A Fermat-like sequence

Tony Reix (Tony.Reix@laposte.net)
2005, 8th of May (v0.7)

1 Definition of the Serie

This serie has been studied by Yannick Saouter in report N2728 of INRIA in 1995 (http://www.inria.fr/rrrt/rr-2728.html). Saouter has shown that this serie exhibits the same kind of properties than the Fermat numbers.

$$a_n = 4^n + 2^n + 1$$
$$A_n = 4^{3^n} + 2^{3^n} + 1$$

2 Properties (Saouter)

$$a_n \text{ prime} \implies n = 3^k \quad \text{(FLS.1)}$$
$$A_n \text{ prime} \iff \exists\, k \geq 2 \ / \ J(k, A_n) = -1 \text{ and } k^{(A_n-1)/2} \equiv -1 \pmod{A_n} \quad \text{(FLS.2)}$$
$$A_n \text{ prime} \iff 5^{(A_n-1)/2} \equiv -1 \pmod{A_n} \quad \text{(FLS.3)}$$
$$A_{n+1} = 3 + A_n(2^{4.3^n} - 2^{3.3^n} + 2.2^{3^n} - 2) \quad \text{(FLS.4)}$$
$$2^{3^{n+1}} - 1 = A_n(2^{3^n} - 1) \quad \text{(FLS.5)}$$
$$\text{Numbers } A_n \text{ are pairwise relatively prime.} \quad \text{(FLS.6)}$$
$$p \text{ prime}, p \mid A_n \implies p \equiv 1 \pmod{2 \times 3^{n+1}} \quad \text{(FLS.7)}$$
$$A_n \equiv 3 \pmod{A_i} \ , \quad i = 0 \ldots n \quad \text{(FLS.8)}$$

3 Properties (Reix)

$$\prod_{i=0}^{n} A_i = 2^{3^{n+1}} - 1 \quad \text{(FLR.1)}$$
$$2(2^{3^n-1} + 1) \prod_{i=0}^{n-1} A_i = A_n - 3 \quad \text{(FLR.2)}$$

$$2^{3^{n+1}} \equiv 1 \pmod{A_i} \quad , \quad i = 0 \dots n \quad \text{(FLR.3)}$$

The number of digits in A_n is: $\approx \lfloor 2 \times 3^n \log(2) + 1 \rfloor \approx \lfloor 3^n \times 0.60206 \rfloor + 1$ (FLR.4)

$$A_n \ \equiv \ 1 \pmod{2^{3^n} 3^{n+1}} \quad \text{(FLR.5)}$$

$$A_i - 1 \ | \ A_n - 1 \quad , \quad i = 0 \dots n \quad \text{(FLR.6)}$$

$$A_n = 1 + 2^{3^n} 3^{n+1} \prod_{i=0}^{n-1} K_i \quad , \ n > 0 \quad \text{where:} \quad K_i = \frac{2^{2.3^i} - 2^{3^i} + 1}{3} \quad \text{(FLR.7)}$$

$$K_i = 1 + 2.3^{i+1} L_i \prod_{j=0}^{i-1} K_j \quad , \ i > 0 \quad \text{where:} \quad L_i = \frac{2^{3^i - 1} - 1}{3} \quad \text{(FLR.8)}$$

$$3K_i = \frac{K_{i+1} - 1}{K_i - 1} \frac{L_i}{L_{i+1}} \quad \text{(FLR.9)}$$

$$A_n = 1 + 2^{3^n - 1} \frac{K_n - 1}{L_n} \quad ; \quad 2^{3^n} + 1 = \frac{K_n - 1}{2L_n} = 3^{n+1} \prod_{i=0}^{n-1} K_i \quad \text{(FLR.10)}$$

$$p \text{ prime}, p \mid A_n \implies p \equiv \pm 1 \pmod 8 \quad \text{(FLR.11)}$$

Proof of (FLR.1):
By using recursively (FLS.5) and (FLR.1), we have:
$2^{3^{n+1}} - 1 = A_n A_{n-1} (2^{3^{n-1}} - 1) = \dots = A_n A_{n-1} \dots A_1 A_0 (2^{3^0} - 1) = \prod_{i=0}^{n} A_i$

Proof of (FLR.2):
By using (FLS.4), we have:
$A_{n+1} = 3 + A_n \big(2^{3^{n+1} + 3^n} - 2^{3^{n+1}} + 2(2^{3^n} - 1)\big)$
$A_{n+1} = 3 + A_n \big(2^{3^{n+1}} (2^{3^n} - 1) + 2(2^{3^n} - 1)\big)$
$A_{n+1} = 3 + A_n \big((2^{3^n} - 1)(2^{3^{n+1}} + 2)\big)$
$A_{n+1} = 3 + A_n \big(\prod_{i=0}^{n-1} A_i\big) 2 (2^{3^{n+1} - 1} + 1)$
$A_{n+1} = 3 + 2(2^{3^{n+1} - 1} + 1) \prod_{i=0}^{n} A_i$

Proof of (FLR.3):
It comes from (FLR.1).

