) - F(A^2,n))w(d)/4,$$
$$R(A^2,n) = (F(I,n) - 2F(A,n) + F(A^2,n))w(d)/4,$$

where $F(I,n) = N(n,d)/w(d)$.

Let d be a discriminant and $H^2(d) = \{K^2 : K \in H(d)\}$. Then

$$|H^2(d)| = 1 \iff H(d) \cong C_2 \times \cdots \times C_2,$$

where C_2 is a cyclic group of order 2.

Theorem 6.1 ([S3]). *Let $d < 0$ be a discriminant with conductor f, $d_0 = d/f^2$ and $|H^2(d)| = 1$. Let $K \in H(d)$ and $n \in \mathbb{N}$ with $R(K, n) > 0$. Then $(n, f^2) = m^2$ for some $m \in \mathbb{N}$ and*

$$R(K,n) = w\Big(\frac{d}{m^2}\Big) \prod_{(\frac{d_0}{p})=1} (1 + \mathrm{ord}_p \frac{n}{m^2}).$$

related reference: N. A. Hall, The number of representations function for binary quadratic forms, Amer. J. Math. 62 (1940), 589-598.

Euler called a positive integer n a convenient number if it satisfies the following criterion: *Let m be an odd number such that $(m, n) = 1$ and $m = x^2 + ny^2$ with $(x, y) = 1$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime.*

Euler listed 65 convenient numbers as follows:

$1, 2, 3, 4, 7 \quad h(-4n) = 1,$

$5, 6, 8, 9, 10, 12, 13, 15, 16, 18,$

$22, 25, 28, 37, 58 \quad h(-4n) = 2,$

$21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78,$

$85, 88, 93, 102, 112, 130, 133,$

$177, 190, 232, 253 \quad h(-4n) = 4,$

$105, 120, 165, 168, 210, 240, 273, 280, 312, 330,$

$345, 357, 385, 408, 462, 520, 760 \quad h(-4n) = 8,$

$840, 1320, 1365, 1848 \quad h(-4n) = 16.$

He was interested in convenient numbers because they helped him find large primes. Gauss observed that a positive integer n is a convenient number if and only if $|H^2(-4n)| = 1$. In 1973 it was known that Euler's list is complete except for possibly one more n.

§7. Formulas for $t_n(a,b)$

triangular numbers: $\frac{x(x-1)}{2} = \binom{x}{2}$ $(x \in \mathbb{Z})$

For $a, b, n \in \mathbb{N}$ let

$$t_n(a,b) = \Big|\{\langle x,y\rangle :\ n = ax(x-1)/2 + by(y-1)/2,\ x,y \in \mathbb{N}\}\Big|.$$

For our convenience we also define $t_0(a,b) = 1$ and $t_{-n}(a,b) = 0$ for $n \in \mathbb{N}$. Let

$$\psi(q) = \sum_{k=1}^{\infty} q^{k(k-1)/2} \quad (|q| < 1).$$

Then clearly

(7.1)

$$\psi(q^a)\psi(q^b) = 1 + \sum_{n=1}^{\infty} t_n(a,b)q^n \quad (|q| < 1).$$

Ramanujan conjectured and Berndt proved that

(7.2)

$$q\psi(q)\psi(q^7) = \sum_{n=1}^{\infty} \left(\frac{-28}{n}\right)\frac{q^n}{1-q^n}\ (|q| < 1),$$

where $(\frac{k}{m})$ is the Legendre-Jacobi-Kronecker symbol.

According to Berndt , (7.2) is of extreme interest, and it would appear to be very difficult to prove it without the addition theorem for elliptic integrals. By (7.1), (7.2) is equivalent to

$$t_n(1,7) = \sum_{k\mid n+1,\,2\nmid k} \left(\frac{k}{7}\right). \tag{7.3}$$

K.S. Williams and Z.H. Sun proved (7.3) and so (7.2) by using the theory of binary quadratic forms.

Theorem 7.1 ([S2, 2009]) Let $a, b, n \in \mathbb{N}$. Then

$$4t_n(a,b) = \begin{cases} R([a,a,\frac{a+b}{4}], 2n+\frac{a+b}{4}) \\ \quad -R([a,0,b], 2n+\frac{a+b}{4}) & \text{if } 4 \mid a+b, \\ R([2a,2a,\frac{a+b}{2}], 4n+\frac{a+b}{2}) & \text{if } 4 \mid a+b-2, \\ R([4a,4a,a+b], 8n+a+b) & \text{if } 2 \nmid a+b. \end{cases}$$

Theorem 7.2 ([S3,2011]. *Let* $a, b, n \in \mathbb{N}$.

