JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

L. E. DICKSON

Quadratic Functions of Forms, Sums of whose Values give all Positive Integers

Journal de mathématiques pures et appliquées 9^e série, tome 7 (1928), p. 319-336.
<http://www.numdam.org/item?id=JMPA_1928_9_7__319_0>

Quadratic Functions or Forms, Sums of Whose Values Give All Positive Integers;

By L. E. DICKSON
(Chicago).

1. We shall obtain several new types of generalizations of theorems on polygonal numbers due to Fermat, Cauchy, and Réalis. We shall also give a complete solution of the following new problem : Find every positive binary quadratic form $B(x, y)$ such that every positive integer is a sum of s values of B. The only important cases are found to be $s = 2$ and $s = 3$. For $s = 2$, we are led to just six quaternary quadratic forms. That each of them actually represents every positive integer p will be proved by descent from p to smaller integers. Fermat stated that this was the method used by him to prove that every p is a sum of four squares. Our proof of this fact and for the remaining five forms involves only ideas familiar to Fermat and justifies our belief that Fermat actually possessed the kind of proof he claimed.

2. *The Possible Forms* B. — Since 1 shall be a sum of values of B, 1 must be represented by B. Hence B is equivalent to $x^2 + gxy + hy^2$. The replacement of x by $x + ky$ adds $2k$ to g. By choice of k, the new g is 0 or 1. Write

$$f = \sum_{i=1}^{s} (x_i^2 + g x_i y_i + h y_i^2), \qquad g = 0 \text{ or } 1. \tag{1}$$

When $s \geqq 4$, f represents every positive integer p, since p is a sum of

four squares x_i^2, and we may assign the value 0 to the remaining x_i and to each y_i. Hence the only interesting cases are $s=2$ and $s=3$.

First, let $g=0$. Since B and f are positive forms, $h>0$. When $s=2$, $h>3$, $f=3$ requires $y_1=y_2=0$, while $x_1^2+x_2^2=3$ is impossible in integers. When $s=3$, $h>7$, $f=7$ requires $y_1=y_2=y_3=0$, while $x_1^2+x_2^2+x_3^2=7$ is impossible.

Second, let $g=1$. Write $X=2x+y$, $d=4h-1$. Then

$$F=4f=\sum_{i=1}^{s}(X_i^2+dy_i^2), \qquad d>0. \tag{2}$$

By hypothesis, f represents all positive integers. Hence F represents all multiples of 4. When $s=2$, $d>12$, $F=12$ gives $y_1=y_2=0$, while $X_1^2+X_2^2=12$ is impossible. When $s=3$, $d>28$, $F=28$ gives $y_1=y_2=y_3=0$, while $X_1^2+X_2^2+X_3^2=28$ is impossible.

Whether $g=0$ or $g=1$, the only possible forms f have $h=1$, 2, or 3 if $s=2$, and $h=1, \ldots, 7$ if $s=3$.

In the derivation of F we had $X_i\equiv y_i \pmod 2$. Let us now remove this condition and allow the X_i and y_i to take arbitrary integral values. Then if F represents a multiple $4n$ of 4, the corresponding f represents n. We first prove this when $s=2$. Then

$$X_1^2+X_2^2-y_1^2-y_2^2\equiv 0 \pmod 4$$

and every square is $\equiv 0$ or 1. If X_1 and X_2 are both even (odd), then y_1 and y_2 are both even (odd). But if one of X_1 and X_2 is even and the other is odd, the same is true of y_1 and y_2. If in the latter case, X_1 and y_1 are not both even, we may permute X_1 and X_2, or permute y_1 and y_2, or permute both pairs, and obtain a new representation of $4n$ by F in which now X_1 and y_1 are both even, and hence X_2 and y_2 are both odd. In all cases we have $X_i\equiv y_i \pmod 2$ for $i=1$, 2. Then $X_i=2x_i+y_i$ for $i=1$ and 2 define integers x_i, which with y_i give a representation of n by f.

A similar proof applies if $s=3$. If X_1, X_2, X_3 are all even (odd), then y_1, y_2, y_3 are all even (odd). If two of X_1, X_2, X_3 are even (odd) and one is odd (even), the same is true of y_1, y_2, y_3.

Hence if $g=1$ it remains only to prove that the form F in (2) represents all multiples of 4.

3. *Method of Descent* (1) *for Quaternary Quadratic Forms.* — The method seems to be limited to forms of Lagrange's type

$$Q = x^2 + ay^2 + bz^2 + abw^2.$$

LEMMA 1. — *For integers satisfying*

$$t^2 + ar^2 + b = pq \qquad (q \not\equiv 0), \tag{3}$$

there will exist a representation of mp by Q with

$$x \equiv raw + tz, \qquad y \equiv tw - rz \pmod{p}, \tag{4}$$

provided there exists a representation of mq by Q with (4) *holding* mod q *instead of* mod p.

