A Simple Group Generated by Involutions Interchanging Residue Classes of the Integers

Stefan Kohl

Institut für Geometrie und Topologie, Universität Stuttgart, 70550 Stuttgart / Germany,
e-mail: `kohl@mathematik.uni-stuttgart.de`

Abstract. We present a new countable simple group, which arises in a natural way from the arithmetical structure of the ring of integers. Its subgroups form a large new class of algorithmically tractable groups, which extends the scope of computational group theory.

1. Introduction

Several types of infinite simple groups are treated in the literature so far:

- Simple groups of Lie type, see e.g. Carter [4].
- Finitely presented simple groups, see e.g. Higman [8], Stein [19].
- Locally finite simple groups, see e.g. Kegel, Wehrfritz [9].
- Composition factors of infinite symmetric groups, see e.g. Baer [1].
- Simple groups which are constructed to have certain given 'strange' properties like having only cyclic proper subgroups or being ordered, see e.g. Ol'shanskii [18], Chehata [5].

The group which is presented in this article belongs to none of these classes. It emerges in a natural way from the arithmetical structure of $\mathbb{Z}$:

1.1 Definition Let $\mathrm{CT}(\mathbb{Z})$ be the group which is generated by the set of all *class transpositions*: Given disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ of $\mathbb{Z}$, we define the *class transposition* $\tau_{r_1(m_1),r_2(m_2)} \in \mathrm{Sym}(\mathbb{Z})$ by

$$\tau_{r_1(m_1),r_2(m_2)}: \quad n \longmapsto \begin{cases} (m_2n + m_1r_2 - m_2r_1)/m_1 & \text{if } n \in r_1(m_1), \\ (m_1n + m_2r_1 - m_1r_2)/m_2 & \text{if } n \in r_2(m_2), \\ n & \text{otherwise}, \end{cases}$$

where we assume that $0 \leqslant r_1 < m_1$ and that $0 \leqslant r_2 < m_2$. For reasons of convenience, we set $\tau := \tau_{0(2),1(2)} : n \mapsto n + (-1)^n$.

1.2 Theorem The group $\mathrm{CT}(\mathbb{Z})$ is simple. It has the following properties:

1. It is countable, but not finitely generated.
2. All finite groups embed in it, and it acts highly transitively on $\mathbb{N}_0$.
3. Its torsion subgroups are divisible.
4. The free group of rank 2 and the modular group $\mathrm{PSL}(2,\mathbb{Z})$ embed in it.
5. All free products of finitely many finite groups embed in it.
6. The class of its subgroups is closed under taking direct products and under taking wreath products with finite groups and with $(\mathbb{Z},+)$.
7. It has finitely generated subgroups which are not finitely presented.
8. It has finitely generated subgroups for which the membership problem is unsolvable.
9. It has uncountably many simple subgroups.
10. It contains a certain permutation of $\mathbb{Z}$ which Lothar Collatz has investigated in the 1930s and whose cycle structure is not known so far.
11. It has a locally finite simple subgroup, which acts highly transitively on $\mathbb{N}_0$.
12. It has simple supergroups which can be obtained by taking one resp. two additional generators and which act highly transitively on $\mathbb{Z}$.

The proof of the simplicity of $\mathrm{CT}(\mathbb{Z})$ is carried out in Section 2. Proofs of Assertions (1) – (8) are given later in this section, and proofs of Assertions (9) – (12) can be found in Sections 2 – 5.

However before starting with the proofs, we need to introduce a couple of basic terms.

1.3 Definition We call a mapping $f : \mathbb{Z} \to \mathbb{Z}$ *residue class-wise affine* if there is a positive integer m such that the restrictions of f to the residue classes $r(m) \in \mathbb{Z}/m\mathbb{Z}$ are all affine. This means that for any residue class $r(m)$ there are coefficients $a_{r(m)}$, $b_{r(m)}$, $c_{r(m)} \in \mathbb{Z}$ such that the restriction of the mapping f to the set $r(m) = \{r + km | k \in \mathbb{Z}\}$ is given by

$$f|_{r(m)} : \ r(m) \to \mathbb{Z}, \ \ n \ \mapsto \ \frac{a_{r(m)} \cdot n + b_{r(m)}}{c_{r(m)}}.$$

We call the smallest possible m the *modulus* of f, written $\mathrm{Mod}(f)$. For reasons of uniqueness, we assume that $\gcd(a_{r(m)}, b_{r(m)}, c_{r(m)}) = 1$ and that $c_{r(m)} > 0$. We define the *multiplier* $\mathrm{Mult}(f)$ of f by $\mathrm{lcm}_{r(m)\in\mathbb{Z}/m\mathbb{Z}}\, a_{r(m)}$ and the *divisor* $\mathrm{Div}(f)$ of f by $\mathrm{lcm}_{r(m)\in\mathbb{Z}/m\mathbb{Z}}\, c_{r(m)}$. We call f *integral* if $\mathrm{Div}(f) = 1$. We call f *class-wise order-preserving* if all $a_{r(m)}$ are positive.

It is easy to see that the permutations of this kind form a countable supergroup of $\mathrm{CT}(\mathbb{Z})$.

1.4 Definition We denote the group consisting of all residue class-wise affine permutations of $\mathbb{Z}$ by $\mathrm{RCWA}(\mathbb{Z})$, and call its subgroups *residue class-wise affine* groups.

The notation '$\mathrm{CT}(\mathbb{Z})$' resp. '$\mathrm{RCWA}(\mathbb{Z})$' reflects that generalizations to suitable rings other than $\mathbb{Z}$ make perfect sense. For the sake of simplicity and to keep the article easy to read, we refrain from following this possibly fruitful direction of research at this point.

The group $\mathrm{RCWA}(\mathbb{Z})$ is not co-Hopfian. In the proof of Assertion (6), we need the following monomorphisms:

1.5 Definition Let f be an injective residue class-wise affine mapping, and let $\pi_f : \mathrm{RCWA}(\mathbb{Z}) \hookrightarrow \mathrm{RCWA}(\mathbb{Z}), \sigma \mapsto \sigma_f$ be the monomorphism defined by the properties $\forall \sigma \in \mathrm{RCWA}(\mathbb{Z})\ f\sigma_f = \sigma f$ and $\mathrm{supp}(\mathrm{im}\,\pi_f) \subseteq \mathrm{im}\,f$. Then we call π_f the *restriction monomorphism* associated to f.

