ACTA ARITHMETICA
XV (1969)

Sums of p-th powers in a P-adic ring

by

M. BHASKARAN (East Lansing, Mich.)

Dedicated to Professor V. G. Iyer

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 is a sum or difference of five p-th powers of elements of A. If A is the rational p-adic ring, then every element in A is a sum of four p-th powers.*

Proof. It is known that every element in J_2 is a sum or difference of three squares. (Stemmler, Acta Arithmetica 6(1961), p. 449). Also it is known that every element in a rational p-adic ring is a sum of four squares. So let us assume p to be $\geqslant 3$. Let a be a unit in J_p. Since every element in J_p is a pth power mod p,

$$a = x_1^p + \mu_1 p, \tag{1}$$

where x_1 and μ_1 are elements in A. If μ_1 is a non-unit, then $a \equiv x_1^p \pmod{p^2}$. Let π be a generator of P and let

$$a = x_1^p + M_1 p\pi.$$

If λ_1 satisfies the congruence $M_1 - x_1^{p-1}\lambda_1 \equiv 0 \pmod{P}$, we easily see that

$$a = (x_1+\lambda_1\pi)^p + (-\lambda_1\pi)^p + M_2 p\pi^2$$

(M_i $(i = 1, 2, \ldots)$ are elements in A).

Again, if λ_2 satisfies the congruence $M_2 - (x_1+\lambda_1\pi)\lambda_2^{p-1} \equiv 0 \pmod{P}$, we see that

$$\begin{aligned} a &= (x_1+\lambda_1\pi+\lambda_2\pi^2)^p + (-\lambda_1\pi)^p + (-\lambda_2\pi^2)^p + M_3 p\pi^3 \\ &\equiv (x_1+\lambda_1\pi+\lambda_2\pi^2)^p + (-\lambda_1\pi-\lambda_2\pi^2)^p \pmod{pP^3}. \end{aligned}$$

This process can be repeated any number of times to see that a is a sum of two pth powers modulo any power of p. Hence, a is a sum of two pth powers. Suppose μ_1 is a unit. Now, we prove that there is a solution for the congruence

(2) $$y_1^p + y_2^p + y_3^p \equiv 0 \pmod{p}$$

with

(3) $$(y_1^p + y_2^p + y_3^p)/p \quad \text{a unit.}$$

Let us take $y_1 = y_2 = 1$ and $y_3 = -2$. Then (2) is satisfied. If $2^p \equiv 2 \pmod{p^2}$, (3) is not satisfied. Then take $y_1 = 1$, $y_2 = 2$ and $y_3 = -3$. If $3^p \equiv 3 \pmod{p^2}$, (3) is not satisfied.

Continue this process. We see that we can continue only a finite number of times, since $(p-1)^p \not\equiv p-1 \pmod{p^2}$. So, after a certain stage, we have a solution for congruence (2) satisfying (3). Let μ_1 be written in the form

(4) $$x_2^p + \mu_2 \pi$$

where x_2 and μ_2 are some elements of A. Substituting (4) in (1), we have

(5) $$a = x_1^p + p x_2^p + \mu_2 p \pi .$$

Let

(6) $$y_1^p + y_2^p + y_3^p = \mu_3 p,$$

where μ_3 is some unit in A. Now, the congruence

(7) $$x_2^p \equiv \mu_3 x^p \pmod{P}$$

has a solution since every element in A is a pth power mod P. Applying (7) and (6) to (5), we get

(8) $$a \equiv x_1^p + x^p (y_1^p + y_2^p + y_3^p) \pmod{pP}.$$

Hence, it easily follows that a is a sum of five pth powers. If a in a non-unit, then also a is a sum of five pth powers. The proof is similar to that of the case of non-units in a rational p-adic ring which is given below. ($p-a$ in (9) is replaced by $\pi - a$ and mod p and mod p^2 in (10) and (11) respectively are replaced by mod P and mod pP).

For the rational p-adic ring, the best possible bound can be obtained. In this case, we replace P by p in (8) and then it follows that every unit is a sum of four pth powers. Now, consider a non-unit. It is of the form βp where β is a unit and $t \geqslant 1$. If $t > 1$,

(9) $$\beta p^t \equiv a^p + (p-a)^p \pmod{p^2}$$

where a is any unit. From (9), it follows easily that βp^t is a sum of two pth powers. If $t = 1$, let us consider (6). μ_3 and β being units, there is a non-unit x such that

(10) $$\mu_3 x^p \equiv \beta \pmod{p}.$$

From (6) and (10), we have

(11) $$\beta p \equiv (y_1^p + y_2^p + y_3^p) x^p \pmod{p^2}.$$

From (11), it easily follows that βp is a sum of three pth powers. Hence, in a rational p-adic ring, every element is a sum of four pth powers. This bound is the best possible since 9 cannot be expressed as a sum of three 7th powers in the 7-adic ring.

MICHIGAN STATE UNIVERSITY
East Lansing, Michigan

Reçu par la Rédaction le 22. 3. 1968