(i) *If* $8 \nmid a$, $8 \nmid b$ *and* $4 \nmid (a+b)$, *then*

$$t_n(a,b) = \frac{1}{4} R([a,0,b], 8n+a+b).$$

(ii) *If* $2 \nmid a, 8 \mid b-4$ *and* $4 \mid (a+b/4)$, *then*

$$t_n(a,b) = \frac{1}{4} R([a,0,b/4], 8n+a+b).$$

Theorem 7.3 ([SW2, 2006]). *Let* $n \in \mathbb{N}$. *If* $n+1 = 3^\alpha n_0$ $(3 \nmid n_0)$, *then*

$$t_n(3,5) = \frac{1+(-1)^\alpha(\frac{n_0}{3})}{2} \sum_{k \mid n+1,\ 2 \nmid k} \left(\frac{k}{15}\right).$$

If $n+2 = 3^\alpha n_0$ $(3 \nmid n_0)$, *then*

$$t_n(1,15) = \frac{1-(-1)^\alpha(\frac{n_0}{3})}{2} \sum_{k \mid n+2,\ 2 \nmid k} \left(\frac{k}{15}\right).$$

Theorem 7.4 ([S2]) For $n \in \mathbb{N}$ and $b \in \{5, 13, 37\}$,

$$t_n(1, b) = \frac{1}{2} \sum_{k | 4n + \frac{b+1}{2}} (\frac{-b}{k}).$$

Theorem 7.5 ([S3]). *Let* $n \in \mathbb{N}$ *and* $b \in \{6, 10, 12, 22, 28, 58\}$.

(i) *If* $b \in \{6, 10, 22, 58\}$, *then*

$$t_n(1, b) = \frac{1}{2} \sum_{k | 8n + b + 1} \left(\frac{-b}{k}\right),$$

$$t_n(2, b/2) = \frac{1}{2} \sum_{k | 8n + 2 + \frac{b}{2}} \left(\frac{-b}{k}\right).$$

(ii) *If* $b \in \{12, 28\}$, *then*

$$t_n(1, b) = \frac{1}{2} \sum_{k | 8n + b + 1} \left(\frac{k}{b/4}\right),$$

$$t_n(4, b/4) = \frac{1}{2} \sum_{k | 8n + 4 + \frac{b}{4}} \left(\frac{k}{b/4}\right).$$

Theorem 7.6. *Let $n \in \mathbb{N}$. If $4n + 23 = 5^\alpha n_1 (5 \nmid n_1)$, then*

$$t_n(1,45) = \begin{cases} \frac{1}{2}\sum_{k\mid \frac{n_1}{9}} (-1)^{\frac{k-1}{2}} (\frac{k}{5}) \\ \quad \text{if } 9 \mid n-1 \text{ and } n_1 \equiv \pm 2 \pmod 5, \\ \frac{1}{2}\sum_{k\mid n_1} (-1)^{\frac{k-1}{2}} (\frac{k}{5}) \\ \quad \text{if } 3 \mid n \text{ and } n_1 \equiv \pm 2 \pmod 5, \\ 0 \qquad \text{otherwise.} \end{cases}$$

Theorem 7.7. *Let $n \in \mathbb{N}$, $a \in \{1,3\}$, $b \in \{7,11,19,31,59\}$ and $4n+(a+3b/a)/2 = 3^\beta n_0$ $(3 \nmid n_0)$. Then $t_n(a,3b/a) > 0$ if and only if $2 \mid \mathrm{ord}_q n_0$ for every prime q with $(\frac{-3b}{q}) = -1$ and*

$$n_0 \equiv \begin{cases} 1 \pmod 3 \\ \quad \text{if } b \in \{11,59\} \text{ and } \beta \equiv \frac{a+1}{2} \pmod 2, \\ 2 \pmod 3 \qquad \text{otherwise.} \end{cases}$$

Moreover, if $t_n(a,3b/a) > 0$, then $t_n(a,3b/a) = \frac{1}{2}\prod_{(\frac{-3b}{p})=1}(1+\mathrm{ord}_p n_0)$.

In [S2,S3], $t_n(a,b)$ was determined for 138 values of (a,b).

related references:

A. Berkovich and H. Yesilyurt, Ramanujan's identities and representation of integers by certain binary and quaternary quadratic forms, Ramanujan J. 20 (2009), 375-408.

