Periodic Continued Fractions in Elementary Number Theory

Michele Elia (Politecnico di Torino)

ABSTRACT: Legendre discovered an elegant property of periodic continued fractions, leading explicitly to the representation of integers that are primes, or possibly a product of primes, congruent 1 modulo 4, as the sum of two squares; he exploited these representations for factoring.

Working within this framework, Shanks conceived the infrastructure method, whereby a baby-giant-step strategy is used to compute class numbers and class groups of any quadratic number field with reduced complexity, thus leading to faster factorization algorithms. In a similar vein, but concerning integers that are the product of primes congruent 3 modulo 4, a property of continued fractions is presented that finds direct application to the factorization of integers. Again in this case, Shanks baby-giant-step strategy can profitably be applied.