Three conjectures about primality testing for Mersenne, Wagstaff and Fermat numbers based on cycles of the Digraph under $x^2 - 2$ modulo a prime

Tony Reix
tony.reix@laposte.net
2009, 2nd of February. Updated 2009, 8th of March.
► Version 0.6 ◄

Conjecture 1 (Mersenne numbers) is mine, based on my work on the use of the Cycles of the *Digraph under* $x^2 - 2$ *modulo a Mersenne prime* for primality testing.
Conjectures 2 (Wagstaff numbers) and 3 (Fermat numbers) are Anton Vrba's (plus some improvements by myself) and they are based on my work on Conjecture 1.
Note that I have provided a proof for the sufficiency of Conjecture 1 and that Robert Gerbicz has provided a proof for the sufficiency of Conjectures 2 and 3. "Dodo" has noticed the need of the complementary condition. Anton Vrba has provided a proof for the sufficiency of Conjecture 2, but failed to prove the converse. So, only are missing the necessity part (the most difficult) of the three conjectures !

Here after, q is a prime > 3 and n is an integer > 1 .

Conjecture 1 $S_0 = 3^2 + 1/3^2$, $S_{i+1} = S_i^2 - 2 \pmod{M_q}$

$$M_q = 2^q - 1 \text{ is a prime iff } S_{q-1} \equiv S_0 \pmod{M_q}$$
$$\text{and iff there is no integer } 0 < i < q-1 \text{ for which } S_i \equiv S_0 \pmod{M_q}$$
$$\text{And we have: } \prod_1^{q-1} S_i \equiv 1 \pmod{M_q} \text{ when } M_q \text{ is a prime.}$$

Conjecture 2 $N_q = 2^q + 1$. $S_0 = 1/4$, $S_{i+1} = S_i^2 - 2 \pmod{N_q}$

$$W_q = \frac{N_q}{3} \text{ is a prime iff } S_{q-1} \equiv S_0 \pmod{W_q}$$
$$\text{and iff there is no integer } 0 < i < q-1 \text{ for which } S_i \equiv S_0 \pmod{N_q}$$
$$\text{And we have: } \prod_1^{q-1} S_i \equiv 1 \pmod{W_q} \text{ when } W_q \text{ is a prime.}$$

Conjecture 3 $S_0 = 1/4$, $S_{i+1} = S_i^2 - 2 \pmod{F_n}$

$$F_n = 2^{2^n} + 1 \text{ is a prime iff } S_{2^n-1} \equiv S_0 \pmod{F_n}$$
$$\text{and iff there is no integer } 0 < i < 2^n - 1 \text{ for which } S_i \equiv S_0 \pmod{F_n}$$
$$\text{And we have: } \prod_1^{2^n-1} S_i \equiv -1 \pmod{F_n} \text{ when } F_n \text{ is a prime.}$$

Note that $3/2 \pmod{W_q}$ can be used as seed instead of $1/4 \pmod{W_q}$ for Wagstaff numbers, and that $-3/2 \pmod{F_n}$ can be used as seed instead of $1/4 \pmod{F_n}$ for Fermat numbers.

1 PARI/gp code

Note that the verification that $S \neq S_0$ is not necessary at each step.
For Mersenne and Wagstaff numbers, it is necessary only when $i \mid q-1$. Since $2 \mid q-1$, at least it must be done every even steps, but also for all odd steps that divide $q-1$. Probably an easy way is to check at all steps !
For Fermat numbers, since $2^n - 1$ is odd, there are much less steps where it is necessary. But such a verification has a very low computational cost !

```
Conj1(q) = {
    M=2^q-1;
    S0=Mod(3^2+1/3^2,M);
    print(S0);
    S=S0;
    for(i=1, q-1,
        S=Mod(S^2-2,M);
        print(S);
        if(S==S0 && i<q-1,print("Not prime");););
    );
    if(S==S0,print("Prime !"),print("Not prime"););
}

Conj2(q) = {
    N=2^q+1;
    W=N/3;
    S0=Mod(1/4,N);
    print(Mod(S0,W));
    S0W=Mod(S0,W);
    S=S0;
    for(i=1, q-1,
        S=Mod(S^2-2,N);
        print(Mod(S,W));
        if(Mod(S,W)==S0W && i<q-1,print("Not prime"););
    );
    if(Mod(S,W)==S0W,print("Prime !"),print("Not prime"););
}

Conj3(n) = {
    F=2^2^n+1;
    S0=Mod(1/4,F);
    print(S0);
    S=S0;
    for(i=1, 2^n-1,
```

```
        S=Mod(S^2-2,F);
        if(S==S0 && i<2^n-1,print("Not prime"););
        print(S);
    );
    if(S==S0,print("Prime !"),print("Not prime"););
}
```

