ON THE REPRESENTATIONS, $N_3(n^2)$ [1]

C. D. OLDS

1. **Introduction.** Let the symbol $N_r(n)$ denote the number of representations of the positive integer n in the form $n=x_1^2+x_2^2+\cdots+x_r^2$, where $x_1, x_2, \cdots, x_r$ are positive or negative integers or zero. We will agree to count the two representations $n=x_1^2+x_2^2+\cdots+x_r^2$, $n=y_1^2+y_2^2+\cdots+y_r^2$, as distinct unless simultaneously $x_\nu=y_\nu$, $\nu=1, 2, \cdots, r$. 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[2] 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[3] stated without proof that if

$$(1) \qquad n = 2^k m = 2^k PQ, \qquad P = \prod_{\nu=1}^{r} p_\nu^{a_\nu}, \qquad Q = \prod_{\nu=1}^{s} q_\nu^{b_\nu},$$

where each p_ν is a prime $\equiv 1 \pmod 4$, and each q_ν is a prime $\equiv 3 \pmod 4$, then

$$(2) \qquad N_3(n^2) = 6P\prod_{\nu=1}^{s}\left[q_\nu^{b_\nu} + 2\,\frac{q_\nu^{b_\nu}-1}{q_\nu - 1}\right].$$

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

In 1940, G. Pall[4] 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[5] in which he derived the analogous formula for $N_5(n^2)$.[6]

---

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

[2] T. J. Stieltjes, "Lettre 45," *Correspondence d'Hermite et de Stieltjes*, vol. 1, Paris, 1905, pp. 89–94.

[3] A. Hurwitz, *Mathematische Werke*, vol. 2, Basel, 1933, p. 751.

[4] G. Pall, Transactions of this Society, vol. 47 (1940), pp. 487–500. See also G. Pall, Journal of the London Mathematical Society, vol. 5 (1930), pp. 102–105. In this paper Pall gives analytical proofs of the formula for $N_r(cn^2)$, $r=3, 5, 7, 11$, c an integer.

[5] A. Hurwitz, Comptes Rendus de l'Académie des Sciences, Paris, vol. 98 (1884), pp. 504–507; *Mathematische Werke*, vol. 2, pp. 5–7. Notice that Hurwitz makes use of certain results announced by Liouville and some formulas of Stieltjes.

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

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*

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

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

$$F(nn') = \sum_{d|n,n'} \mu(d)f(d)F(n/d)F(n'/d), \tag{3}$$

where $\mu(n)$ is the Möbius function,[7] 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 $\alpha_\nu\geqq 0$, $\beta_\nu\geqq 0$, and $p_1, p_2, \cdots, p_r$ are distinct primes. Then it follows from the definition of $F(n)$ that

$$F(p_\nu^{\alpha_\nu+\beta_\nu}) = F(p_\nu^{\alpha_\nu})F(p_\nu^{\beta_\nu}) - f(p_\nu)F(p_\nu^{\alpha_\nu-1})F(p_\nu^{\beta_\nu-1}),$$

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

$$\begin{aligned} F(nn') = \prod_{\nu=1}^{r} F(p_\nu^{\alpha_\nu+\beta_\nu}) &= \prod_{\nu=1}^{r} \left[F(p_\nu^{\alpha_\nu})F(p_\nu^{\beta_\nu}) - f(p_\nu)F(p_\nu^{\alpha_\nu-1})F(p_\nu^{\beta_\nu-1})\right] \\ &= \sum_{d=1,2,3,\cdots} \mu(d)f(d)F(n/d)F(n'/d). \end{aligned}$$

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[8]

$$\sum_{(a)} [f(d'-d'') - f(d'+d'')] = \sum_{(b)} d[f(0) - f(2d)], \tag{4}$$

---

[7] 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.

[8] M. J. Liouville, Journal de Mathématique, (2), vol. 3 (1858), p. 194. Although this identity was first proved arithmetically by T. Pepin, Journal de Mathématique, (4), vol. 4 (1888), p. 94, it is more convenient to refer to the exposition in Uspensky and Heaslet, *Elementary Number Theory*, New York, 1939, p. 462.

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

(a) $2n=d'\delta'+d''\delta''=s'+s''$, d', δ', d'', δ'' odd,

(b) $n=d\delta$, δ odd.

