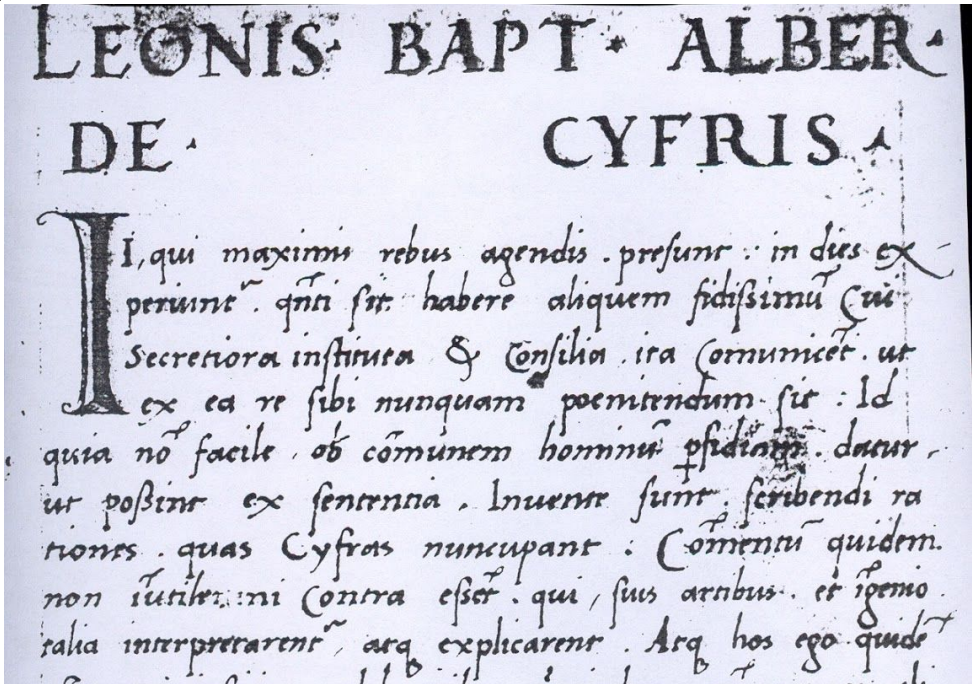
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Communicet . ut
ex ea re sibi nunquam poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutibrum Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Thursday 7th March 2019 – at 10:00 a.m.
Seminar Room -1, Department of Mathematics

Michele Elia

Politecnico di Torino

On a Problem of Perron

Abstract: Oskar Perron gave some additive properties of the fibers of the quadratic character on a prime field GF(p). Specifically, he showed that if A and B are the subsets of quadratic residues and non-residues in GF(p)*, respectively, then, letting

d=(p-1)/4 if p =1 modulo 4, and d=(p+1)/4 if p = 3 modulo 4

1. Every element of A [respectively B] can be written as a sum of two elements of A [respectively B] in exactly d-1 ways.
2. Every element of A [respectively B] can be written as a sum of two elements of B [respectively A] in exactly d ways.

It is shown that, with a suitable adaptation, these properties hold for the subsets of squares and non-squares in any finite field $GF(p^m)$ with odd p.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it