SQUARE-PARTITION CONGRUENCES*

BY E. T. BELL

1. *Introduction.* It is evident that the theory of partitions and that of the representation of an integer as a sum of squares must be closely interwoven since both originate in the elliptic theta and modular functions. In seeking the relations thus suggested, we find at the outset some remarkable types of congruences which deserve independent notice on account of their generality. Each congruence is to the odd prime modulus p; the most frequent type concerns the function expressing the number of ways in which an integer is a sum of p, $3p$, p^2, $3p^2$, p^s $(s > 0)$ or rp squares, where r is prime to p, and one of the following: the familiar denumerants of the classical theory of partitions; two new functions depending upon those partitions of an integer in which no part appears more than r times. Of the latter functions those corresponding to $r = 2, 3, 6$ play a central part in the entire theory. The subject is extensive. We shall give a sketch of the methods used sufficient for its systematic development. For the ϑ, q formulas see, e.g., Tannery-Molk, *Fonctions Elliptiques,* and note that we use Jacobi's theta notation (*Werke,* vol. 1, p. 501), so that π is omitted from ϑ_1'.

2. *Fundamental Identities.* In the usual notation $q_j = q_j(q)$,

$$(1) \qquad \begin{aligned} q_0 &= \Pi(1 - q^{2n}), & q_2 &= \Pi(1 + q^m), \\ q_1 &= \Pi(1 + q^{2n}), & q_3 &= \Pi(1 - q^m), \end{aligned}$$

extending to $n = 1, 2, 3, \cdots$, $m = 1, 3, 5, \cdots$, Euler's identities are

$$(2) \qquad q_1 q_2 q_3 = q_1(\sqrt{q}) q_3 = 1, \qquad q_0 = \Sigma(-1)^n q^{3n^2+n},$$

Σ extending to $n = 0, \pm 1, \pm 2, \cdots$. Denote by $A_j(n, r)$ the coefficient † of q^{2n} in q_j^r $(j = 0, 1)$, of q^n in q_j^r $(j = 2, 3)$.

* Presented to the Society, April 7, 1923.

† The properties of these coefficients have been discussed and a practicable method for their numerical computation given in a paper which will be published in the AMERICAN JOURNAL.

By convention $A_j(0, r) = 1$. By (1) and the first of (2),

$$(3) \qquad A_1(n, r) = (-1)^n A_2(n, -r) = A_3(n, -r) \qquad (r \gtrless 0).$$

Henceforth p is an odd prime > 0, r an arbitrary integer > 0. If $s \neq 0, p$, the binomial coefficient $\binom{p}{s}$ is divisible by p, and hence by (1) we have, using Fermat's theorem,

$$(4) \qquad q_j^{rp} \equiv q_j^r(q^p) \mod p, \qquad (j = 0, 1, 2, 3),$$

which means that the coefficients of like powers of the parameter q are congruent modulo p. Hence we have by (1) and (3), according as n is or is not prime to p,

$$(5) \qquad A_j(n, rp) \equiv 0 \quad \text{or} \quad A_j(n/p, r) \mod p,$$

$$(6) \qquad A_1(n, -rp) \equiv 0 \quad \text{or} \quad (-1)^n A_2(n/p, r) \mod p,$$

$$(7) \qquad \begin{aligned} (-1)^n A_2(n, -rp) \equiv A_3(n, -rp) &\equiv 0 \\ &\text{or} \quad A_1(n/p, r) \mod p; \end{aligned}$$

and by (4) and the second of (2), according as n is not or is $\frac{1}{2}p(3a^2 + a)(a \gtreqless 0)$,

$$(8) \qquad A_0(n, p) \equiv 0, \quad \text{or} \quad (-1)^a \mod p.$$

The summations referring to $n = 0, \pm 1, \pm 2, \cdots$, $m = \pm 1, \pm 3, \pm 5, \cdots$, we have $\vartheta_j = \vartheta_j(q)$,

$$(9) \qquad \begin{gathered} \vartheta_0(-q) = \vartheta_3 = \Sigma q^{n^2}, \qquad \vartheta_1'(q^4) = \Sigma(-1|m)mq^{m^2}, \\ \vartheta_2(q^4) = \Sigma q^{m^2}, \end{gathered}$$

where $(a|b)$ is the Legendre-Jacobi symbol, $(-1|a) = (-1)^{(a-1)/2}$ for a odd; and

$$(10) \qquad \begin{gathered} \vartheta_3 = q_0 q_2^2, \qquad \vartheta_2(q^4) = 2q_0(q^4)q_1^2(q^4)q, \\ \vartheta_1'(q^4) = 2q_0^3(q^4)q. \end{gathered}$$

From the last of these, it follows by (4) that

$$(11) \qquad A_0(n, 3p) \equiv 0 \quad \text{or} \quad (-1|a)a \mod p,$$

according as n is not or is $p(a^2 - 1)/8$ where $a > 0$ is odd.

