MATH. SCAND. 4 (1956), 243–246

# A SPECIAL QUARTIC CONGRUENCE

L. CARLITZ

The solvability of the congruence

$$(1)\qquad x^4+x^3+x^2+x+1 \equiv 0 \pmod{p},$$

where $p$ is a prime, is covered by a special case of a well known theorem (see for example [2, p. 103]). When $p \equiv 1 \pmod 5$, the left member of (1) is congruent to the product of four distinct linear factors, when $p \equiv -1 \pmod 5$, it is congruent to the product of two distinct irreducible quadratics, while when $p \equiv \pm 2 \pmod 5$ it is irreducible. When $p=5$ the left member is congruent to $(x-1)^4$.

It may be of interest to inquire whether like results hold for the reciprocal congruence

$$(2)\qquad x^4+ax^3+bx^2+ax+1 \equiv 0 \pmod{p},$$

where $p$ is an odd prime. The discussion is somewhat more complicated than that of the quartic congruence [1]

$$(3)\qquad x^4+ax^2+b \equiv 0 \pmod{p}.$$

For brevity we put

$$(4)\qquad A = a^2-4b+8, \qquad B = (b+2)^2-4a^2.$$

If $A \equiv c^2 \pmod{p}$, we may easily verify that

$$(5)\qquad \big((a+c)^2-16\big)\big((a-c)^2-16\big) \equiv 16B \pmod{p},$$

while if $B \equiv e^2$, then

$$(6)\qquad (a^2-2b-4-2e)(a^2-2b-4+2e) \equiv a^2A \pmod{p}.$$

Let $f(x)$ denote the left member of (2). Consider first the factorization

$$(7)\qquad f(x) \equiv (x^2+ux+1)(x^2+vx+1) \pmod{p}.$$

This implies $u+v \equiv a$, $uv \equiv b-2$,

$$(u-v)^2 \equiv a^2-4b+8 \equiv A,$$

Received November 6, 1956.

so that it is necessary that $A$ be a quadratic residue of $p$ or be divisible by $p$. Conversely when $A\equiv c^2$, we get a factorization of the form (7) with

$$u \equiv \tfrac{1}{2}(a+c), \qquad v \equiv \tfrac{1}{2}(a-c) .$$

Also the quadratic factors in (7) have for discriminants

$$\tfrac{1}{4}(a+c)^2-4, \qquad \tfrac{1}{4}(a-c)^2-4 , \tag{8}$$

respectively. Note that the product of these discriminants satisfies (5).

In the next place consider the factorization

$$f(x) \equiv (x^2+rx+s)(x^2+r'x+s^{-1}) \qquad (s \not\equiv 1) . \tag{9}$$

This implies

$$r+r' \equiv a, \qquad rr'+s+s^{-1} \equiv b, \qquad r \equiv r's ,$$

which yields

$$(rr')^2-(b+2)rr'+a^2 \equiv 0 . \tag{10}$$

The discriminant of this quadratic is evidently $B$, as defined by (4). If $B\equiv e^2$, it follows that

$$(r-r')^2 \equiv a^2-4rr' \equiv a^2-2b-4\pm e;$$

by (6) the product of these two numbers $\equiv a^2A$. Consequently if $a\not\equiv 0$ and the Legendre symbol $(A/p)=-1$, it is clear that just one of the numbers $a^2-2b-4\pm e$ is a quadratic residue. Conversely when the stated conditions are satisfied, we obtain the factorization (9). The case $a\equiv 0$ requires separate treatment but involves no great difficulty.

If $f(x)$ is a product of four linear factors $(\bmod p)$ then a factorization of the form (7) obtains, and as we have seen, this implies $A\equiv c^2$.

We now state the following results.

THEOREM 1. *If* $(A/p)=(B/p)=-1$ *then* $f(x)$ *is irreducible* $(\bmod p)$.

