Atti. Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. (Ser. 8) 56 (1974), 145-150.

ACCADEMIA NAZIONALE DEI LINCEI

Estratto dai *Rendiconti della Classe di Scienze fisiche, matematiche e naturali*

Serie VIII, vol. LVI, fasc. 2 - Febbraio 1974

Teoria dei numeri. — *A diophantine system of Dickson.* Nota di PHILIP A. LEONARD e KENNETH S. WILLIAMS (*), presentata (**) dal Socio G. SANSONE.

RIASSUNTO. — Nei problemi di ciclotomia interessa conoscere il numero delle soluzioni della congruenza $x^l + y^l + 1 \equiv 0 \pmod{p = ef + 1}$, p dispari. Il caso $e = 5$ fu trattato completamente da L. E. Dickson; gli Autori trattano ora il caso $e = 7$.

1. INTRODUCTION

In a series of papers [1], [2], [3] L. E. Dickson laid the foundations of the modern theory of cyclotomy. His work [2] shows how in principle the cyclotomic numbers of order e (e an odd prime), for primes $p \equiv 1 \pmod{e}$, can be computed in terms of the solutions of a system of $(1/2)(e - 1)$ quadratic diophantine equations. For example, when $e = 5$ the appropriate system is

$$(1.1) \qquad \begin{cases} 16\,p = x^2 + 50\,u^2 + 50\,v^2 + 125\,w^2\,, \\ xw = v^2 - 4\,uv - u^2\,, \end{cases}$$

and Dickson has given a complete treatment of this system [1]. However when $e = 7$, though Dickson treats the problem in some detail, he does not give the precise analogue of the above system, nor does it appear in later papers on cyclotomy. It is the purpose of this paper to give the analogous system to (1.1) when $e = 7$ (see (3.5)) and to give a complete treatment of it, appealing where possible to appropriate results of Dickson. Elsewhere [6], [7] the Authors have used the solutions of the system (3.5) to determine the cyclotomic numbers of order 7, which are lacking in the literature on cyclotomy (see the concluding remarks of [8] for example), and to give necessary and sufficient conditions for 2, 3, 5 and 7 to be seventh powers modulo primes $p \equiv 1 \pmod{7}$ (see [5] for example).

2. NOTATION

Throughout the rest of this paper we will use the following notation. p denotes a prime $\equiv 1 \pmod{7}$, $\zeta = \exp(2\pi i/7)$, $Z[\zeta]$ is the ring of integers of $Q(\zeta)$ (Q–rationals)—it is a unique factorization domain [9]. If π is any prime factor of p in $Z[\zeta]$ we order its conjugates by setting $\pi_k = \sigma_k(\pi)$,

(*) Both Authors were supported under National Research Council of Canada Grant No. A–7233.

(**) Nella seduta del 9 febbraio 1974.

$1 \leq k \leq 6$, where σ_k is the automorphism of $Q(\zeta)$ determined by $\sigma_k(\zeta) = \zeta^k$. The 7-th power character $(\cdot/\pi)_7$ is defined by $(y/\pi)_7 = \zeta^r$ if $y^{(p-1)/7} \equiv \zeta^r \pmod{\pi}$ for any element y of $Z[\zeta]$ such that $y \not\equiv 0 \pmod{\pi}$. The Jacobi sum $J_\pi(m, n)$ is defined for any integers m, n by

$$J_\pi(m, n) = \sum_{x=1}^{p-1} \left(\frac{x^m (x+1)^n}{\pi}\right)_7 . \tag{2.1}$$

Finally, for any integer $a \not\equiv 0 \pmod{p}$, we define the Jacobsthal sum $\varphi_7(a)$ by

$$\varphi_7(a) = \sum_{x=1}^{p-1} \left(\frac{x(x^7 + a)}{p}\right), \tag{2.2}$$

where $(\cdot/p)$ is the familiar Legendre symbol. The basic properties of Jacobi sums are given in [4] and those of Jacobsthal sums in [10].

3. Normalized elements and a one-to-one correspondence

The element $1 - \zeta$ is a prime in $Z[\zeta]$ as its norm is the rational prime 7.

Definition. An element $K \in Z[\zeta]$ is said to be normalized if $K \equiv -1 \pmod{(1-\zeta)^2}$.

