BOUND FOR THE SOLUTIONS OF A DIOPHANTINE EQUATION IN PRIME GALOIS FIELDS

by SAHIB SINGH, *Department of Mathematics, Clarion State College, Clarion, Pennsylvania* 16214

(*Received* 8 *September* 1975)

This paper establishes a bound for the solutions of $x^2+1=y^3$ in prime Galois fields.

The equations $x^2 + c = y^3$ where c varies over rational integers have been investigated by many authors. It is well known that $x^2 + 1 = y^3$ admits no rational integral solution except the trivial one when $x = 0$ (Dickson 1966). Our aim is to examine this equation $x^2 + 1 = y^3$ in $GF(p)$ for all odd primes p, allowing for the exceptions, and look for the existence of its solution $\{ a, a + 1 \}$ with $a \neq 0$, $a + 1 \neq 0$ in $GF(p)$ so that $x^2 \equiv a \pmod{p}$ and $y^3 \equiv (a + 1) \pmod{p}$ hold. We further explore for the existence of an exact upper bound β_1 such that for all odd primes p, with a finite number of exceptions, the above solutions $\{ a, a + 1 \}$ satisfy the condition of $a + 1 \leqslant \beta_1$. It may be stated that for our reference the field $GF(p)$ is understood to have its members the integers $0, 1, 2, \ldots, (p - 1)$ with the two binary operations as addition modulo p and multiplication modulo p respectively.

The above problem under consideration is of the same type as the ones discussed by Dunton (1965) and Bierstedt and Mills (1963) where the upper bounds sought were for the solutions of $x^3 - y^3 = 1$ and $x^4 - y^4 = 1$ respectively in prime Galois fields. For additional information relating to problems of this or more general nature one may refer to Jordan (1964), Lehmer and Lehmer (1962), Lehmer *et al.* (1963), and Singh (1970*a*, *b*).

Since each non-zero member of $GF(p)$ is a cubic residue when $p \equiv 2 \pmod{3}$, therefore we confine ourselves to only those primes p which satisfy $p \equiv 1 \pmod{3}$. It is easy to see that this equation $x^2 + 1 = y^3$ possesses no non-trivial solution in $GF(7)$. We analyse this equation further to show that it is solvable in every $GF(p)$ with $p \neq 7$.

Let ψ denote cubic character mod p and 'ω' an imaginary cube root of unity. In what follows the pairs of integers $\{ a, a + 1 \}$ shown after the symbol $\Rightarrow$ constitute a solution of our equation under the corresponding assumed hypothesis.

(i) $\psi(2) = 1 \Rightarrow \{ 1, 2 \}$

(ii) $\psi(2) = \omega$, $\psi(5) = \omega^2 \Rightarrow \{ 9, 10 \}$

(iii) $\psi(2) = \omega$, $\psi(5) = \omega \Rightarrow \{49, 50\}$

(iv) $\psi(5) = 1 \Rightarrow \{4, 5\}$.

The hypothesis $\psi(2) = \omega^2$ does not yield any new values. Thus it follows that for all primes p greater than 47, we have the existence of at least one solution $\{a, a + 1\}$ of the equation in $GF(p)$. A simple verification shows that our equation is solvable in $GF(p)$ for each odd prime $p \leqslant 47$ where p is different from 7. From above it is also obvious that $a + 1 \leqslant 50$ holds for at least one solution $\{a, a + 1\}$ in $GF(p)$ where p is any odd prime other than 7. Thus we have proved the following theorem.

Theorem 1—There always exists a non-trivial solution $\{a, a + 1\}$ of $x^2 + 1 = y^3$ in $GF(p)$ with $a + 1 \leqslant 50$ where p is any odd prime different from 7.

Now we show that the integer '50' stated in Theorem 1 is an exact upper bound which is attained for infinitely many primes p. For proving this we first give a theorem due to Mills which is a generalization of Kummer's result (Mills 1963). For our reference we call this theorem as Kummer-Mills Theorem which can be stated as under:

Kummer-Mills Theorem—Let n be either an odd integer or an even integer from 2, 4, $2p'$ with p' a prime $\equiv 3 \pmod 4$ and $p_1, p_2, \ldots, p_t$ be any set of distinct primes (different from n, if n is prime). Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_t$ denote nth roots of unity, not necessarily distinct. Then there exist infinitely many primes p satisfying $\psi(p_j) = \varepsilon_j$ $(j = 1, 2, \ldots, t)$ where ψ denotes nth power character mod p.

In order to prove our assertion we assume hence onward that the prime p considered is greater than 47. Let g be a primitive root modulo p. Let ψ_1 be the 6th power character mod p defined by $\psi_1(m) = \beta^b$ where $m \equiv g^b \pmod p$ and $\beta = e^{\frac{2\pi i}{6}}$. Then we conclude that m is a cubic residue mod p if and only if 3 divides b and m is a quadratic residue mod p if and only if b is even. Our chief aim is to define suitably the 6th power character mod p which should not allow the appearance of a solution $\{a, a + 1\}$ before $\{49, 50\}$. Let the 6th power character ψ_1 mod p satisfy the following:

$\psi_1(13) = 1$, $\psi_1(q) = \beta$ where $q \neq 13$ and q varies over all primes $\leqslant 47$ and β is defined as above. By Kummer-Mills Theorem, we have the existence of an infinite number of such primes p which can be used in the above definition of ψ_1. Thus using this definition of 6th power character ψ_1 mod p, we can easily verify that the first non-trivial solution of our equation in every such $GF(p)$ would be $\{49, 50\}$. Thus we have proved the following theorem.

Theorem—There exist infinitely many primes p such that for each such p the first pair of non-trivial consecutive members $\{a, a + 1\}$ with 'a' a quadratic residue and '$(a + 1)$' a cubic residue mod p is with $a + 1 = 50$.

REFERENCES

Bierstedt, R. G., and Mills, W. H. (1963). On the bound for a pair of consecutive quartic residues of a prime. *Proc. Am. math. Soc.*, **14**, 628-32.

Dickson, L. E. (1966). History of The Theory of Numbers, Vol. 2. Chelsea Publishing Company, New York, pp. 539.

Dunton, M. (1965). Bounds for pairs of cubic residues. *Proc. Am. math. Soc.*, **16**, 330-32.

Jordan, J. H. (1964). Pairs of consecutive power residues or non-residues. *Can. J. Math.*, **16**, 310-14.

Lehmer, D. H., and Lehmer, Emma (1962). On runs of residues. *Proc. Am. math. Soc.*, **13**, 102-106.

Lehmer, D. H., Lehmer, E., and Mills, W. H. (1963). Pairs of consecutive power residues. *Can. J. Math.*, **15**, 172-77.

Mills, W. H. (1963). Characters with preassigned values. *Can. J. Math.*, **15**, 169-71.

Singh, Sahib (1970a). Bounds of quadratic residues in arithmetic progression. *J. Number Theory*, **2**, 162-67.

Singh, Sahib (1970b). Bounds of cubic residues in A.P. *Indian J. pure appl. math.*, **1**, 265-68.