Journal of Number Theory 173 (2017) 254–271

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Multiplicative atom decomposition of sets of exceptional units in residue class rings

J.W. Sander

Institut für Mathematik und Angewandte Informatik, Universität Hildesheim, D-31141 Hildesheim, Germany

A R T I C L E   I N F O

Article history:
Received 15 July 2016
Received in revised form 1 September 2016
Accepted 9 September 2016
Available online 15 November 2016
Communicated by D. Goss

MSC:
primary 11A07, 11T30, 16U60
secondary 03G05, 06E20, 20K01

Keywords:
Residue class ring
Unit
Exceptional unit
Atom
Multiplicative

A B S T R A C T

Given the multiplicative group $\mathbb{Z}_n^*$ of units in the ring $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, let $\mathbb{Z}_n^{**}$ denote the set of *exceptional units* in $\mathbb{Z}_n$, i.e. units $u \in \mathbb{Z}_n^*$ satisfying $1-u \in \mathbb{Z}_n^*$. A subset of a finite group G containing all generators of any (cyclic) subgroup of G is called an *atom* of G. Let $\mathscr{A}_n^*$ denote the set of all atoms of $\mathbb{Z}_n^*$. By means of $\mathscr{A}_n^{**} := \{A \in \mathscr{A}_n^* : A \subset \mathbb{Z}_n^{**}\}$, the set $\mathbb{Z}_n^{**}$ trivially decomposes into atoms, i.e. $\mathbb{Z}_n^{**} = \bigcup_{A \in \mathscr{A}_n^{**}}$ as a disjoint union. An explicit construction of that atom decomposition is easily obtained if n is a prime power.

We characterise so-called *tame* integers, i.e. odd $n > 1$ with prime factorisation $n = \prod p_i^{k_i}$, say, for which the atom decomposition of $\mathbb{Z}_n^{**}$ is obtained by multiplicative composition of the atom decompositions of the $\mathbb{Z}_{p_i^{k_i}}^{**}$. Moreover, it is shown that the set of tame integers has density zero.

1. Introduction and terminology

Let R be a commutative ring with $1 \in R$, and let R^* denote the multiplicative group of units in R. A unit $u \in R^*$ is called *exceptional* if $1 - u \in R^*$, i.e. if $u - 1 \in R^*$ or, in

E-mail address: sander@imai.uni-hildesheim.de.

http://dx.doi.org/10.1016/j.jnt.2016.09.027

other words, if there is a $u' \in R^*$ such that $u + u' = 1$. In [13] the author proposed the coinage *exunit* for the term *exceptional unit*, and we shall seize that suggestion.

Exunits were introduced in 1969 by Nagell [10], who studied them to solve certain cubic Diophantine equations. Since then they have proved to be very beneficial when dealing with Diophantine equations of various types. In 1977 Lenstra [9] introduced a method for detecting Euclidean number fields with the aid of exunits, and by further development of this method, quite a few formerly unknown Euclidean number fields were found by different authors. Furthermore, exunits were related to Lehmer's conjecture about Mahler's measure and to cyclic resultants. A more detailed account of exunits including references can be found in [13].

Given a finite abelian group G, let $\langle a\rangle$ denote the cyclic subgroup generated by $a \in G$. Then the *atom* of a is the set

$$\operatorname{atom}(a) = \operatorname{atom}_G(a) := \{b \in \langle a\rangle :\ \langle b\rangle = \langle a\rangle\} \subseteq G$$

of all generators of $\langle a\rangle$. Identifying the group operation in G with multiplication, basic results on cyclic groups imply for any $a \in G$ of order $\operatorname{ord}_G(a) = d$, say, that

$$\operatorname{atom}(a) = \{a^j :\ 1 \le j \le d,\ (j, d) = 1\}$$

(cf. Lemma 3.1), where (m, n) denotes the greatest common divisor of two integers m and n. Consequently $\#\operatorname{atom}(a) = \varphi(d)$ for Euler's totient function φ. Moreover, all elements in $\operatorname{atom}(a)$ have the same order d. It is also evident that different atoms are disjoint. We denote by

$$\mathscr{A}(G) := \{\operatorname{atom}_G(a) :\ a \in G\}$$

the set of all atoms in G. A set $S \subseteq G$ is called G-*atomisable* or simply *atomisable* if there exist $A_1, \dots, A_r \in \mathscr{A}(G)$ such that $S = \bigcup_{i=1}^r A_i$. Clearly, the set $\{A_1, \dots, A_r\}$ atomising S is unique, and we name it the *atom decomposition* of S. Any set $S' \subseteq S$ of r representatives $a_i \in A_i$, $1 \le i \le r$, is called a G-*atomiser* or *atomiser* of S and yields the atom decomposition $\{\operatorname{atom}(a) :\ a \in S'\}$ of S. The group G itself is trivially atomisable with $G = \bigcup_{A \in \mathscr{A}(G)} A$.

The term "atom" originates from the theory of Boolean algebras where it denotes the second minimal elements of a lattice. In our case it refers to the Boolean algebra generated by the subgroups of G. It is not difficult to see that every element of this Boolean algebra is a disjoint union of atoms.

In this paper we consider exunits in the ring $R = \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ of residue classes mod n for integers $n > 1$ and the multiplicative group $G = \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n :\ (a, n) = 1\}$ of units with $\#\mathbb{Z}_n^* = \varphi(n)$. Let us denote the set of exunits in $\mathbb{Z}_n$ by

$$\mathbb{Z}_n^{**} := \{a \in \mathbb{Z}_n^* :\ a - 1 \in \mathbb{Z}_n^*\} = \{a \in \mathbb{Z}_n :\ (a, n) = (a - 1, n) = 1\}.$$