Doklady of the Academy of Sciences of the USSR

E. V. NOVOSELOV

1962

SovietRxiv

Abstract

Full Text

Doklady of the Academy of Sciences of the USSR
1962. Volume 143, No. 6

MATHEMATICS

E. V. NOVOSELOV

SOME FORMULAS CONNECTED WITH THE REDUCED SYSTEM OF RESIDUES

(Presented by Academician I. M. Vinogradov on December 8, 1961)

Introduce the following notation: $m = \prod_p p^{k_p}$ is a fixed natural number; $k_p \geq 0$ and is different from zero for only finitely many primes p. $m_0 = \prod_{p/m} p^{k_p - 1}$, if $k_2 < 2$; $m_0 = \frac{1}{2} \prod p^{k_p - 1}$, if $k_2 \geq 2$. $p_1 p_2 \ldots p_z = \prod_{p/m} p$. δ_p is the exponent to which p belongs modulo $\frac{m}{p^{k_p}}$. s_p is an arbitrary integer satisfying $s_p \delta_p \geq k_p$. Δ_p is the exponent to which $p \neq 2$ belongs modulo $\frac{m_0}{p^{k_p - 1}}$. t_p is an arbitrary integer satisfying $t_p \Delta_p \geq k_p - 1$. The quantities Δ_2 and t_2 are defined analogously. $E^{(m)}$ is the group of residue classes modulo m relatively prime to m. It is known that the group $E^{(s)}$ for $s = 2^k$, $k \geq 2$, decomposes into the direct product of the cyclic group $E_1^{(s)}$ of order two with generator $a_1 = -1$ and the cyclic group $E_2^{(s)}$ of order 2^{k-2}. An arbitrary generator of the latter group in the case $k = k_2 = k_2(m) \geq 2$ will be denoted by a_2. For example, $a_2 = 5$. If, for ε relatively prime to m, the condition

$$\varepsilon = (-1)^{k \bmod 2} a_2^{\delta} (2^{k_2})$$

is satisfied, we set $\operatorname{ind}_2 \varepsilon$ equal to the least of the possible (for the given a_2) natural δ' s. a_p is a certain primitive root modulo p^{k_p}, where p is an odd prime. $\operatorname{ind}_p \varepsilon$ is the index of ε modulo p^{k_p} with base a_p.

$$\log x = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} (x-1)^k;$$

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!} x^k$$

are formal power series.

We shall say that a series of this type converges modulo m at the point $x = x_0$ if all its terms, starting from some one, are divisible by m at $x = x_0$. Divisibility

here is understood in the sense of divisibility of a rational fraction by a modulus. All the series occurring in the text converge modulo the corresponding moduli.

In this article ε everywhere denotes a number relatively prime to m, and p denotes a prime and only a prime number.

1. Suppose first that $m = p^k$, where p is an odd prime. For this case one can prove the formula

$$\operatorname{ind}_p \varepsilon \equiv \frac{\xi}{p} \log \varepsilon^{p-1} \equiv \frac{\xi}{p} \sum_{s=1}^{n} \frac{(-1)^{s-1}}{s} \left(\varepsilon^{p-1} - 1\right)^s \equiv$$

$$\equiv \frac{\xi}{p} \sum_{s=1}^{n} \frac{(-1)^{s-1}}{s} C_n^s \left(\varepsilon^{(p-1)s} - 1\right) \pmod{p^{k-1}}. \tag{1}$$

   Here $n = n(k)$ is any natural number satisfying the condition

$$\frac{1}{s} p^{s-1} \equiv 0 \pmod{p^{k-1}}$$

   for all $s > n$.

