Hurd, Joe

Verification of the Miller-Rabin probabilistic primality test. (English) Zbl 1048.68051

Summary: Using the HOL theorem prover, we apply our formalization of probability theory to specify and verify the Miller-Rabin probabilistic primality test. The version of the test commonly found in algorithm textbooks implicitly accepts probabilistic termination, but our own verified implementation satisfies the stronger property of guaranteed termination. Completing the proof of correctness requires a significant body of group theory and computational number theory to be formalized in the theorem prover. Once verified, the primality test can either be executed in the logic (using rewriting) and used to prove the compositeness of numbers, or manually extracted to standard ML and used to find highly probable primes.

MSC:
68Q65 Abstract data types; algebraic specification
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Keywords:
Formal verification; Random algorithms; Primality test

Software:
NQTHM; HOL; PVS

Full Text: DOI

References:
[16] Rabin, M.O., Probabilistic algorithms, (), 21-39

[19] L. Théry, A quick overview of HOL and PVS, August 1999, Lecture Notes from the Types Summer School ’99: Theory and Practice of Formal Proofs, held in Giens, France


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.