2 Examples for Mersennes

$q = 5, M_5 = 31$

$\pmod{M_5}\ S_0 = 16 \overset{1}{\mapsto} 6 \overset{2}{\mapsto} 3 \overset{3}{\mapsto} 7 \overset{4=q-1}{\mapsto} 16 = S_0$

$q = 7, M_7 = 127$

$\pmod{M_7}\ S_0 = 122 \overset{1}{\mapsto} 23 \overset{2}{\mapsto} 19 \overset{3}{\mapsto} 105 \overset{4}{\mapsto} 101 \overset{5}{\mapsto} 39 \overset{6=q-1}{\mapsto} 122 = S_0$

$q = 11, M_{11} = 2047 = 23 \times 89$

$\pmod{M_{11}}\ S_0 = 464 \overset{1}{\mapsto} 359 \overset{2}{\mapsto} 1965 \overset{3}{\mapsto} 581 \overset{4}{\mapsto} 1851 \overset{5}{\mapsto} 1568 \overset{6}{\mapsto} 175 \overset{7}{\mapsto} 1965 = S_2 \overset{8}{\mapsto} 581 \overset{9}{\mapsto} 1851 \overset{10=q-1}{\mapsto} 1568 \neq S_0$

Note that $S_{10} - S_0 = 1568 - 464 = 2^4 \times 3 \times 23$ where 23 is a factor of M_{11}.

Note that there is a loop of length 5 (dividing $q - 1 = 10$) starting at S_2 and ending at S_6.

Note that $\prod_{i=1}^{10} \equiv 622 \neq 1 \pmod{M_{11}}$ and that $\prod_{i=2}^{6} \equiv -1 \pmod{M_{11}}$.

Note that $622^2 \equiv 1 \pmod{M_{11}}$ and thus $1/622 \equiv 622 \pmod{M_{11}}$.

$q = 13, M_{13} = 8191$

$\pmod{M_{13}}\ S_0 = 7290 \overset{1}{\mapsto} 890 \overset{2}{\mapsto} 5762 \overset{3}{\mapsto} 2519 \overset{4}{\mapsto} 5525 \overset{5}{\mapsto} 5957 \overset{6}{\mapsto} 2435 \overset{7}{\mapsto} 7130 \overset{8}{\mapsto} 3552 \overset{9}{\mapsto} 2562 \overset{10}{\mapsto} 2851 \overset{11}{\mapsto} 2727 \overset{12=q-1}{\mapsto} 7290 = S_0$

$q = 23, M_{23} = 8388607$

$\pmod{M_{23}}\ S_0 = 1864144 \overset{1}{\mapsto} \ldots \overset{22=q-1}{\mapsto} 5115651 \neq S_0$

Note that $S_{22} - S_0 = 7 \times 47 \times 9883$ where $47 \mid M_{23}$.

But no more *interesting properties* for greater composite Mersenne numbers. M_{11} and M_{23} seem *special*.

3 Examples for Wagstaffs , seed $= 3/2$

Hereafter: $S_0 = 3/2$ and $S_1 = 1/4$.

$q = 5, W_5 = 11$

(mod W_5) $S_0 = 7 \overset{1}{\mapsto} 3 \overset{2}{\mapsto} 7 \overset{3}{\mapsto} 3 \overset{4=q-1}{\mapsto} 7 = S_0$

$q = 7, W_7 = 43$

(mod W_7) $S_0 = 23 \overset{1}{\mapsto} 11 \overset{2}{\mapsto} 33 \overset{3}{\mapsto} 12 \overset{4}{\mapsto} 13 \overset{5}{\mapsto} 38 \overset{6=q-1}{\mapsto} 23 = S_0$

$q = 11, W_{11} = 683$

(mod W_{11}) $S_0 = 343 \overset{1}{\mapsto} 171 \overset{2}{\mapsto} 553 \overset{3}{\mapsto} 506 \overset{4}{\mapsto} 592 \overset{5}{\mapsto} 83 \overset{6}{\mapsto} 57 \overset{7}{\mapsto} 515 \overset{8}{\mapsto} 219 \overset{9}{\mapsto} 149 \overset{10=q-1}{\mapsto} 343 = S_0$

4 Examples for Fermats, seed $= -3/2$

Hereafter: $S_0 = -3/2$ and $S_1 = 1/4$.

$n = 2, F_2 = 17$

(mod F_2) $S_0 = 7 \overset{1}{\mapsto} 13 \overset{2}{\mapsto} 14 \overset{3=2^n-1}{\mapsto} 7 = S_0$

$n = 3, F_3 = 257$

(mod F_3) $S_0 = 127 \overset{1}{\mapsto} 193 \overset{2}{\mapsto} 239 \overset{3}{\mapsto} 65 \overset{4}{\mapsto} 111 \overset{5}{\mapsto} 240 \overset{6}{\mapsto} 30 \overset{7=2^n-1}{\mapsto} 127 = S_0$