(FLR.4):
$A_n \approx 2^{2 \times 3^n}$
The number of digits in A_n is more than 10,000,000 for $n = 16$: $\approx 25,916,708$.

Proof of (FLR.5):
By (FLS.7), we have: $A_n \equiv 1 \pmod{3^{n+1}}$.
Since: $A_n = 1 + 2^{3^n}\left(2^{3^n}+1\right)$, we have: $A_n \equiv 1 \pmod{2^{3^n}}$.

Proof of (FLR.6) and (FLR.7):
Since $2^3 \equiv -1 \pmod 3$ and $2^{3^n} = \left(2^3\right)^{3^{n-1}}$, we have: $2^{3^n} \equiv -1 \pmod 3$.
And finally: $2^{2.3^n} - 2^{3^n} + 1 \equiv (-1)^2 - (-1) + 1 \equiv 0 \pmod 3$.

We have: $A_n - 1 = 2^{3^n}\left(2^{3^n}+1\right)$, and $A_{n+1} - 1 = 2^{3^{n+1}}\left(2^{3^{n+1}}+1\right)$.
Since: $2^{3^{n+1}} + 1 = \left(2^{3^n}+1\right)\left(2^{2.3^n} - 2^{3^n} + 1\right)$, we have:

$$\left(A_{n+1}-1\right) = 2^{2.3^n}\left(2^{2.3^n} - 2^{3^n} + 1\right)\left(A_n - 1\right)$$

$$\left(A_{n+1}-1\right) = 2^{\;2\sum_{i=0}^{n} 3^i}\prod_{i=0}^{n}\left(2^{2.3^i} - 2^{3^i} + 1\right)(A_0 - 1)$$

$$\left(A_{n+1}-1\right) = 2^{\;1+2\sum_{i=0}^{n} 3^i}\; 3^{1+n+1}\prod_{i=0}^{n}\frac{2^{2.3^i} - 2^{3^i} + 1}{3}$$

Let $\gamma_n = 1 + 2\sum_{i=0}^{n-1} 3^i$. Let's prove that $\gamma_n = 3^n$.
$\gamma_1 = 1 + 2(1) = 3^1$.
$\gamma_{n+1} = 1+2\sum_{i=0}^{n} 3^i = 1+2\sum_{i=0}^{n-1} 3^i + 2\times 3^n = \gamma_n + 2\times 3^n = 3^n(1+2) = 3^{n+1}$.

So we have:

$$A_n = 1 + 2^{3^n}3^{n+1}\prod_{i=0}^{n-1} K_i \quad , \; n > 0 \quad \text{where: } K_i = \frac{2^{2.3^i} - 2^{3^i} + 1}{3}$$

Proof of (FLR.8), (FLR.9) and (FLR.10):
Since $2^2 \equiv 1 \pmod 3$ we have $2^{3^i - 1} - 1 \equiv (2^2)^k - 1 \equiv 1 - 1 \equiv 0 \pmod 3$.

The binary representation of L_i is: $[10101\ldots10101]_2 = \left[1(01)^{3(3^{i-1}-1)/2}\right]_2$.

We first prove: $(K_{i+1} - 1)L_i = 3(K_i - 1)K_iL_{i+1}$.

$(K_{i+1} - 1)L_i = \frac{1}{3^2}\left(2^{2\times 3^{i+1}} - 2^{3^{i+1}} - 2\right)\left(2^{3^i - 1} - 1\right)$
$\quad = \frac{1}{3^2}\left(2^{7\times 3^i - 1} - 2^{4\times 3^i - 1} - 2^{3^i} - 2^{2\times 3^{i+1}} + 2^{3^{i+1}} + 2\right)$

