A CLASS OF ALGEBRAIC-EXPONENTIAL CONGRUENCES MODULO \( p \)

C. COBELI, M. VĂJĂITU and A. ZAHARESCU

ABSTRACT. Let \( p \) be a prime number, \( J \) a set of consecutive integers, \( \overline{\mathbb{F}}_p \) the algebraic closure of the field \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) and \( \mathcal{C} \) an irreducible curve in an affine space \( \mathbb{A}^r(\overline{\mathbb{F}}_p) \), defined over \( \mathbb{F}_p \). We provide a lower bound for the number of \( r-1 \)-tuples \( (x,y_1,\ldots,y_{r-1}) \) with \( x \in J, y_1,\ldots,y_{r-1} \in \{0,1,\ldots,p-1\} \) for which \( (x,y_1^{\ast},\ldots,y_{r-1}^{\ast}) \) (mod \( p \)) belongs to \( \mathcal{C}(\overline{\mathbb{F}}_p) \).

1. Introduction

In Chapter F, section F9 of his well known book [4] on unsolved problems in number theory, Richard Guy collected some questions on primitive roots. One of them, attributed to Brizolis, asks if for a given prime \( p > 3 \), there is always a primitive root \( g \mod p \), \( 0 < g < p \), and an integer \( x, 0 < x < p \) such that \( x \equiv g^x \mod p \). This question was answered positively in [2], by showing that for any \( \epsilon > 0 \) there is a positive integer \( p(\epsilon) \) such that for any prime \( p > p(\epsilon) \) the number of pairs \( (x,y) \) of primitive roots mod \( p \), \( 0 < x,y < p \) which are solutions of the congruence \( x \equiv y^x \mod p \), is at least \( (1-\epsilon)e^{-\frac{2p}{\log \log p}p} \), where \( \gamma \) denotes Euler’s constant. In the present paper we consider more general congruences, involving \( x,y_1^{\ast},\ldots,y_{r-1}^{\ast} \), and look for all the solutions, including those for which \( y_1,\ldots,y_{r-1} \) are not necessarily primitive roots mod \( p \). We start with a large prime number \( p \) and a set \( J \) of consecutive positive integers, of cardinality \( |J| \leq p \). Denote by \( \overline{\mathbb{F}}_p \) the algebraic closure of the field \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) and let \( \mathcal{C} \) be an irreducible curve of degree \( D \) in an affine space \( \mathbb{A}^r(\overline{\mathbb{F}}_p) \). We assume in the following that \( \mathcal{C} \) is not contained in any hyperplane and that it is defined over \( \mathbb{F}_p \). Denote as usually by \( \mathcal{C}(\mathbb{F}_p) \) the set of points \( z = (z_1,\ldots,z_r) \) on \( \mathcal{C} \) with all the components \( z_1,\ldots,z_r \) in \( \mathbb{F}_p \). The problem is to find integers \( x \in J \) and \( y_1,\ldots,y_{r-1} \in \{0,1,\ldots,p-1\} \) such that

\[
(1) \quad (x,y_1^{\ast},\ldots,y_{r-1}^{\ast}) \pmod{p} \in \mathcal{C}(\mathbb{F}_p).
\]

The method employed in [2] may be adapted to the present context. The first idea is to look for points \( (x,z_1,\ldots,z_{r-1}) \) on the curve \( \mathcal{C} \) for which \( x \) is relatively prime to \( p - 1 \). For any such point \( (x,z_1,\ldots,z_{r-1}) \) we find a solution \( (x,y_1,\ldots,y_{r-1}) \) of (1) by arranging \( y_1,\ldots,y_{r-1} \) such that \( y_j^{\ast} \equiv z_j \mod p \), \( j = 1,\ldots,r-1 \).
1 ≤ j ≤ r − 1. To be precise, we choose a positive integer w such that \(xw \equiv 1 \pmod{p − 1}\), then set \(y_j = z_j^w\) and from Fermat’s Little Theorem one gets \(y_j^x = z_j \pmod{p}\). We combine this idea with a Fourier inversion technique, similar to that used in [3]. Consider the sets

\[
A = \{(x,y_1,\ldots,y_{r−1}) \in J \times \mathbb{Z}^{r−1} : 0 ≤ y_1,\ldots,y_{r−1} < p, (x,p−1) = 1, (x,y_1^x,\ldots,y_{r−1}^x) \equiv (x,p−1) \pmod{p}\}
\]

and

\[
B = \{(x,z_1,\ldots,z_{r−1}) \in J \times \mathbb{Z}^{r−1} : 0 ≤ z_1,\ldots,z_{r−1} < p, (x,p−1) = 1, (x,z_1,\ldots,z_{r−1}) \equiv (x,p−1) \pmod{p}\}.
\]

Our goal is to obtain lower bounds for \(|A|\). By the above remark we know that \(|A| ≥ |B|\), thus it will be enough to find lower bounds for \(|B|\). We will actually obtain an asymptotical estimation for \(|B|\). The result is stated in the following theorem.

