Summer School - Number Theory for Cryptography

F. Morain

Tutorial, 2013/06/25

1. Implement the AMR test.

2. Find a (probable) family of composite integers N satisfying $F(N) = \varphi(N)/4$.

3. Prove Pocklington's theorem.

4. a) Implement the $N-1$ and find proven primes of the form $2 \cdot k! + 1$.
b) Same question with the $N+1$ test and the family $2 \cdot k! - 1$.

4. We consider the equation $k\varphi(N) \mid N-1$ for integers k and N.
a) solve the equation when $k = 1$.

From now on, fix some $k > 1$.
b) Give elementary properties of N's satisfying the equation.
c) Find non-trivial bounds on the number of prime divisors t of a solution N to the equation.

5. a) Implement the AKS algorithm and prove that 89 is prime.
b) Implement Berrizbeitia's variant and find some proven primes.