Journal of Number Theory 159 (2016) 1–6

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Sums of exceptional units in residue class rings

J.W. Sander

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

ARTICLE INFO

Article history:
Received 1 April 2015
Received in revised form 10 July 2015
Accepted 10 July 2015
Available online 2 September 2015
Communicated by David Goss

MSC:
11D45
11D57

Keywords:
Residue class rings
Sums of units
Exceptional units

ABSTRACT

Given a commutative ring R with $1 \in R$ and the multiplicative group R^* of units, an element $u \in R^*$ is called an *exceptional unit* if $1 - u \in R^*$, i.e., if there is a $u' \in R^*$ such that $u + u' = 1$. We study the case $R = \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ of residue classes $\bmod n$ and determine the number of representations of an arbitrary element $c \in \mathbb{Z}_n$ as the sum of two exceptional units. As a consequence, we obtain the sumset $\mathbb{Z}_n^{**} + \mathbb{Z}_n^{**}$ for all positive integers n, with $\mathbb{Z}_n^{**}$ denoting the set of exceptional units of $\mathbb{Z}_n$.

1. Introduction

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 other words, if there is a $u' \in R^*$ such that $u + u' = 1$. For the sake of brevity (and pointedness), we shall use the coinage *exunit* for the term *exceptional unit*.

Exunits were introduced in 1969 by Nagell [6], who studied them to solve certain cubic Diophantine equations. Since then, they proved to be very beneficial when dealing

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

http://dx.doi.org/10.1016/j.jnt.2015.07.018

with Diophantine equations of various types, e.g., for Thue equations [16] and Thue–Mahler equations [17] as demonstrated by Tzanakis and deWeger, discriminant form equations by Smart [13] and lots of others (for more references see [8]). The key idea is the fact that the solution of many Diophantine equations can be reduced to the solution of a finite number of *unit equations* of type $ax + by = 1$, where x and y are restricted to units in the ring of integers of some number field. In the case $a = b = 1$, this means to search for exunits (cf. [7] for a survey). Fortunately, there exists an algorithm [12] to determine all the exunits within a given number field.

In 1977, Lenstra [4] introduced a method for detecting Euclidean number fields with the aid of exunits. By further development of this method, quite a few formerly unknown Euclidean number fields could be found by Leutbecher and Niklasch [5] and Houriet [3]. Exunits were also studied for their own sake, e.g., the calculation of the number of exunits in a number field of given degree and unit rank [7]. Furthermore, exunits were related to Lehmer's conjecture about Mahler's measure by Silverman [10,11] and to cyclic resultants by Stewart [14,15].

In this paper, we consider exunits in the ring $R = \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ of residue classes mod n for positive integers n. Then $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ with

$$\#\mathbb{Z}_n^* = \varphi(n) = n \prod_{p|n,\ p\in\mathbb{P}} \left(1 - \frac{1}{p}\right)$$

for Euler's totient function φ, where $\mathbb{P}$ is the set of primes. We denote by

$$\begin{aligned}\mathbb{Z}_n^{**} &:= \{a \in \mathbb{Z}_n^* : a - 1 \in \mathbb{Z}_n^*\} \\ &= \{a \in \mathbb{Z}_n : \gcd(a, n) = \gcd(a - 1, n) = 1\}\end{aligned}$$

the set of exunits in $\mathbb{Z}_n$. Observe that $\mathbb{Z}_n^{**}$ cannot be a subgroup of the multiplicative group $\mathbb{Z}_n^*$, since $1 \notin \mathbb{Z}_n^{**}$. In 2010, it was shown by Harrington and Jones [2, Theorem 3] that

$$\#\mathbb{Z}_n^{**} = \varphi^*(n) := n \prod_{p|n,\ p\in\mathbb{P}} \left(1 - \frac{2}{p}\right), \tag{1}$$

which also follows immediately from results of Deaconescu [1] or the author [9]. In particular, (1) implies the obvious fact that $\mathbb{Z}_n^{**} = \emptyset$ if and only if n is even. Observe that φ^* is multiplicative, and we apparently have $\varphi^*(n) = \varphi(n) \prod_{p|n}(1 - \frac{1}{p-1})$.

It is an easy consequence of the Chinese remainder theorem that the sumset $\mathbb{Z}_n^* + \mathbb{Z}_n^*$ satisfies

$$\mathbb{Z}_n^* + \mathbb{Z}_n^* := \{u + v : u, v \in \mathbb{Z}_n^*\} = \begin{cases} \mathbb{Z}_n & \text{if } n \text{ is odd}, \\ 2\mathbb{Z}_n & \text{if } n \text{ is even}, \end{cases} \tag{2}$$