The $A_j(n, r)$ are connected with partitions as follows. If in a given partition of n no part appears more than r times and each of precisely a_j distinct parts occurs exactly j times we call the hypercomplex number $(a_1, a_2, \cdots, a_r)$ the r index of the partition, and denote by $B_n(a_1, a_2, \cdots, a_r)$ or $B_n'(a_1, a_2, \cdots, a_r)$ the total number of partitions of n having this index according as all the parts are not or are restricted to be odd. As mentioned, the cases $r = 2, 3, 6$ are of special importance. For our purpose here it is sufficient by what precedes to consider in these cases $A_j(n, r)$ only when $j = 1, 2$. From (1) we have

$$\begin{aligned} A_1(n, 2) &= \Sigma B_n(a_1, a_2)2^{a_1}, \\ A_1(n, 3) &= \Sigma B_n(a_1, a_2, a_3)3^{a_1+a_2}, \\ A_1(n, 6) &= \Sigma B_n(a_1, \cdots, a_6)2^{a_1+2a_3+a_5}3^{a_1+a_2+a_4+a_5}5^{a_2+a_3+a_4}, \end{aligned}$$

the summations referring to all $(a_1, a_2), \cdots, (a_1, \cdots, a_6)$ for n fixed.* The $A_2(n, r)$ for $r = 2, 3, 6$ are written down from these by accenting B.

Let $P(n)$, $Q(n)$, $R(n)$ denote respectively the total number of partitions of n, the number of partitions of n into odd parts, and the number of partitions of n into distinct odd parts. Then, from (1), (2), we have

$$A_0(n, -1) = P(n), \qquad A_1(n, 1) = Q(n),$$
$$A_2(n, 1) = (-1)^n A_3(n, 1) = R(n).$$

The square functions most frequently occurring are $N(n, r)$, the number of representations of n as a sum of r squares whose roots are $\gtreqless 0$, and $M(n, r)$, the number of representations of n as a sum of r odd squares whose roots are > 0. Obviously $M(n, r) = 0$ if n is not of the form $8k + r$, and

$$(12) \quad \vartheta_3^r(q) = \Sigma q^n N(n, r), \qquad \vartheta_2^r(q^4) = 2^r \Sigma q^{8n+r} M(8n + r, r),$$

where Σ refers to $n = 0, 1, 2, \cdots$, with the convention that $N(0, r) = 1$.

* The $A_j(n, 2)$ with a generalization have been fully discussed in a paper to appear in the ANNALS OF MATHEMATICS. They are remarkable as introducing for the first time a species of double periodicity into the theory of partitions. The $A_j(n, r)$, $r = 2, 3, 6, 9$, have been specially considered in the paper cited previously; they have many interesting connections with the class number for binary quadratic forms of a negative determinant.

Consider all the representations of n as a sum of r squares of numbers $\gtrless 0$ of the form $6k + 1$, and let $S_0(n, r)$, $S_1(n, r)$ denote the respective numbers of these representations in which an even, an odd number of squares have square roots of the form $12k + 7$. Write $S(n, r) = S_0(n, r) - S_1(n, r)$. Then $S(n, r)$ vanishes identically if n is not of the form $24k + r$, and from the second of (2) we have

$$(13) \qquad A_0(n, r) = S(24n + r, r),$$

whence it follows by (8) that

$$(14) \qquad S(24n + p, p) \equiv 0 \quad \text{or} \quad (-1)^a \quad \bmod p,$$

according as n is not or is $\frac{1}{2}p(3a^2 + a)(a \gtreqqless 0)$, and by (11)

$$(15) \qquad S(24n + 3p, 3p) \equiv 0 \quad \text{or} \quad a(-1|a) \quad \bmod p,$$

according as n is not or is $p(a^2 - 1)/8$, where $a > 0$ is odd.