**Theorem 1.** Let \(p\) be a prime number, \(J\) a set of consecutive positive integers and \(C\) an irreducible curve of degree \(D\) in \(A^r(F_p)\), defined over \(F_p\) and not contained in any hyperplane. Then

\[
|B| = |J| \frac{\varphi(p−1)}{p−1} + O_D(σ_0(p−1)\sqrt{p\log p}).
\]

Here \(\varphi(\cdot)\) is the Euler function and \(σ_0(p−1)\) is the number of positive divisors of \(p−1\). As a consequence of Theorem 1 we note the following corollary.

**Corollary 1.** Let \(r ≥ 2\) and \(D ≥ 1\) be integers and \(\epsilon > 0\) a fixed real number. Then there is a positive integer \(p(r,D,\epsilon)\) such that for any prime number \(p > p(r,D,\epsilon)\) and any irreducible curve \(C\) of degree \(D\) in \(A^r(F_p)\), defined over \(F_p\) and not contained in any hyperplane, the number of \(r\)-tuples \((x,y_1,\ldots,y_{r−1})\) with \(0 < x, y_1, \ldots, y_{r−1} < p\), \((x,p−1) = 1\) and \((x,y_1^x,\ldots,y_{r−1}^x) \equiv (x,p−1) \pmod{p}\) is at least \((1−\epsilon)e^{−2}\frac{p}{\log\log p}\).

2. Characteristic Functions and Exponential Sums

Our first step is to get an exact formula for \(|B|\) in terms of exponential sums. For this we introduce the following characteristic function:

\[
\phi_J(x) = \begin{cases} 
1, & \text{if } x \in J \text{ and } (x,p−1) = 1 \\
0, & \text{else}.
\end{cases}
\]

Without any loss of generality, we may assume in the proof of Theorem 1 that the set of consecutive integers \(J\) satisfies \(J \subset [1,p−1]\). Let \(C\) be as in the statement of the theorem. Then the number we are interested in, can be written as

\[
|B| = \sum_{(x,z_1,\ldots,z_{r−1}) \in C(F_p)} \phi_J(x).
\]

2. Characteristic Functions and Exponential Sums

Our first step is to get an exact formula for \(|B|\) in terms of exponential sums. For this we introduce the following characteristic function:

\[
\phi_J(x) = \begin{cases} 
1, & \text{if } x \in J \text{ and } (x,p−1) = 1 \\
0, & \text{else}.
\end{cases}
\]

Without any loss of generality, we may assume in the proof of Theorem 1 that the set of consecutive integers \(J\) satisfies \(J \subset [1,p−1]\). Let \(C\) be as in the statement of the theorem. Then the number we are interested in, can be written as

\[
|B| = \sum_{(x,z_1,\ldots,z_{r−1}) \in C(F_p)} \phi_J(x).
\]
Next, using a finite Fourier transform modulo $p$ we write the characteristic function defined above as

$$\phi_J(x) = \sum_{u \in \mathbb{F}_p} \hat{\phi}_J(u)e_p(ux)$$

where $e_p(t) = e^{\frac{2\pi it}{p}}$ for any $t$. The Fourier coefficients $\hat{\phi}_J(u)$ are given by

$$\hat{\phi}_J(u) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \phi_J(x)e_p(-ux).$$

We substitute the expression (3) in (2) to obtain

$$|\mathcal{B}| = \sum_{u \in \mathbb{F}_p} \hat{\phi}_J(u)S_\varepsilon(u),$$

in which

$$S_\varepsilon(u) = \sum_{(x,z_1,\ldots,z_r-1) \in C(\mathbb{F}_p)} e_p(ux).$$

The expression (5) is the basic formula that will be used in the proof of Theorem 1. In order to complete the proof we first need estimates for $\hat{\phi}_J(u)$.

