ON THE REPRESENTATIONS, \( N_3(n^2) \)

C. D. OLDS

1. Introduction. Let the symbol \( N_r(n) \) denote the number of representations of the positive integer \( n \) in the form \( n = x_1 + x_2 + \cdots + x_r \), where \( x_1, x_2, \cdots, x_r \) are positive or negative integers or zero. We will agree to count the two representations \( n = x_1 + x_2 + \cdots + x_r \), \( n = y_1^2 + y_2^2 + \cdots + y_r^2 \), as distinct unless simultaneously \( x_v = y_v, \nu = 1, 2, \cdots, r \). Notice that in a given representation the signs of the roots, as well as their arrangement, are relevant. A zero square, however, is supposed to have only one root.

In a letter written in 1884 to Ch. Hermite, T. J. Stieltjes proved by means of elliptic functions that if \( n = p^k, p \equiv 1 \pmod{8}, p \) prime, then \( N_3(n^2) = 6p^k \). Later in 1907, A. Hurwitz stated without proof that if

\[
(1) \quad n = 2^k m = 2^k PQ, \quad P = \prod_{r=1}^{r} p_r^{a_r}, \quad Q = \prod_{r=1}^{s} q_r^{b_r},
\]

where each \( p_r \) is a prime \( \equiv 1 \pmod{4} \), and each \( q_r \) is a prime \( \equiv 3 \pmod{4} \), then

\[
(2) \quad N_3(n^2) = 6P \prod_{r=1}^{s} \left[ q_r^{b_r} + 2 \frac{b_r}{q_r} - 1 \right].
\]

This result is also implicitly contained in Stieltjes’ letter mentioned above.

In 1940, G. Pall showed that (2) could be derived arithmetically by an application of certain divisibility properties of the Lipschitz integral quaternions. It is the purpose of this paper to give a simple arithmetical proof of (2) by a method which has been evolved from the study of a paper by Hurwitz in which he derived the analogous formula for \( N_6(n^2) \).

\[1\] This is the first part of a paper presented to the Society April 6, 1940, under the title \textit{On the number of representations of the square of an integer as the sum of an odd number of squares.}


\[6\] The author wishes to acknowledge the assistance rendered him by Professor J. V. Uspensky.

499
2. Two lemmas. The arithmetical derivation of (2) depends upon the following propositions:

**Lemma 1.** Let $f(n)$ be an arbitrary arithmetical function, and suppose that $f(nn') = f(n)f(n')$ for any two integers $n$, $n'$, and that $f(n) \neq 0$ for all $n$. If

$$F(n) = \sum_{d \mid n} f(d)$$

where, in particular, $f(1) = F(1) = 1$, then

$$F(nn') = \sum_{d \mid n, n'} \mu(d)f(d)F(n/d)F(n'/d),$$

where $\mu(n)$ is the Möbius function, and the summation extends over all divisors common to both $n$ and $n'$. If we agree to set $F(x) = 0$ if $x$ is not equal to an integer, then the summation can be extended to $d = 1, 2, \cdots$ ending with a number greater than $n$ or $n'$.

**Proof.** Set $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $n' = p_1^{\beta_1}p_2^{\beta_2} \cdots p_r^{\beta_r}$, where $\alpha, \beta \geq 0$, and $p_1, p_2, \cdots, p_r$ are distinct primes. Then it follows from the definition of $F(n)$ that

$$F(p_r^{\alpha_r+\beta_r}) = F(p_r^{\alpha_r})F(p_r^{\beta_r}) - f(p_r)F(p_r^{\alpha_r-1})F(p_r^{\beta_r-1}),$$

for $\nu = 1, 2, \cdots, r$, and for $\alpha, \beta \geq 0$. It is also clear that $F(p^a q^b) = F(p^a)F(q^b)$ provided $p$ and $q$ are distinct primes. Hence

$$F(nn') = \prod_{r=1}^{r} F(p_r^{\alpha_r+\beta_r}) = \prod_{r=1}^{r} \left[ F(p_r^{\alpha_r})F(p_r^{\beta_r}) - f(p_r)F(p_r^{\alpha_r-1})F(p_r^{\beta_r-1}) \right]$$

$$= \sum_{d=1, 2, 3, \cdots} \mu(d)f(d)F(n/d)F(n'/d).$$

The second lemma we need is derived as follows: Let $f(x) = f(-x)$ be an arbitrary even function defined for integral values of $x$; then it is possible to show by purely arithmetical reasoning that

$$\sum_{(d)} [f(d' - d'') - f(d' + d'')] = \sum_{(b)} \sum_{(a)} [f(0) - f(2d)],$$

