Indian J. pure appl. Math., **10**(10) : 1213-1215, October 1979

INTEGER POINTS ON SPECIAL HYPER-ELLIPTIC CURVES IN $GF(p)$

SAHIB SINGH

Department of Mathematics, Clarion State College, Clarion, Pennsylvania 16214, *U.S.A.*

(*Received* 22 *January* 1979)

The bounds for the solution x of the equations $y^2 = (x + a_1)(x + a_2)$ and $y^2 = x(x + t)$ in $GF(p)$ have been discussed.

Chowla and Chowla (1976) made a conjecture that if $a_1, a_2, \ldots, a_r$ are positive rational integers, then there exists a solution x of the equation $y^2 = (x + a_1)(x + a_2) \ldots (x + a_r)$ in $GF(p)$. This solution x satisfies the inequality $x \leqslant B(r)$ for all primes $p > C(r)$ where $B(r)$ and $C(r)$ depend only on the a's and r and not on p. Stephens (1977) has proved this conjecture by using an indirect approach. In his note he concludes that $B(r) = 2^{2a_r}$. In this paper, we give a new and direct proof including some more results when $r = 2$. Our bound is comparatively very small.

For our purpose, the members of $GF(p)$ are $0, 1, 2, 3, \ldots, (p - 1)$ with the binary operations as addition modulo p and multiplication modulo p respectively. The first result in this connection can be formulated in the following theorem :

Theorem 1 — If a_1 and a_2 are distinct rational integers > 0 with $a_1 < a_2$, then there exists a solution $x \geqslant 0$ of the equation $y^2 = (x + a_1)(x + a_2)$ in $GF(p)$ satisfying the inequality $x \leqslant a_2$ for all $p > 2a_2$.

PROOF : Using Legendre's symbol we conclude that $x = 0$ is a solution of the equation if $(a_1 a_2/p) = 1$.

If $(2a_1(a_1 + a_2)/p) = 1$, then it is obvious that $x = a_1$ is a solution.

Under the hypothesis $(2a_1(a_1 + a_2)/p) = (a_1 a_2/p) = -1$, we obtain on multiplication $(2a_1^2 a_2(a_1 + a_2)/p) = 1$ which implies $(2a_2(a_1 + a_2)/p) = 1$ yielding $x = a_2$ as a solution of the given equation. This completes the proof.

It can be easily inferred on the lines of Chowla and Chowla (1976) that the solution $x = a_2$ in Theorem 1 would be attained for infinitely many primes. The actual computation of primes for this purpose would require the solution to satisfy certain equations simultaneously.

Illustration — As an illustration, we consider the equation $y^2 = (x + 1)(x + 5)$. We search for primes p which do not admit any solution $x < 5$. This means that the primes p under this hypothesis must satisfy the following conditions :

$$(2/p) = (3/p) = (5/p) = -1 \ ; (7/p) = 1.$$

It is easy to see that the first such prime p which has $x = 5$ as the least solution of the equation is 53 and the next successive prime is 197.

Strong Condition — If we make the condition strong, as stated in the conjecture, and require that the solution x referred to in Theorem 1 above should be > 0, then we formulate the problem equivalently in the following theorem.

Theorem 2 — If a and t are rational integers > 0, then there exists a solution $x > 0$ of the equation $y^2 = (x + a)(x + a + t)$ in $GF(p)$ which satisfies the inequality $x < (2n + 1)t - a$ for all primes $p > (2n + 2)t$ where $n = [a/t] + 1$. Here $[a/t]$ denotes the largest integer that does not exceed the rational number a/t.

PROOF : By archimedean property, there exists a least positive integer n such that $nt > a$. Clearly this n is same as defined in the statement of Theorem 2. Now we complete the proof on the lines of Theorem 1.

If $(n(n + 1)/p) = 1$, then $nt - a$ is a solution of

$$y^2 = (x + a)(x + a + t). \quad \ldots(1)$$

If $(n(n + 1)/p) = -1$, then we have two cases for discussion :

Case 1 : $\left(\frac{n}{p}\right) = -1, \left(\frac{n+1}{p}\right) = 1$

(i) If $(4n + 2)/p = 1$, then using $(n + 1)/p = 1$ we get

$$\left(\frac{(4n+2)(n+1)}{p}\right) = 1$$

or

$$\left(\frac{(2n+1)(2n+2)}{p}\right) = 1.$$

This yields $x = (2n + 1)t - a$ as a solution of (1).

(ii) If $(4n + 2)/p = -1$, then using $(n/p) = -1$ we obtain

$$\left(\frac{(4n+2)n}{p}\right) = 1$$

or

$$\left(\frac{2n(2n+1)}{p}\right) = 1.$$

This leads to $2nt - a$ as a solution of (1).

Case 2 : $\left(\frac{n}{p}\right) = 1, \left(\frac{n+1}{p}\right) = -1$

By repeating the arguments as in Case 1, we conclude that by using $(4n + 2)/p = 1$, we obtain $2nt - a$ as a solution of (1) where as $(4n + 2)/p = -1$

leads to $(2n + 1)t - a$ as a solution of (1). This takes care of all possibilities and the proof is complete.

Corollary — If $t > 0$, there exists a solution $x > 0$ in $GF(p)$ of $y^2 = x(x + t)$ which satisfies the inequality $x \leqslant 3t$ for all primes $p > 4t$.

PROOF : It is obvious from Theorem 2 above.

By applying the result of Theorem 2 (Singh 1970) we get another bound for the solution x of the equation $y^2 = x(x + t)$ in $GF(p)$. This bound for x satisfies

$$x \leqslant \left(\frac{t-1}{2}\right)^2 \text{ for all } t \geqslant 7.$$

However, the integer 7 mentioned above can be replaced by 5 by observing that $y^2 = x(x + 6)$ has a solution $x = 2$ and $y^2 = x(x + 5)$ is satisfied by $x = 4$.

Thus we conclude that for $t \geqslant 5$, a solution x of $y^2 = x(x + t)$ satisfies $x \leqslant \left(\frac{t-1}{2}\right)^2$. If $t < 5$, then by simple computation it follows that $y^2 = x(x + t)$ has a solution $x \leqslant B(t)$ where

$t =$	1	2	3	4
$B(t) =$	3	4	1	6

Thus by combining the results of this discussion with the result of the above corollary, we have proved the following theorem :

Theorem 3 — If t is a rational integer > 0, then a solution $x > 0$ of $y^2 = x(x + t)$ in $GF(p)$ satisfies the inequality $x \leqslant B(t)$ for all primes $p > B(t) + t$ where

$$B(t) = \max\left\{6, \left(\frac{t-1}{2}\right)^2\right\} \quad \text{when} \quad t \leqslant 13$$

$$= 3t \qquad \text{for} \quad t > 13$$

Remark : The values $B(13)$ and $B(100)$ by our result are 36 and 300 respectively where as the conclusion derived in Stephens (1977) gives $B(13) = 2^{26}$ and $B(100) = 2^{200}$.

REFERENCES

Chowla, P., and Chowla, S. (1976). On the integer points on some special hyper-elliptic curves over a finite field. *J. Number Theory*, **8**, 280-81.

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

Stephens, N. M. (1977). On a conjecture of Chowla and Chowla. *J. Number Theory*, **9**, 276-77.