### 3. Estimates for the Fourier Coefficients

The Fourier coefficients given by (4) behave differently, depending on whether their argument is or is not zero modulo $p$. We have

$$\hat{\phi}_J(u) = \begin{cases} \frac{|\mathcal{J}|p(p-1)}{p^2} + O\left(\frac{\sigma_p(p-1)}{p}\right), & \text{if } u \equiv 0 \pmod{p} \\ O\left(\frac{1}{p} \sum_{d \mid (p-1)} \frac{1}{||ud/p||}\right), & \text{if } u \not\equiv 0 \pmod{p} \end{cases}$$

where $||\cdot||$ denotes the distance to the nearest integer.

In order to prove (6), we use well known properties of the Möbius function to write

$$\hat{\phi}_J(u) = \frac{1}{p} \sum_{x \in \mathcal{J}} e_p(-ux) = \frac{1}{p} \sum_{x \notin \mathcal{J}} e_p(-ux) \sum_{d \mid x} \mu(d)$$

$$= \frac{1}{p} \sum_{d \mid (p-1)} \mu(d) \sum_{x \in \mathcal{J} \atop d \mid x} e_p(-ux).$$

When $u = 0$ one has

$$\hat{\phi}_J(0) = \frac{1}{p} \sum_{d \mid (p-1)} \mu(d)\{x \in \mathcal{J}; d \text{ divides } x\} = \frac{1}{p} \sum_{d \mid (p-1)} \mu(d) \left(\frac{|\mathcal{J}|}{d} + O(1)\right)$$

$$= \frac{|\mathcal{J}|}{p} \sum_{d \mid (p-1)} \frac{\mu(d)}{d} + O\left(\frac{\sigma_p(p-1)}{p}\right).$$
Employing the equality \( \sum_{d \mid (p-1)} \frac{\mu(d)}{d} = \frac{\varphi(p-1)}{p-1} \) (see for example [5]), the relation (6) is proved for \( u = 0 \). Let us assume now that \( u \not\equiv 0 \) (mod \( p \)). The sum \( \sum_{x \in J, d \mid x} e_p(-ux) \) is a geometric progression of ratio \( e_p(-ud) \). It follows easily that

\[
\left| \sum_{x \in J, d \mid x} e_p(-ux) \right| \ll \frac{1}{\|ud/p\|}.
\]

Using (7) for any divisor \( d \) of \( p-1 \), we find that

\[
\hat{\phi}_J(u) \ll \frac{1}{p} \sum_{d \mid (p-1)} \frac{1}{\|ud/p\|},
\]

which proves (6).

4. Proof of Theorem 1

We split the sum in the main formula (5) into two ranges according as to whether \( u = 0 \) or \( u \neq 0 \). We write

\[
|\mathcal{B}| = M + E,
\]

where \( M = \hat{\phi}_J(0)|\mathcal{C}(F_p)| \) contains the principal contribution, giving the main term of the estimation for \( |\mathcal{B}| \), while the remainder is

\[
E = \sum_{0 \neq u \in F_p} \hat{\phi}_J(u) \sum_{(x,x_1,...,x_{r-1}) \in \mathcal{C}(F_p)} e_p(ux).
\]

We now turn our attention to the evaluation of \( M \). By the Riemann Hypothesis for curves over finite fields (Weil [6]), we know that

\[
|\mathcal{C}(F_p)| = p + O_D(\sqrt{p}).
\]

Then using (6), we obtain

\[
M = |J| \frac{\varphi(p-1)}{p} + O_D(\sqrt{p}).
\]

Next, we estimate the remainder \( E \). Since \( \mathcal{C} \) is not contained in any hyperplane it follows for \( u \neq 0 \) that \( ux \) is nonconstant along the curve \( \mathcal{C} \). Then one may apply the Bombieri–Weil inequality (see [1], Theorem 6), which gives

\[
|S_\mathcal{C}(u)| \ll_D \sqrt{p}
\]

for \( u \neq 0 \). Therefore, by (6) we see that

\[
E = \sum_{0 \neq u \in F_p} \hat{\phi}_J(u)S_\mathcal{C}(u) \ll_D \left( \frac{1}{p} \sum_{d \mid (p-1)} \frac{1}{\|ud/p\|} \right) \sqrt{p}
\]

\[
\ll \sigma_u(p-1) \sqrt{p} \log p.
\]

This completes the proof of Theorem 1.
REFERENCES


C. Cobeli, M. Văjăitu, Institute of Mathematics of the Romanian Academy, P.O.Box 1-764, 70700 Bucharest, Romania, e-mail: ccobeli@imar.ro, mvajaitu@imar.ro

A. Zaharescu, Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W. Green St., Urbana, IL 61801, USA, e-mail: zaharesc@math.uiuc.edu