$3(K_i - 1)K_iL_{i+1} = \frac{3}{3^3}\left(2^{2\times 3^i} - 2^{3^i} - 2\right)\left(2^{2\times 3^i} - 2^{3^i} + 1\right)\left(2^{3^{i+1}-1} - 1\right)$
$\quad = \frac{1}{3^2}\left(2^{4\times 3^i} - 2^{3^{i+1}+1} + 2^{3^i} - 2\right)\left(2^{3^{i+1}-1} - 1\right)$
$\quad = \frac{1}{3^2}\left(2^{7\times 3^i - 1} - 2^{2\times 3^{i+1}} + 2^{4\times 3^i - 1} - 2^{3^{i+1}} - 2^{4\times 3^i} + 2^{3^{i+1}+1} - 2^{3^i} + 2\right)$

Thus we now have to prove: $-2^{4\times 3^i-1}+2^{3^{i+1}} = 2^{4\times 3^i-1}-2^{3^{i+1}}-2^{4\times 3^i}+2^{3^{i+1}+1}$, which is equivalent to: $2\times 2^{3^{i+1}} - 2^{3^{i+1}+1} = 2\times 2^{4\times 3^i-1} - 2^{4\times 3^i}$, and which clearly simplifies in: $0=0$, proving (FLR.9).

Now, since for $i=1$ we have: $K_1 = 19 = 1+2\times 3^2 L_1 K_0$, with $K_0=1$ and $L_1=1$, we suppose that (FLR.8) is true for n and we prove that it implies that (FLR.8) is true for $n+1$.

First, write (FLR.9) this way: $K_{i+1} = 1+\big(3(K_i-1)K_iL_{i+1}\big)/L_i$ (I).
By the hypothesis, we have: $\big(K_i-1\big)/L_i = 2\times 3^{i+1}\prod_{j=0}^{i-1}K_j$ (II).
Replacing now $\big(K_i-1\big)/L_i$ from (II) in (I), we have: $K_{i+1} = 1+2\times 3^{i+2}K_iL_{i+1}\prod_{j=0}^{i-1}K_j = 1+2\times 3^{i+2}L_{i+1}\prod_{j=0}^{i}K_j$, which proves (FLR.8) .

Using (II) in (FLR.7) with n replacing i, it easily comes that we have: $A_n = 1+2^{3^n-1}(K_n-1)/L_n$, proving (FLR.10) and providing the factorization of $2^{3^n}+1$.
Notice that $A_n = 1+A2^{3^n-1}$ with $A > 2^{3^n-1}$, showing that usual primality proofs based on Lucas sequences do not apply there.

Proof of (FLR.11):
The proof of (FLS.7) by Saouter provides nearly all we need for proving (FLR.11). Here is my version:
By (FLS.5), we have: $2^{3^{n+1}} \equiv 1 \pmod{A_n}$. If p is prime and $p \mid A_n$, then $2^{3^{n+1}} \equiv 1 \pmod p$, and thus ρ, the order of $2 \pmod p$, divides 3^{n+1}.
By the definition of A_n, we have: $2^{3^n}\big(2^{3^n}+1\big) \equiv 1 \pmod{A_n}$. If ρ were smaller than 3^{n+1}, that would imply: $1\times(1+1)\equiv 1 \pmod p$, which is false.
Thus $\rho = 3^{n+1}$.
Since by Fermat little theorem we have: $2^{p-1}\equiv 1 \pmod p$, then ρ also divides $p-1$. And thus: $p = 1+2k3^{n+1}$ and $2^{(p-1)/2} = 2^{k3^{n+1}} = \big(2^{3^{n+1}}\big)^k \equiv (1)^k \equiv 1 \pmod p$. This means that 2 is a quadratic residue $\pmod p$ and if follows:

$$p \equiv \pm 1 \pmod 8$$

4 Conjectures

$$p \text{ prime}, p \mid K_n \implies p = 1+2k3^{n+1} \quad \text{and} \quad p\equiv 1 \text{ or } 3 \pmod 8 \qquad \text{(FLRC.1)}$$

8 is the first value for n for which $2^{3^n}+1$ does not appear in the Cunningham project. I've found the following factors of $2^{3^8}+1$: $1+2.3^8.4$, $1+2.3^8.2205$, $1+2.3^8.40091760$. And a factor of $2^{3^{14}}+1$: $1+2.3^{14}.380$.

