On the primality of F_{4723} and F_{5387}

François Morain

morain@lix.polytechnique.fr

July 21, 1990 (updated on May 10, 1999)

1 Introduction

We follow the notations of both [2] and [3]. Let F_n (resp. L_n) be the n-th Fibonacci number (resp. Lucas number). The aim of this informal note is to describe a short proof of primality for both F_{4723} and F_{5387}. See the paper [5] for more on this topic.

2 F_{4723}

From [3, (4.1)], one has

$$F_{4k+3} - 1 = F_{k+1} L_{k+1} L_{2k+1}. \tag{1}$$

Here $k = 1180$, $k+1 = 1181$ and $2k+1 = 2361 = 3 \times 787$. From [3] and with the help of factors found by Montgomery and Silverman [7, 8, 9], we get

$$F_{1181} = 5453857 \times C_{240},$$

$$L_{1181} = 59051 \times 21719865481 \times 1762204331274241091 \times PRP_{214},$$

$$L_{2361} = L_3^* \times L_{787}^* \times L_{2361}^*$$

with

$$\begin{aligned} L_{787}^* &= 31481 \times 13224749 \times C_{153} \\ L_{2361}^* &= 10305997600922449 \times C_{313}. \end{aligned}$$

Although the PRP_{214} has been proven prime by the author using ECPP [1], the factored part of $F_{4723} - 1$ is not large enough to use any theorem.

Using [3, (4.2)], we now turn our attention to the factorization of

$$F_{4723} + 1 = F_{2361} L_{2362}.$$

We have

$$F_{2361} = F_3^* \times F_{787}^* \times F_{2361}^*$$

where $F_3^* = 2$,

$$\begin{aligned} F_{787}^* &= 47221 \times 3571442321831904937 \times C_{141}, \\ F_{2361}^* &= PRP_{329}; \end{aligned}$$

$$L_{2362} = L_2^* \times L_{2362}^*$$

with $L_2^* = 3$,

$$L_{2362}^* = 4723 \times 151169 \times 1016560631592041 \times C_{470}.$$

After proving the PRP_{329} to be prime (using also ECPP), our quest is finished, since the factor part of $F_{4k+3} + 1$, namely

$$\begin{aligned} \mathcal{F}_2 = \quad & 32468318781717089958633479517339001223957229525945091610187396896295197 22\\ & 0933909362296817596952345516487745912707060400026433140420075693831568285724\\ & 0573956860335397693227522535348419352807647807045210612970428690483683473177\\ & 4893986465448130161026539395954264063262488919912452658798478391873194656388\\ & 4019388317633987495890987029330803813040613958136778718316818957383724490034 \end{aligned}$$

enables us to use Theorem 17 of [2] with $m = 1$. The computations were done as in [4]. On a DEC Station 3100, using the arithmetic described in [6], the process took about 45 minutes.

Historical comment: Interestingly enough, I had proved this number to be prime a little while ago, using ECPP alone. Then, the process (using a star network) took about 430 days of CPU of SUN 3/60 (approximately 100 days of DEC).

3 F_{5387}

This time, we find that

$$F_{5387} - 1 = F_{1347} L_{1347} L_{2693}.$$

Using [3, (2.4)], we get

$$F_{1347} = F_3^* \times F_{449}^* \times F_{1347}^*. \tag{2}$$

Using the Tables in [3] and that in [7, 8, 9], one has $F_3^* = 2$, $F_{449}^* = P_{94}$ and

$$F_{1347}^* = 2693 \times 759709 \times 66231540964081 \times 2250635393569485855423798723804779449 \times C_{128}.$$

Next

$$L_{1347} = L_3^* \times L_{449}^* \times L_{1347}^*$$

with $L_3^* = 4$ and

$$\begin{aligned} L_{449}^* &= 369079 \times 7219577744649997524991234 6541 \times 3116807561814759915228612 99701 \times P_{30},\\ L_{1347}^* &= 10003891161597271 \times 332169666981841732921 \times PRP_{151}. \end{aligned}$$

And finally $L_{2693}^* = 53402191 \times C_{556}$.

The author has proved the primality of the 151-digit cofactor of L_{1347}^* using ECPP. Collecting data together, we see that the factored part of $F_{5387} - 1$ amounts to

$$\begin{aligned} \mathcal{F}_1 = \quad & 320007079941920199049302161771943263514728 8\\ & 6855964069304259199443299997027759719645400132761 4\\ & 3884014207326372006034171267940979700204591592911 0\\ & 1578332415864546575490751590343455657459016625495 3\\ & 4015753919364010628854132956981689274993661876686 4\\ & 5661602196610355365617565204428751761483155809505 7\\ & 6843817266864395213765743396555066084248225857184 3\\ & 0475265693444630724397478186630622328428231146311 7\\ & 82685533166912533586188568224816516812458663923416. \end{aligned}$$

A little algebra tells us that $\mathcal{F}_1$ satisfies inequality (4) of Theorem 5 in [2] with $m = 1$. Hence, we can now prove that F_{5387} is prime provided that condition (I) of [2, pp. 623] is met. The author checked this using his own program. This computation took about half an hour. The number $a = 3$ was used for all prime factors of $\mathcal{F}_1$.

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[2] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29(130):620–647, 1975.

[3] J. Brillhart, P. L. Montgomery, and R. D. Silverman. Tables of Fibonacci and Lucas factorizations. *Math. Comp.*, 50(181):252–260, January 1988.

[4] H. Cohen and A. K. Lenstra. Implementation of a new primality test. *Math. Comp.*, 48(177):103–121, 1987.

[5] H. Dubner and W. Keller. New Fibonacci and Lucas primes. *Math. Comp.*, 68(225):417–427, January 1999.

[6] J.-C. Hervé, B. Serpette, and J. Vuillemin. BigNum: A portable and efficient package for arbitrary-precision arithmetic. Technical Report 2, Digital Paris Research Laboratory, May 1989.

[7] P. L. Montgomery. Fibonacci/Lucas update. Email to Morain, June 1990.

[8] P. L. Montgomery. Factorization of V1181, V1347. Email to Morain, June 1990.

[9] P. L. Montgomery. 37-digit P-1 factor. Email to Morain, July 1990.