ARITHMETIC CONSEQUENCES OF JACOBI'S TWO–SQUARES THEOREM

Michael D. Hirschhorn

(RAMA126-98)

Abstract.

There is a well-known formula due to Jacobi for the number $r_2(n)$ of representations of the number n as the sum of two squares. This formula implies that the numbers $r_2(n)$ satisfy elegant arithmetic relations. Conversely, these arithmetic properties essentially imply Jacobi's formula. So it is of interest to give direct proofs of these arithmetic relations, and this we do.

Keywords: Jacobi's two–squares theorem, representations, arithmetic relations

AMS Classification 11E25

1. Introduction.

Let $r_k(n)$ denote the number of representations of the positive integer n as the sum of k squares (of integers). Then, as Jacobi showed,

Theorem 1. For $n \geq 1$,

$$r_2(n) = 4(d_1(n) - d_3(n)),$$

where $d_i(n)$ is the number of divisors of n congruent to i modulo 4.

This theorem is equivalent to the q-series identity

$$\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = 1 + 4\sum_{n\geq 1}\left(\frac{q^{4n-3}}{1-q^{4n-3}} - \frac{q^{4n-1}}{1-q^{4n-1}}\right)$$

which can be proved directly ([1]) from Jacobi's triple product identity

$$(-aq;q^2)_\infty(-a^{-1}q;q^2)_\infty(q^2;q^2)_\infty=\sum_{-\infty}^{\infty}a^nq^{n^2}$$

or ([2]) from Jacobi's identity

$$(q)_\infty^3=\sum_{n\geq 0}(-1)^n(2n+1)q^{(n^2+n)/2}.$$

Theorem 1 enables us to give a well-known explicit formula for $r_2(n)$ in terms of the prime factorisation of n. From this formula we can deduce the following result.

Theorem 2.

$$r_2(2n)=r_2(n),$$

$$\text{if } p\equiv 1 \pmod 4 \text{ is prime, } \ r_2(pn)=2r_2(n)-r_2(\frac{n}{p}),$$

$$\text{if } p\equiv 3 \pmod 4 \text{ is prime, } \ r_2(pn)=r_2(\frac{n}{p}).$$

The situation can be reversed. As we shall see, Theorem 2 together with $r_2(1)=4$ implies Theorem 1. This alone would be sufficient reason to look for a direct proof of Theorem 2, but it is also true that Theorem 2 is of great intrinsic interest. I have managed to find such a proof of Theorem 2, and shall present it here.

2. Theorems 1 and 2.

We start by showing that Theorem 1 yields Theorem 2.
From Theorem 1, we readily deduce that

(2.1)

if $n=2^\alpha p_1^{\alpha_1}\ \cdots\ p_k^{\alpha_k}q_1^{\beta_1}\ \cdots\ q_l^{\beta_l}$ where $p_i\equiv 1 \pmod 4$, $q_j\equiv 3 \pmod 4$ are primes, then

$$r_2(n)=\begin{cases}0 & \text{if any } \beta_j \text{ is odd}\\ 4(\alpha_1+1)\ \cdots\ (\alpha_k+1) & \text{if all } \beta_j \text{ are even.}\end{cases}$$

It follows immediately from (2.1) that

(2.2)

$$r_2(2^\alpha n) = r_2(n),$$

if $p \equiv 1 \pmod 4$ is prime and n is p-free, that is, p does not divide n,

$$r_2(p^\alpha n) = (\alpha+1) r_2(n),$$

while if $p \equiv 3 \pmod 4$ is prime and n is p-free,

$$r_2(p^\alpha n) = \begin{cases} 0 & \text{if } \alpha \text{ is odd} \\ r_2(n) & \text{if } \alpha \text{ is even.} \end{cases}$$

