A NOTE ON NUMBERS OF THE FORM $a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$

ROBERT M. THRALL

It has long been known that the only sets of values of α, β which give rise to universal forms $a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$ are $\alpha=1$, $\beta=1, 2, 3$; $\alpha=2$, $\beta=2, 3, 4, 5$. We give here a theorem from which the universal character of all these multiplicative universal forms can be readily established. The methods and arguments used are completely algebraic in character. This note is closely allied to R. D. Carmichael's paper, *Proof that every positive integer is a sum of four integral squares.** We use the formulas on the first page of his proof without recording them here.

We remark that every prime number p is a divisor of the form $a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$ in which a, b, c, d are relatively prime. For if p is prime to α, a theorem from the theory of quadratic residues states that p is a divisor of $a^2+\alpha b^2+\beta$. If p is not prime to α, take $a=c=d=0$, $b=1$. In both cases the bases are seen to be relatively prime.

We now require that α, β be positive integers with $\beta\geqq\alpha>0$. The results obtainable also hold for $\alpha=0$, which case has been treated by R. D. Carmichael.†

THEOREM 1. *For $\alpha<3$ and every prime number $p>\beta$ there exists a positive integer $q\leqq[4\beta/(3-\alpha)]^{1/2}$ such that $p\cdot q=a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$.*

For $p<5$ we verify the truth of the theorem directly. Henceforth consider $p\geqq 5$. Since $p>\beta\geqq\alpha$, from the above remark we have a q' such that $pq'=a^2+\alpha b^2+\beta$, where a and b may evidently be taken less than $p/2$. Hence, $pq'\leqq(1+\alpha)p^2/4+\beta$ or $q'\leqq(1+\alpha)p/4+\beta/p<3p/4+1$; that is, $q'<p$ if $p\geqq 5$, which is the case now under consideration.

Let q be the smallest positive integer such that $pq=a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$. From the above we have $q<p$. Also a, b, c, d are relatively prime, for otherwise the square of their greatest common divisor would divide q, leaving pq_1 in the same form as pq with $q_1<q$ contrary to the hypothesis that q has the smallest value possible.

We now consider the forms in the parentheses of the formula that would correspond to Carmichael's (2):

---

* Duke Mathematical Journal, vol. 2 (1936), pp. 243–245.

† American Mathematical Monthly, vol. 44 (1937), pp. 81–86.

$$A_1 = ax - \alpha by - \beta cz - \alpha\beta dt,$$
$$A_2 = bx + ay + \beta dz - \beta ct,$$
$$A_3 = cx - \alpha dy + az + \alpha bt,$$
$$A_4 = dx + cy - bz + at.$$

The expression A_4 is invariant under any change of x, y, z, t of the form:

$$x' = x + \alpha_1 c + \alpha_2 b + \alpha_3 a,$$
$$y' = y - \alpha_1 d + \alpha_4 b + \alpha_5 a,$$
$$z' = z + \alpha_2 d + \alpha_4 c + \alpha_6 a,$$
$$t' = t - \alpha_3 d - \alpha_5 c + \alpha_6 b,$$

where the α's are arbitrary. Under this transformation A_3 becomes

$$A_3' = A_3 + \alpha_1(c^2 + \alpha d^2) + (\alpha_2 - \alpha\alpha_5)(cb + ad) + (\alpha_3 + \alpha_4)(ac - \alpha bd) + \alpha_6(a^2 + \alpha b^2).$$

We may choose $x = t = 0$, $y = b$, $z = c$ so that $A_4 = 0$. If a prime p divides a number of the form $a^2 + \alpha b^2$, (a, b relatively prime, $\alpha = 1$ or 2), then p is itself of that form, hence $q = 1 \leqq [4\beta/(3-\alpha)]^{1/2}$. For other primes p the greatest common divisor δ of $a^2 + \alpha b^2$ and $c^2 + \alpha d^2$ must be 1. For if δ has a prime power factor p_1^r then $(a^2 + \alpha b^2)/p_1^r = a_1^2 + \alpha b_1^2$; $(c^2 + \alpha d^2)/p_1^r = c_1^2 + \alpha d_1^2$ (this follows from the theory of divisors of the forms $a^2 + b^2$ and $a^2 + 2b^2$); and $p(q/p_1^r)$ has the form considered. We can therefore choose α_1, α_6 (taking $\alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = 0$) so that $A_3' = 1$. Then in (2)* take $\sigma = \rho = 0$ and λ, μ such that the bases in the first two braces are numerically less than or equal to $q/2$. Now suppose that $q > [4\beta/(3-\alpha)]^{1/2}$; that is, that $\beta < q^2(3-\alpha)/4$. The form A is replaced by A' with the new choice of x', y', z', t', and

$$\beta \leqq A'q \leqq \frac{(\alpha + 1)}{4} q^2 + \beta < \frac{(\alpha + 1)}{4} q^2 + \frac{(3 - \alpha)}{4} q^2 = q^2.$$

Hence $0 < A' < q$; but in view of Carmichael's formula (6) this contradicts the minimal nature of q. Therefore, $q \leqq [4\beta/(3-\alpha)]^{1/2}$, and the theorem is proved.