Consider the equation

$$mp = (pX + raw + tz)^2 + a(pY + tw - rz)^2 + bz^2 + abw^2, \tag{5}$$

whose expansion simplifies by means of (3) to

$$\begin{aligned} mp = {} & p^2X^2 + ap^2Y^2 + 2apr Xw + 2pt Xz \\ & + 2apt Yw - 2apr Yz + pq(z^2 + aw^2). \end{aligned} \tag{6}$$

In (6) interchange p with q, X with z, and replace Y by $-w$, w by $-Y$; we get

$$\begin{aligned} mq = {} & q^2z^2 + aq^2w^2 - 2aqrz Y + 2qtz X \\ & + 2aqtw Y + 2aqrw X + pq(X^2 + aY^2). \end{aligned} \tag{7}$$

Multiplying (7) by p/q, we get (6). This proves Lemma 1.

The linear functions in (5) remain unaltered if we replace r, t, X, Y by $r + Rp$, $t + Tp$, $X - Raw - Tz$, $Y - Tw + Rz$, respectively. We choose integers R and T so that

$$|r| \leqq \frac{1}{2}p, \qquad |t| \leqq \frac{1}{2}p. \tag{8}$$

We shall limit our further discussion to the case $a = 1$, $b > 0$. By (8), $t^2 + r^2 + b < p^2$ if $p^2 > 2b$, and then $q < p$ in (3). Hence

(1) We would not expect to prove that every positive integer p is a sum of four squares by descent (i. e. by induction from all integers $< p$ to p) without knowing some relations between the squares leading to a fairly definite equation.

when $p^2 > 2b$, (5) follows from a like equation with p replaced by the smaller number q. This proves:

THEOREM 1. — *For each positive integer p such that $p^2 \leqq 2b$ and for all sets of solutions t, r of the congruence*

$$t^2 + r^2 + b \equiv 0 \pmod{p}, \tag{9}$$

suppose that there exist integral solutions X, Y, z, w of

$$mp = (pX + rw + tz)^2 + (pY + tw - rz)^2 + bz^2 + bw^2. \tag{10}$$

Then for every positive integer p such that $p^2 > 2b$ and for any chosen set of solutions of congruence (9), there exist integral solutions of (10).

LEMMA 2. — *If p is an odd prime, (9) has solutions.*

For $t = 0, 1, \ldots, \frac{1}{2}(p-1)$, the values of t^2 are incongruent modulo p. If no one of them were congruent to any of the $\frac{1}{2}(p+1)$ incongruent values of $-r^2 - b$, there would exist $p+1$ integers incongruent modulo p.

LEMMA 3. — *If p is an odd prime not dividing b, there exist solutions of*

$$u^2 + v^2 + b \equiv 0 \pmod{p^n}. \tag{11}$$

The proof is by induction from $n = k \geqq 1$ to $n = k+1$. Let

$$t^2 + r^2 + b = p^k q, \qquad u = t + p^k x, \qquad v = r + p^k y.$$

Then

$$u^2 + v^2 + b \equiv p^k \mathrm{L} \pmod{p^{k+1}}, \qquad \mathrm{L} = q + 2tx + 2ry.$$

Since b is not divisible by p, t and r are not both divisible by p. Hence we can choose integers x and y so that L is divisible by p.

THEOREM 2. — *If P is any odd integer relatively prime to b, there exist solutions of $t^2 + r^2 + b \equiv 0 \pmod{\mathrm{P}}$.*

Write $\mathrm{P} = \Pi p_i^{n_i}$, where the p_i are distinct primes. By Lemma 3,

there exist integers u_i, v_i such that

$$u_i^2 + v_i^2 + b \equiv 0 \pmod{p_i^{n_i}}.$$

It is known that we can choose integers t, r so that

$$t \equiv u_1, \quad r \equiv v_1 \pmod{p_1^{n_1}}; \quad t \equiv u_2, \quad r \equiv v_2 \pmod{p_2^{n_2}}; \quad \ldots$$

Then $t^2 + r^2 + b$ is divisible by $p_1^{n_1}$, $p_2^{n_2}$, ... and hence by their product P.

THEOREM 3. — *Every positive integer p is a sum of four squares.*

Here $m = 1$, $b = 1$, and $p^2 \leqq 2b$ gives $p = 1$; then (10) has the solutions $X = 1$, $Y = z = w = 0$. By Theorems 1 and 2, every odd integer is a sum of four squares. Since

$$2(x^2 + y^2) = (x + y)^2 + (x - y)^2, \tag{12}$$

the double of any sum of four squares is a sum of four squares.

THEOREM 4. — *Every positive integer is represented by*

$$g = x^2 + y^2 + 2z^2 + 2w^2.$$

By Theorem 3, $4n + 2$ is a sum of four squares. Two of them are even, $(2z)^2$ and $(2w)^2$, while the remaining two, c^2 and d^2, are odd. Hence $c = x + y$, $d = x - y$ for integers x, y. Using (12), we see that every odd integer $2n + 1$ is represented by g. Next, the double of g is $(2z)^2 + (2w)^2 + 2x^2 + 2y^2$.