*If* $A\equiv c^2\not\equiv 0$ *put*

$$c_1 = (a+c)^2-16, \qquad c_2 = (a-c)^2-16 . \tag{11}$$

*Then*

$$f(x) \equiv \chi_1\chi_2\chi_3\chi_4 \qquad (c_1Rp,\ c_2Rp) , \tag{12}$$

$$f(x) \equiv \chi_1\chi_2 q \qquad (c_1Rp,\ c_2Np) , \tag{13}$$

$$f(x) \equiv q_1q_2 \qquad (c_1Np,\ c_2Np) , \tag{14}$$

*where (in each instance) the* $\chi_i$ *denote distinct linear polynomials, the* $q_i$ *distinct quadratics.*

*If* $(A/p)=-1$, $B\equiv e^2\not\equiv 0$, *then*

$$f(x) \equiv q_1q_2 . \tag{15}$$

THEOREM 2. *Repeated factors occur only when* (i) $A \equiv 0$ *or* (ii) $A \equiv c^2 \not\equiv 0$ *and either* $c_1$ *or* $c_2 \equiv 0$.
*In case* (i)

(16) $f(x) \equiv \chi_1^2 \chi_2^2$ $(a^2 - 16Rp)$,

(17) $f(x) \equiv q^2$ $(a^2 - 16Np)$,

(18) $f(x) \equiv \chi^4$ $(a^2 - 16 \equiv 0)$.

*In case* (ii)

(19) $f(x) \equiv \chi_1^2 \chi_2 \chi_3$ $(c_1 \equiv 0,\ c_2 Rp)$,

(20) $f(x) \equiv \chi^2 q$ $(c_1 \equiv 0,\ c_2 Np)$

(21) $f(x) \equiv (x-1)^2(x+1)^2$ $(a \equiv 0,\ b \equiv -2)$.

*The numbers* $c_1$, $c_2$ *have the same meaning as in* (11).

We omit the detailed proofs of these theorems. The following numerical examples illustrate each case.

$x^4 + x^3 - x^2 + x + 1$ irreducible (mod 5),

(12)′ $x^4 - 4x^3 + 3x^2 - 4x + 1 \equiv (x-2)(x-6)(x-3)(x-4)$ (mod 11),

(13)′ $x^4 + x^3 - x^2 + x + 1 \equiv (x-5)(x-7)(x^2 - 4x + 1)$ (mod 17),

(14)′ $x^4 + x^2 + 1 \equiv (x^2 - x + 1)(x^2 + x + 1)$ (mod 5),

(15)′ $x^4 + x^3 - x^2 + x + 1 \equiv (x^2 + 2x - 2)(x^2 - x + 3)$ (mod 7),

(16)′ $x^4 + 6x^3 + 6x + 1 \equiv (x-2)^2(x-6)^2$ (mod 11),

(17)′ $x^4 + x^3 - x^2 + x + 1 \equiv (x^2 - 6x + 1)^2$ (mod 13),

(18′) $x^4 + 3x^3 - x^2 + 3x + 1 \equiv (x-1)^4$ (mod 7),

(19)′ $x^4 + x^3 + 7x^2 + x + 1 \equiv (x-1)^2(x-2)(x-6)$ (mod 11),

(20′) $x^4 + x^3 + 9x^2 + x + 1 \equiv (x-1)^2(x^2 + 3x + 1)$ (mod 13).

We remark that for the congruence (1), $A = B = 5$. Thus irreducibility is implied by $(5/p) = -1$, while (12), (14) and (18) cover the remaining cases. It is, however, not obvious that the conditions in (12) are equivalent to $p \equiv 1 \pmod 5$.

Using the well known formulas for the discriminant of a quartic [3, p. 231] we find that the discriminant of the reciprocal quartic

$$f(x) = x^4 + ax^3 + bx^2 + ax + 1$$

is given by

$$27D = 4(b^2 - 3a^2 + 12)^3 - (54a^2 - 9a^2b + 2b^3 - 72b)^2 .$$

A little computation yields the formula

(22) $$d = A^2 B .$$

In this connection note that when $A \equiv 0$

$$f(x) \equiv (x^2 + \tfrac{1}{2}ax + 1)^2 ,$$

while when $B \equiv 0$ we have

$$f(x) \equiv \begin{cases} (x+1)^2\big(x^2+(a-2)x+1\big) & (b+2 \equiv 2a) \\ (x-1)^2\big(x^2+(a+2)x+1\big) & (b+2 \equiv -2a) . \end{cases}$$

A treatment of the general quartic congruence can be found in a paper by Th. Skolem [4].

## REFERENCES

1. L. Carlitz, *Note on a quartic congruence*, Amer. Math. Monthly 63 (1956), 569–571.
2. H. J. S. Smith, *Collected Mathematical Papers*, vol. 1, Oxford, 1894.
3. H. Weber, *Lehrbuch der Algebra*, Bd. 1, zweite Auflage, Braunschweig, 1898.
4. Th. Skolem, *The general congruence of 4th degree modulo p, p prime*. Norsk Mat. Tidsskr. 34 (1952), 73–80.

DUKE UNIVERSITY, DURHAM, N.C., U.S.A.