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

$$\sum_{(a)} (-1)^{(\delta'-1)/2+(\delta''-1)/2}[f(d'-d'')+f(d'+d'')] = \sum_{(b)} d[f(2d)-(-1)^d f(0)]. \tag{5}$$

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

$$\sigma_k(n) = \sum_{d|n} d^k, \qquad \sigma_0(n) = \sigma(n), \quad 1 \leqq d \leqq n;$$

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

where in the second function the summation extends over all positive integral solutions d, δ of the equation $n=d\delta$, where δ 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 $N_3(2^{2k}m^2)=N_3(m^2)$, 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

$$N_3(m^2) = \tfrac{3}{2}R.$$

On the other hand, R can be expressed by the sum

$$R = \sum_{\nu=0,\pm 1,\pm 2,\cdots} N_2(m^2-4\nu^2),$$

which is extended over all integers ν rendering the argument non-negative. Knowing this, and using the well known result that[9]

$$N_2(n) = 4\rho(n), \qquad n \geqq 1,$$

we obtain at once

$$\begin{aligned} N_3(n^2) = N_3(m^2) &= \tfrac{3}{2} \sum_{\nu=0,\pm 1,\pm 2,\cdots} N_2(m^2 - 4\nu^2) \\ &= \tfrac{3}{2}\cdot 4 \sum_{\nu=0,\pm 1,\pm 2,\cdots} \rho(m^2 - 4\nu^2) \\ &= 6 \sum_{\nu=0,\pm 1,\pm 2,\cdots} \rho((m-2\nu)(m+2\nu)) = 6 \sum_{2m=a+b} \rho(ab), \end{aligned}$$

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:

$$\begin{aligned} f(n) &= 0 \text{ if } n \text{ is even}, \\ f(n) &= (-1)^{(n-1)/2} \text{ if } n \text{ is odd}. \end{aligned}$$

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

$$\begin{aligned} \sum_{2m=a+b} \rho(ab) &= \sum_{2m=a+b} \sum_{d=1,3,5\cdots} \mu(d)(-1)^{(d-1)/2}\rho(a/d)\rho(b/d) \\ &= \sum_{d=1,3,5,\cdots} \mu(d)(-1)^{(d-1)/2} \sum_{2m=a+b} \rho(a/d)\rho(b/d). \end{aligned}$$

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

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

Consequently,

[9] For an arithmetical proof of this result see, for example, Hardy and Wright, *The Theory of Numbers*, Oxford, 1938, p. 241.

$$\sum_{2m=a+b} \rho(ab) = \sum_{d|m} \mu(d)(-1)^{(d-1)/2}\sigma_1(m/d)$$
$$= \left[\sum_{d|P} \mu(d)(-1)^{(d-1)/2}\sigma_1(P/d)\right]$$
$$\cdot\left[\sum_{d|Q} \mu(d)(-1)^{(d-1)/2}\sigma_1(Q/d)\right], \qquad m = PQ.$$

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 $\sigma_1(p^\alpha)=(p^{\alpha+1}-1)/(p-1)$, p prime, that

$$\sum_{d|P} \mu(d)(-1)^{(d-1)/2}\sigma_1(P/d) = \prod_{\nu=1}^{r} \left[\sigma_1(p_\nu^{a_\nu}) - \sigma_1(p_\nu^{a_\nu-1})\right]$$
$$= \prod_{\nu=1}^{r} \left[\frac{p_\nu^{a_\nu+1}-1}{p_\nu-1} - \frac{p_\nu^{a_\nu}-1}{p_\nu-1}\right]$$
$$= \prod_{\nu=1}^{r} p_\nu^{a_\nu} = P.$$

Likewise,

$$\sum_{d|Q} \mu(d)(-1)^{(d-1)/2}\sigma_1(Q/d) = \prod_{\nu=1}^{s} \left[\sigma_1(q_\nu^{b_\nu}) + \sigma_1(q_\nu^{b_\nu-1})\right]$$
$$= \prod_{\nu=1}^{s} \left[\frac{q_\nu^{b_\nu+1}-1}{q_\nu-1} + \frac{q_\nu^{b_\nu}-1}{q_\nu-1}\right].$$

Combining these two results, we obtain the required expression for $N_3(n^2)$, namely,

$$N_3(n^2) = 6P\prod_{\nu=1}^{s} \left[q_\nu^{b_\nu} + 2\,\frac{q_\nu^{b_\nu}-1}{q_\nu-1}\right].$$

STANFORD UNIVERSITY