The congruences in this section appear to be sufficient for the systematic transposition of the classical theory of partitions into congruence relations of the type illustrated in the next. The labor of verifying the congruences numerically may be lightened by observing that $N(n, p)$ is congruent modulo p to twice the total number of representations of n as a sum of p squares with roots all > 0. Similar obvious remarks apply to any of the square functions encountered except those involving only odd squares.

3. *Congruences.* A short selection must suffice. Equating coefficients of like powers of q in $\vartheta_3{}^{rp}q_2{}^{-2rp} = q_0{}^{rp}$ we find

$$\Sigma A_2(s, -2rp)N(2n - s, rp) = A_0(n, rp),$$

the summation referring, as always henceforth unless otherwise noted, to all such $s \geqq 0$ as render the first arguments of the summands positive or zero. Applying (7) we get

$$(16) \quad \Sigma(-1)^s A_1(s, 2r)N(2n - sp, rp) \equiv A_0(n, rp) \quad \bmod p,$$

whence by (11) when $r = 3$,

$$(17) \quad \begin{aligned} &\Sigma(-1)^s A_1(s, 6)N(2n - sp, 3p) \equiv 0 \\ &\qquad\qquad\qquad\qquad \text{or} \quad a(-1|a) \quad \bmod p, \end{aligned}$$

according as n is not or is $p(a^2 - 1)/8$, where $a > 0$ is odd. The ϑ, q identity being read in the alternative form $\vartheta_3{}^{rp} = q_0{}^{rp}q_2{}^{2rp}$ gives by (5) in the same way

$$N(n, rp) \equiv \Sigma A_0(s, r)A_2(n - 2sp, 2rp) \mod p, \tag{18}$$

from which it follows by (5) that

$$n \not\equiv 0 \mod p: \qquad N(n, rp) \equiv 0 \mod p. \tag{19}$$

From (18) and (5), we have

$$N(np, rp) \equiv \Sigma A_0(s, r)A_2(n - 2s, 2r) \mod p, \tag{20}$$

and hence by (8),

$$N(np, p^2) \equiv \Sigma(-1)^a A_2(n - p(3a^2 + a), 2p) \mod p, \tag{21}$$

where Σ extends to all $a \gtreqless 0$ that make $n \geqq p(3a^2 + a)$. Applying (5) to (21) we have

$$n \not\equiv 0 \mod p: \qquad N(np, p^2) \equiv 0 \mod p; \tag{22}$$

$$N(np^2, p^2) \equiv \Sigma(-1)^a A_2(n - (3a^2 + a), 2) \mod p, \tag{23}$$

where Σ extends to all $a \gtreqless 0$ that make $n \geqq 3a^2 + a$. Again from (20), (11) we find

$$N(np, 3p^2) \equiv \Sigma a(-1|a)A_2(n - \tfrac{1}{4}p(a^2 - 1), 6p) \mod p, \tag{24}$$

where Σ extends to all odd $a > 0$ that make $4n \geqq p(a^2 - 1)$.

Applying (5) to (24), we get

$$n \not\equiv 0 \mod p: \qquad N(np, 3p^2) \equiv 0 \mod p, \tag{25}$$

$$N(np^2, 3p^2) \equiv \Sigma a(-1|a)A_2(n - \tfrac{1}{4}(a^2 - 1), 6) \mod p, \tag{26}$$

where Σ extends to all odd $a > 0$ that make $4n \geqq a^2 - 1$.

Similarly, from the second of (10), we find

$$\Sigma A_1(s, -2r)M(8n - 8s + r, r) = A_0(n, r), \tag{27}$$

$$M(8n + r, r) = \Sigma A_0(s, r)A_1(n - s, 2r). \tag{28}$$

To derive the associated congruences we replace r by rp

and proceed as before. Thus (27) gives

$$\Sigma(-1)^s A_2(s,2r)M(8n+rp-8sp,rp) \equiv A_0(n,rp) \mod p; \tag{29}$$

$$\Sigma(-1)^s A_2(s,6)M(8n+3p-8sp,3p) \equiv 0 \text{ or } a(-1|a) \mod p \tag{30}$$

