Acta Math. Univ. Comenianae
Vol. LXXI, 1(2002), pp. 113–117

A CLASS OF ALGEBRAIC-EXPONENTIAL CONGRUENCES MODULO p

C. COBELI, M. VÂJÂITU AND A. ZAHARESCU

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

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 $x \equiv g^x \pmod p$. 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 $x \equiv y^x \pmod p$, is at least $(1-\epsilon)e^{-2\gamma}\frac{p}{(\log\log p)^2}$, where γ denotes Euler's constant. In the present paper we consider more general congruences, involving $x, y_1^x, \dots, y_{r-1}^x$, and look for all the solutions, including those for which $y_1, \dots, y_{r-1}$ are not necessarily primitive roots mod p. We start with a large prime number p and a set $\mathcal{J}$ of consecutive positive integers, of cardinality $|\mathcal{J}| \le p$. Denote by $\overline{\mathbf{F}}_p$ the algebraic closure of the field $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ and let $\mathfrak{C}$ be an irreducible curve of degree D in an affine space $\mathbb{A}^r(\overline{\mathbf{F}}_p)$. We assume in the following that $\mathfrak{C}$ is not contained in any hyperplane and that it is defined over $\mathbf{F}_p$. Denote as usually by $\mathfrak{C}(\mathbf{F}_p)$ the set of points $\mathbf{z} = (z_1, \dots, z_r)$ on $\mathfrak{C}$ with all the components $z_1, \dots, z_r$ in $\mathbf{F}_p$. The problem is to find integers $x \in \mathcal{J}$ and $y_1, \dots, y_{r-1} \in \{0, 1, \cdots, p-1\}$ such that

$$(x, y_1^x, \dots, y_{r-1}^x) \pmod p \in \mathfrak{C}(\mathbf{F}_p)\,. \tag{1}$$

The method employed in [**2**] may be adapted to the present context. The first idea is to look for points $(x, z_1, \dots, z_{r-1})$ on the curve $\mathfrak{C}$ for which x is relatively prime to $p-1$. For any such point $(x, z_1, \dots, z_{r-1})$ we find a solution $(x, y_1, \dots, y_{r-1})$ of (1) by arranging $y_1, \dots, y_{r-1}$ such that $y_j^x \equiv z_j \pmod p$,

Received September 29, 2001.
2000 *Mathematics Subject Classification.* Primary 11T99.

$1 \le j \le r-1$. 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 $y_j^x = z_j^{xw} \equiv z_j \mod p$. We combine this idea with a Fourier inversion technique, similar to that used in [**3**]. Consider the sets

$$\mathcal{A} = \big\{(x, y_1, \dots, y_{r-1}) \in \mathcal{J} \times \mathbb{Z}^{r-1} \colon\ 0 \le y_1, \dots, y_{r-1} < p,$$
$$(x, y_1^x, \dots, y_{r-1}^x) \pmod{p} \in \mathfrak{C}(\mathbf{F}_p)\big\}$$

and

$$\mathcal{B} = \big\{(x, z_1, \dots, z_{r-1}) \in \mathcal{J} \times \mathbb{Z}^{r-1} \colon\ 0 \le z_1, \dots, z_{r-1} < p,\ (x, p-1) = 1,$$
$$(x, z_1, \dots, z_{r-1}) \pmod{p} \in \mathfrak{C}(\mathbf{F}_p)\big\}\,.$$

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

Theorem 1. *Let p be a prime number, $\mathcal{J}$ a set of consecutive positive integers and $\mathfrak{C}$ an irreducible curve of degree D in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$, defined over $\mathbf{F}_p$ and not contained in any hyperplane. Then*

$$|\mathcal{B}| = |\mathcal{J}|\frac{\varphi(p-1)}{p-1} + O_D\Big(\sigma_0(p-1)\sqrt{p}\log p\Big).$$

Here $\varphi(\cdot)$ is the Euler function and $\sigma_0(p-1)$ is the number of positive divisors of $p-1$. As a consequence of Theorem 1 we note the following corollary.

Corollary 1. *Let $r \ge 2$ and $D \ge 1$ 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 $\mathfrak{C}$ of degree D in $\mathbb{A}^r(\overline{\mathbf{F}}_p)$, defined over $\mathbf{F}_p$ and not contained in any hyperplane, the number of $r-$tuples $(x, y_1, \dots, y_{r-1})$ with $0 < x, y_1, \dots, y_{r-1} < p$, $(x, p-1) = 1$ and $(x, y_1^x, \dots, y_{r-1}^x) \pmod{p} \in \mathfrak{C}(\mathbf{F}_p)$ is at least $(1-\epsilon)e^{-2\gamma}\frac{p}{\log\log p}$.*

2. Characteristic Functions and Exponential Sums

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

$$\phi_{\mathcal{J}}(x) = \begin{cases} 1, & \text{if } x \in \mathcal{J} \text{ and } (x, p-1) = 1 \\ 0, & \text{else}\,. \end{cases}$$

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

$$|\mathcal{B}| = \sum_{(x, z_1, \dots, z_{r-1}) \in \mathfrak{C}(\mathbf{F}_p)} \phi_{\mathcal{J}}(x)\,. \tag{2}$$

