STUFE OF A FINITE FIELD

SAHIB SINGH
Clarion State College, Clarion, Pennsylvania 16214

INTRODUCTION

Stufe of a field is connected with the property of integer -1 in that field. It is defined to be the least integer s such that $-1 = \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_s^2$, where each α_i belongs to the field. In [2] Chowla and Chowla have determined the stufe of a cyclotomic field. Pfister has shown in [3] that the stufe of a finite field is ≤ 2. Our aim is to elaborate this result further. We do this in the following theorem.

Theorem. Stufe of $GF(p^n)$, where p is prime and $n \geq 1$, is always one except for the case when n is odd and $p \equiv 3 \pmod 4$, in which case its value is two.

Proof. We know that the non-zero elements of $GF(p^n)$, denoted by $GF^*(p^n)$, form a cyclic multiplicative group. Also, it is well known that if G is a cyclic group of order k and m divides k, then there exists a unique subgroup of order m in G. Since $(p - 1)$ divides $(p^n - 1)$ for all n, therefore it follows that the members of $GF^*(p)$ constitute the unique subgroup of order $(p - 1)$ in $GF^*(p^n)$. Now we develop the proof by considering different cases.

Case 1. Let $p = 2$. If λ is a generator of $GF^*(2^n)$, then $\lambda^{(2^n-1)} = 1$, which means that $\lambda^{2^n} = \lambda$ implying that λ is a square which enables us to conclude that each element of $GF^*(2^n)$ is a square and thus -1 is a square. In the subsequent cases, p is understood to be an odd prime.

Case 2. Let n be even. From the above analysis it is clear that if λ is a generator of $GF^*(p^n)$, then

$$\lambda^{\left(\frac{p^n-1}{p-1}\right)}$$

is a primitive root mod p. In view of the values of p and n we conclude that

$$\left(\frac{p^n - 1}{p - 1}\right)$$

is even, which again means that this primitive root mod p is a square implying that -1 is a square.

Case 3. Let n be odd. In this case,

$$\frac{p^n - 1}{p - 1}$$

is odd. Thus half the members of $GF^*(p)$ which are quadratic residues mod p would be squares and the remaining half are not. If $p \equiv 1 \pmod 4$, it is well known that (-1) is a quadratic residue mod p and hence is a square. If $p \equiv 3 \pmod 4$, then (-1) is a quadratic non-residue mod p and therefore is not a square. In this case -1 is the sum of two squares, which easily follows from (3) or (4).

REFERENCES

1. G H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1965.
2. P. Chowla and S. Chowla, "Determination of the Stufe of Certain Cyclotomic Fields," Journal of Number Theory, Vol. 2 (1970), pp. 271-272.
3. Albert Pfister, "Zur Darstellung Von — I Als Summe Von Quadraten in einem Körper," Journal of London Math. Society, Vol. 40 (1965), pp. 159-165.
4. Sahib Singh, "Decomposition of Each Integer as Sum of Two Squares in a Finite Integral Domain," to appear in the Indian Journal of Pure and Applied Mathematics.
5. B. L. Van Der Waerden, Algebra, Vol. 1, Frederick Ungar Pub. Co., N. Y., 1970.

(Continued from page 79.)

(i)
$$L_n = \prod_{k=1}^{[n/2]} (\omega^{2k-1} + 3 + \omega^{-2k+1})$$

(ii)
$$F_n = \prod_{k=1}^{[n/2]} (\omega^{2k} + 3 + \omega^{-2k}) .$$

Donald E. Knuth
Professor
Stanford University
Stanford, California 94305

FIBONACCI CURIOSITY

The THIRTEENTH PERFECT NUMBER is built on the prime $p = 521 = L_{13}$

$$2^{520}(2^{521} - 1) .$$

Brother Alfred Brousseau