In the sequel, we prove Assertions (1) – (8) of Theorem 1.2:

1. It can be seen easily that the multiplier resp. divisor of the product of two residue class-wise affine permutations divides the product of the multipliers resp. divisors of the factors. Further it is obvious that inversion interchanges multiplier and divisor. Therefore as there are infinitely many primes and as for any positive integer n there is a class transposition $\tau_{1(2),0(2n)}$ with multiplier and divisor n, the group $\mathrm{CT}(\mathbb{Z})$ is not finitely generated.
2. Any finite symmetric group S_m has a monomorphic image in $\mathrm{CT}(\mathbb{Z})$: Let $m \geqslant 2$, and let S_m act naturally on the set $\{0, 1, \ldots, m-1\}$. Then an example of a corresponding monomorphism is

$$\begin{aligned}\varphi_m &: \mathrm{S}_m \hookrightarrow \mathrm{CT}(\mathbb{Z}),\\ &\quad \sigma \mapsto (\sigma^{\varphi_m} :\ n \mapsto n + (n \mod m)^\sigma - n \mod m)\,.\end{aligned}$$

   Just like the group S_m itself, its image under φ_m acts m - transitively on the set $\{0, 1, \ldots, m-1\}$. Since m can be chosen arbitrary large and as class transpositions map nonnegative integers to nonnegative integers, this means that the group $\mathrm{CT}(\mathbb{Z})$ acts highly transitively on $\mathbb{N}_0$.
3. We show that given an element $g \in \mathrm{CT}(\mathbb{Z})$ of finite order and a positive integer k, there is always an $h \in \mathrm{CT}(\mathbb{Z})$ such that $h^k = g$: Since the element g has finite order, it permutes a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes on all of which it is affine. A k-th root h can be constructed from g by 'slicing' cycles $\prod_{i=2}^{l} \tau_{r_1(m_1),r_i(m_i)}$ on $\mathcal{P}$ into cycles $\prod_{i=1}^{l} \prod_{j=\max(2-i,0)}^{k-1} \tau_{r_1(km_1),r_i+jm_i(km_i)}$ of the k-fold length on the refined partition which one gets from $\mathcal{P}$ by decomposing any $r_i(m_i) \in \mathcal{P}$ into residue classes (mod km_i).
4. The free group of rank 2 embeds in $\mathrm{CT}(\mathbb{Z})$. An example of an embedding is given by

$$\begin{aligned}\varphi_{\mathrm{F}_2} :\ \mathrm{F}_2 = \langle a, b\rangle \ &\hookrightarrow\ \mathrm{CT}(\mathbb{Z}),\\ a \ \mapsto\ (\tau \cdot \tau_{0(2),1(4)})^2,\ \ b \ &\mapsto\ (\tau \cdot \tau_{0(2),3(4)})^2.\end{aligned}$$

This can be seen by applying the Table-Tennis Lemma (see for example la Harpe [6], Section II.B.) to the infinite cyclic groups generated by the images of a and b under φ_{F_2} and the sets $0(4) \cup 1(4)$ and $2(4) \cup 3(4)$. Likewise, the Table-Tennis Lemma can be used to show that

$$\varphi_{\mathrm{PSL}(2,\mathbb{Z})}: \ \mathrm{PSL}(2,\mathbb{Z}) \ \cong \ \langle a, b \mid a^3 = b^2 = 1 \rangle \ \hookrightarrow \ \mathrm{CT}(\mathbb{Z}),$$
$$a \ \mapsto \ \tau_{0(4),2(4)} \cdot \tau_{1(2),0(4)}, \ \ b \ \mapsto \ \tau$$

is an embedding of the modular group $\mathrm{PSL}(2,\mathbb{Z})$. In this case one can use the sets $0(2)$ and $1(2)$ in place of $0(4) \cup 1(4)$ and $2(4) \cup 3(4)$.

5. Let $G_0, \dots, G_{m-1}$ be finite groups. To see that their free product embeds in $\mathrm{CT}(\mathbb{Z})$, proceed as follows: First consider regular permutation representations φ_r of the groups G_r on the residue classes (mod $|G_r|$). Then take conjugates $H_r := (\mathrm{im}\,\varphi_r)^{\sigma_r}$ of the images of these representations under mappings $\sigma_r \in \mathrm{CT}(\mathbb{Z})$ which map $0(|G_r|)$ to $\mathbb{Z} \setminus r(m)$. Finally use that point stabilizers in regular permutation groups are trivial and apply the Table-Tennis Lemma to the groups H_r and the residue classes $r(m)$ to see that the group generated by the H_r's is isomorphic to their free product.
6. Given any two subgroups $G, H \leqslant \mathrm{RCWA}(\mathbb{Z})$, the group generated by $G^{\pi_{n \mapsto 2n}}$ and $H^{\pi_{n \mapsto 2n+1}}$ is clearly isomorphic to $G \times H$. As the image of a class transposition $\tau_{r_1(m_1),r_2(m_2)}$ under a restriction monomorphism $\pi_{n \mapsto mn+r}$ is $\tau_{mr_1+r(mm_1),mr_2+r(mm_2)}$, the same argument can be used for our group $\mathrm{CT}(\mathbb{Z})$ as well.
   Looking at the monomorphisms π_{mn+r} and φ_m, it is immediate to see that the classes of isomorphism types of subgroups of $\mathrm{RCWA}(\mathbb{Z})$ resp. $\mathrm{CT}(\mathbb{Z})$ are closed under forming wreath products with finite permutation groups as well. Further given a subgroup G, a subgroup isomorphic to $G \wr (\mathbb{Z},+)$ is generated by $G^{\pi_{n \mapsto 4n+3}}$ and $\tau \cdot \tau_{0(2),1(4)}$. This is seen best by checking that the orbit of the residue class 3(4) under the action of the cyclic group $\langle \tau \cdot \tau_{0(2),1(4)} \rangle$ consists of disjoint residue classes, thus that the conjugates of $G^{\pi_{n \mapsto 4n+3}}$ under powers of $\tau \cdot \tau_{0(2),1(4)}$ have pairwise disjoint supports.
7. By Assertion (6), the group $\mathrm{CT}(\mathbb{Z})$ contains nontrivial wreath products $G \wr (\mathbb{Z},+)$. By the main theorem in Baumslag [2], these are not finitely presented.
8. Let $\mathrm{F}_2 = \langle a, b \rangle$ be the free group of rank 2. Further let $r_1, \dots, r_k \in \mathrm{F}_2$ be the relators of a finitely presented group with unsolvable word problem – such a group exists by Novikov [17] and Boone [3]. Then the membership problem for the group

