Journal of Number Theory 137 (2014) 179–185

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Menon's identity in residually finite Dedekind domains

C. Miguel

Instituto de Telecomunicações, Beira Interior University, Department of Mathematics, Covilhã, Portugal

A R T I C L E I N F O

Article history:
Received 26 November 2013
Accepted 29 November 2013
Available online 4 January 2014
Communicated by David Goss

MSC:
11A25
20D99

Keywords:
Burnside's lemma
Dedekind domain
Group action
Residually finite ring

A B S T R A C T

In this note we give an extension of the well-known Menon's identity to residually finite Dedekind domains.

1. Introduction

The starting point for this paper is an unusual relation between the divisor function and the Euler totient function, which states that for every $n \in \mathbb{N} = \{1, 2, \ldots\}$

$$\sum_{a \in U(\mathbb{Z}_n)} gcd(a-1, n) = \varphi(n)\tau(n), \tag{1}$$

where $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \colon\ gcd(n, a) = 1\}$, φ is the Euler totient function and $\tau(n)$ is the number of positive divisors of n. This interesting arithmetical identity, known as

E-mail address: celino@ubi.pt.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.11.003

Menon's identity, is due to P.K. Menon [12]. This identity has been generalized by many authors (see e.g. [5–7,16–18]). However, all these generalizations are in the setting of the traditional domain of the rational integers. As is well-known there are other number systems that are in many ways analogous to the rational integers. For instance, the ring $\mathbb{F}[X]$ of all polynomials in one variable with coefficients in a field $\mathbb{F}$, the p-adic integers, the ring $\mathcal{O}_K$ of integers in a number field K or more generally a Dedekind domain. The question naturally arises as to whether we can establish similar assertions in a more general framework.

The aim of this paper is to extend Menon's identity to a special case of Dedekind domains, namely, residually finite Dedekind domains. That is, Dedekind domains $\mathfrak{D}$ such that for each non-zero ideal $\mathfrak{n}$ of $\mathfrak{D}$, the residue class ring $\mathfrak{D}/\mathfrak{n}$ is finite. The positive rational integer $N(\mathfrak{n})$ defined by

$$N(\mathfrak{n}) = |\mathfrak{D}/\mathfrak{n}|$$

is called the norm of the ideal $\mathfrak{n}$.

Residually finite rings (also called rings of finite norm property) have historically commanded strong interest (see e.g. [8,11]). The reason for this historical interest comes from algebraic number theory. Indeed, the ring $\mathcal{O}_K$ of integers in a number field (or more generally, in a global field) is a residually finite Dedekind domain.

As is well-known factorization into irreducible elements frequently fails for Dedekind domains. But using ideals in place of elements we can save unique factorization. Unique factorization of ideals in a Dedekind domain permits calculations that are analogous to some familiar manipulations involving ordinary integers (for details, see [13, Chapter 1]). Moreover, we can define a generalized Euler totient function type for a non-zero ideal of a Dedekind domain. Let $\mathfrak{n}$ be a non-zero ideal in a Dedekind domain $\mathfrak{D}$, then the generalized Euler totient function, which is denoted by $\varphi_{\mathfrak{D}}(\mathfrak{n})$, is defined to be the order of the multiplicative group of units in the factor ring $\mathfrak{D}/\mathfrak{n}$, with the convention that $\varphi_{\mathfrak{D}}(\mathfrak{D}) = 1$. That is,

$$\varphi_{\mathfrak{D}}(\mathfrak{n}) = \begin{cases} 1 & \text{if } \mathfrak{n} = \mathfrak{D}, \\ |U(\mathfrak{D}/\mathfrak{n})| & \text{otherwise.} \end{cases}$$

Notice that, since we only consider residually finite Dedekind domains, it follows that $\varphi_{\mathfrak{D}}$ is a finite valued function. This function shares the same basic properties as the usual Euler's totient function. For example

$$\varphi_{\mathfrak{D}}(\mathfrak{n}) = N(\mathfrak{n}) \prod_{\mathfrak{p} \mid \mathfrak{n}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$