

**Résumé.** Dans cet article, nous étudions des racines primitives.

**Abstract.** In this article, we study primitive roots.

**Keywords.** Your keywords come here.

**Mathematics Subject Classification (2010).** Your MSC numbers come here.

## 1. Introduction

In this paper, we prove that, for any prime  $p \in \mathbb{N}$ , the group of units in the quotient ring  $\mathbb{Z}/(p)$  is cyclic. This is important in many aspects of number theory.

## 2. Primitive roots

We start with a definition.

**Definition 2.1.** *Let  $n \in \mathbb{N}$  be any non-zero number. We say that a number  $a \in \mathbb{Z}$  is a primitive root modulo  $n$  when  $a + (n) \in \mathbb{Z}/(n)$  is a generator for the group of units in the quotient ring  $\mathbb{Z}/(n)$ .*

Our aim now is to show that, for any prime  $p \in \mathbb{N}$ , there exists a primitive root modulo  $p$ . We use a lemma, in which  $\varphi$  denotes the *Euler phi function*.

**Lemma 2.2.** *Let  $G$  be a finite commutative group (written multiplicatively). Then  $G$  is cyclic if and only if, for each divisor  $d$  of  $|G|$ ,*

$$|\{g \in G \mid g \text{ is of order } d\}| \leq \varphi(d).$$

*Proof.* Write  $m = |G|$  and, whenever  $d$  divides  $m$ ,  $G_d \subseteq G$  for the set of elements of order  $d$ . By Lagrange's Theorem these form a partition of  $G$ :

$$G = \bigcup_{d|m} G_d.$$

Counting on both sides shows that  $m = \sum_{d|m} |G_d|$ . If  $|G_d| \leq \varphi(d)$  for each divisor  $d$  of  $m$ , then

$$m = \sum_{d|m} |G_d| \leq \sum_{d|m} \varphi(d) = m$$

by a well-known property of  $\varphi$ . Hence necessarily  $|G_d| = \varphi(d)$  for each divisor  $d$  of  $m$ , thus in particular  $|G_m| = \varphi(m) \neq 0$ , saying precisely that  $G$  is cyclic.

The converse is left to the reader. □

Without proof we mention the following.

**Proposition 2.3.** *If  $G$  is a finite commutative group, and for every divisor  $d$  of  $|G|$  we have that*

$$|\{g \in G \mid g^d = 1\}| \leq d,$$

*then  $G$  is cyclic.*

We can now state our main result.

**Theorem 2.4.** *For every prime  $p \in \mathbb{N}$ , the group  $(\mathbb{Z}/(p))^\times$  is cyclic.*

*Proof.* The number of roots of the polynomial  $X^d - 1$ , viewed as polynomial with coefficients in the field  $\mathbb{Z}/(p)$ , is less than or equal to  $d$ . The previous proposition applies to the group of units of this field. □

**Example 2.5.** It is easy to verify that 2 is a primitive root modulo 11.

**Remark 2.6.** For more information on the lay-out of this article for the *Cahiers*, the official *Guide to Authors* can be found at the following address:

<http://ehres.pagesperso-orange.fr/Cahiers/Ctgdc.htm>.

## References

- [1] [C. F. Gauss, 1801] *Disquisitiones Arithmeticae*.

Carl Friedrich Gauss  
Mathematisches Institut  
University of Göttingen  
Bunsenstrasse 3-5  
37073 Göttingen (Germany)  
my.email@server.univ.xy