Časopis pro pěstování matematiky

Štefan Porubský

Translated geometric progressions and covering systems

Časopis pro pěstování matematiky, Vol. 103 (1978), No. 2, 141--146

Persistent URL: http://dml.cz/dmlcz/108625

Časopis pro pěstování matematiky, roč. 103 (1978), Praha

TRANSLATED GEOMETRIC PROGRESSIONS AND COVERING SYSTEMS

Štefan Porubský, Bratislava

(Received February 25, 1976)

Two types of results are proved or reproved in the paper, namely as indicated in the title, on the so-called translated geometric progressions and covering systems of congruences. The proofs are based on some mutual connections between these two notions.

1. PRELIMINARIES

It seems that the name translated geometric progression goes back to J. Maxfield, and M. LeVan devoted a series of papers to it.

Translated geometric progression (or TGP) is a set of integers of the form

$$\{ar^n + b : n = 1, 2, 3, \ldots\},$$

where a, r, b are integers with $a \geqq 1$ and $r > 1$. Given a TGP $\mathscr{S}$, let $P_{\mathscr{S}}$ denote the set of all prime factors of integers in $\mathscr{S}$. According to Theorem 1 of [4], $P_{\mathscr{S}}$ is infinite for every TGP $\mathscr{S}$.

For $p \in P_{\mathscr{S}}$ let $ar^{n(p)} + b$ denote the least element of $\mathscr{S}$ divisible by p and $e(p)$ the exponent to which r belongs modulo p if $(r, p) = 1$; we put $e(p) = 1$ if $(r, p) > 1$.

The next lemma gave the impetus to this paper.

Lemma 1. *Let* $S_p = \{n : p \mid ar^n + b\}$ *for* p *in* $P_{\mathscr{S}}$. *Then one of the following alternatives holds*:

a. *if* $p \mid (a, b)$ *or* $p \mid (r, b)$, *then* $S_p = \{1, 2, 3, \ldots\}$,

b. *if* $p \nmid r$ *and* $p \nmid a$, *then* $S_p = \{n : n \equiv n(p) \bmod e(p)\}$.

A subset P of $P_{\mathscr{S}}$ is said to be *admissible* (on TGP $\mathscr{S}$) if each element from $\mathscr{S}$ has a prime factor in P. *A minimal admissible set* on $\mathscr{S}$ is an admissible set no proper subset of which is also admissible on $\mathscr{S}$. It may happen that some $\mathscr{S}$ have finite admissible sets. Such TGP's are the subject of consideration in [1] (cf. also part 3 of this paper).

If P is a finite minimal admissible set on $\mathscr{S}$ let

$$L(P) = \begin{cases} \text{l.c.m.} \ [e(p_i) : p_i \in P], & \text{if} \quad (p_i, r) = 1 \quad \text{for all } i, \\ 1 \quad \text{otherwise}. \end{cases}$$

Lemma 2. (LEVAN [3]). *Let P be a finite minimal admissible set on $\mathscr{S}$, q a prime divisor of $L(P)$ and α the highest power of q that divides $L(P)$. Let $A(q) = \{p \in P : q \mid e(p)\}$. For each $p \in A(q)$ let $f(p, q)$ be the highest power of q which divides $e(p)$. Then*

(i) *there are at least q distinct $p_i \in P$ such that $q^\alpha \mid e(p_i)$,*

(ii) *the set $\{n(p) : p \in A(q)\}$ contains a complete residue system modulo q,*

(iii) $\sum_{p \in A(q)} q^{-f(p,q)} \geqq 1.$

On a subset $P = \{p_1, p_2, \ldots, p_t\}$ of $P_{\mathscr{S}}(t > 1)$, define the following reflexive and symmetric relations (after LEVAN):

$p_i \, R^{(1)} \, p_j$ if $(e(p_i), e(p_j)) > 1$,

$p_i \, R^{(n)} \, p_j$ if there exists a p_k such that $p_i \, R^{(1)} \, p_k$ and $p_k \, R^{(n-1)} \, p_j$.

Lemma 3 (LeVan [3]). *If P is a finite minimal admissible set on $\mathscr{S}$ then there exists a v such that $R^{(v)} = P \times P$.*

Lemma 4 (LeVan [3]). *Let P be a finite minimal admissible set on $\mathscr{S}$ and q any prime divisor of $L(P)$. Then*

$$L(P) \leqq q \cdot 2^{t-q} \leqq 2^{t-1},$$

where t denotes the number of elements in P.

The following notion that we shall use was introduced by P. ERDÖS. A system of residue classes

$$a_i \bmod n_i, \quad 0 < a_i \leqq n_i \quad \text{for} \quad i \in I \tag{1}$$

is said to be *covering* if every integer belongs at least to one of these classes. Covering system (1) is said to be *irredundant* if none of its proper subsystems is also covering. Finally, an *exactly covering system* is a covering system with pairwise disjoint classes.

Now consider a TGP $\mathscr{S}$ and an admissible set P on it. Obviously, the system

$$n(p) \bmod e(p) \quad \text{for} \quad p \in P \tag{2}$$

is a covering system. If in addition P is a minimal admissible set, then this covering system is irredundant. The converse question of finding $\mathscr{S}$ to a given covering system (1) we are able to answer in the affirmative only if (1) is finite (cf. also Theorem 4).

