A CONGRUENCE SATISFIED BY THE THETA-CONSTANT ϑ_3

L. CARLITZ

Let

$$\vartheta_3 = \sum_{-\infty}^{\infty} q^{n^2}$$

and let p denote an arbitrary odd prime. The following congruence appears incidentally in [1, formula (3.7)]:

$$\vartheta_3^{2(p-1)} \sum_{r=0}^{m} \binom{m}{r}^2 k^{2r} \equiv 1 \pmod{p}, \tag{1}$$

where $p=2m+1$ and k^2 has its usual significance in the theory of elliptic functions. The congruence (1) is to be interpreted in the following way. Using the familiar identity

$$k^2 = 16q \prod_{1}^{\infty} \left(\frac{1+q^{2n}}{1+q^{2n-1}}\right)^8, \tag{2}$$

(1) can be written entirely in terms of q or entirely in terms of k^2. It follows from (2) that

$$k^2 = \sum_{n=1}^{\infty} a_n q^n \qquad (a_1 = 16), \tag{3}$$

where the a_n are rational integers, and that

$$q = \sum_{n=1}^{\infty} b_n k^{2n} \qquad (b_1 = 1/16), \tag{4}$$

where the denominators of the b_n are powers of 2. If we substitute from (3) into (1) we get a certain set of congruences; if we substitute from (4) we get another set. By Lemma 1 of [1] these congruences are equivalent. We now show how the second substitution can be carried out explicitly.

We recall that the complete elliptic integral of the first kind is given by

$$K = \frac{\pi}{2} F\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right),$$

Received by the editors February 9, 1959.

where F denotes the hypergeometric function; also we recall that

$$\vartheta_3^2 = 2K/\pi.$$

Consequently (1) becomes

$$\left\{F\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right)\right\}^{p-1} \sum_{r=0}^{m} \binom{m}{k}^2 k^{2r} \equiv 1 \pmod{p}. \tag{5}$$

Now

$$F\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right) = \sum_{r=0}^{\infty} \frac{\left(\frac{1}{2}\right)_r \left(\frac{1}{2}\right)_r}{r!r!} k^{2r};$$

also

$$\left(\frac{1}{2}\right)_r = \frac{1}{2} \frac{3}{2} \cdots \frac{2r-1}{2} = \frac{(2r)!}{2^{2r}r!},$$

so that

$$\frac{\left(\frac{1}{2}\right)_r}{r!} = \frac{1}{2^{2r}}\binom{2r}{r}. \tag{6}$$

We recall that, if [2, p. 419]

$$a = a_0 + a_1 p + a_2 p^2 + \cdots \qquad (0 \leqq a_i < p),$$
$$b = b_0 + b_1 p + b_2 p^2 + \cdots \qquad (0 \leqq b_i < p),$$

then

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2} \cdots \pmod{p}.$$

It follows that if

$$r = r_0 + r_1 p + r_2 p^2 + \cdots \qquad (0 \leqq r_i < p),$$

then

$$\binom{2r}{r} \equiv \binom{2r_0}{r_0}\binom{2r_1}{r_1}\binom{2r_2}{r_2} \cdots \pmod{p}; \tag{7}$$

in particular

$$\binom{2r}{r} \equiv 0$$

unless

$$0 \leqq r_i < p/2 \qquad (i = 0, 1, 2, \cdots).$$

Using (6) and (7), we get

$$\begin{aligned} F\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right) \\ &\equiv \sum_{r_0=0}^{m} \sum_{r_1=0}^{m} \cdots \binom{2r_0}{r_0}^2 \binom{2r_1}{r_1}^2 \cdots \left(\frac{k}{4}\right)^{2(r_0+r_1p+\cdots)} \\ &\equiv \prod_{j=0}^{\infty} \left\{ \sum_{s=0}^{m} \binom{2s}{s}^2 \left(\frac{k}{4}\right)^{2p^js} \right\} \pmod{p}. \end{aligned}$$