From (2.2) it is not hard to deduce Theorem 2, as follows.
It is clear that

$$r_2(2n) = r_2(n).$$

and that if p is an odd prime and n is p-free, the remaining relations hold.
So we now suppose $n = p^\alpha m$, where $\alpha \geq 1$ and m is p-free. If $p \equiv 1 \pmod 4$ then

$$r_2(pn) = r_2(p^{\alpha+1}m) = (\alpha+2) r_2(m), \quad r_2(n) = (\alpha+1) r_2(m), \quad r_2(\frac{n}{p}) = \alpha r_2(m),$$

and

$$r_2(pn) = 2r_2(n) - r_2(\frac{n}{p}),$$

while if $p \equiv 3 \pmod 4$,

$$r_2(pn) = r_2(p^{\alpha+1}m), \quad r_2(\frac{n}{p}) = r_2(p^{\alpha-1}m),$$

and

$$r_2(pn) = r_2(\frac{n}{p}),$$

since both equal 0 or $r_2(m)$, according as α is even or odd. ■

Conversely, (2.2) follows easily from Theorem 2 by induction on α; (2.2) together with $r_2(1) = 4$ yields (2.1), and this is equivalent to Theorem 1.

3. Proof of Theorem 2.

We shall establish Theorem 2 via generating functions. Indeed, we shall prove the equivalent result

(3.1)

$$\sum_{n\geq 0} r_2(2n)q^n = \sum_{n\geq 0} r_2(n)q^n,$$

$$\sum_{n\geq 0} r_2(pn)q^n + \sum_{n\geq 0} r_2(n)q^{pn} = 2\sum_{n\geq 0} r_2(n)q^n \quad \text{if } p \equiv 1 \pmod 4 \text{ is prime,}$$

$$\sum_{n\geq 0} r_2(pn)q^n = \sum_{n\geq 0} r_2(n)q^{pn} \quad \text{if } p \equiv 3 \pmod 4 \text{ is prime.}$$

We have

$$\sum_{-\infty}^{\infty} q^{n^2} = \sum_{n \text{ even}} q^{n^2} + \sum_{n \text{ odd}} q^{n^2} = \sum_{-\infty}^{\infty} q^{4n^2} + \sum_{-\infty}^{\infty} q^{4n^2+4n+1} = T_0(q^2) + 2qT_1(q^2)$$

where

$$T_0(q) = \sum_{-\infty}^{\infty} q^{2n^2} \quad \text{and} \quad T_1(q) = \sum_{n\geq 0} q^{2n^2+2n}.$$

Thus

(3.2)

$$\sum_{n\geq 0} r_2(n)q^n = \left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = \big(T_0(q^2) + 2qT_1(q^2)\big)^2 = \big(T_0(q^2)^2 + 4q^2T_1(q^2)^2\big) + 4qT_0(q^2)T_1(q^2).$$

It follows that

$$\sum_{n\geq 0} r_2(2n)q^n = T_0(q)^2 + 4qT_1(q)^2$$

$$= \left(\sum_{-\infty}^{\infty} q^{2n^2}\right)^2 + 4q\left(\sum_{n\geq 0} q^{2n^2+2n}\right)^2$$

$$
\begin{aligned}
&= \sum_{m,n=-\infty}^{\infty} q^{2m^2+2n^2} + \sum_{m,n=-\infty}^{\infty} q^{2m^2+2m+2n^2+2n+1} \\
&= \sum_{m,n=-\infty}^{\infty} q^{(m+n)^2+(m-n)^2} + \sum_{m,n=-\infty}^{\infty} q^{(m+n+1)^2+(m-n)^2} \\
&= \sum_{k\equiv l \pmod 2} q^{k^2+l^2} + \sum_{k\not\equiv l \pmod 2} q^{k^2+l^2} \\
&= \sum_{k,l=-\infty}^{\infty} q^{k^2+l^2} = \sum_{n\geq 0} r_2(n)q^n.
\end{aligned}
$$

Next, let p be an odd prime.