Lemma 5. *To every finite covering system* (1) *there exists a* TGP *and such an admissible set on it that the associated system* (2) *coincides with* (1).

Proof. Fix an arbitrary integer a. Then choose a prime $p_i > a$ from the class $1 \bmod n_i$ for $i \in I$ (it is clear that p_i's may be chosen distinct if necessary). For a primitive root g_i modulo p_i $(i \in I)$ the solutions r of the system

$$r \equiv g_i^{(p_i-1)/n_i} \bmod p_i, \quad i \in I$$

belong to the exponent n_i modulo p_i $(i \in I)$. Finally, if b satisfies

$$-b \equiv a r^{a_i} \bmod p_i$$

then the TGP $\{ar^n + b\}$ and $\{p_i\}_{i \in I}$ fulfil the required conditions. By the way, from the proof we see that if (1) is irredundant, then the admissible sets constructed in the proof are minimal.

2. APPLICATIONS TO COVERING SYSTEMS

In this section we prove some results on covering systems. The theorems which now follow are immediate consequences of the lemmata above and therefore we omit their proofs here.

Theorem 1. *Let*

$$a_i \bmod n_i, \quad 0 < a_i \leqq n_i \quad \text{for} \quad i = 1, \ldots, k, \quad k > 1 \tag{3}$$

be an irredundant covering system. Let q be a prime divisor of the l.c.m. $[n_1, \ldots, n_k] = L$ *and α the highest power of q that divides L. Let* $\mathrm{A}(q) = \{i : 1 \leqq i \leqq k, q \mid n_i\}$. *For each $i \in \mathrm{A}(q)$ let $f(i, q)$ be the highest power of q which divides n_i. Then*

(i) *there are at least q distinct i's such that $q^\alpha \mid n_i$,*
(ii) *the set $\{a_i : i \in \mathrm{A}(q)\}$ contains a complete residue system modulo q,*
(iii) $\sum_{i \in \mathrm{A}(q)} q^{-f(i,q)} \geqq 1$.

An analogue of part (i) is proved even for covering systems on rings in [6]. As to part (ii), this can be proved at least for covering systems on integral domains.

Perhaps it is not worthless to notice that the whole Theorem is a simple consequence of this – to our knowledge – unproved statement:

If (3) *is an irredundant covering system and $q \mid L$, then the system*

$$a_i \bmod q^{f(i,q)} \quad \text{for} \quad i \in \mathrm{A}(q)$$

is covering, too.

Theorem 2. *Let* (3) *be an irredundant covering system. Then there exists a v such that for every pair of indices $i, j = 1, \ldots, k$ we can find a sequence $n_i = n_{t_1}, n_{t_2}, \ldots, n_{t_v} = n_j$ of moduli of* (3) *with*

$$(n_{t_s}, n_{t_{s+1}}) > 1$$

for each $s = 1, 2, \ldots, v - 1$.

Corollary ([6]). *Given a modulus n_i of an irredundant covering system* (3) *there exists an n_j $(j \neq i)$ in* (3) *with $(n_i, n_j) > 1$.*

Theorem 3. *In every irredundant covering system* (3) *we have*

$$n_i \leqq [n_1, n_2, \ldots, n_k] \leqq q \cdot 2^{k-q} \leqq 2^{k-1}$$

for any prime divisor q of a modulus in (3).

This theorem answers the following question: *Given a k, what is the largest possible value of the greatest modulus in an irredundant covering system consisting of k classes*? It is quite obvious that the adjective "irredundant" cannot be removed from the question. The bound 2^{k-1} is the best possible for every k, and it is attained for exactly covering systems described by S. K. STEIN in [7].

3. SOME REMARKS ON LEVAN'S RESULTS

In the following two last sections we turn our attention back to the translated geometric progressions.

Theorem 4. *Let* (3) *be a covering system and $\{m_j\}_{j \in I'}$ the set of all distinct moduli in it each of them appearing exactly s_j times in* (3). *Let a positive integer r possess the property that for each $j \in I'$, $r^{m_j} - 1$ has at least s_j primitive prime factors. Then for any a (or b) there is a b (or a) such that* TGP $\{ar^n + b\}$ *has an admissible set of cardinality k.*

Proof. Assign to each $i \in I$ a primitive prime factor p_i of $r^{n_i} - 1$ (i.e. $p_i \mid r^{n_i} - 1$ but $p_i \nmid r^m - 1$ for $m < n_i$). According to our hypotheses all p_i's are distinct and it is evident that $e(p_i) = n_i$. Then for any a (or b) we can solve the system

$$a \cdot r^{a_i} + b \equiv 0 \bmod p_i \quad \text{for} \quad i = 1, \ldots, k$$

in b (or a). The rest of the proof is now straightforward.

