Primality Tests for Specific Classes of Proth Numbers

Predrag Terzić

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

September 22 , 2014

Abstract: Polynomial time primality tests for specific classes of Proth numbers are introduced .
Keywords: Primality test , Polynomial time , Prime numbers .
AMS Classification: 11A51 .

1 Introduction

Theorem 1.1. *(Proth's theorem)*
If p is a Proth number , of the form $k \cdot 2^n + 1$ with k odd and $k < 2^n$, then if for some integer a ,

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

then p is prime .

See [1] .
In this note I present for which classes of Proth numbers we can choose value of $a = 3, 5, 7, 11$

2 The Main Result

Theorem 2.1. *Let $N = k \cdot 2^n + 1$ with $n > 1$, $k < 2^n$ and $3 \nmid k$, thus*

$$N \text{ is prime iff } 3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$$

Proof :
Necessity : *If N is prime then $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$*

Let N be a prime , then according to Euler criterion :

$$3^{\frac{N-1}{2}} \equiv \left(\frac{3}{N}\right) \pmod{N}$$

If N is prime then $N \equiv 2 \pmod{3}$ and therefore : $\left(\frac{N}{3}\right) = -1$.
Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{3}{N}\right) = -1$.
Hence , $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then N is prime*

If $3^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then according to Proth's theorem N is prime .

Theorem 2.2. *Let* $N = k \cdot 2^n + 1$ *with* $n > 1$, $k < 2^n$, $3 \mid k$, *and*

$$\begin{cases} k \equiv 3 \pmod{30}, & \textit{with } n \equiv 1,2 \pmod{4} \\ k \equiv 9 \pmod{30}, & \textit{with } n \equiv 2,3 \pmod{4} \\ k \equiv 21 \pmod{30}, & \textit{with } n \equiv 0,1 \pmod{4} \\ k \equiv 27 \pmod{30}, & \textit{with } n \equiv 0,3 \pmod{4} \end{cases}$$

, thus

N *is prime iff* $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Proof :

Necessity : *If* N *is prime then* $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Let N be a prime , then according to Euler criterion :

$$5^{\frac{N-1}{2}} \equiv \left(\frac{5}{N}\right) \pmod{N}$$

If N is a prime then $N \equiv 2,3 \pmod{5}$ and therefore : $\left(\frac{N}{5}\right) = -1$.

Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{5}{N}\right) = -1$.

Hence , $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If* $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ *then* N *is prime*

If $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then according to Proth's theorem N is prime .

Theorem 2.3. *Let* $N = k \cdot 2^n + 1$ *with* $n > 1$, $k < 2^n$, $3 \mid k$, *and*

$$\begin{cases} k \equiv 3 \pmod{42}, & \textit{with } n \equiv 2 \pmod{3} \\ k \equiv 9 \pmod{42}, & \textit{with } n \equiv 0,1 \pmod{3} \\ k \equiv 15 \pmod{42}, & \textit{with } n \equiv 1,2 \pmod{3} \\ k \equiv 27 \pmod{42}, & \textit{with } n \equiv 1 \pmod{3} \\ k \equiv 33 \pmod{42}, & \textit{with } n \equiv 0 \pmod{3} \\ k \equiv 39 \pmod{42}, & \textit{with } n \equiv 0,2 \pmod{3} \end{cases}$$

, thus

N *is prime iff* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Proof :

Necessity : *If* N *is prime then* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Let N be a prime , then according to Euler criterion :

$$7^{\frac{N-1}{2}} \equiv \left(\frac{7}{N}\right) \pmod{N}$$

If N is prime then $N \equiv 3,5,6 \pmod{7}$ and therefore : $\left(\frac{N}{7}\right) = -1$.

Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{7}{N}\right) = -1$.

Hence , $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ *then* N *is prime*

If $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then according to Proth's theorem N is prime .

Theorem 2.4. *Let $N = k \cdot 2^n + 1$ with $n > 1$, $k < 2^n$, $3 \mid k$, and*

$$\begin{cases} k \equiv 3 \pmod{66}, & \textit{with } n \equiv 1,2,6,8,9 \pmod{10} \\ k \equiv 9 \pmod{66}, & \textit{with } n \equiv 0,1,3,4,8 \pmod{10} \\ k \equiv 15 \pmod{66}, & \textit{with } n \equiv 2,4,5,7,8 \pmod{10} \\ k \equiv 21 \pmod{66}, & \textit{with } n \equiv 1,2,4,5,9 \pmod{10} \\ k \equiv 27 \pmod{66}, & \textit{with } n \equiv 0,2,3,5,6 \pmod{10} \\ k \equiv 39 \pmod{66}, & \textit{with } n \equiv 0,1,5,7,8 \pmod{10} \\ k \equiv 45 \pmod{66}, & \textit{with } n \equiv 0,4,6,7,9 \pmod{10} \\ k \equiv 51 \pmod{66}, & \textit{with } n \equiv 0,2,3,7,9 \pmod{10} \\ k \equiv 57 \pmod{66}, & \textit{with } n \equiv 3,5,6,8,9 \pmod{10} \\ k \equiv 63 \pmod{66}, & \textit{with } n \equiv 1,3,4,6,7 \pmod{10} \end{cases}$$

, thus

N is prime iff $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Proof :

Necessity : *If N is prime then $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$*

Let N be a prime , then according to Euler criterion :

$$11^{\frac{N-1}{2}} \equiv \left(\frac{11}{N}\right) \pmod{N}$$

If N is prime then $N \equiv 2,6,7,8,10 \pmod{11}$ and therefore : $\left(\frac{N}{11}\right) = -1$.

Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{11}{N}\right) = -1$.

Hence , $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then N is prime*

If $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then according to Proth's theorem N is prime .

References

[1] "Proth's theorem" Wikipedia, The Free Encyclopedia. Wikimedia Foundation, Inc.