M.D. Hirschhorn, The number of representations of a number by various forms, Discrete Math. 298(2005), 205-211.

§8. The expansion of $\prod_{k=1}^{\infty}(1-q^{ak})(1-q^{bk})$

Theorem 8.1 ([S1, 2008]). *Let $a, b \in \mathbb{N}$ and $q \in \mathbb{R}$ with $|q| < 1$. Then*

$$\prod_{k=1}^{\infty}(1-q^{ak})(1-q^{bk})$$
$$= 1 + \sum_{n=1}^{\infty} \frac{1}{2}\Big(R(a+b, 12(a-b), 36(a+b); 24n+a+b)$$
$$- R(4(a+b), 12(a-b), 9(a+b); 24n+a+b)\Big)q^n.$$

In the case $a+b=24$, the result was given in [SW2].

§9. Constructing x and x^2 for primes $p = ax^2 + by^2$

1. (Gauss, 1825; Cauchy proved) If $p \equiv 1 \pmod 4$ is a prime and $p = x^2 + y^2$ with $x \equiv 1 \pmod 4$, then

$$2x \equiv \binom{(p-1)/2}{(p-1)/4} \pmod{p}.$$

(Chowla, Dwork and Evans, 1986)

$$\binom{(p-1)/2}{(p-1)/4} \equiv \frac{2^{p-1}+1}{2}\left(2x - \frac{p}{2x}\right) \pmod{p^2}.$$

(Cosgrave, Dilcher, 2010)

$$\binom{(p-1)/2}{(p-1)/4}$$
$$\equiv \left(2x - \frac{p}{2x} - \frac{p^2}{8x^3}\right)$$
$$\times \left(1 + \frac{1}{2}pq_p(2) - \frac{1}{8}p^2(q_p(2)^2 - 2E_{p-3})\right) \pmod{p^3},$$

where $q_p(2) = (2^{p-1} - 1)/p$ and E_n is the Euler number.

2. (Jacobi, 1827) If $p \equiv 1 \pmod 3$ is a prime and $4p = L^2 + 27M^2$ with $L \equiv 1 \pmod 3$, then

$$L \equiv -\binom{2(p-1)/3}{(p-1)/3} \equiv \frac{1}{2}\binom{(p-1)/2}{(p-1)/6} \pmod p.$$

Gauss: $L \equiv (\frac{p-1}{3})!^{-3} \pmod p$.

(Evans, 1985, unpublished; Yeung, 1989, JNT)

$$\binom{2(p-1)/3}{(p-1)/3} \equiv -L + \frac{p}{L} \pmod{p^2}.$$

(Cosgrave, Dilcher, 2010)

$$\binom{2(p-1)/3}{(p-1)/3}$$
$$\equiv \Big(-L + \frac{p}{L} + \frac{p^2}{L^3}\Big)\Big(1 + \frac{1}{6}p^2 B_{p-2}(\tfrac{1}{3})\Big) \pmod{p^3}.$$

Z.H.Sun: Let $\{U_{2n}\}$ be given by $U_0 = 1$ and $U_{2n} = -2\sum_{k=0}^{n-1}\binom{2n}{2k}U_{2k} \quad (n \ge 1)$. Then $B_{p-2}(\frac{1}{3}) \equiv 6U_{p-3} \pmod p$.

3. (Stern, 1846) If $p \equiv 1 \pmod 8$ is a prime and so $p = x^2 + 2y^2$ with $x \equiv 1 \pmod 4$, then

$$2x \equiv (-1)^{\frac{p-1}{8}} \binom{\frac{p-1}{2}}{\frac{p-1}{8}} \pmod p.$$

4. (Eisenstein, 1848) If $p \equiv 3 \pmod 8$ is a prime and so $p = x^2 + 2y^2$ with $x \equiv 1 \pmod 4$, then

$$2x \equiv -(-1)^{\frac{p-3}{8}} \binom{\frac{p-1}{2}}{\frac{p-3}{8}} \pmod p.$$

5. (Cauchy) If $p \equiv 1 \pmod{20}$ is a prime and so $p = x^2 + 5y^2$, then

$$4x^2 \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{20}} \binom{\frac{p-1}{2}}{\frac{3(p-1)}{20}} \pmod p.$$

