Werk

Label: Article

Jahr: 1950

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0075|log134

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

A SHORT PROOF OF A THEOREM OF ŠT. SCHWARZ CONCERNING FINITE FIELDS.

L. RÉDEI, Szeged (Hungary).

(Received January 23th, 1950.)

SCHWARZ[1]) recently proved a theorem concerning the important problem of factorization of binomal polynomials in finite fields. He also gave[1]) interesting applications of his theorem, especially a generalization of the VINOGRADOV'S estimation of the least primitive root mod p. The theorem mentioned above is as follows:[2])

Let K be a finite field of characteristic p having P elements. Then the polynomial

$$x^m - a \quad (a \neq 0, \epsilon K;\ p \nmid m) \tag{1}$$

has in the field K just

$$\frac{1}{k}\sum_{t|k}'\mu\left(\frac{k}{t}\right)d_t \quad (d_t = (m, P^t - 1)) \tag{2}$$

irreducible factors of degree k, the summation being extended over all t with

$$a^{d'_t} = 1 \quad \left(d'_t = \frac{P^t - 1}{d_t}\right) \tag{3}$$

and $\mu(t)$ being the MÖBIUS function.

In what follows I give an elegant proof of this important theorem. The proof is based upon a Lemma which — as far as I am informed — is unknown in the formulation given here.

Lemma. The greatest common divisor of the polynomials

$$x^m - a,\ x^n - b \quad (a, b \neq 0;\ m, n \geqq 1) \tag{4}$$

in an arbitrary field has the degree 0 or $d = (m, n)$. The second case occurs, if and only if the relation

$$a^{\frac{n}{d}} = b^{\frac{m}{d}} \tag{5}$$

holds.

[1]) ŠT. SCHWARZ: On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent mod p, Časopis pro pěst. mat. a fys., **74** (1949), p. 1—16.

[2]) L. c. p. 2 (Theorem 1) and p. 13 (Generalization of Theorem 1).