$$\langle (a,a), (b,b), (1,r_1), \dots, (1,r_k) \rangle < \mathrm{F}_2 \times \mathrm{F}_2$$

   is unsolvable (cp. Mihailova [15], [16]; see also Lyndon, Schupp [14], Chapter IV.4). Thus as $\mathrm{F}_2 \times \mathrm{F}_2$ embeds in $\mathrm{CT}(\mathbb{Z})$, there are finitely generated subgroups $G < \mathrm{CT}(\mathbb{Z})$ with unsolvable membership problem.

The proofs of Assertions (2) – (6) describe explicit constructions. They are implemented in the author's GAP [7] package RCWA [11]. This package provides a large variety of functionality for computing with residue class-wise affine groups and for exhibiting their structure.

2. The Group $\mathrm{CT}(\mathbb{Z})$ is Simple

The aim of this section is to show that the group $\mathrm{CT}(\mathbb{Z})$ is simple. For this we need some lemmata:

2.1 Lemma *Given two class transpositions $\tau_{r_1(m_1),r_2(m_2)}$, $\tau_{r_3(m_3),r_4(m_4)}$ not equal to τ, there is always a product π of 6 class transpositions such that $\tau_{r_1(m_1),r_2(m_2)}^\pi = \tau_{r_3(m_3),r_4(m_4)}$.*

Proof: Let $r_5(m_5), r_6(m_6) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$ be disjoint residue classes such that $\cup_{i=3}^6 r_i(m_i) \neq \mathbb{Z}$, and $r_7(m_7), r_8(m_8) \subset \mathbb{Z} \setminus \cup_{i=3}^6 r_i(m_i)$ be disjoint residue classes. Then the following hold:

1. $\tau_{r_1(m_1),r_2(m_2)}{}^{\tau_{r_1(m_1),r_5(m_5)} \cdot \tau_{r_2(m_2),r_6(m_6)}} = \tau_{r_5(m_5),r_6(m_6)}$.
2. $\tau_{r_5(m_5),r_6(m_6)}{}^{\tau_{r_5(m_5),r_7(m_7)} \cdot \tau_{r_6(m_6),r_8(m_8)}} = \tau_{r_7(m_7),r_8(m_8)}$.
3. $\tau_{r_7(m_7),r_8(m_8)}{}^{\tau_{r_3(m_3),r_7(m_7)} \cdot \tau_{r_4(m_4),r_8(m_8)}} = \tau_{r_3(m_3),r_4(m_4)}$.

The assertion follows. □

2.2 Lemma *Let $\sigma, \upsilon \in \mathrm{RCWA}(\mathbb{Z})$, and put $m := \mathrm{Mod}(\sigma)$. If υ is integral and fixes all residue classes (mod m) setwisely, then $[\sigma, \upsilon]$ is also integral.*

Proof: Since υ fixes residue classes (mod m), an affine partial mapping α of $[\sigma, \upsilon]$ is a product $\alpha_\sigma^{-1}\alpha_{\upsilon^{-1}}\alpha_\sigma\alpha_\upsilon$ of affine partial mappings α_σ, α_υ and $\alpha_{\upsilon^{-1}}$ of σ, υ resp. υ^{-1}. The assertion follows since the subgroup generated by translations and reflections is normal in the affine group of $\mathbb{Q}$. □

2.3 Lemma *Let G be a subgroup of $\mathrm{RCWA}(\mathbb{Z})$ which contains $\mathrm{CT}(\mathbb{Z})$. Then any nontrivial normal subgroup $N \trianglelefteq G$ has an integral element $\iota \neq 1$.*

Proof: Let $\sigma \in N \setminus \{1\}$, and let $m := \mathrm{Mod}(\sigma)$. Without loss of generality we can assume that there is a residue class $r(m)$ such that $r(m)^\sigma \neq r(m)$. Put $\iota := [\sigma, \tau_{r(2m),r+m(2m)}] \in N \setminus \{1\}$. By Lemma 2.2, ι is integral. □

Now we can prove our theorem:

2.4 Theorem *The group* $\mathrm{CT}(\mathbb{Z})$ *is simple.*

Proof: We have to show that any nontrivial normal subgroup $N \trianglelefteq \mathrm{CT}(\mathbb{Z})$ contains any class transposition. By Lemma 2.1 all class transpositions $\neq \tau$ are conjugate in $\mathrm{CT}(\mathbb{Z})$. Further we have $\tau = \tau_{0(4),1(4)} \cdot \tau_{2(4),3(4)}$. Thus it is already sufficient to show that one class transposition $\neq \tau$ lies in N.

By Lemma 2.3 the normal subgroup N has an integral element $\iota_1 \neq 1$. Let $m \geqslant 3$ be a large enough multiple of the modulus of ι_1 such that there is a residue class $r(m) \in \mathbb{Z}/m\mathbb{Z}$ which ι_1 does not fix setwisely. Then put $\iota_2 := \tau_{r(2m),r+m(2m)} \cdot \tau_{r(2m)^{\iota_1},r+m(2m)^{\iota_1}} = [\tau_{r(2m),r+m(2m)}, \iota_1] \in N$.