LEMMA 4. — *If* $b \equiv 3 \pmod 4$, $x^2 + y^2 + b \equiv 0 \pmod{2^n}$ *has solutions.*

This is first proved when $n = 3$. If $b \equiv 3 \pmod 8$, take $x = 1$, $y = 2$. If $b \equiv 7 \pmod 8$, take $x = 1$, $y = 0$. We next proceed by induction from $n = m \geqq 3$ to $n = m + 1$. Hence let $\xi^2 + \eta_1^2 + b = 2^m q$. Take $x = \xi + 2^{m-1} X$, $y = \eta_1 + 2^{m-1} Y$. Then

$$x^2 + y^2 + b \equiv 2^m N \pmod{2^{m+1}}, \qquad N \equiv q + \xi X + \eta Y.$$

Since ξ and η_1 are not both even, we can choose integers X and Y so that N is even.

We may now extend the proof of Theorem 2 and obtain :

THEOREM 5. — *If* $b \equiv 3 \pmod 4$ *and if* p *is any integer relatively prime to* b, *there exist solutions of* $t^2 + r^2 + b \equiv 0 \pmod p$.

THEOREM 6. — *Every positive integer is represented by*

$$h = x^2 + y^2 + 3z^2 + 3w^2.$$

We apply Theorem 1 with $m = 2$, $b = 3$. Then $p^2 \leqq 2b$ only when p is 1 or 2. Take $z = w = 0$; then (10) becomes $2 = p(X^2 + Y^2)$ and evidently has integral solutions. Next, let p be any positive integer not divisible by 3. Then $t^2 + r^2 + 3 \equiv 0 \pmod p$ has solutions by Theorem 5. Hence Theorem 1 shows that the double of every positive integer p not divisible by 3 is represented by h. Let also p be odd. Evidently $x + y + z + w$ is even. If $x + y$ is odd, $x^2 + y^2$ and $z^2 + w^2$ are $\equiv 1 \pmod 4$ and $2p = h \equiv 0 \pmod 4$, contrary to hypothesis. Hence $x + y = 2X$, $x - y = 2Y$, $z + w = 2Z$, $z - w = 2W$. By (12), h is now the double of a like form. Hence every odd p not divisible by 3 is represented by h. This holds also for every odd p divisible by 3 since the triple of h is a form of type h. Hence every positive odd integer is represented by h. The same is true of its double by (12).

THEOREM 7. — *Every positive multiple of* 4 *is represented by*

$$\Phi = x^2 + y^2 + 7z^2 + 7w^2.$$

We apply Theorem 1 with $m = 4$, $b = 7$. Then $p^2 \leqq 2b$ only when $p \leqq 3$. If $p = 1$ or 2, take $z = w = 0$; then (10) becomes $4 = p(X^2 + Y^2)$ and is solvable. If $p = 3$, $t^2 = r^2 = 1$ by (8) and (9); then (10) holds if $X = w = 0$, $Y = r$, $z = 1$. Next, let p be any positive integer not divisible by 7. Then $t^2 + r^2 + 7 \equiv 0 \pmod p$ has solutions by Theorem 5. Hence Theorem 1 shows that $4p$ is represented by Φ. This holds also when p is divisible by 7 since 7Φ is a form of type Φ.

THEOREM 8. — *Every positive multiple of* 4 *is represented by*

$$\psi = x^2 + y^2 + 11z^2 + 11w^2.$$

We apply Theorem 1 with $m = 4$, $b = 11$. Then $p^2 \leqq 2b$ only

when $p \leqq 4$. If $p = 1$, 2 or 4, take $z = w = 0$; then (10) becomes $4 = p(X^2 + Y^2)$ and is solvable. If $p = 3$, take $z = 0$, $w = 1$; then (8), (9), (10) become

$$t^2 \equiv 0 \text{ or } 1, \qquad t^2 \equiv 0 \text{ or } 1, \qquad t^2 + r^2 \equiv 1 \pmod 3,$$
$$1 = (3X + r)^2 + (3Y + t)^2.$$

Hence $t^2 + r^2 = 1$. The final equation holds if $X = Y = 0$. We repeat the last part of the proof of Theorem 7 with 7 replaced by 11, and Φ by ψ.

Theorem 8 is new. Attempts to prove it by means of ternary forms have failed.

We have now proved by descent :

THEOREM 9. — *Every positive integer is represented by each of the six forms* (1) *having* $s = 2$, $g = 0$ *or* 1, $h = 1$, 2, *or* 3.

4. *The Case* $s = 3$. — We take $y_2 = y_3 = 0$ and prove that the resulting quaternary form represents all positive integers. Use will be made of the classic theorem that every positive integer not of the form

$$4^k(8n + 7) \tag{13}$$

is a sum of three squares without a common divisor > 1.