The Möbius function is defined as follows: $\mu(1) = 1, \mu(n) = 0$ if $n$ has a squared factor; $\mu(p_1p_2 \cdots p_r) = (-1)^r$, if all the primes $p_1, p_2, \cdots, p_r$ are different.

the summations extending respectively over all positive integral solutions of the equations

(a) \(2n = d'd' + d''d'' = s' + s'', \quad d', \delta', d'', \delta'' \text{ odd,}
\)
(b) \(n = d\delta, \quad \delta \text{ odd.}
\)

If in (4) we replace \(f(x)\) by \((-1)^{x/2}f(x), \ x \text{ even, we obtain after a few simple reductions,}
\)

\[
\sum_{(a)} (-1)^{(d'-1)/2+(d''-1)/2} [f(d' - d'') + f(d' + d'')]
\]

\[=(\sum_{(b)} d[f(2d) - (-1)^d f(0)]).
\]

Now define two arithmetical functions \(\sigma_k(n)\) and \(\rho_k(n)\) as follows:

\[
\sigma_k(n) = \sum_{d|n} d^k, \quad \sigma_0(n) = \sigma(n), \quad 1 \leq d \leq n;
\]

\[
\rho_k(n) = \sum_{n=d\delta, \delta \text{ odd}} (-1)^{(d-1)/2 d^k}, \quad \rho_0(n) = \rho(n),
\]

where in the second function the summation extends over all positive integral solutions \(d, \delta\) of the equation \(n = d\delta\), where \(\delta\) is odd.

On setting \(f(x) = 1\) in (5), and supposing that \(n\) is odd (= \(m\)) we obtain the following.

**Lemma 2.**

\[
\sum_{2m=s'+s''} \rho(s')\rho(s'') = \sigma_1(m),
\]

where the summation extends over all positive, odd integers \(s', s''\), satisfying the equation \(2m = s' + s''\).

3. The formula for \(N_3(n^2)\). Using the definition of \(n\) given by (1), and noticing that \(N_3(2^{2s}m^2) = N_3(m^2)\), we see that we need only seek an expression for the number of solutions of the equation \(m^2 = x^2 + y^2 + z^2\). Since \(m^2 \equiv 1 \pmod{4}\), then one of the roots of this equation must be odd, while the other two must be even. Denote by \(R\) the number of solutions in which \(x\) is even. Then it is a simple matter to verify that

\[
N_3(m^2) = \frac{3}{2}R.
\]

On the other hand, \(R\) can be expressed by the sum

\[
R = \sum_{v=0, \pm 1, \pm 2, \ldots} N_3(m^2 - 4v^2),
\]
which is extended over all integers \( \nu \) rendering the argument non-negative. Knowing this, and using the well known result that \[ N_2(n) = 4\rho(n), \quad n \geq 1, \]
we obtain at once

\[
N_3(n^2) = N_2(m^2) = \frac{3}{2} \sum_{\nu=0, \pm 1, \pm 2, \cdots} N_2(m^2 - 4\nu^2) = \frac{3}{2} \cdot 4 \sum_{\nu=0, \pm 1, \pm 2, \cdots} \rho(m^2 - 4\nu^2) = 6 \sum_{\nu=0, \pm 1, \pm 2, \cdots} \rho((m - 2\nu)(m + 2\nu)) = 6 \sum_{2m=a+b} \rho(ab),
\]
where the last sum extends over all positive odd integers \( a, b \) which satisfy the equation \( 2m = a + b \).