ξ is relatively prime to p, and

$$\xi^{-1} \equiv \frac{1}{p} \log a_p^{p-1} \pmod{p^{k-1}}.$$

In particular, if $\varepsilon^{p-1} \equiv 1 + pt \pmod{p^k}$, and $a_p^{p-1} \equiv 1 + pt_0 \pmod{p^k}$, then

$$\operatorname{ind}_p \varepsilon \equiv \xi \left(t - \frac{p}{2} t^2 + \frac{p^2}{3} t^3 - \frac{p^3}{4} t^4 + \cdots\right) \pmod{p^{k-1}},$$

where

$$\xi^{-1} \equiv t_0 - \frac{p}{2} t_0^2 + \frac{p^2}{3} t_0^3 - \frac{p^3}{4} t_0^4 + \cdots \pmod{p^{k-1}}.$$

We note that one can choose the primitive root a_p so that the condition $\xi \equiv 1 \pmod{p^{k-1}}$ is satisfied. For this it is enough to choose a_p (such a choice is always possible) satisfying the condition:

$$a_p^{p-1} \equiv e^p \equiv 1 + p + \frac{p^2}{2!} + \frac{p^3}{3!} + \frac{p^4}{4!} + \cdots + \frac{p^s}{s!} + \cdots \pmod{p^k}.$$

II. Let us now consider the case $m = 2^k,\ k \geq 2$. It can be shown that

$$2+\frac{2^2}{2}+\frac{2^3}{3}+\frac{2^4}{4}+\frac{2^5}{5}+\cdots+\frac{2^n}{n}\equiv 0 \pmod{2^k}, \tag{2}$$

starting from some $n=n(k)$. Using this formula, the following facts are proved:

1. The projection $E^{(m)}$ onto the cyclic direct factor $E_2^{(m)}$ of order 2^{k-2} is given by the formula:

$$\pi(\varepsilon)\equiv e^{\log\varepsilon} \pmod{m}. \tag{3}$$

Here $\log\varepsilon$ is taken modulo m.

2. The formula holds

$$\operatorname{ind}_2\varepsilon\equiv\frac{\xi}{4}\log\varepsilon\equiv\frac{\xi}{4}\sum_{s=1}^{n}\frac{(-1)^{s-1}}{s}(\varepsilon-1)^s\equiv$$

$$\equiv\frac{\xi}{4}\sum_{s=1}^{n}\frac{(-1)^{s-1}}{s}C_n^s(\varepsilon^s-1) \pmod{2^{k-2}}. \tag{4}$$

Here $n=n(k)$ is any natural number satisfying the condition

$$\frac{1}{s}2^{s-2}\equiv 0 \pmod{2^{k-2}} \quad \text{for all } s>n.$$

ξ is relatively prime to 2, and

$$\xi^{-1}\equiv\frac{1}{4}\log a_2 \pmod{2^{k-2}}.$$

In particular, if

$$\varepsilon\equiv 1+2t \pmod{2^k}, \quad a_2\equiv 1+2t_0 \pmod{2^k},$$

then

$$\operatorname{ind}_2\varepsilon\equiv\xi\left(\frac{t(1-t_0)}{2}+\frac{2}{3}t^3-\frac{2^2}{4}t^4+\frac{2^3}{5}t^5-\cdots\right) \pmod{2^{k-2}},$$

where

$$\xi^{-1}\equiv\frac{t_0(1-t_0)}{2}+\frac{2}{3}t_0^3-\frac{2^2}{4}t_0^4+\frac{2^3}{5}t_0^5-\cdots \pmod{2^{k-2}}.$$

We note that, with a_2 satisfying the condition

$$a_2 \equiv e^4 \equiv 1 + 4 + \frac{4^2}{2!} + \frac{4^3}{3!} + \frac{4^4}{4!} + \cdots \pmod{2^k},$$

and only with such an a_2, one has $\xi \equiv 1 \pmod{2^{k-2}}$, and the formula for $\operatorname{ind}_2 \varepsilon$ takes its simplest form.

III. We now pass to the general case, where m is arbitrary. The well-known theorem asserting that

$$E^{(m)} \cong \prod_{p/m} E(p^{k_p})$$

gives us the decomposition

$$E^{(m)} = E_1^{(m)} \times E_2^{(m)} \times \prod_{\substack{p \neq 2 \\ p/m}} L_p^{(m)} \tag{5}$$

of the group $E^{(m)}$ into the direct product of its cyclic subgroups:

$$E_1^{(m)} \text{ is a cyclic group } \begin{cases} \text{trivial, if } k_2 < 2, \\ \text{of order 2, if } k_2 \geqslant 2; \end{cases}$$

$$E_2^{(m)} \text{ is a cyclic group of order } m_0;$$

$$L_p^{(m)} \text{ is a cyclic group of order } p - 1.$$

In the case $m = 2^k$ these notations coincide with those adopted earlier.
Let us first give a general characterization of the decomposition (5).

