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:
$(1) : V_n = U_{n+1} - U_{n-1}$
$(2) : U_n = \dfrac{(3+\sqrt{8})^n - (3-\sqrt{8})^n}{\sqrt{32}}$
$(3) : V_n = (3+\sqrt{8})^n + (3-\sqrt{8})^n$
$(4) : U_{m+n} = U_m U_{n+1} - U_{m-1} U_n$
Now let p be a prime and $e \geq 1$. Suppose $U_n \equiv 0 \pmod{p^e}$. Then $U_n = bp^e$ for some b . Let $U_{n+1} = a$. By the recurrence relation and (4) , we have:
$U_{2n} = bp^e\,(2a - 6bp^e) \equiv 2aU_n \pmod{p^{e+1}}$
$U_{2n+1} = U_{n+1}^2 - U_n^2 \equiv a^2 \pmod{p^{e+1}}$
Similarly:
$U_{3n} = U_{2n+1}U_n - U_{2n}U_{n-1} \equiv 3a^2 U_n \pmod{p^{e+1}}$
$U_{3n+1} = U_{2n+1}U_{n+1} - U_{2n}U_n \equiv a^3 \pmod{p^{e+1}}$
In general:
$U_{kn} \equiv ka^{k-1}U_n \pmod{p^{e+1}}$
$U_{kn+1} \equiv a^k \pmod{p^{e+1}}$

Taking $k = p$ we get:
$(5): U_n \equiv 0 \pmod{p^e} \leadsto U_{np} \equiv 0 \pmod{p^{e+1}}$
Expanding $(3 \pm \sqrt{8})^n$ by the Binomial Theorem we find that (2) and (3) give us:
$U_n = \sum_k \binom{n}{2k+1} 3^{n-2k-1} 8^k$
$V_n = \sum_k \binom{n}{2k} 2 \cdot 3^{n-2k} 8^k$
Let us set $n = p$ where p is an odd prime. From Binomial Coefficient of Prime $\binom{p}{k}$ is a multiple of p except when $k = 0$ or $k = p$. We find that:
$U_p \equiv 8^{\frac{p-1}{2}} \pmod{p}$
$V_p \equiv 6 \pmod{p}$
If $p \neq 2$ then by Fermat's Little Theorem
$8^{p-1} \equiv 1 \pmod{p}$
Hence:
$\left(8^{\frac{p-1}{2}} - 1\right)\left(8^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$
$8^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$
When $U_p \equiv -1 \pmod{p}$ we have:
$U_{p+1} = 6U_p - U_{p-1} = 6U_p + V_p - U_{p+1} \equiv -U_{p+1} \pmod{p}$
Hence:
$U_{p+1} \equiv 0 \pmod{p}$
When $U_p \equiv +1 \pmod{p}$ we have:
$U_{p-1} = 6U_p - U_{p+1} = 6U_p - V_p - U_{p-1} \equiv -U_{p-1} \pmod{p}$
Hence:
$U_{p-1} \equiv 0 \pmod{p}$
Thus we have shown that:
$(6): \forall p \in \mathbb{P} : \exists \epsilon(p) : U_{p+\epsilon(p)} \equiv 0 \pmod{p}$
where $\epsilon(p)$ is an integer such that $|\epsilon(p)| \leq 1$.
Now let $N \in \mathbb{N}$
Let $m \in \mathbb{N}$ such that $m(N)$ is the smallest positive integer such that:
$U_{m(N)} \equiv 0 \pmod{N}$
Let $a \equiv U_{m+1} \pmod{N}$
Then $a \perp N$ because $\gcd\{U_n, U_{n+1}\} = 1$
Hence the sequence:
$U_m, U_{m+1}, U_{m+2}, \ldots$ is congruent modulo N to $aU_0, aU_1.aU_2, \ldots$
Then we have:
$(7): U_n \equiv 0 \pmod{N} \iff n = km(N)$
for some integer k.
(This number $m(N)$ is called the rank of apparition of N in the sequence.)
We have the identity:
$2U_{n+1} = 6U_n + V_n$
So any common factor of U_n and V_n must divide U_n and $2U_{n+1}$.

As $U_n \perp U_{n+1}$; this implies that $\gcd\{U_n, V_n\} \leq 2$.
So U_n and V_n have no odd factor in common.
So if $S_n \equiv 0 \pmod{(4 \cdot 3^n - 1)}$:
$U_{2 \cdot 3^n} = U_{3^n} V_{3^n} \equiv 0 \pmod{(4 \cdot 3^n - 1)}$
$U_{3^n} \not\equiv 0 \pmod{(4 \cdot 3^n - 1)}$
Now, if $m = m(4 \cdot 3^n - 1)$ is the rank of apparition of $4 \cdot 3^n - 1$ it mas be divisor of $2 \cdot 3^n$ but not of 3^n . So $m = 2 \cdot 3^n$.
Now we prove that $N = 4 \cdot 3^n - 1$ must therefore be prime.
Let the prime decomposition of N be $p_1^{e_1} \dots p_r^{e_r}$.
All primes p_j are greater than 3 because N is odd and congruent to -1 modulo 3 .
From (5), (6), (7) we know that $U_t \equiv 0 \pmod{4 \cdot 3^n - 1}$, where:
$t = \text{lcm}\{p_1^{e_1-1}(p_1 + \epsilon_1), \dots, p_r^{e_r-1}(p_r + \epsilon_r)\}$
where each $\epsilon_j = \pm 1$.
It follows that t is a multiple of $m = 2 \cdot 3^n$.
Let $N_0 = \prod_{j=1}^{r} p_j^{e_j-1}(p_j + \epsilon_j)$.
We have:
$N_0 \leq \prod_{j=1}^{r} p_j^{e_j-1} \left(p_j + \frac{p_j}{5}\right) = \left(\frac{6}{5}\right)^r N$
Also because $p_j + \epsilon_j$ is even $t \leq \frac{N_0}{2^{r-1}}$ because a factor of 2 is lost every time the LCM of two even numbers is taken.
Combining these results, we have:
$m \leq t \leq 2\left(\frac{3}{5}\right)^r N \leq 4\left(\frac{3}{5}\right)^r N < 3m$
Hence $r \leq 2$ and $t = m$ or $t = 2m$
Therefore $e_1 = 1$ and $e_r = 1$
If N is not prime, we must have:
$N = 4 \cdot 3^n - 1 = \left(2 \cdot 3^k + 1\right)\left(2 \cdot 3^l - 1\right)$
where $\left(2 \cdot 3^k + 1\right)$ and $\left(2 \cdot 3^l - 1\right)$ are prime.
When n is odd, that last factorization is obviously impossible, so N is prime.

∎