5 Numerical Data

$A_0 = 3 + 2 \times (2^0 + 1]$
$A_1 = 3 + 2A_0 \times 5$
$A_2 = 3 + 2A_0A_1 \times 257$
$A_3 = 3 + 2A_0A_1A_2 \times (2^{26} + 1)$
$A_4 = 3 + 2A_0A_1A_2A_3 \times 65537 \times \dots$

$A_0 = 7 = (2^{3^0} + 1)2^{3^0} + 1 = 1 + 2^{3^0}3^1$

$A_1 = 73 = (2^{3^1} + 1)2^{3^1} + 1 = 1 + 2^{3^1}3^2K_0$
$K_0 = 1$

$A_2 = 262657 = (2^{3^2} + 1)2^{3^2} + 1 = 1 + 2^{3^2}3^3 19 = 1 + 2^{3^2}3^3K_0K_1$
$K_1 = 19 = 1 + 2.3^2K_0L_1$
$L_1 = 1$

$A_3 = (2^{3^3} + 1)2^{3^3} + 1 = 1 + 2^{3^3}3^4 19 * 87211 = 1 + 2^{3^3}3^4K_0K_1K_2$
$K_2 = 87211 = 1 + 2.27.1.19.5.17 = 1 + 2.3^3K_0K_1L_2$
$L_2 = 5.17$

$A_4 = (2^{3^4} + 1)2^{3^4} + 1 = 1 + 2^{3^4}3^5K_0K_1K_2K_3$
$K_3 = 6004799458421419 = 1 + 2.3^4K_0K_1K_2L_3$
$L_3 = 2731.8191$

$A_5 = (2^{3^5} + 1)2^{3^5} + 1 = 1 + 2^{3^5}3^6K_0K_1K_2K_3K_4$
$K_4 = 19 \dots 51 = 1 + 2.3^5K_0K_1K_2K_3L_4$
$L_4 = 5^2.11.17.31.41.257.61681.4278255361$

$61681 = 1 + 2^4.3.5.257$
$4278255361 = 1 + 2^8.3.5.17.65537$

6 To Be Studied

$$(2^k)^{2^{3^n-1}\prod_{i=1}^n K_i} \equiv 2^{4k} \pmod{A_n} \quad \text{(FLRC.2)}$$

$$(2^k)^{2^{3^n-3}\prod_{i=1}^n K_i} \equiv 2^{k} \pmod{A_n} \quad \text{(FLRC.3)}$$

$$(2^{3^n})^{\prod_{i=1}^n K_i} \equiv 2^{3^n} \pmod{A_n} \quad \text{(FLRC.4)}$$

$5^{2^3} = 41^2 \equiv 2 \pmod{A_1}$
$5^{2^2} \equiv 41 \pmod{A_1}$

$(-2)^{3^2} \equiv -1 \pmod{A_1}$
$41 = 1 + 2^3.5$
$(2^1)^{2^8 \times 19} \equiv (2^1)^4 \pmod{A_2}$
$(2^2)^{2^8 \times 19} \equiv (2^2)^4 \pmod{A_2}$
$(2^3)^{2^8 \times 19} \equiv (2^3)^4 \pmod{A_2}$
$(2^4)^{2^8 \times 19} \equiv (2^4)^4 \pmod{A_2}$
$(2^3)^{19} \equiv (2^3) \pmod{A_2}$
$2^{19} \equiv -(2^{10} + 2^1) \pmod{A_2}$
$5^{2^8.19} \equiv -16 \pmod{A_2}$
$(-16)^{3^3} \equiv -1 \pmod{A_2}$
$(-16)^7 \equiv -2 \pmod{A_2}$
$5^{2^9 \times 19 \times 17} = 246273 \equiv 2 \pmod{A_2}$
$246273 = 1 + 2^9.13.37$
$13 \times 37 = 481 = 1 + 2^5.3.5$
$8^{87211} \equiv 8 \pmod{A_3}$
$64^{87211} \equiv 64 \pmod{A_3}$
$(2^{3^2})^{87211} \equiv 2^{3^2} \pmod{A_3}$
$512^{19} \equiv 512 \pmod{A_3}$
$4096^{87211} \equiv 4096 \pmod{A_3}$
$512^{2^{26} \times 19 \times 87211} \equiv 2^{36} \pmod{A_3}$
$(2^1)^{2^{26} \times 19 \times 87211} \equiv (2^1)^4 \pmod{A_3}$
$(2^2)^{2^{26} \times 19 \times 87211} \equiv (2^2)^4 \pmod{A_3}$
$(2^3)^{2^{26} \times 19 \times 87211} \equiv (2^3)^4 \pmod{A_3}$
$(2^4)^{2^{26} \times 19 \times 87211} \equiv (2^4)^4 \pmod{A_3}$
$2^{19 \times 87211} \equiv -(2^{46} + 2^{19}) \pmod{A_3}$