Algorithmic Number Theory - List 3

Task 1 (30 pts)
Implement the *Shanks-Tonelli Algorithm* (see Sect.6 from `https://www.maa.org/sites/default/files/pdf/upload_library/22/Polya/07468342.di020786.02p0470a.pdf`).

Prove that your implementation is correct by implementing tests for a few primes p of length at least 128-bit.