Clearly $K = \sum_{i=1}^{6} a_i \zeta^i$ is normalized if and only if

$$\sum_{i=1}^{6} a_i \equiv -1 \pmod 7, \qquad \sum_{i=1}^{6} i a_i \equiv 0 \pmod 7. \tag{3.1}$$

The following results concerning normalized elements are either implicit in the literature or easily proved from known results.

(I) If $K = \sum_{i=1}^{6} a_i \zeta^i \in Z[\zeta]$ is normalized and such that $K\overline{K} = p$ then ([2], pp. 365–366)

$$\sum_{i=1}^{6} i^2 a_i \equiv \sum_{i=1}^{6} i^4 a_i \equiv 0 \pmod 7; \tag{3.2}$$

moreover (using (3.2)),

$$a_1 - a_2 - a_5 + a_6 \equiv a_1 + a_2 - 2a_3 - 2a_4 + a_5 + a_6 = 0 \pmod 7, \tag{3.3}$$

and the integers $x_1, \cdots, x_6$ defined by

$$\begin{cases} x_1 = -a_1 - a_2 - a_3 - a_4 - a_5 - a_6 , \\ x_2 = a_1 - a_6 , \\ x_3 = a_2 - a_5 , \\ x_4 = a_3 - a_4 , \\ 7x_5 = a_1 + a_2 - 2a_3 - 2a_4 + a_5 + a_6 , \\ 7x_6 = a_1 - a_2 - a_5 + a_6 , \end{cases} \tag{3.4}$$

satisfy ([2], pp. 366–367) the diophantine system

$$(3.5)\quad \begin{cases} 72\,p = 2x_1^2 + 42(x_2^2+x_3^2+x_4^2) + 343\,(x_5^2+3x_6^2)\,, \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + \\ \qquad + 48x_3x_4 + 98x_5x_6 = 0\,, \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + \\ \qquad + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0\,, \end{cases}$$

with $x_1 \equiv 1 \pmod 7$.

(II) For any solution $(x_1, \cdots, x_6)$ of (3.5) we have (reducing the equations modulo 8, 3 and 7)

$$(3.6)\quad \begin{cases} x_2 + x_3 + x_6 \equiv 0 & \pmod 2, \\ 2x_2 + 2x_4 + x_6 + x_7 \equiv 0 & \pmod 4, \\ 2x_1 + 2x_2 + x_5 + 3x_6 \equiv 0 & \pmod 4, \\ x_1 + x_5 \equiv 0 & \pmod 3, \\ x_2 + 2x_3 + 3x_4 \equiv 0 & \pmod 7; \end{cases}$$

moreover, with $\lambda = 1$ if $x_1 \equiv 1 \pmod 7$ and $\lambda = -1$ if $x_1 \equiv -1 \pmod 7$, the integers $a_1, a_2, a_3, a_4, a_5, a_6$ defined by,

$$(3.7)\quad \begin{cases} 12\lambda a_1 = -2x_1 + 6x_2 + 7x_5 + 21x_6\,, \\ 12\lambda a_2 = -x_1 + 6x_3 + 7x_5 - 21x_6\,, \\ 12\lambda a_3 = -2x_1 + 6x_4 - 14x_5\,, \\ 12\lambda a_4 = -2x_1 - 6x_4 - 14x_5\,, \\ 12\lambda a_5 = -2x_1 - 6x_3 + 7x_5 - 21x_6\,, \\ 12\lambda a_6 = -2x_1 - 6x_2 + 7x_5 + 21x_6\,, \end{cases}$$

give (from (3.6) and [2], pp. 366–367) $K = \sum_{i=1}^{6} a_i\,\zeta^i$, a normalized element of $Z[\zeta]$ such that $K\bar{K} = p$.

Putting assertions (I) and (II) together we have

THEOREM 1. *There is a one-to-one correspondence between normalized elements* $K \in Z[\zeta]$ *satisfying* $K\bar{K} = p$ *and solutions* $\pm(x_1, \cdots, x_6)$ of (3.5).

4. NUMBER OF SOLUTIONS

In this section we use Theorem 1 and the unique factorization property of $Z[\zeta]$ to calculate the number of solutions of (3.5). Again we state some known results.

(III) If $K \in Z[\zeta]$ is such that $K\bar{K} = p$ then K possesses a unique normalized associate K_1 such that $K_1\bar{K}_1 = p$ ([2], p. 375).