Then

$$
\begin{aligned}
\sum_{-\infty}^{\infty} q^{n^2} &= \sum_{n\equiv 0 \pmod p} q^{n^2} + \sum_{r=1}^{(p-1)/2} \left(\sum_{n\equiv r \pmod p} q^{n^2} + \sum_{n\equiv -r \pmod p} q^{n^2} \right) \\
&= \sum_{-\infty}^{\infty} q^{(pn)^2} + \sum_{r=1}^{(p-1)/2} \left(\sum_{-\infty}^{\infty} q^{(pn+r)^2} + \sum_{-\infty}^{\infty} q^{(pn-r)^2} \right) \\
&= \sum_{-\infty}^{\infty} q^{p^2n^2} + 2\sum_{r=1}^{(p-1)/2} q^{r^2} \sum_{-\infty}^{\infty} q^{p^2n^2+2prn} \\
&= T_0(q^p) + 2\sum_{r=1}^{(p-1)/2} q^{r^2} T_{r^2}(q^p)
\end{aligned}
$$

where

$$
T_0(q) = \sum_{-\infty}^{\infty} q^{pn^2} \quad \text{and for } 1 \leq r \leq (p-1)/2,\ \ T_{r^2}(q) = \sum_{-\infty}^{\infty} q^{pn^2+2rn}.
$$

Thus

$$
\sum_{n\geq 0} r_2(n)q^n = \left(\sum_{-\infty}^{\infty} q^{n^2} \right)^2 = \left(T_0(q^p) + 2\sum_{r=1}^{(p-1)/2} q^{r^2} T_{r^2}(q^p) \right)^2.
$$

It follows that

$$
\sum_{n\geq 0} r_2(pn)q^n = T_0(q)^2 + 8 \sum_{\substack{\text{all pairs } \{r,s\} \text{ with} \\ r,s\in\{1,\cdots,(p-1)/2\}, \\ r^2+s^2\equiv 0 \pmod p}} q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q).
$$

If $p \equiv 3 \pmod 4$, the congruence $r^2 + s^2 \equiv 0 \pmod p$ with $r, s \in \{1, \cdots, (p-1)/2\}$ has no solution, and

$$\sum_{n \geq 0} r_2(pn)q^n = T_0(q)^2 = \left(\sum_{-\infty}^{\infty} q^{pn^2}\right)^2 = \sum_{m,n=-\infty}^{\infty} q^{p(m^2+n^2)} = \sum_{n \geq 0} r_2(n)q^{pn}.$$

On the other hand if $p \equiv 1 \pmod 4$ we have

$$\begin{aligned}\sum_{n \geq 0} r_2(pn)q^n + \sum_{n \geq 0} r_2(n)q^{pn} &= 2T_0(q)^2 + 8 \sum_{\substack{\text{all pairs } \{r,s\} \text{ with} \\ r,s \in \{1,\cdots,(p-1)/2\}, \\ r^2+s^2 \equiv 0 \pmod p}} q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q) \\ &= 2\left\{ T_0(q)^2 + 4 \sum_{\substack{allpairs\ \{r,s\} \text{ with} \\ r,s \in \{1,\cdots,(p-1)/2\}, \\ r^2+s^2 \equiv 0 \pmod p}} q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q) \right\} \\ &.\end{aligned}$$

To complete the proof we need to show that

(3.3)

$$T_0(q)^2 + 4 \sum_{\substack{\text{all pairs } \{r,s\} \text{ with} \\ r,s \in \{1,\cdots,(p-1)/2\}, \\ r^2+s^2 \equiv 0 \pmod p}} q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q) = \sum_{n \geq 0} r_2(n)q^n.$$

We need to know that since $p \equiv 1 \pmod 4$ we can write

$$p = a^2 + b^2$$

with $a, b \in \{1, \cdots, (p-1)/2\}$.

Thus we have

$$\begin{aligned}T_0(q)^2 &= \left(\sum_{-\infty}^{\infty} q^{pn^2}\right)^2 = \sum_{m,n=-\infty}^{\infty} q^{pm^2+pn^2} = \sum_{m,n=-\infty}^{\infty} q^{(am+bn)^2+(bm-an)^2} \\ &= \sum_{ak+bl \equiv 0 \pmod p} q^{k^2+l^2}.\end{aligned}$$

