Bollettino Unione Matematica Italiana

Richard Bellman

A note on the solution of polynomial congruences.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **19** (1964), n.1, p. 60–63.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1964_3_19_1_60_0>

A note on the solution of polynomial congruences

Nota di RICHARD BELLMAN (California U. S. A.) (*)

Summary. - *The number of solutions of the congruence*

$$(1) \qquad f(x) \equiv 0(p),$$

where $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, *may, as is well known, be expressed in the form*

$$N = \frac{1}{p} \sum_{t,x} e^{2\pi i t f(x)/p},$$

where t *and* x *run independently through the values* 0, 1, 2, ..., p − 1. *This result is an immediate consequence of the relation*

$$\sum_t e^{2\pi i t y/p} = 0, \qquad y \not\equiv 0(p),$$
$$= p, \qquad y \equiv 0(p).$$

In this note we wish to present an alternative expression for the number of solutions of (1).

1. Introduction.

The number of solutions of the congruence

$$(1.1) \qquad f(x) \equiv 0(p),$$

where $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, may, as is well known, be expressed in the form

$$(1.2) \qquad N = \frac{1}{p} \sum_{t,x} e^{2\pi i t f(x)/p},$$

where t and x run independently through the values 0, 1, 2, ...,

(*) Pervenuta alla Segreteria dell' U. M. I. il 24 dicembre 1963.

$p-1$. This result in an immediate consequence of the relations

$$(1.3)\qquad \sum_t e^{2\pi i t y/p} = 0, \qquad y \not\equiv 0(p),$$
$$= p, \qquad y \equiv 0(p).$$

In this note we wish to present an alternative expression for the number of solutions of (1.1).

2 An equivalent vector-matrix congruence.

The equation $f(x) = 0$ is readily seen to be the characteristic equation of the matrix

$$(2.1)\qquad A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ -a_n & -a_{n-1} & -a_{n-2} & \dots & -a_1 \end{bmatrix},$$

see [1], p. 225.

Using arguments completely analogous to that for the complex field, we see that a necessary and sufficient condition for a non-trivial solution of the vector-matrix congruence

$$(2.2)\qquad Ax \equiv \lambda x(p)$$

where x is now the n-dimensional column vector with components $x_1, x_2, \dots, x_n$, and λ is a scalar, is that

$$(2.3)\qquad f(\lambda) \equiv 0(p).$$

Each root of (2.3) generates a ray of solutions kx, where $k = 1, 2, \dots, p-1$.

3. Multidimensional exponential sum.

Let t be an n-dimensional vector with components $t_1, t_2, \dots, t_n$ and let (t, x) denote, as usual, the vector inner product. We can then write, as the number of nontrivial solutions of (2.2),

$$\sum_t \sum_\lambda \sum_x{}' e^{\frac{2\pi i}{p}(t,\, Ax-\lambda x)}, \tag{3.1}$$

where (u, v) denotes the usual in inner product and Σ' denotes the fact that $x = 0$ is omitted in the summation.

Since each solution of $f(\lambda) = 0$ generates $p-1$ solutions of (2.2), we have

$$N = \frac{1}{p^n(p-1)} \sum_t \sum_\lambda \sum_x{}' e^{\frac{2\pi i}{p}(t,\, Ax-\lambda x)} \tag{3.2}$$

We eliminate the prime by writing

$$N = \frac{1}{p^n(p-1)} \sum_{t,\lambda,x} e^{\frac{2\pi i}{p}(t,\, Ax-\lambda x)} - \frac{p}{p-1}. \tag{3.3}$$

Summing over the scalar λ first, we have finally

$$N = \frac{1}{p^{n-1}(p-1)} \sum_{(t,x)\equiv 0(p)} e^{2\pi i(t\; Ax)/p} - \frac{p}{p-1}. \tag{3.4}$$

If A is symmetric, we write $t = u+v$, $x = u-v$, and obtain

$$N = \frac{1}{p^{n-1}(p-1)} \sum_{(u,u)\equiv(v,v)(p)} e^{\frac{2\pi i}{p}[(u,\, Au)-(v,\, Av)]} - \frac{1}{p-1}. \tag{3.5}$$

This, in turn, may be written

$$N = \frac{1}{p^{(n-1)}(p-1)} \sum_k \Big| \sum_{(u,u)\equiv k(p)} e^{\frac{2\pi i}{p}(u,\, Au)} \Big|^2 - \frac{p}{p-1}, \tag{3.6}$$

an interesting formula.

4. Example.

Consider the congruence

$$\lambda^3 + a \equiv 0(p). \tag{4.1}$$

The corresponding matrix is

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & 0 & 0 \end{bmatrix} \tag{4.2}$$

Hence. the number of solutions of (4.1) is given by

$$N = \frac{1}{p^2(p-1)} \sum_S e^{\frac{2\pi i}{p}(t_1 x_2 + t_2 x_3 - a t_3 x_1)} - \frac{p}{p-1}, \tag{4.3}$$

where the set of values S is determinea by

$$t_1 x_1 + t_2 x_2 + t_3 x_3 = 0.$$

REFERENCE

[1] R. Bellman, *Introduction to Matrix Analysis*, McGraw Hill Book Company. Inc., New York, 1960.