6. (Jacobi, 1827) If $p \equiv 1 \pmod 7$ is a prime and so $p = x^2 + 7y^2$ with $x \equiv 1 \pmod 7$, then

$$2x \equiv \binom{\frac{3(p-1)}{7}}{\frac{p-1}{7}} \pmod p.$$

7. (Eisenstein, 1848) If $p \equiv 2 \pmod 7$ is an odd prime and so $p = x^2 + 7y^2$ with $x \equiv 3 \pmod 7$, then

$$2x \equiv \binom{\frac{3(p-2)}{7}}{\frac{p-2}{7}} \pmod p.$$

8. (Eisenstein, 1848) If $p \equiv 4 \pmod 7$ is a prime and so $p = x^2 + 7y^2$ with $x \equiv 5 \pmod 7$, then

$$2x \equiv \binom{\frac{3(p-4)}{7}}{\frac{p-4}{7}} \pmod p.$$

9. Let $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ be a prime and so $4p = x^2 + 11y^2$.

(i) (Jacobi, 1827) If $p = 11n + 1$ and $x \equiv 2 \pmod{11}$, then

$$x \equiv \binom{3n}{n}\binom{6n}{3n}\Big/\binom{4n}{2n} \pmod{p}.$$

(ii) (Lee, 2002) If $p = 11n+3$ and $x \equiv 1 \pmod{11}$, then

$$x \equiv \binom{3n+1}{n}\binom{6n+1}{3n}\Big/\binom{4n+1}{2n} \pmod{p}.$$

(iii) (Lee, 2002) If $p = 11n+4$ and $x \equiv 7 \pmod{11}$, then

$$x \equiv \binom{3n+1}{n}\binom{6n+2}{3n}\Big/\binom{4n+1}{2n} \pmod{p}.$$

(iv) (Lee, 2002) If $p = 11n+5$ and $x \equiv 8 \pmod{11}$, then $x \equiv \binom{3n+1}{n}\binom{6n+2}{3n+1}\Big/\binom{4n+1}{2n} \pmod{p}$.

(v) (Lee, 2002) If $p = 11n+6$ and $x \equiv 5 \pmod{11}$, then $x \equiv \binom{3n+2}{n}\binom{6n+4}{3n+2}\Big/\binom{4n+3}{2n+1} \pmod{p}$.

10. (Z. H. Sun, 2011, Adv. in Appl. Math.) For $a, b, n \in \mathbb{N}$ let $\lambda(a, b; n) \in \mathbb{Z}$ be given by

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

(1) Suppose $2 \nmid ab$ and p is 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

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

(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 $n = (a + b)(p - 1)/8$. If $2 \nmid a$, $2 \mid b$, $8 \nmid b$ and $8 \mid p - 1$, then

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

In 1892 Klein and Fricke showed that

$$\lambda(1, 1; (p + 3)/4) = 4x^2 - 2p$$

for primes $\quad p = x^2 + y^2 \equiv 1 \pmod 4$ with $2 \nmid x$.

In his “lost” notebook Ramanujan conjectured that

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

In 1985 Stienstra and Beukers proved that

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

Example 9.1 Let $p > 5$ be a prime. Then

$$\lambda(1,2;(3p+5)/8) = (-1)^{\frac{y}{2}}(4x^2 - 2p) \quad \text{for } p = x^2 + 2y^2 \equiv 1 \pmod 8,$$

$$\lambda(1,5;(3p+1)/4) = (-1)^{x-1}(4x^2 - 2p) \quad \text{for } p = x^2 + 5y^2 \equiv 1,9 \pmod{20},$$

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

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

§10. **Ramanujan's conjectures on Euler products for a type of Dirichlet series**

For $k = 1, 2, \ldots, 12$ let

$$q \prod_{m=1}^{\infty} (1 - q^{km})(1 - q^{(24-k)m})$$
$$= \sum_{n=1}^{\infty} \phi_k(n) q^n \quad (|q| < 1).$$

Ramanujan conjectured that the Dirichlet series $\sum_{n=1}^{\infty} \frac{\phi_k(n)}{n^s}$ $(k = 1, 2, 3, 4, 6, 8, 12)$ have Euler products and gave the explicit Euler products in the cases $k = 1, 2, 3$. Unfortunately his formulae for $k = 2, 3$ are wrong. In 1982 Rangachari outlined the proofs of the formulae for $k = 1, 2, 3$ using class field theory and modular forms. But Rangachari's formulae for $k = 2, 3$ are also wrong and his proofs are neither clear nor elementary. So it remains to correct the results and to give elementary proofs of them.

