(d, B) - exceptional numbers with applications to cryptology

Jacek Pomykała

Warsaw University, Poland
pomykala@mimuw.edu.pl

Session: 1. Analytic Number Theory

In the lecture we define (d, ζ^i, B)-exceptional primes p. We prove the upper bound for the corresponding primes when $i = 0$. The possible extensions will be announced. As an application the lower bound for the number of large prime q-orders $(q|d)$ of elements generated by small intervals $[1, B] \mod p$ is established. In this connection the computational efficiency of cryptographic systems designs will be underlined.