SUMS OF FOUR OR MORE VALUES OF $\mu x^2+\nu x$ FOR INTEGERS x*

BY GORDON PALL†

1. *Introduction.* My object is to prove the following theorem.

THEOREM 1. *Let* $0<\nu<\mu, f(x)=\mu x^2+\nu x$. *Let* T *denote the table of all sums of four values of* $f(x)$ *for integers* x *arranged in order of magnitude. The largest gap between consecutive entries of* T *is*

$$(1)\qquad \mu-\nu,\ \textit{if}\ \mu\geqq 3\nu/2;\qquad 5\nu-3\mu,\ \textit{if}\ \mu\leqq 3\nu/2.$$

An immediate corollary is the following result.

THEOREM 2. *Let* $0<\nu<\mu$, $s\geqq 4$. *The largest gap in the table of all sums of* s *values of* $f(x)$ *for integers* x *is*

$$(2)\ \mu-\nu,\ \textit{if}\ s\mu\geqq(s+2)\nu;\quad (s+1)\nu-(s-1)\mu,\ \textit{if}\ s\mu\leqq(s+2)\nu.$$

For, if $s\geqq 4$, we need only add $(s-4)f(-1)$ to every entry of T, notice that a gap $\mu-\nu$ actually occurs from $4f(0)$ to $f(-1)+3f(0)$, that no gap greater than $\mu-\nu$ can exceed $5\nu-3\mu-(s-4)(\mu-\nu)$, and that the last number actually occurs, when it is positive, as the gap from $sf(-1)$ to $f(1)+(s-1)f(0)$.

Let us now recall‡ that the only quadratic functions $q(x)$ which are integers $\geqq 0$ for every integer x, and which take the values 0 and 1 for certain integers x, are obtained from the function

$$(3)\qquad \tfrac{1}{2}mx^2+\tfrac{1}{2}(m-2)x,$$

where m is a positive integer, by replacing x by $x-k$ or $k-x$, k an integer. By Theorem 2, the table of all sums of s values of $q(x)$ possesses as its maximum gap the number 1 if $3\leqq m\leqq s+2$, $m-(s+1)$ if $m\geqq s+2$. One corollary is that every integer $\geqq 0$ is a sum of $m-2$ values of (3) for integers x, all but four of which are 0 or 1, at least if $m\geqq 6$; and of four values if $m=3, 4, 5$; (previously proved by Dickson).

---

* Presented to the Society, November 29, 1930.

† National Research Fellow in Mathematics, California Institute of Technology.

‡ L. E. Dickson, this Bulletin, vol. 33 (1927), p. 714.

Our problem, since we allow x to have all integer values, is very much simpler than Dickson's in this Bulletin (vol. 33 (1927), pp. 713–720; vol. 34 (1928), pp. 63–72 and pp. 205–217).

2. *Proof of Theorem* 1. We require two lemmas.

LEMMA 1.* *The equations*

$$a = x_1^2 + \cdots + x_4^2, \quad b = x_1 + \cdots + x_4, \tag{4}$$

are solvable in integers x_i if and only if

$$a \equiv b \text{ (mod 2)}, \ 4a \geqq b^2, \ 4a - b^2 \textit{ not of the form } 4^h(8v + 7). \tag{5}$$

LEMMA 2.† *The equation*

$$p = (3x_1^2 + 2x_1) + \cdots + (3x_4^2 + 2x_4)$$

is solvable in integers x_i, for every $p \geqq 0$.

Let B_a denote the largest b, for a given $a \geqq 0$, for which equations (4) are solvable in integers x_i. If $a \not\equiv 0$ (mod 4), B_a is, by Lemma 1, the largest integer $b \equiv a$ (mod 2) and satisfying (5_2). Hence

$$(B_a + 2)^2 > 4a, \qquad (a \not\equiv 0, \text{mod } 4). \tag{6}$$

Then all values b for which (4) are solvable are

$$B_a, B_a - 2, B_a - 4, \cdots, -B_a + 2, -B_a. \tag{7}$$

We verify that, if a is odd,

$$B_{a+1} \leqq B_a + 1, \tag{8}$$

for otherwise $B_{a+1} \geqq B_a + 3$, $(B_{a+1} - 1)^2 > 4a$, which contradicts $(B_{a+1})^2 \leqq 4(a+1)$.

CASE I. $\mu \geqq 3\nu$. Then 2ν and $\mu - \nu$ are permitted as gaps in T. In view of (7) we can pass by differences 2ν to $a\mu + B_a\nu$ from any element $a\mu + b\nu$ of T, if a is odd. In view of (8) we can pass from $a\mu + B_a\nu$ to $(a+1)\mu + B_{a+1}\nu$ by an increment $\leqq \mu - \nu$. Trivially,

* A modification of a lemma of Cauchy, this is evident from the identity $4a - b^2 = (x_1 + x_2 - x_3 - x_4)^2 + (x_1 - x_2 + x_3 - x_4)^2 + (x_1 - x_2 - x_3 + x_4)^2$.

