Primality Criterion for Safe Primes

Predrag Terzić
Podgorica, Montenegro
e-mail: pedja.terzic@hotmail.com

February 12, 2017

Abstract: Polynomial time primality test for safe primes is introduced.
Keywords: Primality test, Polynomial time, Prime numbers.
AMS Classification: 11A51.

1 Introduction

In 1750 Euler stated following theorem

Theorem 1.1. Let \( p \equiv 3 \pmod{4} \) be prime, then \( 2p + 1 \) is prime iff \( 2p + 1 \mid 2^p - 1 \).

In 1775 Lagrange gave a proof of the theorem. In this note we provide a proof to the theorem that is similar to the Euler-Lagrange theorem.

2 The Main Result

Theorem 2.1. Let \( p \equiv 5 \pmod{6} \) be prime, then \( 2p + 1 \) is prime iff \( 2p + 1 \mid 3^p - 1 \).

Proof. Suppose \( q = 2p + 1 \) is prime. \( q \equiv 11 \pmod{12} \) so 3 is quadratic residue module \( q \) and it follows that there is an integer \( n \) such that \( n^2 \equiv 3 \pmod{q} \). This shows \( 3^p = 3^{(q-1)/2} \equiv n^{q-1} \equiv 1 \pmod{q} \) showing \( 2p + 1 \) divides \( 3^p - 1 \).

Conversely, let \( 2p + 1 \) be factor of \( 3^p - 1 \). Suppose that \( 2p + 1 \) is composite and let \( q \) be its least prime factor. Then \( 3^p \equiv 1 \pmod{q} \) and so we have \( p = k \cdot \text{ord}_q(3) \) for some integer \( k \). Since \( p \) is prime there are two possibilities \( \text{ord}_q(3) = 1 \) or \( \text{ord}_q(3) = p \). The first possibility cannot be true because \( q \) is an odd prime number so \( \text{ord}_q(3) = p \). On the other hand \( \text{ord}_q(3) \mid q - 1 \), hence \( p \) divides \( q - 1 \). This shows \( q > p \) and it follows \( 2p + 1 > q^2 > p^2 \) which is contradiction since \( p > 3 \), hence \( 2p + 1 \) is prime.

Q.E.D.