By the choice of m we can now choose two distinct residue classes $r_1(2m), r_2(2m) \notin \{r(2m), r+m(2m), r(2m)^{\iota_1}, r+m(2m)^{\iota_1}\}$. Then we have

$$\begin{aligned}\tau_{r_1(2m),r_2(2m)} &= \iota_2^{\tau_{r(2m),r_1(4m)} \cdot \tau_{r+m(2m),r_2(4m)}} \\ &\quad \cdot \iota_2^{\tau_{r(2m),r_1+2m(4m)} \cdot \tau_{r+m(2m),r_2+2m(4m)}} \in N,\end{aligned}$$

which completes the proof of the theorem. □

2.5 Remark Assume $\mathrm{CT}(\mathbb{Z}) \leqslant G \leqslant \mathrm{RCWA}(\mathbb{Z})$, and let N be a nontrivial normal subgroup of G. Then the proof of Theorem 2.4 shows in fact that N contains $\mathrm{CT}(\mathbb{Z})$.

2.6 Definition Given a set of primes $\mathbb{P}$, let $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z}) < \mathrm{CT}(\mathbb{Z})$ denote the subgroup which is generated by all class transpositions whose moduli have only prime factors in $\mathbb{P}$.

2.7 Corollary *If the set* $\mathbb{P}$ *contains 2, then* $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ *is simple as well. Hence the group* $\mathrm{CT}(\mathbb{Z})$ *has uncountably many simple subgroups.*

Proof: In case $2 \in \mathbb{P}$, all of our arguments in this section apply to $\mathrm{CT}_{\mathbb{P}}(\mathbb{Z})$ as well: In the proof of Lemma 2.1, we can choose the four residue classes $r_5(m_5), \dots, r_8(m_8)$ in such a way that all prime factors of their moduli already divide $m_1m_2m_3m_4$. The proofs of Lemma 2.2, Lemma 2.3 and Theorem 2.4 likewise do not require the presence of class transpositions whose moduli have certain odd factors. □

3. Collatz' Permutation Lies in $\mathrm{CT}(\mathbb{Z})$

In 1932, Lothar Collatz investigated the permutation

$$\alpha \in \mathrm{RCWA}(\mathbb{Z}): \quad n \ \mapsto \begin{cases} \frac{2n}{3} & \text{if } n \in 0(3), \\ \frac{4n-1}{3} & \text{if } n \in 1(3), \\ \frac{4n+1}{3} & \text{if } n \in 2(3) \end{cases}$$

of the integers (cp. Keller [10], Wirsching [20]).

The permutation α commutes with the involution $n \mapsto -n$, thus the cycle structures of its restrictions to the positive resp. negative integers are the same. The fixed points of α are -1, 0 and 1. In Keller [10] it is shown that α has at most finitely many cycles of any given finite length. It further looks likely that the only finite cycles are the transpositions $\pm(2\ 3)$, the 5-cycles $\pm(4\ 5\ 7\ 9\ 6)$ and the 12-cycles $\pm(44\ 59\ 79\ 105\ 70\ 93\ 62\ 83\ 111\ 74\ 99\ 66)$. However according to Wirsching [20] the latter has still not been proven, and in particular it is not yet known whether the cycle

$$(\ \dots\ 32\ 43\ 57\ 38\ 51\ 34\ 45\ 30\ 20\ 27\ 18\ 12\ 8\ 11\ 15\ 10\ 13\ 17\ 23\ 31\ \dots\ )$$

of α is finite or infinite.

In spite of this we can show that the permutation α lies in $\mathrm{CT}(\mathbb{Z})$ by determining an explicit factorization into generators.

The major obstacle we are confronted with when trying to obtain such a factorization is the fact that multiplier and divisor of α are coprime, whereas multiplier and divisor of a class transposition are always the same. We have already observed that the multiplier resp. divisor of a product of two residue class-wise affine mappings always divides the product of the multipliers resp. divisors of the factors. In the given case we need to form a product of class transpositions in such a way that one prime divisor gets eliminated from the multiplier of the product, but appears in the denominators of all of its affine partial mappings.

As a first step towards a solution of the factorization problem, we hence attempt to determine some product of class transpositions which has coprime multiplier and divisor. It turns out that 6 class transpositions are sufficient to form such a product: Given an odd prime p, the permutation

$$\begin{aligned}\sigma_p \ :=\ & \tau_{0(8),1(2p)} \cdot \tau_{4(8),2p-1(2p)} \\ & \cdot \tau_{0(4),1(2p)} \cdot \tau_{2(4),2p-1(2p)} \\ & \cdot \tau_{2(2p),1(4p)} \cdot \tau_{4(2p),2p+1(4p)} \ \in\ \mathrm{CT}(\mathbb{Z})\end{aligned}$$

has multiplier p and divisor 2.
Indeed, evaluating this product yields

$$\sigma_p:\ \ n \ \mapsto \begin{cases} (pn+2p-2)/2 & \text{if } n \in 2(4), \\ n/2 & \text{if } n \in 0(4) \setminus (4(4p) \cup 8(4p)), \\ n+2p-7 & \text{if } n \in 8(4p), \\ n-2p+5 & \text{if } n \in 2p-1(2p), \\ n+1 & \text{if } n \in 1(2p), \\ n-3 & \text{if } n \in 4(4p), \\ n & \text{if } n \in 1(2) \setminus (1(2p) \cup 2p-1(2p)). \end{cases}$$

The GAP [7] package RCWA [11] provides a factorization routine for residue class-wise affine permutations, which uses certain elaborate heuristics. The permutations σ_p and their images under restriction monomorphisms $\pi_{n \mapsto mn+r}$ play a key role in this routine. It has been used to obtain the following factorization of α:

