Primality criterion for $N = 4 \cdot 3^n - 1$

Predrag Terzić

Bulevar Pera Ćetkovića 139 , Podgorica , Montenegro
e-mail: predrag.terzic@protonmail.com

Abstract: Polynomial time primality test for numbers of the form $4 \cdot 3^n - 1$ is introduced .
Keywords: Primality test , Polynomial time , Prime numbers .
AMS Classification: 11A51 .

Theorem 0.1. *Let $N = 4 \cdot 3^n - 1$ where $n \geq 0$. Let $S_i = S_{i-1}^3 - 3S_{i-1}$ with $S_0 = 6$. Then N is prime iff $S_n \equiv 0 \pmod{N}$.*

Proof. The sequence $\langle S_i \rangle$ is a reccurence relation with a closed-form solution. Let $\omega = 3+\sqrt{8}$ and $\bar{\omega} = 3 - \sqrt{8}$. It then follows by induction that $S_i = \omega^{3^i} + \bar{\omega}^{3^i}$ for all i :

$S_0 = \omega^{3^0} + \bar{\omega}^{3^0} = (3 + \sqrt{8}) + (3 - \sqrt{8}) = 6$

$S_n = S_{n-1}^3 - 3S_{n-1} =$

$= \left(\omega^{3^{n-1}} + \bar{\omega}^{3^{n-1}}\right)^3 - 3\left(\omega^{3^{n-1}} + \bar{\omega}^{3^{n-1}}\right) =$

$= \omega^{3^n} + 3\omega^{2 \cdot 3^{n-1}}\bar{\omega}^{3^{n-1}} + 3\omega^{3^{n-1}}\bar{\omega}^{2 \cdot 3^{n-1}} + \bar{\omega}^{3^n} - 3\omega^{3^{n-1}} - 3\bar{\omega}^{3^{n-1}} =$

$= \omega^{3^n} + 3\omega^{3^{n-1}}(\omega\bar{\omega})^{3^{n-1}} + 3\bar{\omega}^{3^{n-1}}(\omega\bar{\omega})^{3^{n-1}} + \bar{\omega}^{3^n} - 3\omega^{3^{n-1}} - 3\bar{\omega}^{3^{n-1}} =$

$= \omega^{3^n} + \bar{\omega}^{3^n}$

The last step uses $\omega\bar{\omega} = (3 + \sqrt{8})(3 - \sqrt{8}) = 1$.

Necessity

If N is prime then S_n is divisible by $4 \cdot 3^n - 1$.

For $n = 0$ we have $N = 3$ and $S_0 = 6$, so $N \mid S_0$, otherwise since $4 \cdot 3^n - 1 \equiv 11 \pmod{12}$ for odd $n \geq 1$ it follows from properties of the Legendre symbol that $\left(\frac{3}{N}\right) = 1$. This means that 3 is a quadratic residue modulo N. By Euler's criterion, this is equivalent to $3^{\frac{N-1}{2}} \equiv 1 \pmod{N}$. Since $4 \cdot 3^n - 1 \equiv 3 \pmod{8}$ for odd $n \geq 1$ it follows from properties of the Legendre symbol that $\left(\frac{2}{N}\right) = -1$. This means that 2 is a quadratic nonresidue modulo N. By Euler's criterion, this is equivalent to $2^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Combining these two equivalence relations yields

$72^{\frac{N-1}{2}} = \left(2^{\frac{N-1}{2}}\right)^3 \left(3^{\frac{N-1}{2}}\right)^2 \equiv (-1)^3(1)^2 \equiv -1 \pmod{N}$

Let $\sigma = 3\sqrt{8}$ and define X as the ring $X = \{a + b\sqrt{8} \mid a, b \in \mathbb{Z}_N\}$. Then in the ring X, it follows that

$(12 + \sigma)^N = 12^N + 3^N \left(\sqrt{8}\right)^N =$

$= 12 + 3 \cdot 8^{\frac{N-1}{2}} \cdot \sqrt{8} =$

$= 12 + 3(-1)\sqrt{8} =$

$= 12 - \sigma$,
where the first equality uses the Binomial Theorem in a finite field, and the second equality uses Fermat's little theorem.
The value of σ was chosen so that $\omega = \dfrac{(12+\sigma)^2}{72}$. This can be used to compute $\omega^{\frac{N+1}{2}}$ in the ring X as
$\omega^{\frac{N+1}{2}} = \dfrac{(12+\sigma)^{N+1}}{72^{\frac{N+1}{2}}} =$
$= \dfrac{(12+\sigma)(12+\sigma)^{N}}{72 \cdot 72^{\frac{N-1}{2}}} =$
$= \dfrac{(12+\sigma)(12-\sigma)}{-72} =$
$= -1.$
Next, multiply both sides of this equation by $\bar{\omega}^{\frac{N+1}{4}}$ and use $\omega\bar{\omega} = 1$ which gives
$\omega^{\frac{N+1}{2}} \bar{\omega}^{\frac{N+1}{4}} = -\bar{\omega}^{\frac{N+1}{4}}$
$\omega^{\frac{N+1}{4}} + \bar{\omega}^{\frac{N+1}{4}} = 0$
$\omega^{\frac{4 \cdot 3^n - 1 + 1}{4}} + \bar{\omega}^{\frac{4 \cdot 3^n - 1 + 1}{4}} = 0$
$\omega^{3^n} + \bar{\omega}^{3^n} = 0$
$S_n = 0$
Since S_n is 0 in X it is also 0 modulo N .

Sufficiency
If S_n is divisible by $4 \cdot 3^n - 1$ then $4 \cdot 3^n - 1$ is prime.

For $n = 0$ we have $N = 3$ and $S_0 = 6$, so $N \mid S_n$ and N is prime, otherwise consider the sequences:
$U_0 = 0, U_1 = 1, U_{n+1} = 6U_n - U_{n-1}$
$V_0 = 2, V_1 = 6, V_{n+1} = 6V_n - V_{n-1}$
The following equations can be proved by induction:
$(1) : V_n = U_{n+1} - U_{n-1}$
$(2) : U_n = \dfrac{(3+\sqrt{8})^n - (3-\sqrt{8})^n}{\sqrt{32}}$
$(3) : V_n = (3+\sqrt{8})^n + (3-\sqrt{8})^n$
$(4) : U_{m+n} = U_m U_{n+1} - U_{m-1} U_n$

One can show if $S_n \equiv 0 \pmod{(4 \cdot 3^n - 1)}$:
$U_{2 \cdot 3^n} = U_{3^n} V_{3^n} \equiv 0 \pmod{(4 \cdot 3^n - 1)}$
$U_{3^n} \not\equiv 0 \pmod{(4 \cdot 3^n - 1)}$

Theorem 0.2. *With $a, b \in \mathbb{Z}$ let $f(x) = x^2 - ax + b$, $\Delta = a^2 - 4b$ and let n be a positive integer with $\gcd(n, 2b) = 1$ and $\left(\dfrac{\Delta}{n}\right) = -1$. If F is an even divisor of $n+1$ and*

$$V_{F/2} \equiv 0 \pmod{n}, \ \gcd(V_{F/2q}, n) = 1 \textit{ for every odd prime } q \mid F,$$

then every prime p *dividing* n *satisfies* $p \equiv \left(\frac{\Delta}{p}\right) \pmod{F}$. *In particular if* $F > \sqrt{n} + 1$ *then* n *is prime.*

One can show if $S_n \equiv 0 \pmod{(4 \cdot 3^n - 1)}$ the conditions from Theorem 0.2 are fulfilled , hence $4 \cdot 3^n - 1$ is prime.

■