a) The subgroup $E_1^{(m)}$ is generated by the class

$$e_1 \equiv 2^{s_2 \delta_2 + 1} - 1 \pmod{m}.$$

b) $E_2^{(m)}$ is the subgroup of $E^{(m)}$ consisting of the classes $\varepsilon \bmod m$ for which

$$\varepsilon \equiv 1 \pmod{p_1 p_2 \cdots p_z}, \qquad \text{if } k_2 < 2,$$

$$\varepsilon \equiv 1 \pmod{2 p_1 p_2 \cdots p_z}, \qquad \text{if } k_2 \geqslant 2.$$

c) The subgroup $L_p^{(m)}$ is generated by the class $e_p^{p^{k_p - 1}}$, where

$$e_p \equiv p^{s_p\delta_p} + (1 - p^{s_p\delta_p})a_p \pmod{m}.$$

d) $E_3^{(m)} = E_1^{(m)} \times E_2^{(m)}$ is the subgroup of $E^{(m)}$ consisting of the residue classes $\varepsilon \bmod m$ for which $\varepsilon \equiv 1 \pmod{p_1 p_2 \cdots p_z}$.

e) $\prod\limits_{\substack{p \neq 2 \\ p|m}} L_p^{(m)}$ is the subgroup of $E^{(m)}$ consisting of the residue classes $\varepsilon \bmod m$ for which $\varepsilon^{p-1} \equiv 1 \pmod{p^{k_p}}$ for every odd prime p dividing m.

f) The projection $\pi_1 : E^{(m)} \to E_3^{(m)}$ is given by the formula

$$\pi_1(\varepsilon) \equiv \sum_{p|m} (1 - p^{s_p\delta_p})\varepsilon^{1-p^{k_p-1}} \equiv \prod_{p|m} \{p^{s_p\delta_p} + (1 - p^{s_p\delta_p})\varepsilon\}^{1-p^{k_p-1}} \pmod{m}. \tag{6}$$

g) The projection $\pi : E_3^{(m)} \to E_2^{(m)}$ is given by the formula:

$$\pi(\varepsilon) \equiv \varepsilon^{\log \varepsilon} \pmod{m}. \tag{7}$$

IV. Let us now try to characterize the subgroup $E_2^{(m)}$.

a) Let $k_2 < 2$. An arbitrary element ε of the cyclic group $E_2^{(m)}$ is represented in the form

$$\varepsilon \equiv e^{p_1 p_2 \cdots p_z t} \equiv 1 + p_1 p_2 \cdots p_z t + \frac{(p_1 p_2 \cdots p_z t)^2}{2!} + \cdots \equiv \left(e^{p_1 p_2 \cdots p_z}\right)^t \pmod{m},$$

where t is uniquely determined modulo m_0.

b) An arbitrary generator l of the cyclic group $E_2^{(m)}$ in the case $k_2 < 2$ is represented in any of the forms:

1)

$$l \equiv \prod_{p|m} e_p^{p-1} \pmod{m}, \qquad \text{where } e_p \equiv p^{s_p\delta_p} + (1 - p^{s_p\delta_p})a_p \pmod{m}.$$

2)

$$l \equiv 1 + p_1 p_2 \cdots p_z t_0 \pmod{m},$$

where t_0 is relatively prime to m_0 and is uniquely determined modulo m_0.

3)

$$l \equiv e^{p_1 p_2 \cdots p_z t_1} \pmod{m},$$

where t_1 is relatively prime to m_0 and is uniquely determined modulo m_0.

Conversely, for any t_0 and t_1 relatively prime to m_0, and any set $\{a_p\}$ of primitive roots, formulas 1)–3) give certain generators of the group $E_2^{(m)}$.

c) If $k_2 \geqslant 2$, the preceding assertions remain valid with $p_1p_2\cdots p_z$ replaced by $2p_1p_2\cdots p_z$.

