

CYCLES, EULERIAN DIGRAPHS AND THE SCHÖNEMANN–GAUSS THEOREM

HEINRICH STEINLEIN

To the memory of Andrzej Granas with gratitude

ABSTRACT. In 19th century, Fermat’s little theorem “ $a^p \equiv a \pmod{p}$ ” for $a \in \mathbb{Z}$, p prime” was generalized in two directions: Schönemann proved a corresponding congruence for the coefficients of monic polynomials, whereas Gauss found a congruence result with p replaced by any $n \in \mathbb{N}$. Here, we shall give an elementary proof of the common generalization of these two results.

1. Introduction

Schönemann [4] proved the following generalization of Fermat’s little theorem:

THEOREM 1.1. *Let q be a prime number and*

$$P_d(x) := x^r + a_{r-1}^{(d)}x^{r-1} + \dots + a_0^{(d)}, \quad d = 1 \text{ or } d = q$$

with integer coefficients such that the zeros of P_q are the q -th powers of the zeros of P_1 . Then $a_j^{(q)} \equiv a_j^{(1)} \pmod{q}$ for $j = 0, \dots, r-1$.

In fact, with the choice $P_1(x) := x - a$, Theorem 1.1 reduces just to Fermat’s little theorem. On the other hand, there are several generalizations of Fermat’s little theorem in the number theoretical context, the most general one being as follows:

2020 *Mathematics Subject Classification.* 11C08, 05C45, 11C20.

Key words and phrases. Schönemann–Gauss congruences; characteristic polynomial; Eulerian digraph.