$$\begin{aligned}\alpha = {} & \tau_{0(6),4(6)} \cdot \tau_{0(6),5(6)} \cdot \tau_{0(6),3(6)} \cdot \tau_{0(6),1(6)} \cdot \tau_{0(6),2(6)} \\ & \cdot\tau_{2(3),4(6)} \cdot \tau_{0(3),4(6)} \cdot \tau_{2(3),1(6)} \cdot \tau_{0(3),1(6)} \cdot \tau_{0(36),35(36)} \\ & \cdot\tau_{0(36),22(36)} \cdot \tau_{0(36),18(36)} \cdot \tau_{0(36),17(36)} \cdot \tau_{0(36),14(36)} \cdot \tau_{0(36),20(36)} \\ & \cdot\tau_{0(36),4(36)} \cdot \tau_{2(36),8(36)} \cdot \tau_{2(36),16(36)} \cdot \tau_{2(36),13(36)} \cdot \tau_{2(36),9(36)} \\ & \cdot\tau_{2(36),7(36)} \cdot \tau_{2(36),6(36)} \cdot \tau_{2(36),3(36)} \cdot \tau_{2(36),10(36)} \cdot \tau_{2(36),15(36)} \\ & \cdot\tau_{2(36),12(36)} \cdot \tau_{2(36),5(36)} \cdot \tau_{21(36),28(36)} \cdot \tau_{21(36),33(36)} \cdot \tau_{21(36),30(36)} \\ & \cdot\tau_{21(36),23(36)} \cdot \tau_{21(36),34(36)} \cdot \tau_{21(36),31(36)} \cdot \tau_{21(36),27(36)} \cdot \tau_{21(36),25(36)} \\ & \cdot\tau_{21(36),24(36)} \cdot \tau_{26(36),32(36)} \cdot \tau_{26(36),29(36)} \cdot \tau_{10(18),35(36)} \cdot \tau_{5(18),35(36)} \\ & \cdot\tau_{10(18),17(36)} \cdot \tau_{5(18),17(36)} \cdot \tau_{8(12),14(24)} \cdot \tau_{6(9),17(18)} \cdot \tau_{3(9),17(18)} \\ & \cdot\tau_{0(9),17(18)} \cdot \tau_{6(9),16(18)} \cdot \tau_{3(9),16(18)} \cdot \tau_{0(9),16(18)} \cdot \tau_{6(9),11(18)} \\ & \cdot\tau_{3(9),11(18)} \cdot \tau_{0(9),11(18)} \cdot \tau_{6(9),4(18)} \cdot \tau_{3(9),4(18)} \cdot \tau_{0(9),4(18)} \\ & \cdot\tau_{0(6),14(24)} \cdot \tau_{0(6),2(24)} \cdot \tau_{8(12),17(18)} \cdot \tau_{7(12),17(18)} \cdot \tau_{8(12),11(18)} \\ & \cdot\tau_{7(12),11(18)} \cdot \sigma_3^{-1} \cdot \tau_{7(12),17(18)} \cdot \tau_{2(6),17(18)} \cdot \tau_{0(3),17(18)} \cdot \sigma_3^{-3}.\end{aligned}$$

This shows constructively that $\alpha \in \mathrm{CT}(\mathbb{Z})$.

4. A Locally Finite Simple Subgroup of $\mathrm{CT}(\mathbb{Z})$

The class transpositions which interchange residue classes with the same modulus generate a proper subgroup of $\mathrm{CT}(\mathbb{Z})$:

4.1 Definition Let $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ denote the subgroup of $\mathrm{CT}(\mathbb{Z})$ which is generated by all integral class transpositions.

The group $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ acts highly transitively on $\mathbb{N}_0$ for the same reasons as $\mathrm{CT}(\mathbb{Z})$ does so. Finitely generated subgroups of $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ act faithfully on the set of residue classes modulo the lcm of the moduli of the generators. Therefore they are finite. Hence the group $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ is locally finite. We still have to show the second property announced in the section title:

4.2 Theorem *The group $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ is simple.*

Proof: We have to show that any nontrivial normal subgroup $N \trianglelefteq \mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ contains any class transposition of the form $\tau_{r_1(m),r_2(m)}$.

Let $\iota_1 \in N \setminus \{1\}$. Further let m be a large enough multiple of the modulus of ι_1 such that there is a residue class $r(m) \in \mathbb{Z}/m\mathbb{Z}$ which ι_1 does not fix setwisely. Then

$$\iota_2 := \tau_{r(2m),r+m(2m)} \cdot \tau_{r(2m)^{\iota_1},r+m(2m)^{\iota_1}} = [\iota_1, \tau_{r(2m),r+m(2m)}] \in N$$

is a product of two class transpositions with modulus $2m$ and disjoint supports.

We make the following observations:

1. All products of two integral class transpositions with the same modulus $m \geqslant 4$ and disjoint supports are conjugate in the group $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$: Let $(r_i(m))_{i\in\{1,\dots,4\}}$ and $(\tilde{r}_i(m))_{i\in\{1,\dots,4\}}$ each be 4-tuples of pairwise disjoint residue classes. Then we have
$$\left(\tau_{r_1(m),r_2(m)}\cdot\tau_{r_3(m),r_4(m)}\right)^{\prod_{i=1}^{4}\tau_{r_i(m),\tilde{r}_i(m)}} \;=\; \tau_{\tilde{r}_1(m),\tilde{r}_2(m)}\cdot\tau_{\tilde{r}_3(m),\tilde{r}_4(m)},$$
where we read $\tau_{r_i(m),\tilde{r}_i(m)}$ as the identity if $r_i = \tilde{r}_i$.
2. Given class transpositions $\tau_1 = \tau_{r_1(m),r_2(m)}$ and $\tau_2 = \tau_{r_3(2m),r_4(2m)}$ with disjoint supports, we have
$$\begin{aligned}\tau_1 \;=\; & \tau_2 \cdot \tau_{r_1(2m),r_2(2m)} \\ & \cdot\, \tau_2 \cdot \tau_{r_1+m(2m),r_2+m(2m)}.\end{aligned}$$
Therefore any integral class transposition $\neq \tau$ can be written as a product of two suitable products of two integral class transpositions with disjoint supports.
3. Given $k \in \mathbb{N}$, any integral class transposition can be written as a product of k integral class transpositions with the k-fold modulus. This can be seen from the equality $\tau_{r_1(m),r_2(m)} = \prod_{i=0}^{k-1}\tau_{r_1+im(km),r_2+im(km)}$.

In the second paragraph of the proof we can choose m to be a multiple of any given positive integer. Therefore from Observations (1) – (3) we can conclude that N contains indeed any integral class transposition. Hence the group $\mathrm{CT}_{\mathrm{int}}(\mathbb{Z})$ is simple, as claimed. □

5. Two Simple Supergroups of CT($\mathbb{Z}$)

In this section we present two simple subgroups of $\mathrm{RCWA}(\mathbb{Z})$ which properly contain $\mathrm{CT}(\mathbb{Z})$ and which act highly transitively on $\mathbb{Z}$.

