Rendiconti del Seminario Matematico della Università di Padova

Haridas Bagchi

Note on the two congruences $ax^2 + by^2 + e \equiv 0$, $ax^2 + by^2 + cz^2 + dw^2 \equiv 0$ (mod. p), where p is an odd prime and $a \neg\equiv 0, b \neg\equiv 0, c \neg\equiv 0, d \neg\equiv 0$ (mod. p)

Rendiconti del Seminario Matematico della Università di Padova, tome 18 (1949), p. 311-315

<http://www.numdam.org/item?id=RSMUP_1949__18__311_0>

NOTE ON THE TWO CONGRUENCES $ax^2 + by^2 + e \equiv 0$, $ax^2 + by^2 + cz^2 + dw^2 \equiv 0 \pmod{p}$, WHERE p IS AN ODD PRIME AND $a \not\equiv 0$, $b \not\equiv 0$, $c \not\equiv 0$, $d \not\equiv 0 \pmod{p}$

Nota (*) *di* HARIDAS BAGCHI, M. A., Ph. D.
Offg. Head of the Department of Pure Mathematics, Calcutta University.

Introduction. - The object of the present note is to generalise two *known* propositions of the Theory of Numbers, *viz.*, that each of the two arithmetical congruences:

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

$$\text{and} \quad (ii) \qquad x^2 + y^2 + z^2 + w^2 \equiv 0, \qquad \pmod{p}$$

is possible, provided that p is an odd prime. The basic principle to be made use of is the same as that employed by Professors HARDY and WRIGHT in the book noted below (1).

---

1. - Suppose that p is an odd prime and that a, b, c are integers prime to p.

Then in the first place we observe that, as x runs through the sequence of integral values:

$$(1) \qquad 0, 1, 2, 3, \ldots, \frac{p-1}{2},$$

(*) Pervenuta in Redazione il 19 Maggio 1949.

(1) Vide HARDY and WRIGHT's « *Theory of Numbers* » (1945), § 6 · 7 (p. 70) and § 20 · 5 (p. 300).

no two integers of the set:

(2) $$\{ ax^2 \},$$

can be congruent. For a congruential relation of the form:

$$ax_1^2 \equiv ax_2^2 \qquad (\text{mod. } p),$$

would be equivalent to:

$$a(x_1 + x_2)(x_1 - x_2) \equiv 0 \qquad (\text{mod. } p).$$

This is absurd, seeing that:

and: $$a \not\equiv 0 \qquad (\text{mod. } p);$$

$$x_1 + x_2 \not\equiv 0, \quad x_1 - x_2 \not\equiv 0 \quad (\text{mod. } p),$$

for $x_1 < \frac{p}{2}$ and $x_2 < \frac{p}{2}$.

Hence the $\frac{p+1}{2}$ numbers of the set (2) must be all *incongruent*.

In the second place we notice that, when y runs through the series of integral values (1), no two members of the set:

(3) $$\{ -by^2 - e \},$$

can be congruent. For a relation like:

$$-by_1^2 - e \equiv -by_2^2 - e \qquad (\text{mod. } p),$$

would be tantamount to:

$$b(y_1 + y_2)(y_1 - y_2) = 0 \qquad (\text{mod. } p).$$

But such a relation is untenable, for

$$b \not\equiv 0 \qquad (\text{mod. } p),$$

and: $$y_1 + y_2 \not\equiv 0, \quad y_1 - y_2 \not\equiv 0 \qquad (\text{mod. } p),$$

for $$y_1 < \frac{p}{2}, \qquad y_2 < \frac{p}{2}.$$

Consequently the $\frac{p+1}{2}$ numbers of the set (3) must be all *incongruent*. Bearing in mind that the residue of an arbitrary or unrestricted integer *w.r.t.* the modulus p must belong to the set of p numbers, *viz.*:

$$0, 1, 2, \ldots\ldots, p-1,$$

it follows that the totality of a set of mutually incongruent integers can never exceed p. Hence remarking that the aggregate number of integers, included in the two sets (2) and (3), (counted together), is:

$$\frac{p+1}{2} + \frac{p+1}{2} > p,$$

we reach the conclusion that *some* number of the set (2) must be congruent to *some* number of the set (3), so that the congruence:

$$ax^2 \equiv -by^2 - c \qquad (\text{mod}, p),$$

must be *possible*.

We have thus disposed of the generalised form of the congruence (*i*), mentioned in the *Introduction*. The generalised proposition may be formally enunciated as follows:

If p be an odd prime and:

$$a \not\equiv 0, \quad b \not\equiv 0, \quad e \not\equiv 0, \qquad (\text{mod. } p),$$

then there must exist integers x, y, which are each numerically $< \frac{p}{2}$ and satisfy the congruence:

$$ax^2 + by^2 + e \equiv 0, \qquad (\text{mod. } p).$$

It is scarcely necessary to add that because of the relation: $e \not\equiv 0$ (mod. p), x, y cannot vanish simultaneously.

2. - We shall now start with four given integers, each of which is prime to an odd prime number p.

Then, by Art. 1, each of the two congruences:

$$ax^2 + by^2 + e \equiv 0 \qquad (\text{mod. } p),$$

$$cz^2 + dw^2 - e \equiv 0 \qquad (\text{mod. } p),$$

is possible; so that by addition the congruence:

$$ax^2 + by^2 + cz^2 + dw^2 \equiv 0 \qquad (\text{mod. } p),$$

is also possible.

We have thus arrived at the *extended* form of the congruence (*ii*), mentioned in the Introduction. The extended proposition evidently reads as follows:

If p be an odd prime and

$$a \not\equiv 0, \quad b \not\equiv 0, \quad c \not\equiv 0, \quad d \not\equiv 0 \qquad (\text{mod. } p),$$

then there must exist integers x, y, z, w (not all zero), which are each $< \frac{p}{2}$ and conform to the congruential relation:

$$ax^2 + by^2 + cz^2 + dw^2 \equiv 0, \qquad (\text{mod. } p).$$

That is to say, subject to the afore-said restrictions on a, b, c, d, it must be possible to choose the integers x, y, z, w, so that the integer

(I) $$ax^2 + by^2 + cz^2 + dw^2$$

shall be a multiple of p (say, np).

In the particular case when $a = b = c = d = 1$, we know (²) that the least multiple of an odd prime p, which admits of representation in the form (I), is no other than p itself.

Inquisitive readers may propose to tackle the similar problem in the more general case, when a, b, c, d are any given integers, prime to p. The precise form of the query is to investigate about the *least* multiple of a given odd prime number p, which can, by a proper adjustment of the integers x, y, z, w, be put in the form:

$$ax^2 + by^2 + cz^2 + dw^2 ,$$

it being implied that a, b, c, d are four *pre-assigned* integers, prime to p.

(²) See Hardy and Wright (loc. cit., Art. 20 · 5, p. 300).