



Problem 11. «Conjecture»

Let \mathbb{F}_2 be the finite field with two elements and n be any positive integer larger than or equal to 3. Let $f(X)$ be an irreducible polynomial of degree n over \mathbb{F}_2 . It is known that the set of the equivalence classes β of polynomials over \mathbb{F}_2 modulo $f(X)$ is a finite field of order 2^n , that we shall denote by \mathbb{F}_{2^n} . It is known that different choices of the irreducible polynomial give automorphic finite fields and such choice has then no incidence on the algebraic problems on the corresponding fields.

Problem for a special prize! Prove or disprove the following

Conjecture. Let k be co-prime with n . For every $\beta \in \mathbb{F}_{2^n}$, let $F(\beta) = \beta^{4^k - 2^k + 1}$. Let $\Delta = \{F(\beta) + F(\beta + 1) + 1; \beta \in \mathbb{F}_{2^n}\}$. For every distinct nonzero v_1, v_2 in \mathbb{F}_{2^n} , we have

$$|\{(x, y, z) \in \Delta^3; v_1x + v_2y + (v_1 + v_2)z = 0\}| = 2^{2n-3}.$$

Example for $n = 3$: we can take $f(X) = X^3 + X + 1$, then each element β of the field \mathbb{F}_{2^3} can be written as a polynomial of degree at most 2: $a_0 + a_1X + a_2X^2$, with $a_0, a_1, a_2 \in \mathbb{F}_2$. The element 0 corresponds to the null polynomial; and the unity, denoted by 1, corresponds to the constant polynomial 1. We can calculate the table of multiplication in \mathbb{F}_{2^3} (the table of addition just corresponds to adding polynomials of degree at most 2); this allows calculating any power of any element of the field and check the property.