ACTA ARITHMETICA
XX (1972)

Diagonal forms of prime degree p in a P-adic ring

by

M. Bhaskaran (Kensington, N.S.W.)

We generalize a theorem appearing in [1], in the following way:

Theorem. *Let A be a P-adic ring where P is a prime ideal lying above the rational prime p. Let J_p denote the ring generated by p-th powers of elements of A. Then every element in J_p can be represented by the form*

$$a_1x_1^p+a_2x_2^p+\ldots+a_5x_5^p \tag{1}$$

where the coefficients a_i $(i=1,2,\ldots,5)$ are arbitrary elements in J_p prime to p.

If A is the rational p-adic ring, then four variables will be sufficient.

To prove the theorem, we require the following lemmas.

Lemma 1. *There is a solution for the equation*

$$x_1^p+x_2^p+x_4^p = \mu p$$

in A for a suitable element $\mu\in A$ prime to p.

This is proved in [1], p. 218.

Lemma 2. *Let a be a given element in J_p. Then a can be represented in the form* (1), *if there is a solution for the congruence*

$$a \equiv a_1x_1^p+\ldots+a_4x_4^p \bmod pP. \tag{2}$$

Proof. Let π generate the ideal P. Suppose (2) is satisfied. Then

$$a = a_1X_1^p+\ldots+a_4X_4^p+\lambda p\pi$$

for suitable elements $X_1,\ldots,X_4$, λ in A.

If $\pi\nmid\lambda$, write a in the form

$$a = a_1X_1^p+\ldots+a_4(X_4+\nu\pi)^p-a_4(\nu\pi)^p-a_4x_4^{p-1}\nu p\pi+\lambda p\pi \bmod pP^2$$

where $\nu\in A$.

We can choose ν in such a manner that $\lambda-a_4x_4^{p-1}\nu\equiv 0 \bmod P$.

From this and from the fact that $-a_4(\nu\pi)^p \equiv a_5 X^p(\nu\pi)^p \bmod pP^2$, it follows that there is a solution for the congruence

(3) $$a = a_1 x_1^p + \ldots + a_5 x_5^p \bmod pP^2.$$

If $\pi | \lambda$, it is obvious that there is a solution for (3).

As in [1], we can repeat the process to see that a can be represented in the form (1).

Hence the lemma.

Proof of the theorem. If there is a solution for (2), then there is a solution for the equation $a_1 x_1^p + \ldots + a_4 x_4^p = a$ in the rational p-adic ring. In view of this and Lemma 2, our task is reduced to solving the congruence (2).

Let $\bar{a}_4$ be the inverse of $a_4 \bmod pP$. Multiplying (2) by $\bar{a}_4$ and denoting $a\bar{a}_4$ by a', aa_i by a_i' $(i = 1, \ldots, 5)$, we see that our problem is equivalent to solving the congruence

(4) $$a_1' x_1^p + a_2' x_2^p + a_3' x_3^p + x_4^p \equiv a' \bmod pP.$$

Now we will prove that there is a solution $x_2 = X_2$, $x_3 = X_3$, $x_4 = X_4$ to the congruence

(5) $$a_2' x_2^p + a_3' x_3^p + x_4^p \equiv \mu' p \bmod pP$$

for some μ' prime to p.

It is known that an element in A is in J_p if and only if it is a pth power mod p. Hence it is easy to see that a_2' and a_3' are of this form.

Let

$$a_2' = b_2' p + \mu_2' p \quad \text{and} \quad a_3' = b_3' p + \mu_3' p.$$

If μ_2' and $\mu_3' \equiv 0 \bmod P$, then solving (5) is equivalent to solving

(6) $$(b_2' x_2)^p + (b_3' x_3)^p + x_4^p \equiv \mu p \bmod pP$$

which is possible in view of Lemma 1, since there is always a solution for the linear congruence $ax = b$ in A where a and b are given elements prime to p.

So let us assume that one of the μ_i''s, say μ_2', is prime to π.

Then solve the equation

$$(b_2' x_2)^p + x_4^p = 0$$

by putting $b_2' x_2 = 1$ and $x_4 = -1$ when p is odd. If $\bar{b}_2'$ is the inverse of $b_2' \bmod pP$, we easily see that $X_2 = \bar{b}_2'$, $X_3 = 0$, $X_4 = -1$ is a solution for (6) when p is odd.

Suppose $p = 2$. Put $b_2' x_2 = 1$ and $x_4 = 1$. Then we easily see that $X_2 = \bar{b}_2'$, $X_3 = 0$, $X_4 = 1$ is a solution for (6) when $p = 2$ if $1 + \bar{b}_2'^2 \mu_2'$ is prime to 2. If $1 + \bar{b}_2'^2 \mu_2'$ is not prime to 2, and μ_3' is prime to 2, put $b_2' x_2 = 1$ and $b_3' x_3 = 1$ in (6). If $\bar{b}_2'$ and $\bar{b}_3'$ are the inverses of b_2' and b_3' respectively mod pP, then we see that $X_2 = \bar{b}_2'$, $X_3 = \bar{b}_3'$ and $X_4 = 0$ is a solution for (6). If μ_3' is not prime to 2, then $X_2 = 0$, $X_3 = \bar{b}_3'$ and $X_4 = 1$ is a solution for (6).

Now

(7) $$a' = a_1' Y_1^p + \gamma p$$

for suitable elements Y_1 and γ in A. If $\pi | \gamma$, then by the arguments of Lemma 2, we see that a' can be represented by the form $a_1' x_1^p + a_2' x_2^p$.

So let us assume that γ is prime to π.

Let

$$\gamma = \mu X^p \bmod P$$

for some X in A where μ is the same as in (5).

From (5) and (7), we have

$$a' = a_1' Y_1^p + X^p(a_2' X_2^p + a_3' X_3^p + X_4^p) \bmod pP$$

which is of the form (4).

Hence the theorem.

Reference

[1] M. Bhaskaran, *Sums of p-th powers in a P-adic ring*, Acta Arith. 15 (1969), pp. 217–219.

UNIVERSITY OF NEW SOUTH WALES
Kensington, N.S.W., Australia

Received on 15. 9. 1970 (110)