A Note on the Mean Value of Numbers of the Solutions of $x^\alpha \equiv 1 \pmod{n}$

Xiu Yuan YU

Department of Mathematics, Hangzhou Teachers’ College, Hangzhou 310012, P. R. China
and
Department of Mathematics, Quzhou College, Quzhou 324000, P. R. China
E-mail: yuxiuyuan@hotmail.com

Abstract  Let $T = T(p, q, \alpha)$ be the number of solutions of the congruence $x^\alpha \equiv 1 \pmod{p^\eta q^\theta}$. Let $A$ and $B$ be sets of primes satisfying $x_1 < p \leq x_2$ and $y_1 < q \leq y_2$, respectively. A mean value estimation of $\frac{1}{|A||B|} \sum_{p \in A} \sum_{q \in B} \log T(p, q, \alpha)$ is given.

Keywords  Congruence, Number of solutions, Mean value

MR(2000) Subject Classification  11T71, 68P25, 94A60

In this paper we are interested in the mean value of the numbers of solutions of the congruence

$$x^\alpha \equiv 1 \pmod{n}, \quad \alpha = e^\beta - 1, \quad (x, n) = 1,$$  \hfill (1)

which is related with the research on cryptography.

Suppose that $n = p^\eta q^\theta$ with different primes $p$ and $q$, and positive integers $\eta$ and $\theta$. Let $T(\alpha, n)$ be the number of solutions of the congruence (1).

By the behaviours of congruences [1], it is easy to verify that

$$T(\alpha, n) = (\alpha, \varphi(p^\eta))(\alpha, \varphi(q^\theta)).$$  \hfill (2)

In the following, we use $|S|$ or $\#S$ to denote the number of elements in a set $S$. We suppose that $y_2, y_1, x_2,$ and $x_1$ are positive integers satisfying

$$y_2 > y_1 > x_2 > x_1,$$  \hfill (3)

and denote the sets

$$A = \{p; \, p \text{ is a prime, } x_1 < p \leq x_2\}, \quad B = \{q; \, q \text{ is a prime, } y_1 < q \leq y_2\}.$$
We also suppose that $\alpha = e^\beta - 1$ is a fixed positive integer, that

$$\alpha = r_1^{m_1} r_2^{m_2} \cdots r_t^{m_t} = \prod_{i=1}^t r_i^{m_i} =: \prod r^m,$$

and that

$$r_i^{m_i} \leq \frac{1}{3} (\min(x_1, y_1) - 1), \quad 1 \leq i \leq t,$$

where $r_1, r_2, \ldots, r_t$ are different primes, and $m_1, m_2, \ldots, m_t$ are positive integers.

**Lemma 1** [2] Let $\pi(x)$ be the number of primes $p \leq x$. Then there are constants $a_1, a_2,$ and $a_3$, such that

(i) $\pi(x) = \int_2^x \frac{du}{\log u} + O\left(xe^{-a_1 \sqrt{\log x}}\right), \quad x \to \infty$;

(ii) $\pi(x_2) - \pi(x_1) \geq a_3 \int_{x_1}^{x_2} \frac{dx}{\log x}, \quad x_2 > 2x_1, \quad x_1 > a_2$.

**Lemma 2** [2] Let $\pi(x; a, b)$ be the number of primes not exceeding $x$ in $\{n = ak + b, k = 1, 2, \ldots\}$, where $(a, b) = 1, 1 \leq b \leq a < y \leq x$. Then

$$\pi(x; a, b) - \pi(x - y; a, b) < \frac{2y}{\varphi(a) \log^2 a}.$$

From (2), we have

$$\sum_{p \in A} \sum_{q \in B} \log T(n, \alpha) = \sum_{p \in A} \sum_{q \in B} (\log(\alpha, \varphi(p^n)) + \log(\alpha, \varphi(q^b)))$$

$$= |B| \sum_{p \in A} \log(\alpha, \varphi(p^n)) + |A| \sum_{q \in B} \log(\alpha, \varphi(q^b)), \quad (6)$$

and, by the behaviour of the von Mangoldt function $\Lambda(n)$, we have

$$\sum_{p \in A} \log(\alpha, \varphi(p^n)) = \sum_{p \in A, d|\alpha, p^{n-1}(p-1)} \sum_{d|\alpha, d|p^{n-1}(p-1)} \Lambda(d) = \sum_{d|\alpha, d|p^{n-1}(p-1)} \Lambda(d)$$

$$= \sum_{d|\alpha, p^{n-1}(p-1) \equiv 0 \pmod{d}} \sum_{d|\alpha, p^{n-1}(p-1) \equiv 0 \pmod{d}} \Lambda(d)$$

$$= \sum_{i=1}^t \sum_{j_1=1}^{m_1} \sum_{p \in A, p^{n-1}(p-1) \equiv 0 \pmod{r_i^{m_i}}} \Lambda(r_i^{m_i}).$$

From (5) we know $r_i^{m_i}$ cannot divide $p \in A$, so the above is

$$\sum_{p \in A} \log(\alpha, \varphi(p^n)) = \sum_{i=1}^t \log r_i \sum_{j_1=1}^{m_1} \sum_{p \equiv 1 \pmod{r_i^{m_i}}} 1.$$ \quad (7)

Similarly,

$$\sum_{q \in B} \log(\alpha, \varphi(q^b)) = \sum_{i=1}^t \log r_i \sum_{j_1=1}^{m_1} \sum_{q \equiv 1 \pmod{r_i^{m_i}}} 1.$$ \quad (8)