Carmichael numbers for $\mathbf{GL}(m)$

Eugene Karolinsky, Dmytro Seliutin

We propose a generalisation of Carmichael numbers, where the multiplicative group $\mathbb{G}_m = \mathrm{GL}(1)$ is replaced by $\mathrm{GL}(m)$ for $m \geq 2$. Our construction is based on the analogue of Fermat's little theorem for $\mathrm{GL}(m)$. We prove basic properties of these families of numbers and give some examples.

Let us recall basic information about Carmichael numbers.

Definition 1. A composite number $n \in \mathbb{N}$ is called *Carmichael* if $a^{n-1} = 1$ for any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 1. *(Korselt's criterion)*
Let $n \in \mathbb{N}$ be a composite number. The following are equivalent:

1) n is a Carmichael number,

2) n is squarefree and if $p|n$, then $p-1\big|n-1$.

Now we pass to Carmichael numbers for $\mathrm{GL}(m)$, where $m > 1$. Let us introduce some notation:

$$D_m(n) = \prod_{k=1}^{m} \Phi_k(n),$$

$$\nabla_m(n) = \prod_{p|n} p^{\lceil \log_p m \rceil - 1},$$

$$K_m(n) = n \nabla_m(n) D_m(n),$$

where p is a prime number, $\Phi_k(x)$ kth cyclotomic polynomial.

Definition 2. A composite number $n \in \mathbb{N}$ is called an *m-Carmichael number* if $A^{K_m(n)} = I$ for all $A \in \mathrm{GL}(m, \mathbb{Z}/n\mathbb{Z})$.

Theorem 2. *Let $n \in \mathbb{N}$ be a composite number. The following are equivalent:*

1) n is an m-Carmichael number,

2) if $p|n$, then $D_m(p)\big|K_m(n)$.

Theorem 3. *If $n \in \mathbb{N}$ is a nontrivial prime power (i.e. $n = p^k$, where $k > 1$ and p is a prime number), then n is an m-Carmichael number for all $m > 1$.*