We first show that every positive integer m is represented by each of the forms $g = x_1^2 + x_2^2 + x_3^2 + hy^2$ ($h = 1, \ldots, 7$). If m is not of the form (13), this is true with $y = 0$. It now suffices to prove that g represents $8n + 7$, since $2^k x_1, \ldots, 2^k y$ then give a representation of (13) by g. We exhibit a value of y for which $8N + 7 - hy^2$ is positive and not of the form (13) and hence is a sum of three squares. For $h = 1$, 2, 4, 5, or 6, take $y = 1$. For $h = 3$, take $y = 1$ or 2 according as $N = 0$ or $N > 0$. For $h = 7$, take $y = 1$ if $N = 0$, 1, or 2; but take $y = 2$ if $N \geqq 3$.

Every positive multiple of 4 is represented by each of the forms $X_1^2 + X_2^2 + X_3^2 + dy^2$, where $d = 4h - 1$, $h = 1, \ldots, 7$. Let m be of the form (13) and a multiple of 4, whence $k \geqq 1$. Take $y = 2^{k-1}$. Then

$$m - dy^2 = 4^{k-1}P, \qquad P = 4(8n + 7) - d \equiv 1 \pmod 4.$$

Thus P is positive for every n and $h \leqq 7$. Hence P is a sum of three squares, and the same is true of 4^{h-1}P.

THEOREM 10. — *Every positive integer is represented by each of the fourteen forms* (1) *having* $s = 3$, $g = 0$ *or* 1, $h = 1, \ldots, 7$.

3. *Polygonal Numbers.* — When x is an integer $\geqq 0$,

$$p_{m+2}(x) = \frac{1}{2} m(x^2 - x) + x \tag{14}$$

is called a polygonal number of order $m+2$. In particular,

$$p_3(x) = \frac{1}{2} x(x+1)$$

is a triangular number and $p_4(x) = x^2$ is a square. Fermat stated that he was the first to discover the beautiful theorem that every integer $A \geqq 0$ is a sum of $m+2$ polygonal numbers of order $m+2$ (whence A is a sum of three triangular numbers, and a sum of four squares). Cauchy gave the first proof in 1815, and showed that all but four of the polygonal numbers may be taken to be the special ones 0 or 1. Two much simpler proofs have been given by the writer in papers cited below.

When x takes all integral values, positive, negative, or zero, the numbers (14) shall be called generalized polygonal numbers $g_{m+2}(x)$. No one of them is negative. Since $p_3(-x) = p_3(x-1)$, every $g_3(x)$ is an ordinary triangular number. Henceforth we take $m > 2$.

THEOREM 11. — *Every integer* $A \geqq 0$ *is a sum of three generalized pentagonal numbers* $g_5(x)$.

By (13), $24A + 3$ is a sum of three squares u^2, v^2, w^2 without a common divisor > 1. Hence from

$$u^2 + v^2 + w^2 \equiv 0 \pmod 3, \qquad u^2 + v^2 + w^2 \equiv 3 \pmod 4,$$

we see that $u^2 \equiv v^2 \equiv w^2 \equiv 1$ both modulo 3 and modulo 4. Hence u, v, w are each of the form $6s \pm 1$, and their squares are of the form

$(6x-1)^2$, where x is positive, negative, or zero. Thus

$$24A+3=\Sigma(6x-1)^2=3+\Sigma 12(3x^2-x), \qquad A=\Sigma\tfrac{1}{2}(3x^2-x)=\Sigma g_5(x),$$

where the summations extend over three values of x.

THEOREM 12. — *Every integer* $A\geq 0$ *is a sum of three generalized hexagonal numbers* $g_6(x)$.

For, $8A+3$ is a sum of three odd squares $(4x-1)^2$, whence $A=\Sigma(2x^2-x)=\Sigma g_6(x)$. Second proof : Every A is a sum of three triangular numbers $t=\frac{1}{2}y(y+1)$. According as $y=2z$ or $y=2z-1$, $t=g_6(-z)$ or $g_6(z)$.

The only earlier paper on this subject is by S. Réalis. (1). By long proofs he obtains the inferior theorems that every A is a sum of four numbers $g_5(x)$ or four $g_6(x)$. That he was content to use four when three suffice is remarkable in view of the fact just noted that the generalized hexagonal numbers coincide with the triangular numbers.

THEOREM 13. — *Every* A *is a sum of four numbers* $g_7(x)$.

In fact (2), every A is a sum of four values of $p_7(x-2)$ for integers $x\geq 0$. They are values of $g_7(x)$.

THEOREM 14. — *Every* A *is a sum of four numbers* $g_8(x)$.

Except (3) when $A\equiv 4 \pmod 8$, every $A\geq 0$ is a sum of four values of $p_8(x-5)$ for integers $x\geq 0$. They are values of $g_8(x)=3x^2-2x$. If n is a sum of four values of the latter, then $4n+4$ is a sum of four values of

$$12x^2-8x+1=(1-2x)(1-6x)=y(3y-2)=g_8(y), \qquad y=1-2x.$$

---

(1) *Nouv. Corresp. Math.*, t. 4. 1878, p. 27-30.

