JOURNAL OF NUMBER THEORY 8, 280–281 (1976)

On the Integer Points on Some Special Hyper-elliptic Curves over a Finite Field

P. CHOWLA AND S. CHOWLA

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

Communicated by S. Chowla

Received July 9, 1973

If $\ell_r(p)$ is the least positive integral value of x for which $y^2 \equiv x(x+1) \cdots (x+r-1) \pmod p$ has a solution, we conjecture that $\ell_r(p) \leqslant r^2 - r + 1$ with equality for infinitely many primes p. A proof is sketched for $r = 5$. A further generalization to $y^2 \equiv (x + a_1) \cdots (x + a_r)$ is suggested, where the a's are fixed positive integers.

1

Consider the equation

$$y^2 \equiv x(x+1)(x+2) \cdots (x+r-1) \pmod p \tag{1}$$

where, on the right, we have a product of r consecutive factors.

We conjecture that when the prime p exceeds a certain limit depending on r alone, (1) always has a solution with

$$1 \leqslant x \leqslant B(r),$$

where $B(r)$ depends on r alone and is independent of the prime p.

Moreover, we conjecture that *when r is a prime*, we may take

$$B(r) = r^2 - r + 1,$$

and that this bound cannot be improved. This means that when r is a prime there exist primes p for which (1) has no solution for $1 \leqslant x < r^2 - r + 1$ but has a solution for $x = r^2 - r + 1$.

We illustrate the conjecture with a proof for $r = 5$. We wish to show that the congruence

$$y^2 \equiv x(x+1) \cdots (x+4) \pmod p \tag{2}$$

always has a solution with $1 \leqslant x \leqslant 5^2 - 5 + 1$ for *all* primes $p > 27$.

Consider first the case when all the numbers from 1 to 4 are quadratic residues (R, for short), while 5 is a quadratic nonresidue (N, for short) The following scheme or "pattern" is self-evident:

1	2	3	4	5	6	7	8	9	10	11	12		
R	R	R	R	N	R	R	R	R	N	R	R		
13	14	15	16	17	18	19	20	21	22	23	24	25	26
R	R	N	R	R	R	R	N	R	R	R	R	R	R

Thus (2) has a solution $x = 21$, but has no solution for $1 \leqslant x \leqslant 20$. Explanation: We put R below 7 because if 7 were an N, (2) would already be solved with $x = 3$.

Similarly 11, 13, 17, 19, 23, are R's. It is clear from Derichlet's theorem that there exists a prime p with the above pattern of R's and N's. For example our prime p can be chosen to be $\equiv 2 \pmod 5$ for then $(5/p) = (p/5) = (2/5) = -1$. Similarly we can take $p \equiv 9(28)$ for then

$$(7/p) = (p/7) = (9/7) = +1.$$

Since the several congruence conditions imposed on the prime p are easily seen to be compatible, Durichlet's theorem shows the existence of primes p with the pattern of R's and N's in our example. We consider one more pattern.

1	2	3	4	5	6	7	8	9
R	N	N	R	N	R	R	N	R

Thus if 2 and 3 are N's, $x = 5$ solves Eq. (2) (if 5 is an R, then $x = 1$, already, will do).

The remaining patterns for $r = 5$ are left as an exercise for the reader.

2

Let $a_1, a_2, \ldots, a_r$ be fixed positive integer. We conjecture that the congruence $y^2 \equiv (x + a_1) \cdots (x + a_r) \bmod p$ always has a solution with $1 \leqslant x \leqslant B(r)$ for all primes $p > C(r)$. Here $B(r)$ and $C(r)$ depend only on the a's and r, *not* on p.

Note added in proof (May 18, 1976). The first conjecture is easily proved; the second, if true, may be hard to prove. There is a vast related literature, which will be the subject of another note.