We now give a corollary which is useful in some applications of the theorem.

COROLLARY 1. *If* $q \leqq 3$ *and* $\alpha + \beta + 1 < 9$, *then* $q \leqq 2$.

For, referring to (2) with $q = 3$, we see that by choosing x', y', z', t',

* References are to equations in Carmichael's proof.

μ, λ, ρ, σ as in the proof of Theorem 1 we have $3A' \leqq 1+\alpha+\beta<9$. Therefore $A'<3$. But A' is an integer, and if it is less than three this contradicts the minimal character of q.

A form $ax^2+by^2+cz^2+dt^2$ is called universal when it represents all positive integers. From the multiplicative property of the form $a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$ we see that if it represents every prime number it is universal. If the number q, defined in the preceding theorem, is one, then the form does represent every prime and therefore every positive integer. We turn to the consideration of particular values for α, β. In the following paragraphs the theory of the forms $a^2+\beta c^2$ will be assumed.

The case $\alpha=\beta=1$ gives $q \leqq 2^{1/2}$. Hence $q=1$, and we have the following theorem:

THEOREM 2. *Every positive integer is a sum of four integral squares.*

That the forms $a^2+\alpha b^2+\beta c^2+\alpha\beta d^2$, with $(\alpha, \beta)=(1, 2)$, $(1, 3)$, $(2, 2)$, $(2, 3)$, $(2, 4)$ are universal follows readily by application of Theorem 1 and its corollary. We shall treat just one typical case, $\alpha=2$, $\beta=3$, among these.

If $\alpha=2, \beta=3$, we have $q \leqq (12)^{1/2}$ or $q \leqq 3$. But, since $\alpha+\beta+1=6<9$, the corollary applies and $q \leqq 2$. If $2p=a^2+2b^2+3c^2+6d^2$, then a and c are of like parity. If they are both even, $p=b^2+2(a/2)^2+3d^2+6(c/2)^2$. If they are both odd, by proper choice of sign for a and c we have $(a^2+3c^2)/4=\lambda^2+3\mu^2$, where $\lambda+3\mu=a$, $\lambda-\mu=c$, and $p=b^2+2\lambda^2+3d^2+6\mu^2$. We have now proved the following theorem:

THEOREM 3. *Every positive integer is representable in the form*

$$a^2+2b^2+3c^2+6d^2.$$

The case $\alpha=2$, $\beta=5$ gives $q \leqq (20)^{1/2}$ or $q \leqq 4$. But if $4p=a^2+2b^2+5c^2+10d^2$, (p an odd prime), then a and c must both be even, and $2p=b^2+2(a/2)^2+5d^2+10(c/2)^2$. Hence $q \leqq 3$. But, since $\alpha+\beta+1=8<9$, the corollary gives $q \leqq 2$, and

$$2p = a^2 + 2b^2 + 5c^2 + 10d^2, \tag{1}$$

where a and c must be of like parity. If they are even, $p=b^2+2(a/2)^2+5d^2+10(c/2)^2$. Hence suppose

$$a, c \text{ odd}. \tag{2}$$

Then by taking residues (mod 4) in (1),

$$b \equiv d \pmod 2. \tag{3}$$

Now by (1)

$$(4)^* \qquad p = \left(\frac{a + 2b + 5c + 10d}{6}\right)^2 + 2\left(\frac{a - b + 5c - 5d}{6}\right)^2 + 5\left(\frac{a + 2b - c - 2d}{6}\right)^2 + 10\left(\frac{a - b - c + d}{6}\right)^2.$$

In view of (2) and (3), the numerators in (4) are all even. Then, unless exactly three of a, b, c, d are divisible by 3, we can choose signs for a, b, c, d so that

$$(5) \qquad a - b - c + d \equiv 0 \pmod 3.$$

Then all the other numerators in (4) are divisible by 3.

In the exceptional case either a and b or c and d are divisible by 3. But the identity

$$(6) \qquad 9(A^2 + 2B^2) = (A \pm 4B)^2 + 2(2A \mp B)^2$$

(repeated if necessary) shows that any multiple of 3 of the form x^2+2y^2 can be expressed in that form with x, y prime to 3. Then (5) can be verified as above, and $q = 1$. We have now proved the following theorem:

THEOREM 4. *Every positive integer is representable in the form*

$$a^2+2b^2+5c^2+10d^2.$$

UNIVERSITY OF ILLINOIS

A MOMENT-GENERATING FUNCTION WHICH IS USEFUL IN SOLVING CERTAIN MATCHING PROBLEMS†

EDWIN G. OLDS

1. **Introduction.** In a book published several years ago, Fry‡ devoted considerable attention to various aspects of a problem which he called, "the psychic research problem." His introductory problem is the following: "A spiritualistic medium claims to be able to tell the

---

* Formula (4) and the rest of the proof of this theorem were suggested by Gordon Pall.

† Presented to the Society and The Institute of Mathematical Statistics, December 30, 1937.

‡ T. C. Fry, *Probability and Its Engineering Uses*, Van Nostrand, New York, 1928, pp. 41–77.