The problem is now reduced to the evaluation of the expression \( \sum \rho(ab) \). To this end we use Lemma 1. Define \( f(n) \) as follows:

\[
f(n) = 0 \text{ if } n \text{ is even}, \quad f(n) = (-1)^{(n-1)/2} \text{ if } n \text{ is odd}.
\]

Then \( f(nn') = f(n)f(n') \) for any two integers \( n, n' \) as required. For odd \( n \)

\[
F(n) = \sum_{d|n} f(d) = \sum_{d|n} (-1)^{(d-1)/2} = \sum_{n=d\delta, \delta \text{ odd}} (-1)^{(\delta-1)/2} = \rho(n).
\]

Setting \( n = ab \), we obtain from Lemma 1,

\[
\rho(ab) = \sum_{d=1,3,5,\cdots} \mu(d)(-1)^{(d-1)/2}\rho(a/d)\rho(b/d),
\]

where \( \rho(x) = 0 \) if \( x \) is not an integer. It follows that

\[
\sum_{2m=a+b} \rho(ab) = \sum_{2m=a+b} \sum_{d=1,3,5,\cdots} \mu(d)(-1)^{(d-1)/2}\rho(a/d)\rho(b/d)
= \sum_{d=1,3,5,\cdots} \mu(d)(-1)^{(d-1)/2} \sum_{2m=a+b} \rho(a/d)\rho(b/d).
\]

Now let \( d \) be any common divisor of \( a \) and \( b \), and set \( a = \alpha d, \beta = \beta d \), \( \alpha, \beta \) odd. Then, using Lemma 2, we see that

\[
\sum_{2m=a+b} \rho(a/d)\rho(b/d) = \sum_{2m/d=\alpha+\beta} \rho(\alpha)\rho(\beta) = \sigma_1(m/d), \quad m/d \text{ odd}.
\]

Consequently,

\footnote{For an arithmetical proof of this result see, for example, Hardy and Wright, \textit{The Theory of Numbers}, Oxford, 1938, p. 241.}
\[
\sum_{2m = a + b} \rho(ab) = \sum_{d | m} \mu(d)\left(-1\right)^{(d-1)/2}\sigma_1(m/d)
\]
\[
= \left[ \sum_{d | P} \mu(d)\left(-1\right)^{(d-1)/2}\sigma_1(P/d) \right]
\cdot \left[ \sum_{d | Q} \mu(d)\left(-1\right)^{(d-1)/2}\sigma_1(Q/d) \right], \quad m = PQ.
\]

Now using the properties of \(\mu(n)\), and being careful of the sign of \((-1)^{(d-1)/2}\) according as \(d | P\) or \(d | Q\), we can easily show, if we notice that \(\sigma_1(p^a) = (p^{a+1} - 1)/(p - 1)\), \(p\) prime, that
\[
\sum_{d | P} \mu(d)\left(-1\right)^{(d-1)/2}\sigma_1(P/d) = \prod_{r=1}^{r} \left[ \sigma_1(p_r^{a_r}) - \sigma_1(p_r^{a_r - 1}) \right]
\]
\[
= \prod_{r=1}^{r} \left[ \frac{p_r^{a_r + 1} - 1}{p_r - 1} - \frac{p_r^{a_r} - 1}{p_r - 1} \right]
\]
\[
= \prod_{r=1}^{r} p_r^{a_r} = P.
\]
Likewise,
\[
\sum_{d | Q} \mu(d)\left(-1\right)^{(d-1)/2}\sigma_1(Q/d) = \prod_{r=1}^{s} \left[ \sigma_1(q_r^{b_r}) + \sigma_1(q_r^{b_r - 1}) \right]
\]
\[
= \prod_{r=1}^{s} \left[ \frac{q_r^{b_r + 1} - 1}{q_r - 1} + \frac{b_r - 1}{q_r - 1} \right].
\]

Combining these two results, we obtain the required expression for \(N_3(n^2)\), namely,
\[
N_3(n^2) = 6P \prod_{r=1}^{s} q_r^{b_r} + 2 \frac{q_r^{b_r} - 1}{q_r - 1}.
\]

Stanford University