In the following two propositions, $l \equiv 1+p_1p_2\cdots p_z t_0^{\delta} \pmod m$ in the case $k_2 < 2$, and $l \equiv 1 + 2p_1p_2\cdots p_z t_0^{\delta} \pmod m$ in the case $k_2 \geqslant 2$, are certain generators of $E_2^{(m)}$.

d) Let $k_2 < 2$. Put $1 + p_1p_2 \dots p_z t \equiv (1 + p_1p_2 \dots p_z t_0) \pmod m$. Then

$$\delta \equiv \frac{\xi}{p_1p_2\dots p_z} \log(1 + p_1p_2 \dots p_z t) \equiv$$

$$\equiv \xi \left(t - \frac{p_1p_2\dots p_z}{2} t^2 + \frac{(p_1p_2\dots p_z)^2}{3} t^3 - \dots \right) \pmod{m_0}. \tag{8}$$

Here $(\xi, m_0) = 1$ and

$$\xi^{-1} \equiv \frac{1}{p_1p_2\dots p_z} \log(1 + p_1p_2 \dots p_z t_0) \pmod{m_0}.$$

An analogous assertion holds for the case $k_2 \geq 2$, with $p_1p_2 \dots p_z$ replaced by $2p_1p_2 \dots p_z$.

e) Let $k_2 < 2$. Fix some system of primitive roots $\{a_p\}$ and suppose that

$$\prod_{p/m} e_p^{p-1} \equiv 1 + p_1p_2 \dots p_z t_0 \pmod m$$

for

$$e_p \equiv p^{s_p\delta_p} + (1 - p^{s_p\delta_p}) a_p \pmod m.$$

If $\varepsilon \equiv 1 + p_1p_2 \dots p_z t \pmod m$, then

$$\sum_{p/m_0} \frac{1 - t_p^{\Delta_p}}{p-1} \operatorname{ind}_p \varepsilon \equiv \frac{\xi}{p_1p_2\dots p_z} \log(1 + p_1p_2 \dots p_z t) \pmod{m_0}, \tag{9}$$

where $(\xi, m_0) = 1$ and

$$\xi^{-1} \equiv \frac{1}{p_1p_2\dots p_z} \log(1 + p_1p_2 \dots p_z t_0) \pmod{m_0}.$$

An analogous assertion holds for the case $k_2 \geq 2$, with $p_1 p_2 \dots p_z$ replaced by $2p_1 p_2 \dots p_z$.

In addition to item e), note that the system $\{a_p\}$ of primitive roots (we include a_2 among them) can be chosen so that the condition $\xi \equiv 1 \pmod{m_0}$ is satisfied. For this it is enough to choose (which is always possible) $\{a_p\}$ so that the relation

$$\prod_{p/m} e_p^{p-1} \equiv \begin{cases} e^{p_1 p_2 \dots p_z} \pmod{m}, & \text{if } k_2 < 2, \\ e^{2p_1 p_2 \dots p_z} \pmod{m}, & \text{if } k_2 \geq 2 \end{cases}$$

holds.

For the special case $m = p^k$, item e) gives the well-known formula due to A. G. Postnikov,

$$\frac{\operatorname{ind}(1+pt)}{p-1} \equiv \frac{\xi}{p} \log(1+pt) \pmod{p^{k-1}}, \tag{10}$$

as well as an explicit expression for ξ^{-1} modulo p^{k-1}:

$$\xi^{-1} \equiv \frac{1}{p} \log(1+pt_0) \pmod{p^{k-1}}, \qquad \text{if } a_p^{p-1} \equiv 1 + pt_0 \pmod{p^k}.$$

We note that formula (10), by virtue of the relation

$$(p-1)\log(1+pt) \equiv \log(1+pt)^{p-1} \pmod{p^{k-1}},$$

is nothing other than formula (1) for $\varepsilon \equiv 1+pt \pmod{p^k}$. In fact these formulas are equivalent.

All the facts set forth above were obtained by the author in considering the properties of the exponential and logarithmic functions in the polyadic domain. Relation (2) is not new, although it was obtained by the author independently.

Kazan State University
named after V. I. Ulyanov-Lenin

Received
29 XI 1961

Note: Figure translations are in progress. See original paper for figures.