Corollary 1. *If* (3) *is irredundant then under the hypotheses of Theorem* 4 *there is a* TGP *with a minimal admissible set of cardinality k.*

Our Theorem 4 and its proof was motivated by ideas used in LeVan's proof of Theorem 2 in [1]. If we consider an exactly covering system

$$2^{i-1} \bmod 2^i \quad \text{for} \quad i = 1, \ldots, k-1, \quad \text{and}$$
$$2^{k-1} \bmod 2^{k-1}$$

then our reasoning coincides in essence with that of LEVAN's proof in [1]. The following corollaries are rewriten from [1] in this spirit.

Corollary 2. *Under the hypotheses of Theorem* 4 *for any b there exists an a such that every member of* TGP $\{ar^n + b\}$ *is composite.*

Corollary 3. *Let* $n_1, \ldots, n_k, r$ *be integers greater than* 1. *Let for each* $i = 1, \ldots, k$ *there exist a primitive prime factor* p_i *of* $r^{n_i} - 1$ *in such a way that all the* $p_i's$ *are distinct. If* $f = f(n_1, \ldots, n_k)$ *denotes the number of distinct covering systems with moduli* $n_1, \ldots, n_k$, *then for any b (or a) there exist at least f a's (or b's) incongruent* mod $p_1 \ldots p_k$ *which satisfy the conclusion of Theorem* 4.

4. COPRIME ELEMENTS IN TGP'S

Theorem 5. *For every* $N \geqq 0$ *there is a* TGP *containing at most N primes.*

Proof. Let (1) be a covering system.Define the so-called *covering function* of (1) in the following way:

$$m(n) = \text{card}\,\{i \in I : n \equiv a_i \bmod n_i\}\,.$$

Now, if $\mathscr{S}$ is a TGP and $P_{\mathscr{S}}$ the set of all prime divisors of its elements, then $\mathscr{S}$ contains a prime if and only if $m(n) = 1$ for at least one n, where $m(n)$ is the covering function of the covering system (2) assigned to $P_{\mathscr{S}}$.

The remaining part of the proof is now easy to foresee. A covering function of a finite covering system is obviously periodic. Therefore, let (3) be a finite covering system whose covering function takes the value 1 at at most N points in every interval of length equal to its period n_0 (e.g., take an exactly covering system and add to it several suitable residue classes). A TGP $\mathscr{S}$ constructed for this system (3) in the way described in Lemma 5 contains at most N primes, since only 1's in the interval $[0, n_0]$ can represent prime numbers.

Theorem 6. *For every* $M \geqq 1$ *there is a* TGP $\mathscr{S}$ *whose every element has at least M distinct prime factors.*

The proof parallels the previous one. Consider a finite covering system (3) with a covering function $m(n) \geqq M$ for every n.

Theorem 7. *Let* $\mathscr{S}$ *be a* TGP *and* $\varkappa = \min\{\text{card}\,P : P$ *is admissible on* $\mathscr{S}\}$. *Then the cardinality of the set of all distinct prime diviors of elements in a maximal subprogression of coprime elements from* $\mathscr{S}$ *is at least* $\varkappa$.

Proof. Let A be a set of coprime elements from $\mathscr{S}$ and P the set of their all prime divisors. If card $P \leqq \varkappa$, then the system

$$n(p) \bmod e(p) \quad \text{for} \quad p \in P$$

cannot be covering and therefore we can find an element $ar^n + b$ in $\mathscr{S}$ whose exponent n belongs to none of these classes. But then this element is certainly coprime with each element in A.

Corollary. TGP $\mathscr{S}$ *contains an infinite subprogression of coprime elements if and only if there is no finite admissible set on* $\mathscr{S}$.

The idea of the previous proof can be used to strengthen the last Corollary. Namely, in the next theorem we answer a question posed by LeVan in [5] whether in such an $\mathscr{S}$ there exists an infinite subprogression having the property that each its element is coprime with all preceding elements of $\mathscr{S}$.

Theorem 8. *A* TGP $\mathscr{S}$ *contains an infinite subprogression having the property that each of its elements is coprime to all the preceding elements of* $\mathscr{S}$ *if and only if* $\mathscr{S}$ *has no finite admissible set.*

Proof. Let A be a finite subprogression of the above mentioned character and x an element of $\mathscr{S}$ greater than the elements of A. If P_x now denotes the set of all prime divisors of elements in $\mathscr{S}$ less than x, then the system

$$n(p) \bmod e(p) \quad \text{for} \quad p \in P_x$$

is not covering. If x_1 is the least element of $\mathscr{S}$ not covered by this system, then x_1 is obviously coprime to all the preceding elements in $\mathscr{S}$. Induction completes the proof.

References

[1]—[4] *LeVan, M. O.:* Notes on translated geometric progressions I—IV. J. natur. Sci. Math. *9*, 33—37 (1969); *12*, 375—377, 379—388 (1972); *13*, 45—50 (1973).

[5] *LeVan, M. O.:* Autoreferat. Zentralblatt 182, 67.

[6] *Porubský, Š.:* On covering systems on rings. Math. Slovaca *28*, 147—152 (1978)

[7] *Stein, S. K.:* Unions of arithmetical sequences. Math. Ann. *134*, 289—294 (1958).

Author's address: 886 25 Bratislava, ul. Obrancov mieru 49 (Matematický ústav SAV).