Now it is also easily verified that

$$\frac{1}{2^{2s}}\binom{2s}{s} = \frac{\left(\frac{1}{2}\right)_s}{s!} \equiv (-1)^s \binom{m}{s} \pmod{p}$$

for $0 \leqq s \leqq m$; therefore

$$F\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right) \equiv \prod_{j=0}^{\infty} \sum_{s=0}^{m} \binom{m}{s}^2 k^{2p^is} \pmod{p}. \tag{8}$$

If for brevity we put

$$S(k^2) = \sum_{s=0}^{m} \binom{m}{s}^2 k^{2s},$$

then it is clear that (5) reduces to

$$S(k^2) \prod_{j=0}^{\infty} S^{p-1}(k^{2p^j}) \equiv 1 \pmod{p}. \tag{9}$$

Thus (9) is the form assumed by (1) when q is expressed in terms of k^2. But (9) can be verified immediately. For if $Q(k^2)$ denotes the left member of (9), it is clear that

$$\begin{aligned} Q(k^2) &= S^p(k^2) \prod_{j=1}^{\infty} S^{p-1}(k^{2p^j}) \\ &\equiv S(k^{2p}) \prod_{j=1}^{\infty} S^{p-1}(k^{2p^j}) \\ &\equiv Q(k^{2p}) \pmod{p}. \end{aligned}$$

This evidently implies $Q(k^2)\equiv 1$. We have therefore an alternative proof of (1).

It is not clear how to carry out explicitly the transformation of (1) into what may be called its q-form. Put

$$k^{2r} = \sum_{s=r}^{\infty} a_{rs}q^s;$$

it follows from (2) that the coefficients a_{rs} are rational integers. Now let

$$\vartheta_3^s = \sum_{n=0}^{\infty} R_s(n)q^n,$$

so that $R_s(n)$ is the number of representations of n as a sum of s squares. Then it is easily seen that (1) implies the following two results.

$$R_{2(p-1)}(n) + \sum_{s=1}^{n} R_{2(p-1)}(n-s)\sum_{r=1}^{s}\binom{m}{r}^2 a_{rs} \pmod{p} \qquad (n \geqq 1), \tag{10}$$

$$R_2(n) \equiv R_2(n/p) + \sum_{n=s+pt} R_2(t)\sum_{r=1}^{s}\binom{m}{r}^2 a_{rs} \pmod{p}. \tag{11}$$

If we recall the familiar formulas

$$k^{1/2} = \vartheta_2/\vartheta_3, \qquad k'^{1/2} = \vartheta_0/\vartheta_3,$$

where

$$\vartheta_0 = \sum_{-\infty}^{\infty} (-1)^n q^{n^2}, \qquad \vartheta_2 = \sum_{-\infty}^{\infty} q^{(2n-1)^2/4}$$

it is easily verified that (1) implies

$$\vartheta_2^{2(p-1)} S(k^{-2}) \equiv 1 \pmod{p}, \tag{12}$$

$$\vartheta_0^{2(p-1)} S(k^{2}) \equiv k'^{p-1} \pmod{p}. \tag{13}$$

Since

$$S(x) = (1-x)^m P_m\left(\frac{1+x}{1-x}\right),$$

where $P_m(x)$ is the Legendre polynomial, (13) can also be written in the form

$$\vartheta_0^{2(p-1)} P_m\left(\frac{1+k^2}{1-k^2}\right) \equiv 1 \pmod{p}. \tag{14}$$

Similarly, (1) and (12) can also be written in terms of the Legendre polynomial.

Finally, since

$$(\vartheta_0\vartheta_2\vartheta_3)^4 = 2^4 q \prod_1^\infty (1 - q^{2n})^{12},$$

it follows from (1), (12) and (13) that

$$\left\{q \prod_1^\infty (1 - q^{2n})^{12}\right\}^{(p-1)/2} S^3(k^2) \equiv (kk')^{p-1} \pmod{p}. \tag{15}$$

References

1. L. Carlitz, *Arithmetic properties of elliptic functions*, Math. Z. vol. 64 (1956) pp. 425–434.

2. E. Lucas, *Théorie des nombres*, Paris, 1891.

Duke University