Let $d < 0$ be a discriminant with $h(d) = 3$. Suppose that I is the principal class and A is a generator of $H(d)$. We recall that $F(A,n) = \frac{1}{2}(R(I,n) - R(A,n))$ is a multiplicative function of n. Define

$$L(A,s) = \sum_{n=1}^{\infty} \frac{F(A,n)}{n^s} \quad (Re(s) > 1).$$

Theorem 10.1 ([SW2]). *Let $d < 0$ be a discriminant with $h(d) = 3$. Let f be the conductor of d and $H(d) = \{I, A, A^2\}$ with $A^3 = I$. Let $s \in \mathbb{C}$ with $Re(s) > 1$. If $d \neq -92, -124$, then*

$$\begin{aligned} &L(A,s) \\ &= \prod_{\substack{p \mid d \\ p \nmid f}} \frac{1}{1 - p^{-s}} \prod_{(\frac{d}{p}) = -1} \frac{1}{1 - p^{-2s}} \\ &\quad \times \prod_{\substack{p \in R(I) \\ p \nmid d}} \frac{1}{(1 - p^{-s})^2} \prod_{\substack{p \in R(A) \\ p \nmid d}} \frac{1}{1 + p^{-s} + p^{-2s}}, \end{aligned}$$

where p runs over all primes.

Theorem 10.2. *Let $s \in \mathbb{C}$ with $Re(s) > 1$. Then $\phi_1(n), \phi_2(n), \phi_6(n)$ are multiplicative functions. Moreover,*

$$\sum_{n=1}^{\infty} \frac{\phi_1(n)}{n^s} = \frac{1}{1-23^{-s}} \prod_{(\frac{p}{23})=-1} \frac{1}{1-p^{-2s}} \times \prod_{p=2x^2+xy+3y^2} \frac{1}{1+p^{-s}+p^{-2s}} \times \prod_{p=x^2+xy+6y^2 \neq 23} \frac{1}{(1-p^{-s})^2},$$

$$\sum_{n=1}^{\infty} \frac{\phi_2(n)}{n^s} = \frac{1}{1-11^{-s}} \prod_{\substack{p \equiv 2,6,7,8,10 \pmod{11} \\ p \neq 2}} \frac{1}{1-p^{-2s}} \times \prod_{p=3x^2+2xy+4y^2} \frac{1}{1+p^{-s}+p^{-2s}} \times \prod_{p=x^2+11y^2 \neq 11} \frac{1}{(1-p^{-s})^2}$$

and

$$\sum_{n=1}^{\infty} \frac{\phi_6(n)}{n^s}$$
$$= \prod_{p \equiv 5 \pmod 6} \frac{1}{1-p^{-2s}} \prod_{p=x^2+27y^2} \frac{1}{(1-p^{-s})^2}$$
$$\times \prod_{p=4x^2+2xy+7y^2} \frac{1}{1+p^{-s}+p^{-2s}},$$

where p runs over all primes.

Let $d < 0$ be a discriminant such that $H(d) = \{I, A, A^2, A^3\}$ with $A^4 = I$. Then $F(A,n) = \frac{1}{2}(R(I,n) - R(A^2,n))$ is multiplicative. Define

$$L(A,s) = \sum_{n=1}^{\infty} \frac{F(A,n)}{n^s}.$$

Theorem 10.3. *Let $d < 0$ be a discriminant such that $H(d) = \{I, A, A^2,\ A^3\}$ with $A^4 = I$. Let f be the conductor of d and $s \in \mathbb{C}$ with $Re(s) > 1$. If $d \neq -220, -252$, then*

$$
\begin{aligned}
L(A,s) = & \prod_{(\frac{d}{p})=-1} \frac{1}{1-p^{-2s}} \prod_{\substack{p|d, p\nmid f \\ p\in R(I)}} \frac{1}{1-p^{-s}} \\
& \times \prod_{\substack{p|d, p\nmid f \\ p\in R(A^2)}} \frac{1}{1+p^{-s}} \prod_{\substack{p\nmid d \\ p\in R(I)}} \frac{1}{(1-p^{-s})^2} \\
& \times \prod_{\substack{p\nmid d \\ p\in R(A^2)}} \frac{1}{(1+p^{-s})^2} \prod_{\substack{p\nmid d \\ p\in R(A)}} \frac{1}{1+p^{-2s}} \ ,
\end{aligned}
$$

where p runs over all primes.