(IV) If no one of the integers m, n, $m+n$ is divisible by 7 then $J_\pi(m, n)$ is a normalized element of $Z[\zeta]$ such that $J_\pi(m, n)\,\overline{J_\pi(m, n)} = p$. (That $J_\pi(m, n)$ is normalized follows using a well-known calculation of Davenport and Hasse. See [4], p. 153 for example.)

(V) The unique normalized associate K_1 of $K = \pi_1 \pi_4 \pi_5$ (resp. $K = \pi_1 \pi_2 \pi_4$) is $K_1 = J_\pi(1, 1)$ (resp. $K_1 = J_\pi(1, 2)$). (This is due to Kummer. See, for example, [2], p. 376.)

(VI) If $K \in Z[\zeta]$ is normalized and such that $K\bar{K} = p$ then either

$$K = \sigma_k(J(1, 1)) \tag{4.1}$$

or

$$K = \sigma_k(J(1, 2)), \tag{4.2}$$

for some k $(1 \leq k \leq 6)$.

(This follows from the above remarks, and the factorization $p = \pi_1 \pi_2 \pi_3 \pi_4 \pi_5 \pi_6$).

The conjugates in (4.1) are distinct. However since $\sigma_2(\pi_1 \pi_2 \pi_4) = \pi_1 \pi_2 \pi_4$, $\pi_1 \pi_2 \pi_4$ is an integer of $Q(\sqrt{-7})$, and (4.2) gives only two distinct conjugates. Hence there are $6 + 2 = 8$ possibilities for K and by Theorem 1 we have

THEOREM 2. *If p is a prime $\equiv 1 \pmod 7$ there are exactly 16 integral solutions of the system* (3.5).

5. NATURE OF SOLUTIONS

Replacing π by $-\pi$ is necessary, as $\pi_1 \pi_2 \pi_4$ is an integer of $Q(\sqrt{-7})$, we may suppose that

$$\pi_1 \pi_2 \pi_4 = t + u\sqrt{-7} \tag{5.1}$$

where

$$p = t^2 + 7u^2 \quad , \quad t \equiv 1 \pmod 7. \tag{5.2}$$

Hence

$$J(1, 2) = \pi_1 \pi_2 \pi_4 ,$$

and it and its conjugate give rise (using (3.4)) to the 4 solutions

$$\pm(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0). \tag{5.3}$$

If $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution arising (using (3.4)) from any of the conjugates in (4.1) it is easy to check that the six conjugates give the

twelve solutions:

$$(5.4)\qquad \pm(x_1, x_2, x_3, x_4, x_5, x_6)\left\langle \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & -\frac{1}{2} \end{array} \right\rangle^k$$

where $k = 0, 1, 2, 3, 4, 5$.

THEOREM 3. *If p is a prime $= 1 \pmod 7$ the 16 integral solutions of* (3.5) *consist of 4 trivial solutions given by* (5.3) *and 12 non-trivial solutions given by* (5.4).

6. FORMULAE FOR THE NON-TRIVIAL SOLUTIONS

From the work of Whiteman [10] (or as easily established directly) we have

$$(6.1)\qquad \sum_{i=0}^{6} \varphi_7(4g^i)\,\zeta_7 = 7\sum_{x=1}^{p-2} \zeta^{\mathrm{ind}_g\, x(x+1)},$$

where g is a primitive root (mod p) and $\mathrm{ind}_g(a)$ ($a \not\equiv 0 \pmod p$) is the unique integer m such that $a \equiv g^m \pmod p$, $0 \le m \le p-2$. Replacing π by an appropriate conjugate if necessary, we may suppose that

$$(6.2)\qquad (g/\pi)_7 = \zeta,$$

so (6.1) gives

$$(6.3)\qquad J_\pi(1,1) = \frac{1}{7}\sum_{i=0}^{6} \varphi_7(4g^i)\,\zeta^i,$$

so that if $J_\pi(1,1) = \sum_{i=1}^{6} a_i \zeta^i$ we have

$$(6.4)\qquad 7a_i = \varphi_7(4g^i) - \varphi_7(4) \qquad (i = 1, 2, \cdots, 6).$$