We identify these simple groups in the kernels of certain epimorphisms $\pi^+ : \mathrm{RCWA}^+(\mathbb{Z}) \to (\mathbb{Z},+)$ and $\pi^- : \mathrm{RCWA}(\mathbb{Z}) \to \mathbb{Z}^\times \cong \mathrm{C}_2$, where $\mathrm{RCWA}^+(\mathbb{Z}) < \mathrm{RCWA}(\mathbb{Z})$ denotes the subgroup consisting of all class-wise order-preserving elements. Using the notation for the coefficients introduced in Definition 1.3, these epimorphisms are given by
$$\pi^+ :\ \sigma \;\mapsto\; \frac{1}{m}\sum_{r(m)\in\mathbb{Z}/m\mathbb{Z}} \frac{b_{r(m)}}{a_{r(m)}}$$
and
$$\pi^- :\ \sigma \;\mapsto\; (-1)^{\sigma^{\pi^+} + \frac{1}{m}\sum_{r(m):\ a_{r(m)}<0}(m-2r)}$$
(see Sections 2.11 and 2.12 in Kohl [12]).

5.1 Definition We denote the kernels of π^+ resp. π^- by K^+ resp. K^-.

It is easy to see that $\mathrm{CT}(\mathbb{Z}) \lneqq K^+ \lneqq K^- \lneqq \mathrm{RCWA}(\mathbb{Z})$.

Our simple groups will be the subgroups of K^+ and K^- which are generated by the elements which are *tame* in the following sense:

5.2 Definition We call an element $\sigma \in \mathrm{RCWA}(\mathbb{Z})$ *tame* if it permutes a partition $\mathcal{P}$ of $\mathbb{Z}$ into finitely many residue classes on all of which it is affine, and *wild* otherwise. We call a group $G < \mathrm{RCWA}(\mathbb{Z})$ *tame* if there is a common such partition for all elements of G, and *wild* otherwise. We call partitions with the described properties *respected partitions* of σ resp. G.

5.3 Definition We denote the normal subgroups of K^+ resp. K^- which are generated by the tame elements by $\tilde{K}^+$ resp. $\tilde{K}^-$.

Obviously, finite residue class-wise affine groups and integral residue class-wise affine permutations are tame. Tameness is invariant under conjugation: If $\alpha \in \mathrm{RCWA}(\mathbb{Z})$ respects a partition $\mathcal{P}$, then a conjugate α^β respects the partition consisting of the images of the intersections of the residue classes in $\mathcal{P}$ with the sources of the affine partial mappings of β under β. Of course the product of two tame permutations is in general not tame. Further, tameness of products does not induce an equivalence relation on the set of tame permutations: Let for example $a := \tau_{1(6),4(6)}$, $b := \tau_{0(5),2(5)}$ and $c := \tau_{3(4),4(6)}$. Then ab and bc are tame, but ac is not. If a tame group does not act faithfully on a respected partition, the kernel of the action clearly does not act on $\mathbb{N}_0$. Thus as the group $\mathrm{CT}(\mathbb{Z})$ acts on $\mathbb{N}_0$, its tame subgroups are finite. It can be shown that a residue class-wise affine group is tame if and only if the set of moduli of its elements is bounded (see Theorem 2.5.8 in [12]).

It is easy to see that all tame elements of $\mathrm{RCWA}(\mathbb{Z})$ can be written as products of class transpositions and members of the following two series:

5.4 Definition Let $r(m) \subset \mathbb{Z}$ be a residue class.

1. We define the *class shift* $\nu_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ by

$$\nu_{r(m)}: \ n \ \mapsto \ \begin{cases} n+m & \text{if } n \in r(m), \\ n & \text{otherwise.} \end{cases}$$

2. We define the *class reflection* $\varsigma_{r(m)} \in \mathrm{RCWA}(\mathbb{Z})$ by

$$\varsigma_{r(m)}: \ n \ \mapsto \ \begin{cases} -n+2r & \text{if } n \in r(m), \\ n & \text{otherwise,} \end{cases}$$

where we assume $0 \leqslant r < m$.

For convenience, we set $\nu := \nu_{\mathbb{Z}} : n \mapsto n+1$ and $\varsigma := \varsigma_{\mathbb{Z}} : n \mapsto -n$.

Likewise it is easy to see that class shifts and class reflections do neither lie in K^+ nor in K^-.

5.5 Lemma *We have*

1. $\tilde{K}^+ := \langle \mathrm{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}^{-1} \rangle$ *and*
2. $\tilde{K}^- := \langle \mathrm{CT}(\mathbb{Z}), \nu_{1(3)} \cdot \nu_{2(3)}, \varsigma_{0(2)} \cdot \nu_{0(2)} \rangle$.

Proof: We identify 2 resp. 3 series of generators:

1. Looking at respected partitions, we check that $\tilde{K}^+$ is generated by
   (a) all class transpositions and
   (b) all quotients of two class shifts with disjoint supports whose union has a nontrivial complement in $\mathbb{Z}$.

   For this we consider the process of factoring a given tame $\vartheta \in K^+$ into these elements:

   ad (a) Let $\mathcal{P}$ be a respected partition of ϑ. Divide ϑ by a product of class transpositions which respects $\mathcal{P}$ as well and which induces on $\mathcal{P}$ the same permutation as ϑ does.

   ad (b) Factor the remaining quotient which is integral and fixes the partition $\mathcal{P}$ into quotients of two class shifts with disjoint supports which respect $\mathcal{P}$. This works since the lattice in $\mathbb{Z}^n$ consisting of all vectors with zero coordinate sum is spanned by the differences of two distinct canonical basis vectors.
2. Looking at respected partitions, we check that $\tilde{K}^-$ is generated by
   (a) all products of a class reflection and a class shift with the same support which has a nontrivial complement in $\mathbb{Z}$,
   (b) all class transpositions and
   (c) all products of two class shifts with disjoint supports whose union has a nontrivial complement in $\mathbb{Z}$.