† This is equivalent to the readily demonstrable fact that every integer $\geqq 4$ and of the form $3p + 4$ is a sum of four squares prime to 3.

$$(a + 2)\mu - B_{a+2}\nu - \{(a + 1)\mu + B_{a+1}\nu\} \leqq \mu - \nu.$$

Hence, by induction from a to $a+2$, we pass throughout the table.

CASE II. $(5/3)\nu<\mu<3\nu$. Then $\delta=2\mu-4\nu$ and $-\delta$ are both $\leqq\mu-\nu$. Hence, if $a\equiv 1 \pmod 4$ and $b-2\geqq -B_{a+2}$ we can reach $a\mu+B_a\nu$ from the entry $a\mu+b\nu$ by successive increments $\mu-\nu$, $\mu-\nu$, $-\delta$, over entries of T. Thus we can pass from $\mu-\nu$ to $\mu+\nu$, thence over 2μ, $3\mu-\nu$, $4\mu-2\nu$, to $5\mu-3\nu$ and hence to $5\mu+3\nu$. If $a\equiv 1 \pmod 4$ and $\geqq 5$ we pass from $a\mu+B_a\nu$ to $(a+1)\mu+(B_a-1)\nu$, $(a+2)\mu+(B_a-2)\nu$, $(a+4)\mu+(B_a-6)\nu$, and hence to $(a+4)\mu+B_{a+4}\nu$, completing the induction.

CASE III. Finally we have the interesting case $\mu\leqq 5\nu/3$.

Denote by M_p the class of all $\mu a+\nu b$ such that

$$p = 3a + 2b,\ \ 4a \geqq b^2,\ \ a \equiv b \pmod 2,\ \ (5_3). \tag{9}$$

By Lemmas 1 and 2 there exists a solution a, b of (9) for every integer $p\geqq 0$. Table T coincides with the ordered class of all the elements of all classes M_p.

Let A_p, a_p denote, respectively, the largest and the least values of a satisfying (9); and b_p, B_p the corresponding b's. If p is odd the values a of M_p are

$$A_p, A_p - 4, A_p - 8, \cdots, a_p;$$

the corresponding b's being b_p, b_p+6, $b_p+12,\cdots$, B_p. Then also $b_p\leqq 1$, $B_p\geqq -3$, $a_p\geqq 1$, and

$$4(A_p + 4) < (b_p - 6)^2,\ \ 4(a_p - 4) < (B_p + 6)^2,\ \ (p \text{ odd}). \tag{10}$$

If p is odd the difference between two adjacent elements of M_p is allowable, since

$$4\mu - 6\nu \leqq \mu - \nu, \text{ and } 6\nu - 4\mu \leqq 5\nu - 3\mu.$$

The increment from an element $a_1\mu+b_1\nu$ of M_q to an element $a_2\mu+b_2\nu$ of M_{q+1} is $\leqq\mu-\nu$ or $5\nu-3\mu$, respectively, if

(i) $\mu \geqq 1\frac{1}{2}\nu,\ a_2 \geqq a_1 + 1;$ or (ii) $\mu \leqq 1\frac{1}{2}\nu,\ a_1 \leqq a_2 + 3.$

Hence the theorem for the present case will follow from the following lemma.

LEMMA 3. *For every even* $p \geqq 2$,

$$A_p \leqq A_{p-1} + 1, \quad a_{p+1} \leqq a_p + 1; \tag{11}$$

$$a_{p-1} \leqq a_p + 3, \qquad A_p \leqq A_{p+1} + 3. \tag{12}$$

The proof of (11_1) is typical. By (9_2) and (9_3) with $p-1$ and p in place of p, $A_p \equiv A_{p-1}+1 \pmod 4$. Hence the contrary of (11_1) would imply $A_p = A_{p-1}+5+4v_1$, and consequently $b_p = b_{p-1}-7-6v_1$, where $v_1 \geqq 0$. Hence, by $4A_p \geqq (b_p)^2$,

$$4(A_{p-1} + 5 + 4v_1) \geqq (b_{p-1} - 7 - 6v_1)^2,$$

contradicting (10_1) with $p-1$ in place of p, since

$$4(1 + 4v_1) \leqq 2(1 + 6v_1)(6 - b_{p-1}) + (6v_1 + 1)^2.$$

THE CALIFORNIA INSTITUTE OF TECHNOLOGY

GROUPS GENERATED BY TWO OPERATORS WHOSE SQUARES ARE INVARIANT

BY G. A. MILLER

It is well known that two operators of order two generate the dihedral group whose order is twice the order of the product of these operators. The groups that can be generated by two operators which have a common square are also well known. The groups considered in the present article are obviously a generalization of these two categories of well known groups. We shall represent their two generators by s and t. From the fact that s^2 and t^2 are invariant operators of the group G generated by s and t it results directly that

$$s^{-1}sts = t^{-1}stt = ts = (st)^{-1}s^2t^2,$$
$$s^{-1}tss = t^{-1}tst = st = (ts)^{-1}s^2t^2.$$

From these equations it follows that the abelian group H generated by s^2, t^2, and st is invariant under G and that its index under G cannot exceed 2.

A necessary and sufficient condition that H be identical with G is that G be abelian and can be generated by the product of two of its operators and the squares of these operators. It is not