Next, using a finite Fourier transform modulo p we write the characteristic function defined above as

$$\phi_{\mathcal{J}}(x) = \sum_{u\in\mathbf{F}_p} \hat{\phi}_{\mathcal{J}}(u)e_p(ux) \tag{3}$$

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

$$\hat{\phi}_{\mathcal{J}}(u) = \frac{1}{p}\sum_{x\in\mathbf{F}_p} \phi_{\mathcal{J}}(x)e_p(-ux). \tag{4}$$

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

$$|\mathcal{B}| = \sum_{u\in\mathbf{F}_p} \hat{\phi}_{\mathcal{J}}(u)S_{\mathfrak{C}}(u)\,, \tag{5}$$

in which

$$S_{\mathfrak{C}}(u) = \sum_{(x,z_1,\dots,z_{r-1})\in\mathfrak{C}(\mathbf{F}_p)} e_p(ux)\,.$$

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 $\hat{\phi}_{\mathcal{J}}(u)$.

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

$$\hat{\phi}_{\mathcal{J}}(u) = \begin{cases} \frac{|\mathcal{J}|\varphi(p-1)}{p^2} + O\left(\frac{\sigma_0(p-1)}{p}\right), & \text{if } u\equiv 0 \pmod p \\ O\left(\frac{1}{p}\sum_{d|(p-1)}\frac{1}{\|ud/p\|}\right), & \text{if } u\not\equiv 0 \pmod p \end{cases} \tag{6}$$

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

$$\begin{aligned}\hat{\phi}_{\mathcal{J}}(u) &= \frac{1}{p}\sum_{\substack{x\in\mathcal{J}\\(x,p-1)=1}} e_p(-ux) = \frac{1}{p}\sum_{x\in\mathcal{J}} e_p(-ux)\sum_{\substack{d|x\\d|(p-1)}}\mu(d)\\ &= \frac{1}{p}\sum_{d|(p-1)}\mu(d)\sum_{\substack{x\in\mathcal{J}\\d|x}} e_p(-ux)\,.\end{aligned}$$

When $u=0$ one has

$$\begin{aligned}\hat{\phi}_{\mathcal{J}}(0) &= \frac{1}{p}\sum_{d|(p-1)}\mu(d)|\{x\in\mathcal{J};d \text{ divides } x\}| = \frac{1}{p}\sum_{d|(p-1)}\mu(d)\left(\frac{|\mathcal{J}|}{d}+O(1)\right)\\ &= \frac{|\mathcal{J}|}{p}\sum_{d|(p-1)}\frac{\mu(d)}{d} + O\left(\frac{\sigma_0(p-1)}{p}\right)\,.\end{aligned}$$

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

$$\left| \sum_{x\in\mathcal{J},\, d|x} e_p(-ux) \right| \ll \frac{1}{\|ud/p\|} \,. \tag{7}$$

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

$$\hat{\phi}_{\mathcal{J}}(u) \ll \frac{1}{p} \sum_{d|(p-1)} \frac{1}{\|ud/p\|} \,,$$

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

$$|\mathcal{B}| = M + E \,, \tag{8}$$

where $M = \hat{\phi}_{\mathcal{J}}(0)|\mathfrak{C}(\mathbf{F}_p)|$ contains the principal contribution, giving the main term of the estimation for $|\mathcal{B}|$, while the remainder is

$$E = \sum_{0\neq u\in\mathbf{F}_p} \hat{\phi}_{\mathcal{J}}(u) \sum_{(x,z_1,\dots,z_{r-1})\in\mathfrak{C}(\mathbf{F}_p)} e_p(ux) \,.$$

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

$$|\mathfrak{C}(\mathbf{F}_p)| = p + O_D\left(\sqrt{p}\right).$$

Then using (6), we obtains

$$M = |\mathcal{J}| \, \frac{\varphi(p-1)}{p} + O_D\left(\sqrt{p}\right).$$

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

$$|S_{\mathfrak{C}}(u)| \ll_D \sqrt{p}$$

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

$$\begin{aligned} E = \sum_{0\neq u\in\mathbf{F}_p} \hat{\phi}_{\mathcal{J}}(u) S_{\mathfrak{C}}(u) &\ll_D \left(\frac{1}{p} \sum_{d|(p-1)} \sum_{u=1}^{p-1} \frac{1}{\|ud/p\|} \right) \sqrt{p} \\ &\ll \sigma_0(p-1)\sqrt{p}\log p. \end{aligned}$$

This completes the proof of Theorem 1.

References

1. Bombieri E., *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71–105.
2. Cobeli C. and Zaharescu A., *An exponential congruence with solutions in primitive roots*, Rev. Roumaine Math. Pures Appl. **44**(1) (1999), 15–22.
3. ______, *Generalization of a problem of Lehmer*, Manuscripta Math. **104** (2001), 301–307.
4. Guy R. K., *Unsolved problems in Number Theory*, Springer-Verlag, New York-Berlin, 1981, (second edition 1994).
5. Ram Murty M., *Problems in Analytic Number Theory*, Springer-Verlag, New York, 2001.
6. Weil A., *Sur les courbes algébriques et les variétés qui s'en déduisent,* Paris, Hermann, 1948.

C. Cobeli, M. Vâjâitu, 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`