   Similar as above, we consider the process of factoring a given tame permutation $\vartheta \in K^-$ into these elements:

   ad (a) Let $m \geqslant 2$ be a multiple of $\mathrm{Mod}(\vartheta)$. Make ϑ class-wise order-preserving via divisions from the left by products $\varsigma_{r(m)} \cdot \nu_{r(m)}$, where $r(m)$ runs over all residue classes (mod m) on which ϑ is order-reversing.

   ad (b) Let $\mathcal{P}$ be a respected partition of ϑ of length at least 3. Divide ϑ by a product of class transpositions which respects $\mathcal{P}$ as well and which induces on $\mathcal{P}$ the same permutation as ϑ does.

   ad (c) Factor the remaining quotient which is integral and fixes $\mathcal{P}$ into products of two class shifts with disjoint supports and inverses of such products. This works since for $n \geqslant 3$ the lattice in $\mathbb{Z}^n$ consisting of all vectors with even coordinate sum is spanned by the sums of two distinct canonical basis vectors.

Now we collapse series (1.b.), (2.a.) and (2.c) by taking orbit representatives under the conjugation action of $\mathrm{CT}(\mathbb{Z})$ to obtain the indicated single generators. □

5.6 Theorem *The groups $\tilde{K}^+$ and $\tilde{K}^-$ are simple, and they act highly transitively on $\mathbb{Z}$.*

Proof: First we prove the simplicity of $\tilde{K}^+$ and $\tilde{K}^-$. From Remark 2.5 we know that nontrivial normal subgroups of these groups contain $\mathrm{CT}(\mathbb{Z})$.

1. Let N be a nontrivial normal subgroup of $\tilde{K}^+$. Let $r_1(m_1)$ and $r_2(m_2)$ be two disjoint residue classes whose union is not $\mathbb{Z}$. Then for any residue class $r_3(m_3) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$ we have
$$\nu_{r_1(m_1)} \cdot \nu_{r_2(m_2)}^{-1} \ = \ [\tau_{r_1(m_1),r_2(m_2)}, \nu_{r_3(m_3)} \cdot \nu_{r_2(m_2)}^{-1}] \ \in \ N.$$
Putting $r_1(m_1) := 1(3)$ and $r_2(m_2) := 2(3)$, the simplicity of $\tilde{K}^+$ follows from Lemma 5.5, Assertion (1).
2. Let N be a nontrivial normal subgroup of $\tilde{K}^-$. Given disjoint residue classes $r_1(m_1)$ and $r_2(m_2)$ whose union is not $\mathbb{Z}$, for any residue class $r_3(m_3) \subset \mathbb{Z} \setminus (r_1(m_1) \cup r_2(m_2))$ we have
$$\begin{aligned}\nu_{r_1(m_1)} \cdot \nu_{r_2(m_2)} \ &= \ [\tau_{r_1(m_1),r_2(m_2)}, \nu_{r_3(m_3)} \cdot \varsigma_{r_1(m_1)}] \\ &\quad \cdot [\tau_{r_1(m_1),r_2(m_2)}, \varsigma_{r_1(m_1)} \cdot \nu_{r_1(m_1)}] \ \in \ N.\end{aligned}$$
This shows in particular that N contains $\nu_{1(3)} \cdot \nu_{2(3)}$.
Let $r(m) \subsetneq \mathbb{Z}$ be a residue class. Then for an arbitrary residue class $\tilde{r}(\tilde{m}) \subset \mathbb{Z} \setminus r(m)$ we have
$$\begin{aligned}\varsigma_{r(m)} \cdot \nu_{r(m)} \ &= \ [\tau_{r(m),\tilde{r}(\tilde{m})}, \varsigma_{r(m)} \cdot \nu_{\tilde{r}(\tilde{m})}] \\ &\quad \cdot [\tau_{\tilde{r}(2\tilde{m}),\tilde{r}+\tilde{m}(2\tilde{m})}, \varsigma_{\tilde{r}(2\tilde{m})} \cdot \nu_{\tilde{r}(2\tilde{m})}] \\ &\quad \cdot (\nu_{\tilde{r}(2\tilde{m})} \cdot \nu_{\tilde{r}+\tilde{m}(2\tilde{m})} \cdot \tau_{\tilde{r}(2\tilde{m}),\tilde{r}+\tilde{m}(2\tilde{m})})^{-1} \ \in \ N.\end{aligned}$$
This shows in particular that N contains also $\varsigma_{0(2)} \cdot \nu_{0(2)}$, and the simplicity of $\tilde{K}^-$ follows from Lemma 5.5, Assertion (2).

Now we show that both groups act highly transitively on $\mathbb{Z}$.

1. Consider $\tilde{K}^+$:
Let k be a positive integer, and let $(n_1, \dots, n_k)$ and $(\tilde{n}_1, \dots, \tilde{n}_k)$ be two k-tuples of pairwise distinct integers. We have to show that there is an element $\sigma \in \tilde{K}^+$ such that $(n_1^\sigma, \dots, n_k^\sigma) = (\tilde{n}_1, \dots, \tilde{n}_k)$.
Let $m := 2k + 1$, and choose a residue class $r(m)$ which does not contain one of the points n_i or $\tilde{n}_i$. Define $\sigma_1, \tilde{\sigma}_1 \in \tilde{K}^+$ by
$$\sigma_1 \ := \prod_{i:n_i<0} (\nu_{r(m)} \cdot \nu_{n_i(m)}^{-1})^{\lfloor \frac{n_i}{m} \rfloor} \ \text{ resp. } \ \tilde{\sigma}_1 \ := \prod_{i:\tilde{n}_i<0} (\nu_{r(m)} \cdot \nu_{\tilde{n}_i(m)}^{-1})^{\lfloor \frac{\tilde{n}_i}{m} \rfloor}.$$
Then the images of all points n_i resp. $\tilde{n}_i$ under σ_1 resp. $\tilde{\sigma}_1$ are nonnegative. Since we know that $\mathrm{CT}(\mathbb{Z})$ acts highly transitively on $\mathbb{N}_0$, we can choose a $\sigma_2 \in \mathrm{CT}(\mathbb{Z}) < \tilde{K}^+$ which maps the images of the n_i under σ_1 to the images of the $\tilde{n}_i$ under $\tilde{\sigma}_1$. Now the permutation $\sigma := \sigma_1 \cdot \sigma_2 \cdot \tilde{\sigma}_1^{-1}$ serves our purposes.