(2) DICKSON, *Generalizations of the theorem of Fermat and Cauchy on polygonal numbers* (*Bulletin American Mathematical Society*, vol. 34, Jan.-Feb., 1928. Theorem 4).

(3) *Ibid.*, Theorem 6.

It remains to prove that every $A = 4(2k+1)$ is a sum of four numbers $g_8(x)$. By the last remark, this will be true if $2k$ is a sum of four numbers $g_8(x)$. By the theorem quoted, the latter is true unless $2k = 4(2l+1)$. This again is a sum of four numbers $g_8(x)$ if $2l$ is. Hence the theorem is proved by descent.

THEOREM 15. — *If $m \geqq 7$, every positive integer A is a sum of $m-2$ numbers $g_{m+2}(x)$.*

For (1), every A is a sum of $m-6$ numbers 0 or 1 and four values of $p_{m+2}(x-3)$ for integers $x \geqq 0$. All $m-2$ summands are values of $g_{m+2}(x)$.

But fewer than $m-2$ summands do not serve for every A. In fact, $p(-1) = m-1$ is the least $g(x)$ which exceeds $p(1) = 1$. Hence $A = m-2$ requires $m-2$ summands 1. Thus there is no improvement of either Theorem 15 or Theorem 14.

The values in order of $g_7(x)$ are 0, 1, 4, 7, 13, 18, ... No sum of three is 10 or 16. Again, 11 is not a sum of two $g_5(x)$, while 5 is not a sum of two $g_6(x)$.

THEOREM 16. — *The number of summands in Theorems 11-15 is a minimum.*

For interesting forms of Theorems 11-15, see § 9, end.

6. *A Waring Problem.* — Find every quadratic function $q(x)$ having a positive coefficient of x^2, which takes only integral values for all integers $x \geqq 0$ such that every positive integer A is a sum of a limited number l of those values of $q(x)$ which are integers $\geqq 0$ for integers $x \geqq 0$.

Let $q(x) = \alpha x^2 + \beta x + \gamma$. Take $x = 0, 1, 2$. Then γ, $\alpha + \beta$, $4\alpha + 2\beta$ are integers. Hence 2α is a positive integer m, and 2β is an integer. Since q does not represent every A, $l > 1$, and a sum of two or more values of q must give $A = 1$. Hence $q(u) = 1$, $q(k) = 0$ for

(1) *Ibid.*, Theorem 5.

certain integers $u \geqq 0$, $k \geqq 0$. Let k be as small as possible. Then

$$q(x) = q(x) - q(k) = \tfrac{1}{2}(x-k)[m(x+k)+2\beta].$$

Since $q(u)=1$, $2\beta = h - m(u+k)$, $h = 2/(u-k)$. Since h is an integer, $u-k = \pm 1$ or ± 2. If $u-k=\pm 1$, $q(x)$ is $p_{m+2}(\pm x \mp k)$ in the notation (14). For every such polygonal function the minimum l has been found (1). For the new case $u-k=\pm 2$,

$$q(x) = \tfrac{1}{2}(x-k)[m(x-k\mp 2)\pm 1]. \tag{15}$$

For the lower signs, $k = u+2 \geqq 0$. Since

$$q(k\pm 1) = \tfrac{1}{2}(1-m) \tag{16}$$

is an integer, m is odd. The case $m=1$ may be excluded. For the lower signs, this is true by the definition of k as least. For the upper signs, when $m=1$, (15) becomes $p_3(x-k-1)$, wich was treated in the papers cited.

The derivative of (15) is zero when $x-k=\pm v$, where

$$v = (2m-1)/(2m),$$

whence x lies between k and $k\pm 1$. This x is the abscissa of the minimum point of the parabola $y=q(x)$. But

$$q(k)=0, \qquad q(k\pm 2) = q(u) = 1,$$

and (16) is negative. Hence for the points on the parabola below the x-axis, the only integral abscissa is $k\pm 1$. Thus $q(x) \geqq 0$ for every integer $x \geqq 0$ except $x = k \pm 1$, which is therefore the only value of x to be excluded in our problem.

We first treat (15) for the upper signs. Write $X = x-k-2$. Then

$$q(x) = g(X) = \tfrac{1}{2}(X+2)(mX+1) = 1 + f(X), \tag{17}$$

$$f(X) = \tfrac{1}{2}m(X^2 - X) + tX, \qquad t = \tfrac{1}{2}(3m+1). \tag{18}$$

(1) DICKSON, *Bulletin Amer. Math. Soc.*, vol. 34, Jan.-Feb., and March-April, 1928.

THEOREM 17. — *If* $m=2M+1>1$, *every integer* $N\geqq 37m-6$ *is a sum of four values of* $f(X)$ *for integers* $X\geqq 0$ *and* $3M-1$ *numbers* 0 *or* 1.