Thus the solution $(x_1, \cdots, x_6)$ of (3.5) with $x_1 \equiv 1 \pmod 7$ corresponding to $J_\pi(1,1)$ is given by

$$(6.5)\qquad \left\{ \begin{array}{l} x_1 = 1 + \varphi_7(4), \\ 7x_2 = \varphi_7(4g) - \varphi_7(4g^6), \\ 7x_3 = \varphi_7(4g^2) - \varphi_7(4g^5), \\ 7x_4 = \varphi_7(4g^3) - \varphi_7(4g^4), \\ 49x_5 = \varphi_7(4g) + \varphi_7(4g^2) - 2\varphi_7(4g^3) - 2\varphi_7(4g^4) + \varphi_7(4g^5) + \varphi_7(4g^6) \\ 49x_6 = \varphi_7(4g) - \varphi_7(4g^2) - \varphi_7(4g^5) + \varphi_7(4g^6), \end{array} \right.$$

recalling that $\sum_{i=0}^{6} \varphi_7(4g^i) = -7$ (See [10]). We have by (5.4) and (6.5):

THEOREM 4. *If g is a primitive root* (mod p) (p *a prime* $\equiv 1 \pmod 7$) *the six non-trivial solutions* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *of* (3.5) *with* $x_1 \equiv 1 \pmod 7$, *corresponding to* $J_\pi(i, i)$, $1 \leq i \leq 6$, *are given by*

$$x_1 = 1 + \varphi_7(4),$$

$$7x_2 = \varphi_7(4g^i) - \varphi(4g^{6i}),$$

$$7x_3 = \varphi_7(4g^{2i}) - \varphi_7(4g^{5i}),$$

$$7x_4 = \varphi_7(4g^{3i}) - \varphi_7(4g^{4i}),$$

$$49x_5 = \varphi_7(4g^i) + \varphi_7(4g^{2i}) - 2\varphi_7(4g^{3i}) - 2\varphi_7(4g^{4i}) + \varphi_7(4g^{5i}) + \varphi_7(4g^{6i}),$$

$$49x_6 = \varphi_7(4g^i) - \varphi_7(4g^{2i}) - \varphi_7(4g^{5i}) + \varphi_7(4g^{6i}),$$

where, for each i, $\bar{i}$ is the unique integer such that $i\bar{i} \equiv 1 \pmod 7$, $1 \leq \bar{i} \leq 6$.

5. CONCLUSION

It is important to note that Theorems 3 and 4 establish that the diophantine system (3.5), provided the trivial solutions are excluded, determines a unique solution $x_1 = 1 \pmod 7$, given by $x_1 = 1 + \varphi_7(4)$ (compare [5], [8]). Since $\varphi_7(4)$ is odd if and only if 2 is a 7th power (mod p), x_1 even is a necessary and sufficient condition for 2 to be a 7th power (mod p) (See [7]).

REFERENCES

[1] L. E. DICKSON, *Cyclotomy, higher congruences, and Waring's problem*, I, II, « Amer. J. Math. », *57*, 391–424, 463–474 (1935).

[2] L. E. DICKSON, *Cyclotomy and trinomial congruences*, « Trans. Amer. Math. Soc. », *37*, 363–380 (1935).

[3] L. E. DICKSON, *Cyclotomy when e is composite*, « Trans. Amer. Math. Soc. », *38*, 187–200 (1935).

[4] K. IRELAND and M. I. ROSEN, *Elements of Number Theory*, Bogden and Quigley, Tarrytown, New York, 1972.

[5] E. LEHMER, *Abstract: On the quintic character of 2*, « Bull. Amer. Math. Soc. », *55*, 62–63 (1949).

[6] P. A. LEONARD and K. S. WILLIAMS, *The cyclotomic numbers of order seven*, « Proc. Amer. Math. Soc. », to appear.

[7] P. A. LEONARD and K. S. WILLIAMS, *The septic character of 2, 3, 5 and 7*, « Pacific J. Math. », to appear.

[8] T. STORER, *Cyclotomy and difference sets*, Chicago, Markham, 1967.

[9] K. UCHIDA, *Class numbers of imaginary abelian number fields*, III, « Tohoku Math. J. », II Series, *23*, 573–580 (1971).

[10] A. L. WHITEMAN, *Cyclotomy and Jacobsthal sums*, « Amer. J. Math. », *74*, 89–99 (1952).