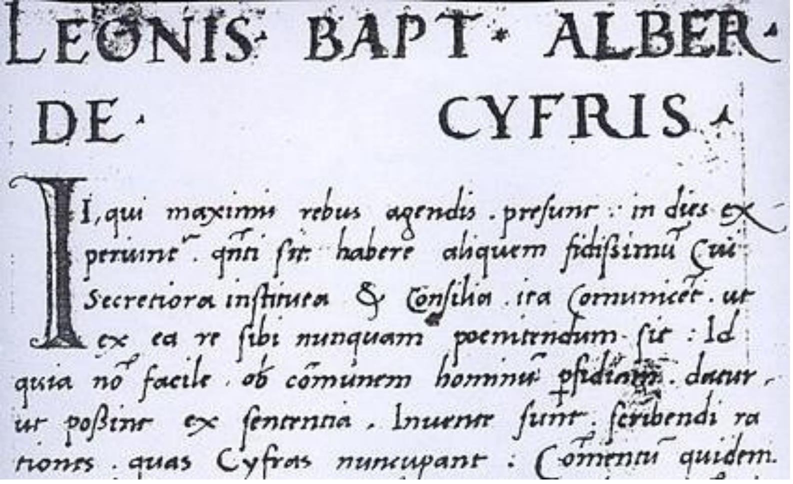

LEONIS BAPT· ALBER·
DE· CYFRIS·

Ii, qui maximis rebus agendis . presunt : in dies experiunt . quanti sit habere aliquem fidissimu cui Secretiora instituta & Consilia . ita comunicet . ut ex ea re sibi nunquam poenitendum sit : Id quia no facile . ob comunem hominu pfidiam . datur, ut possint ex sententia . Inventi sunt . scribendi rationes . quas Cyfras nuncupant : Comentu quidem.

De Cifris Augustae Taurinorum

Friday, 6 December 2019 – at 15.00
Sala Orsi, Università di Torino
Dipartimento di Matematica, Via Carlo Alberto 10

Michele Elia
Politecnico di Torino

Continued fractions and factoring

Abstract: Legendre found that the continued fraction expansion of $\sqrt{N}$ 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 $\sqrt{N}$ 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 $\sqrt{N}$ are derived.

For Information: danilo.bazzanella@polito.it, fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it, nadir.murru@polito.it, lea.terracini@unito.it.

CONTATTI
Associazione De Componendis Cifris
direttore@decifris.it, segreteria@decifris.it