Implicit linear difference equations over residue class rings

M. Heneralov

V. N. Karazin Kharkiv National University, Ukraine
E-mail: me2001.com@gmail.com

Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ be a residue class ring modulo $m = p_1^{k_1} \dots p_r^{k_r}$, where $p_1, \dots, p_r$ are pairwise disctinct primes and $k_1, \dots, k_r$ are natural numbers. Let $A, B, F_n \in \mathbb{Z}_m$ ($n \in \mathbb{Z}_+ = \{0, 1, 2, \dots\}$). Consider the linear difference equation

$$BX_{n+1} = AX_n + F_n, \quad n \in \mathbb{Z}_+, \tag{1}$$

over $\mathbb{Z}_m$. If B is non-invertible, this equation is said to be implicit.

The elements $a, b, f_n \in \{0, \dots, m-1\}$ are representatives of the residue classes $A, B, F_n \in \mathbb{Z}_m$, *respectively.* Denote the following greatest common divisor: $d = \gcd(a, b, m)$ and introduce $N = \prod_{j\,:\,p_j \nmid b} p_j^{k_j}$ (if $p_j \mid b$ for all $j = 1, \dots, r$, then $N = 1$).

Theorem 1. *The following assertions hold.*

1. *The equation (1) has finitely many solutions if and only if $d = 1$. Moreover, the amount of these solutions is equal to N.*
2. *The equation (1) has no solutions if and only if $d \nmid f_n$ for some $n \in \mathbb{Z}_+$.*
3. *The equation (1) has infinitely many solutions if and only if $d \neq 1$ and $d \mid f_n$ for all $n \in \mathbb{Z}_+$.*

Corollary 1. *Equation (1) has a unique solution if and only if $d = 1$ and $N = 1$. In particular, the homogeneous equation*

$$BX_{n+1} = AX_n, \quad n \in \mathbb{Z}_+ \tag{2}$$

has only trivial solution if and only if $d = 1$ and $N = 1$.

Corollary 2. *The equation (1) has a unique solution if and only if B is nilpotent and A is an invertible element of the ring $\mathbb{Z}_m$.*

Corollary 3. *If the homogeneous equation (2) has only trivial solution, then for any sequence $\{F_n\}_{n=0}^{\infty}$ Equation (1) has a unique solution.*

We also proved the theorem about solvability of the initial problem $X_0 = Y_0 \in \mathbb{Z}_m$ for Equation (1).