We now show that for each pair $\{r,s\}$ with $r,s\in\{1,\cdots,(p-1)/2\}$ and $r^2+s^2\equiv 0 \pmod p$,

$$\begin{aligned} q^{(r^2+s^2)/p}T_{r^2}(q)T_{s^2}(q) &= \sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} = \sum_{ak+bl\equiv -r \pmod p} q^{k^2+l^2} \\ &= \sum_{ak+bl\equiv s \pmod p} q^{k^2+l^2} = \sum_{ak+bl\equiv -s \pmod p} q^{k^2+l^2}. \end{aligned}$$

It then follows that

$$\begin{aligned} &T_0(q)^2 + 4\sum_{\text{all relevant pairs } \{r,s\}} q^{(r^2+s^2)/p}T_{r^2}(q)T_{s^2}(q) \\ &= \sum_{ak+bl\equiv 0 \pmod p} q^{k^2+l^2} \\ &\quad + \sum_{\text{all relevant pairs } \{r,s\}} \Bigg(\sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} + \sum_{ak+bl\equiv -r \pmod p} q^{k^2+l^2} \\ &\qquad + \sum_{ak+bl\equiv s \pmod p} q^{k^2+l^2} + \sum_{ak+bl\equiv -s \pmod p} q^{k^2+l^2} \Bigg) \\ &= \sum_{k,l=-\infty}^{\infty} q^{k^2+l^2} = \sum_{n\geq 0} r_2(n)q^n. \end{aligned}$$

First observe that

$$\begin{aligned} \sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} &= \sum_{ak+bl\equiv r \pmod p} q^{(-k)^2+(-l)^2} = \sum_{a(-k)+b(-l)\equiv r \pmod p} q^{k^2+l^2} \\ &= \sum_{ak+bl\equiv -r \pmod p} q^{k^2+l^2}, \end{aligned}$$

and similarly

$$\sum_{ak+bl\equiv s \pmod p} q^{k^2+l^2} = \sum_{ak+bl\equiv -s \pmod p} q^{k^2+l^2}.$$

Also

$$\sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} = \sum_{ak+bl\equiv r \pmod p} q^{l^2+(-k)^2} = \sum_{bk+a(-l)\equiv r \pmod p} q^{k^2+l^2}$$

$$= \sum_{bk-al\equiv r \pmod p} q^{k^2+l^2}.$$

Now if $bk - al \equiv r \pmod p$ then (multiply by $sr^{-1} \pmod p$) $ak + bl \equiv s$ or $-s \pmod p$. In either case, all four sums are equal.

So there is only one thing left to prove, and that is

$$q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q) = \sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2}.$$

Suppose

$$ak + bl \equiv r \pmod p.$$

Then

$$bk - al \equiv s \text{ or } -s \pmod p.$$

If $ak + bl = r + mp$ and $bk - al = s + np$ then

$$k = am + bn + (ar + bs)/p, \quad l = bm - an + (br - as)/p,$$

$$k^2 + l^2 = pm^2 + pn^2 + 2rm + 2sn + (r^2 + s^2)/p$$

and

$$\begin{aligned} \sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} &= \sum_{m,n=-\infty}^{\infty} q^{pm^2+pn^2+2rm+2sn+(r^2+s^2)/p} \\ &= q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q). \end{aligned}$$

On the other hand, if $ak + bl = r + mp$ and $bk - al = -s - np$ then

$$k = am - bn + (ar - bs)/p, \quad l = bm + an + (br + as)/p,$$

$$k^2 + l^2 = pm^2 + pn^2 + 2rm + 2sn + (r^2 + s^2)/p$$

and again

$$\sum_{ak+bl\equiv r \pmod p} q^{k^2+l^2} = q^{(r^2+s^2)/p} T_{r^2}(q) T_{s^2}(q),$$

and the proof is complete. ■

References

[**1**] M. D. Hirschhorn, A simple proof of Jacobi's two-square theorem, *Amer. Math. Monthly*, **92** (1985), 579–580.

[**2**] M. D. Hirschhorn, Jacobi's two-square theorem and related identities, Ramanujan Journal, **3** (1999), 153–158.

School of Mathematics
UNSW
Sydney
Australia 2052
m.hirschhorn@unsw.edu.au