2. Consider $\tilde{K}^-$:
   Let $\varphi_m : \mathrm{S}_m \hookrightarrow \mathrm{CT}(\mathbb{Z})$ denote the monomorphism given in the introduction. Then the conjugate of $\mathrm{im}\,\varphi_m$ under $\nu^{-2\lfloor m/4 \rfloor} \in \tilde{K}^-$ acts m-transitively on the set $\{-2\lfloor m/4 \rfloor, \dots, m - 2\lfloor m/4 \rfloor - 1\}$. The assertion follows since m can be chosen arbitrary large. □

5.7 Remark We have $\tilde{K}^+ = K^+$ and $\tilde{K}^- = K^-$ if and only if the group $\mathrm{RCWA}(\mathbb{Z})$ is generated by its tame elements. The question whether this is the case remains open. Compare the corresponding factorization routine in [11]. In case of a positive answer, it is $\mathrm{RCWA}(\mathbb{Z}) = \langle \mathrm{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$:

1. It is $\nu = \varsigma_{0(2)} \cdot \tau \cdot \left(\varsigma_{0(2)}^{\tau_{1(4),2(4)}} \cdot \varsigma_{0(2)}^{\tau_{1(2),0(4)}} \right)^{\tau_{0(2),1(4)}} \in \langle \mathrm{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$.
2. It is $\nu_{0(2)} = \tau\nu$, $\nu_{1(2)} = \nu_{0(2)}^{\tau}$, $\varsigma_{1(2)} = \varsigma_{0(2)}^{\tau}$ and $\varsigma = \varsigma_{0(2)} \cdot \nu_{1(2)} \cdot \varsigma_{1(2)}$. Therefore we know that $\{\nu_{0(2)}, \nu_{1(2)}, \varsigma_{1(2)}, \varsigma\} \subset \langle \mathrm{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$.
3. Let $r(m) \subsetneq \mathbb{Z}$ be a residue class $\neq 1(2)$. We choose a residue class $\tilde{r}(\tilde{m}) \subset \mathbb{Z} \setminus (0(2) \cup r(m))$, and put $\vartheta := \tau_{0(2),\tilde{r}(\tilde{m})} \cdot \tau_{\tilde{r}(\tilde{m}),r(m)} \in \mathrm{CT}(\mathbb{Z})$. Then we have $\{\nu_{r(m)}, \varsigma_{r(m)}\} = \{\nu_{0(2)}^{\vartheta}, \varsigma_{0(2)}^{\vartheta}\} \subset \langle \mathrm{CT}(\mathbb{Z}), \varsigma_{0(2)} \rangle$.

Acknowledgements

I would like to thank Laurent Bartholdi for his hint that the classes of subgroups of $\mathrm{CT}(\mathbb{Z})$ and $\mathrm{RCWA}(\mathbb{Z})$ are closed under taking wreath products with $(\mathbb{Z}, +)$. Likewise I would like to thank Bettina Eick for her continuing encouragement and for her valuable suggestions concerning the layout of this article.

References

1. Reinhold Baer. Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich. *Studia Math.*, 5:15–17, 1934.
2. Gilbert Baumslag. Wreath products and finitely presented groups. *Math. Z.*, 75:22–28, 1961.
3. W. W. Boone. The word problem. *Ann. of Math.*, 70:207–265, 1959.
4. Roger W. Carter. *Simple Groups of Lie Type*. Wiley Classics Library Edition. John Wiley & Sons, 1972.
5. C. G. Chehata. An algebraically simple ordered group. *Proc. London Math. Soc. (3)*, 2:183–197, 1952.
6. Pierre de la Harpe. *Topics in Geometric Group Theory*. Chicago Lectures in Mathematics, 2000.
7. The GAP Group. *GAP – Groups, Algorithms, and Programming; Version 4.4.7*, 2006. (`http://www.gap-system.org`).
8. Graham Higman. *Finitely Presented Infinite Simple Groups*. Notes on Pure Mathematics. Department of Pure Mathematics, Australian National University, Canberra, 1974.
9. Otto H. Kegel and Bertram A. F. Wehrfritz. *Locally Finite Groups*. North-Holland Publishing Company, 1973.

10. Timothy P. Keller. Finite cycles of certain periodically linear permutations. *Missouri J. Math. Sci.*, 11(3):152–157, 1999.
11. Stefan Kohl. *RCWA - Residue Class-Wise Affine Groups*, 2005. GAP package (`http://www.gap-system.org/Packages/rcwa.html`).
12. Stefan Kohl. *Restklassenweise affine Gruppen*. Dissertation, Universität Stuttgart, 2005.
13. Jeffrey C. Lagarias. The 3x+1 problem and its generalizations. *Amer. Math. Monthly*, 92:1–23, 1985.
14. Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Springer-Verlag, 1977. Reprinted in the Springer Classics in Mathematics Series, 2000.
15. K. A. Mihailova. The occurrence problem for direct products of groups. (Russian). *Dokl. Acad. Nauk. SSSR*, 119:1103–1105, 1958.
16. K. A. Mihailova. The occurrence problem for direct products of groups. (Russian). *Mat. Sb.*, 70(112):241–251, 1966.
17. P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. (Russian). *Trudy Math. Inst. Steklov*, 44:143, 1955.
18. Alexander Yu. Ol'shanskii. Infinite groups with cyclic subgroups. (Russian). *Dokl. Akad. Nauk. SSSR*, 245(4):785–787, 1979.
19. Melanie Stein. Groups of piecewise linear homoeomorphisms. *Trans. Amer. Math. Soc.*, 332(2):477–514, 1992.
20. Günther J. Wirsching. The dynamical system on the natural numbers generated by the 3n+1 function. Habilitationsschrift, Katholische Universität Eichstätt, 1996.