according as n is not or is $p(a^2-1)/8$ where $a > 0$ is odd; while from (28),

$$M(8n+rp,rp) \equiv \Sigma A_0(s,r)A_1(n-sp,2rp) \mod p; \tag{31}$$

$$n \not\equiv 0 \mod p: \quad M(8n+rp,rp) \equiv 0 \mod p; \tag{32}$$

$$M(8np+rp,rp) \equiv \Sigma A_0(s,r)A_1(n-s,2r) \mod p; \tag{33}$$

$$M(8np+p^2,p^2) \equiv \Sigma(-1)^a A_1(n-\tfrac{1}{2}p(3a^2+a),2p) \mod p, \tag{34}$$

where Σ extends to all $a \gtreqless 0$ that make $2n \geqq p(3a^2+a)$;

$$M(8np^2+p^2,p^2) \equiv \Sigma(-1)^a A_1(n-\tfrac{1}{2}(3a^2+a),2) \mod p, \tag{35}$$

where Σ extends to all $a \gtreqless 0$ that make $2n \geqq 3a^2+a$;

$$n \not\equiv 0 \mod p: \quad M(8np+p^2,p^2) \equiv 0 \mod p; \tag{36}$$

$$M(8np+3p^2,3p^2) \equiv \Sigma a(-1|a)A_1(n-\tfrac{1}{8}p(a^2-1),6p) \mod p; \tag{37}$$

$$n \not\equiv 0 \mod p: \quad M(8np+3p^2,3p^2) \equiv 0 \mod p; \tag{38}$$

$$M(8np^2+3p^2,3p^2) \equiv \Sigma a(-1|a)A_1(n-\tfrac{1}{8}(a^2-1),6) \mod p, \tag{39}$$

the summations in (37), (39) extending to all odd $a > 0$ making the first arguments of $A_1 \geqq 0$. Putting $r = 1$ in (29) and applying (13), (14) we find

$$\Sigma(-1)^s A_2(s,2)M(8n+p-8sp,p) \equiv 0 \text{ or } (-1)^a \mod p \tag{40}$$

according as n is not or is $\tfrac{1}{2}p(3a^2+a)(a \gtreqless 0)$. Similarly, from (16), under the same conditions, we have

$$\Sigma(-1)^s A_1(s,2)N(n-sp,p) \equiv 0 \text{ or } (-1)^a \mod p. \tag{41}$$

The number of congruences obtainable in this way is practically unlimited. Thus the memoir of Jacobi * on infinite series whose exponents are contained simultaneously in two different quadratic forms alone furnishes an inexhaustible supply, and the modular equations in elliptic functions give many more. Quadratic forms other than simple sums of squares appear in this connection. For example consider all the representations of n in the form

$$a_1^2 + a_2^2 + \cdots + a_r^2 + 3(b_1^2 + b_2^2 + \cdots + b_r^2),$$

in which a_j, $b_j \lesseqgtr 0$ and $a_j \equiv 1 \mod 6$, $b_j \equiv 1 \mod 4$ $(j = 1, 2, \cdots, r)$. Let $T_0(n, r)$ denote the total number of these representations in which an even number of the b_j are of the form $8k + 5$, and $T_1(n, r)$ the total number in which an odd number of the b_j are of the form $8k + 5$. Write

$$T(n, r) = T_0(n, r) - T_1(n, r).$$

Then Jacobi's result (*Werke*, vol. 2, p. 285)

$$q^4 q_0^2(q^{24}) = \Sigma(-1)^k q^{(6i+1)^2+3(4k+1)^2},$$

where Σ refers to $i, k = -\infty$ to $+\infty$, gives

$$A_0(n, 2r) = T(48n + 4r, r),$$

from which we find by successive applications of (5), for $s \geqq 0$,

(42) $n \equiv 0 \mod p$: $T(48np^s + 4rp^{s+1}, rp^{s+1}) \equiv 0 \mod p$,

(43) $T(48np^{s+1} + 4rp^{s+1}, rp^{s+1}) \equiv A_0(n, 2r) \mod p$,

(44) $T(48np^{s+1} + 4p^{s+1}, p^{s+1}) \equiv A_0(n, 2) \mod p$.

Considerations of space preclude the giving of further examples.

THE UNIVERSITY OF WASHINGTON

* *Werke*, vol. 2, pp. 219–288; CRELLE'S JOURNAL, vol. 37, pp. 61–94, 221–254.