Theorem 10.4. *Let* $s \in \mathbb{C}$ *with* $Re(s) > 1$*. Then* $\phi_3(n), \phi_4(n), \phi_8(n)$ *and* $\phi_{12}(n)$ *are multiplicative functions. Moreover,*

$$\sum_{n=1}^{\infty} \frac{\phi_3(n)}{n^s} = \frac{1}{1+7^{-s}} \prod_{\substack{p \equiv 3,5,6 \pmod 7 \\ p \neq 3}} \frac{1}{1-p^{-2s}}$$

$$\times \prod_{p \equiv 2,8,11 \pmod{21}} \frac{1}{1+p^{-2s}}$$

$$\times \prod_{p = x^2+xy+16y^2} \frac{1}{(1-p^{-s})^2}$$

$$\times \prod_{p = 4x^2+xy+4y^2 \neq 7} \frac{1}{(1+p^{-s})^2} ,$$

$$\sum_{n=1}^{\infty} \frac{\phi_4(n)}{n^s}$$
$$= \frac{1}{1+5^{-s}} \prod_{p\equiv 11,13,17,19 \pmod{20}} \frac{1}{1-p^{-2s}}$$
$$\times \prod_{p\equiv 3,7 \pmod{20}} \frac{1}{1+p^{-2s}} \prod_{p=x^2+20y^2} \frac{1}{(1-p^{-s})^2}$$
$$\times \prod_{p=4x^2+5y^2\neq 5} \frac{1}{(1+p^{-s})^2} \ ,$$

$$\sum_{n=1}^{\infty} \frac{\phi_8(n)}{n^s}$$
$$= \prod_{p\equiv 5,7 \pmod{8}} \frac{1}{1-p^{-2s}} \prod_{p\equiv 3 \pmod{8}} \frac{1}{1+p^{-2s}}$$
$$\times \prod_{p=x^2+32y^2} \frac{1}{(1-p^{-s})^2} \prod_{p=4x^2+4xy+9y^2} \frac{1}{(1+p^{-s})^2} \ ,$$

$$\sum_{n=1}^{\infty} \frac{\phi_{12}(n)}{n^s}$$
$$= \prod_{\substack{p\equiv 3 (\text{mod } 4)\\ p\neq 3}} \frac{1}{1-p^{-2s}} \prod_{p\equiv 5 \ (\text{mod } 12)} \frac{1}{1+p^{-2s}}$$
$$\times \prod_{p=x^2+36y^2} \frac{1}{(1-p^{-s})^2} \prod_{p=4x^2+9y^2} \frac{1}{(1+p^{-s})^2},$$

where p runs over all primes.

§11. The number of representations of n by $ax^2+by(y-1)/2$, $ax^2+by(3y-1)/2$ and $ax(x-1)/2+by(3y-1)/2$

Let

$$r(n=f(x,y)) = |\{\langle x,y\rangle \in \mathbb{Z}^2 :\ n=f(x,y)\}|.$$

In 2008 Z.H. Sun ([S1]) determined

$r(n=(3x^2-x)/2+b(3y^2-y)/2)$ for $b=1,2,5$.

In 2011, using some results for binary quadratic forms Z.H. Sun ([S4]) determined

$$r(n = x^2 + by(y-1)/2)$$

in the cases $b = 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 14, 15, 16, 21, 29, 30, 35, 39, 51, 65, 95$,

$$r(n = x^2 + b(3y^2 - y)/2)$$

in the cases $b = 1, 2, 3, 4, 5, 7, 8, 13, 17$ and

$$r(n = (x^2 - x)/2 + b(3y^2 - y)/2)$$

in the cases $b = 1, 2, 3, 5, 7, 10, 11, 14, 15, 19, 26, 31, 34, 35, 55, 59, 91, 115, 119, 455$.

For example, we have

$$r\Big(n = x^2 + b\frac{y(y-1)}{2}\Big) = 2\sum_{k \mid 8n+b} \Big(\frac{-2b}{k}\Big)$$

$$\text{for}\quad b = 3, 5, 11, 29,$$

$$r\Big(n = x^2 + b\frac{y(3y-1)}{2}\Big) = \sum_{k \mid 24n+b} \Big(\frac{-6b}{k}\Big)$$

$$\text{for}\quad b = 5, 7, 13, 17$$

and

$$r\Big(n = \frac{x(x-1)}{2} + b\frac{y(3y-1)}{2}\Big) = \sum_{k|12n+\frac{b+3}{2}} \Big(\frac{-3b}{k}\Big)$$

for $b = 7, 11, 19, 31, 59$.

There are huge similar results conjectured by R.S. Melham in his preprint “Analogues of Jacobi’s two-square theorem”.

R.S. Melham, Analogues of Jacobi’s two-square theorem: an informal account, Integers 10(2010), 83-100.