We apply the result proved by Cauchy :

LEMMA 5. — *If* a *and* b *are positive odd integers and*

$$b^2<4a, \qquad b^2+2b+4>3a, \tag{19}$$

there exist integers $\geqq 0$ *satisfying*

$$a=x^2+y^2+z^2+w^2, \qquad b=x+y+z+w. \tag{20}$$

Evidently $N=f(x)+f(y)+f(z)+f(w)+r$ is equivalent to

$$N=\tfrac{1}{2}m(a-b)+tb+r, \qquad 0\leqq r\leqq E. \tag{21}$$

The following discussion holds when E is not restricted to the present value $3M-1$, nor t to the value in (18), but with the single restriction $2t\geqq m$. Insert the value of a from (21) in (19) and replace r by E or 0 in the first or second inequality. We get

$$b<\frac{2V^{\frac{1}{2}}+2m-4t}{m}, \qquad b>\frac{U^{\frac{1}{2}}+m-6t}{2m}, \tag{22}$$

$$U=24mN+(6t-m)^2-16m^2, \qquad V=2mN+(2t-m)^2-2mE. \tag{23}$$

Then b and U are positive if $N\geqq\frac{2}{3}m$. There will occur at least d positive integers between the limits (22) if their difference exceeds d, and hence if

$$4V^{\frac{1}{2}}-U^{\frac{1}{2}}>P, \qquad P=2md-3m+2t. \tag{24}$$

The left member is $\geqq 0$ if

$$16V-U=8m(N-4E)+4(2t-m)^2+3(2t-3m)^2\geqq 0. \tag{25}$$

Then (24) holds if its square holds and hence if

$$F\equiv(2V+W)^2-UV>0, \qquad 8W=U-P^2. \tag{26}$$

In the present case, $2t=3m+1$, $2E=3m-5$. Take $d=2$. Hence

$$U=24mN+48m^2+48m+9, \qquad V=2mN+m^2+9m+1,$$
$$P=4m+1, \qquad W=3mN+4m^2+5m+1,$$
$$F=m^2N^2-36m^3N+10m^2N-12m^4-204m^3+76m^2+9m.$$

Hence $F>0$ if $N\geqq 37m-6$. Then $N>4E$ and (25) holds. Since $d=2$, there is a positive odd integer b between the limits (22). Since $E\geqq m-1$, we may choose r so that $tb+r\equiv N \pmod m$. Then (21) yields an integral value of $\frac{1}{2}(a-b)$ and hence an odd integer a. Since all the conditions in Lemma 5 are satisfied, Theorem 17 is proved.

When $x\geqq k+2$, $X\geqq 0$. We saw that $k+1$ is the only value of x to be excluded. Hence the summands in our problem for $q(x)$ are the values of $q(x)$ for $x=0, 1, \ldots, k$, and all the values of function (17) for integers $x\geqq 0$.

First, let $k=0$. Then the summands are $q(0)=0$ and the values of (17). By theorem 17, every integer $\geqq L=4+37m-6$ is a sum of $3M-1$ numbers 0 or 1 and four values of $1+f(X)$, and hence is a sum of $3M+3$ numbers chosen from 0 and values of (17). We next prove this also for all positive integers $<L=74M+35$. The values $<L$ of (17) are

(27) $1, 3M+3, 8M+6, 15M+10, 24M+15, 35M+21, 48M+28, 63M+36.$

The sums by four of these numbers and 0 are

0-4, 3M+3-6, 6M+6-8, 8M+6-9, 9M+9, 10, 11M+9-11,
12M+12, 14M+12, 13, 15M+10-13, 16M+12-14,
17M+15, 18M+13-15, 19M+15-16, 21M+16, 17, 22M+18,
23M+16-18, 24M+15-19, 26M+19, 20, 27M+18-21,
29M+22, 30M+20-22, 31M+22, 23, 32M+21-24,
33M+23, 24, 34M+25, 35M+21-25, 36M+26, 38M+24-27,
39M+25-28, 40M+27, 28, 41M+27-29, 42M+28, 29,
43M+27-30, 44M+30, 45M+30-31, 46M+30-32,
47M+31, 32, 48M+28-33, 49M+33, 50M+31-34,
51M+31-34, 53M+34-36, 54M+34-36, 55M+37,
56M+34-37, 57M+37-38, 58M+37, 38, 59M+36-39,
60M+40, 61M+40, 62M+39-41, 63M+36-41,
64M+40-42, 65M+41, 42, 66M+39-43, 67M+42, 43,
68M+44, 69M+42-45, 70M+42-45, 71M+42-46,
72M+43-46, 73M+45-47, 74M+45-47.

The maximum gap $3M$ is from $3M+6$ to $6M+6$, since all later

gaps are $\leqq 2M+1$. Hence every integer $<L$ is derived from an entry of the table by adding at most $3M-1$.

THEOREM 18. — *If* $m=2M+1>1$, *every positive integer is a sum of* $3M+3$ *positive or zero values of* $\frac{1}{2}x[m(x-2)+1]$ *for integers* $x\geqq 0$. *The number* $6M+5$ *is not a sum of fewer than* $3M+3$ *such values.*

7. THEOREM 19. — *If* $m=2M+1>7$, *every integer* $N\geqq 37m-29$ *is a sum of four values of* $f(X)$ *and* $3M-4$ *numbers* 0 *or* 1.

