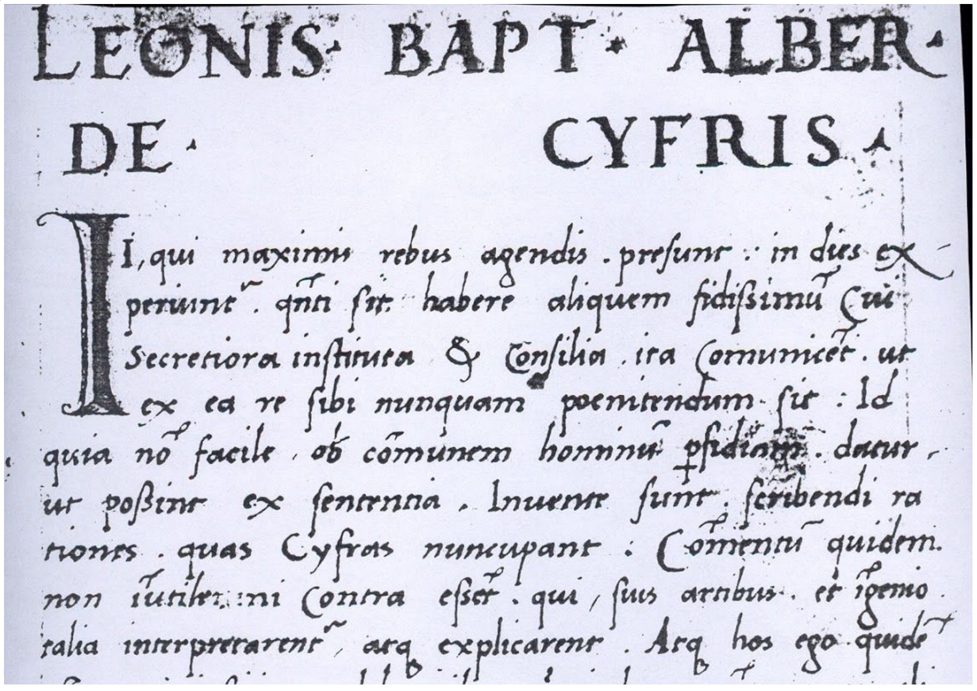
LEONIS BAPT ALBER
DE CYFRIS

Ii, qui maximis rebus agendis presunt: in dies ex
periunt̄. quāti sit habere aliquem fidissimū cui
Secretiora instituta & Consilia ita comunicet. ut
ex ea re sibi nunquam poenitendum sit: Id
quia nō facile ob cōmunem hominū pfidiam. datur
ut possint ex sententia. Inuente sunt scribendi ra
tiones. quas Cyfras nuncupant: Comentū quidem
non inutilem: ni contra esset. qui suis artibus et ingenio
talia interpretarent̄, atq explicarent. Atq hos ego quidē

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

DE CIFRIS

FBK ICT
CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY
FONDAZIONE BRUNO KESSLER

Wednesday 30th October 2019 – at 10:00 a.m.
Department of Mathematics
Seminar Room -1, Department of Mathematics

MICHELE ELIA

Politecnico di Torino

Continued Fractions and Factoring

Abstract: Legendre found that the continued fraction expansion of √ N having odd period leads directly to an explicit representation of N as the sum of two squares. Similarly, it is shown here that the continued fraction expansion of √ N having even period directly produces a factor of a composite N. Shanks' infrastructural method is then revisited, and some consequences of its application to factorization by means of the continued fraction expansion of √ N are derived.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it