Since $M>3$, $E=3M-4\geqq m-1$ and we may choose $r\leqq E$ so that $tb+r\equiv N \pmod m$. We have the same t and d as in § 6, but now $2E=3m-11$. Hence we have the same U, P, W, while V is increased by $6m$. Hence F is increased by

$$24m^2N-144m^3+408m^2+18m.$$

Now $F>0$ if $N\geqq 37m-29$.

Let $k=1$. The summands are $q(0)=0$, $q(1)=3M+1$ and the values of function (17). Their sum by four are

(28) 0-4, $3M+1$-6, $6M+2$-8, $8M+6$-9, $9M+3$-10, $11M+7$-11, ...,

The first gap $3M-3$ is the maximum gap since it is not less than the largest later gap $2M+1$ in the table of § 6. This proves :

THEOREM 20. — *If* $m=2M+1>7$, *every positive integer is a sum of* $3M$ *positive or zero values of* $\frac{1}{2}(x-1)[m(x-3)+1]$ *for integers* $x\geqq 0$. *The integer* $3M$ *requires* $3M$ *such summands.*

To prove a theorem analogous to theorem 19 for $m=7$, we must take $d=4$ to have two odd values β and $\beta+2$ of b. The latter with $r=E=5$ gives $tb+r\equiv t\beta+6 \pmod m$, which with $t\beta+r$ ($r\leqq E$) give a complete set of residues. We find that $F>0$ if $N\geqq 829$. Hence to extend Theorem 20 to the case $m=7$, we would have to verify it for all $N<829$.

8. *Function* (15) *for the lower signs.* — Write $X = x - k$. Then $q(x)$ becomes $f(X)$ in (18), except that now

$$t = \tfrac{1}{2}(3m - 1) = 3M + 1.$$

Give to k its least value 2. We saw that $k - 1 = 1$ is the only value $\geqq 0$ of x for which $q(x)$ is negative. Hence the summands are $q(0) = 1$ and the values of $f(X)$ for integers $X \geqq 0$:

(29) $0, 1, 3M+1, 8M+3, 15M+6, 24M+10, 35M+15, 48M+21, 63M+28.$

THEOREM 21. — *If* $m = 2M + 1$, *every integer* $N \geqq l$ *is a sum of four values of* $f(X)$ *with* $t = 3M + 1$ *and* E *numbers* 0 *or* 1, *where* $E = 3M - 3$, $l = 37m - 45$ *if* $M > 2$; $E = 4$, $l = 147$ *if* $M = 2$; $E = 1$, $l = 310$ *if* $M = 1$.

For $M \geqq 2$, $E \geqq m - 1$ and we may take $d = 2$. Then $P = 4m - 1$. First, let $M > 2$. Then $2E = 3m - 9$ and

$$U = 24mN + 48m^2 - 48m + 9, \qquad V = 2mN + m^2 + 5m + 1,$$
$$W = 3mN + 4m^2 - 5m + 1,$$
$$F = m^2N^2 - 36m^3N + 46m^2N - 12m^4 - 132m^3 + 244m^2 + 33m.$$

Then $F > 0$ if $N \geqq 37m - 45$.

Second, let $M = 2$. Then

$$U = 120N + 969, \qquad V = 10N + 41, \qquad W = 15N + 76,$$
$$F = 25N^2 - 3550N - 14765 > 0 \qquad \text{if} \qquad N \geqq 147.$$

Third, let $M = 1$. As at the end of § 7, we may take $d = 4$. Then

$$U = 9(8N + 33). \qquad V = 6N + 19, \qquad P = 23, \qquad W = 9N - 29.$$

Then $F = 9(N^2 - 308N - 618) > 0$ if $N \geqq 310$.

THEOREM 22. — *If* $m = 2M + 1$, *every positive integer* N *is a sum of* E *numbers* 0 *or* 1 *and four positive or zero values of* $\frac{1}{2}(x-2)(mx-1)$ *for integers* $x \geqq 0$ *where* $E = 3M - 3$ *if* $M > 2$, $E = 4$ *if* $M = 2$, $E = 1$ *if* $M = 1$.

This is true by theorem 21 if $N \geqq l$. For $M \geqq 2$, it suffices to verify

it when $N < 37m - 38 = 74M - 1$. The sums by four of the numbers (29) are

$$0\text{-}4,\ 3M+1\text{-}4,\ 6M+2\text{-}4,\ 8M+3\text{-}6,\ 9M+3,4,\ 11M+4\text{-}6,$$
$$12M+4,\ 14M+5,6,\ 15M+6\text{-}9,\ 16M+6\text{-}8,\ 17M+6,\ 18M+7\text{-}9,$$
$$19M+7,8,\ 21M+8,9,\ 22M+8,\ 23M+9\text{-}11,\ 24M+9\text{-}13,$$
$$26M+10,11,\ 27M+10\text{-}13,\ 29M+11,\ 30M+12\text{-}14,\ 31M+12,13,$$
$$32M+12\text{-}15,\ 33M+13,14,\ 34M+13,\ 35M+14\text{-}18,\ 36M+14,$$
$$38M+15\text{-}18,\ 39M+15\text{-}18,\ 40M+16,17,\ 41M+16\text{-}18,$$
$$42M+17,18,\ 43M+17\text{-}20,\ 44M+18,\ 45M+18,19,\ 46M+18\text{-}20,$$
$$47M+19,20,\ 48M+19\text{-}24,\ 49M+20,\ 50M+20\text{-}23,\ 51M+21\text{-}24,$$
$$53M+21\text{-}23,\ \ldots.$$

In the continuation from $53M$ to $74M$, all gaps are $\leqq M+1$. The second gap $3M-2$ is a maximum if $M>2$, since it is not less than the largest later gap $2M+1$. If $M=2$, the maximum gap is $2M+1$ (beginning $12M+4$). For $M=1$, Theorem 22 was verified for $N<310$ by a separate table.

9. *A Generalization.* — In the most general Waring problem for a quadratic function $f(x)$, its values for integers $x \geqq 0$ are not assumed to be all integers. Let ξ be the least integer $x \geqq 0$ for which $f(x)$ is an integer $\geqq 0$. Then $f(x)$ is not used as a summand when $x < \xi$. Write $X = x - \xi$, $q(X) = f(X+\xi)$. Hence the summands are certain values of $q(X)$ for $X \geqq 0$, while $q(0)$ is an integer $\geqq 0$. The coefficient of X^2 is positive since there must be infinitely many positive integral summands.

Changing the notations, we consider

$$f(x) = \frac{t}{d}x^2 + \frac{n}{d}x + c, \qquad t>0, \qquad c \geqq 0, \qquad d>0,$$

where t, n, c, d are all integers, and t, n, d have no common divisor >1. Without loss of generality we may assume that d is relatively prime to both t and n. For, if $t = pT$, $d = pD$, where p is a prime, let x be any integer $\geqq 0$ such that $f(x)$ is an integer. Then

$$Df(x) = Tx^2 + \frac{n}{p}x + Dc$$

is an integer. Since n is not divisible by p, x is a multiple pX of p. Hence the integral values of $f(x)$ for integers $x \geqq 0$ coincide with the integral values of

$$\frac{p^2T}{D}X^2 + \frac{n}{D}X + c$$

for integers $X \geqq 0$. Similarly, if $n = pN$, $d = pD$, then $x = pX$ and $f(x)$ becomes

$$\frac{pt}{D}X^2 + \frac{pN}{D}X + c.$$

This reduction from d to D may be repeated.

If $d = 2$, then t and n are odd and $f(x)$ is an integer for every integer x. The latter is evidently true also if $d = 1$. For such a function $f(x)$, Waring's problem was treated partially in §§ 6-8. It has been treated completely (1) when $f(x)$ is an integer $\geqq 0$ for every integer $\geqq 0$. Here let $d > 2$.

The discussion is simplest when $t = 1$, $d = p^k$, where p is a prime. Then n is not divisible by p. Hence x and $x + n$ are not both divisible by p. But their product must be divisible by p^k if $f(x)$ is an integer. Hence one of them is divisible by p^k. According as $x = p^kX$ or $x + n = p^kX$, f becomes

$$X(p^kX \pm n) + c$$

for the upper or lower sign. Hence the integral values of

$$\frac{1}{p^k}(x^2 + nx) + c \qquad (n \text{ not divisible by prime } p) \tag{30}$$

for integers $x \geqq 0$ coincide with the values of

$$p^kz^2 + nz + c \tag{31}$$

for all positive, negative, and zero integral values of z.

For $c = 0$, $n = 1 - p^k$, (31) is a generalized polygonal number of order $2(p^k + 1)$. Hence those numbers coincide with the positive or zero integral values, for integers $x \geqq 0$, of the single function (30). The small orders are 6, 8, 10, 12, 16, 18, 20, 24.

---

(1) DICKSON, *Amer. Jour. Math.*, 1928.

Next, let $t=1, d=2p^k$. Then n is odd and not divisible by the odd prime p. The preceding proof shows that the integral values of $f(x)$ for integers $x \geqq 0$ coincide with the values of $\frac{1}{2}(p^k z^2+nz)+c$ for all integers z. For $c=0$, $n=2-p^k$, the latter is a generalized polygonal number of order p^k+2. The small orders are 5, 7, 9, 11, 13, 15, 19, 21, 25.

For an infinitude of integers w (including all <22 except 14 and 17), all generalized polygonal numbers of order w coincide with the positive or zero integral values of a single function $f(x)$ for integers $x \geqq 0$. Hence theorems 11-16 may be interpreted as theorems on the representation of all positive integers as sums of positive or zero integral values of $f(x)$ for integers $x \geqq 0$.

An elaborate investigation of all these Waring problems will be given in a later memoir.