An algorithm for finding the factors of Fermat numbers

Emmanuil Manousos

APM Institute for the Advancement of Physics and Mathematics, Athens, Greece

Abstract. In this article we present an algorithm for finding the factors Q of composite Fermat numbers. The algorithm finds the Q factors with less tests than required through the equation $2^n \times K+1$.

1. Introduction

Available factorization tests fail in the case of Fermat numbers. So, the factors Q of Fermat numbers $F_S = 2^{2^S}+1$, $S \in \mathbb{N}$, are calculated through equation

$$Q = 2^n \cdot K + 1, \tag{1}$$

where K is an odd number and n is a integer, $n \geq S+2$. The algorithm we present in this paper finds the factors Q with less tests than required through equation (1).

2. The algorithm

There exists a sequence of odd numbers of the form Q (see, [3], section 3) for which $T(Q) \geq Q$ and $T(Q^*) \geq Q^*$ (see [3], section 4). Fermat numbers and their factors (see [1-5]) belong to this sequence. Starting from this fact, we get an algorithm for calculating factors of composite Fermat numbers.

Every Fermat number has at least one factor of the form

$$Q = 2^{N+2} + 1 - 3 \cdot 2^n - 2^{n+2} \cdot \lambda \tag{2}$$

in an interval $\Omega_N = \left[2^{N+1}, 2^{N+2}\right]$ and at least one factor of the form

$$Q = 2^{M+2} + 1 - 5 \cdot 2^n - 2^{n+2} \cdot l \tag{3}$$

in another interval $\Omega_M = \left[2^{M+1}, 2^{M+2}\right]$.

Considering that Q belongs to either the interval Ω_N or Ω_M, we get the possible values of λ and l,

$$\begin{aligned} &\lambda = 0,1,2,\ldots,2^{N-n-1}-1 \\ &l = -1,0,1,\ldots,2^{M-n-1}-2 \end{aligned}. \tag{4}$$

From equations (4) we get the following inequalities,

$$\begin{aligned} &N \geq n+1 \\ &M \geq n+2 \end{aligned}. \tag{5}$$

Changing the value of K in equation (1) by $\delta K = 2$ the value of Q changes by $\delta Q = 2^{n+1}$. Changing the value of λ by $\delta\lambda = 1$ or l by $\delta l = 1$ in equations (2), (3) the value of Q changes by $\delta Q = -2^{n+2}$. Therefore equations (2), (3) give the possible factors of a Fermat number with half the number of tests given by equation (1).

We give an example.

Example 1. For $F_5 = 2^{32} + 1$ we have $n = 5 + 2 = 7$ and from equations (2), (3) we get

$$\begin{aligned} Q &= 2^{N+2} + 1 - 3 \cdot 2^7 - 2^9 \cdot \lambda \\ Q &= 2^{M+2} + 1 - 5 \cdot 2^7 - 2^9 \cdot l \end{aligned} . \tag{6}$$

From equations (4) we get

$$\begin{aligned} \lambda &= 0, 1, 2, \ldots, 2^{N-8} - 1 \\ l &= -1, 0, 1, \ldots, 2^{M-8} - 2 \end{aligned} . \tag{7}$$

From inequalities (5) (or from equations (7)) we get $N \geq 8$ and $M \geq 9$.

For $N = 8$, $M = 9$, from equations (6), (7) we get

$$Q = 2^{10} + 1 - 3 \cdot 2^7 - 2^9 \cdot \lambda ,$$

$$Q = 2^{11} + 1 - 5 \cdot 2^7 - 2^9 \cdot l$$

and $\lambda = 0$, $l = -1, 0$. The first equation gives $Q = 2^{10} + 1 - 3 \cdot 2^7 = 641$. The second equation for $l = -1$ gives

$$Q = 2^{11} + 1 - 5 \cdot 2^7 - 2^9 \cdot (-1) = 1921$$

and for $l = 0$ gives

$$Q = 2^{11} + 1 - 5 \cdot 2^7 = 1409 .$$

$Q = 641$ is a factor of the F_5, therefore the second factor of F_5 is given by the second of the equations (6). We give values $M = 9, 10, 11, \ldots$ until we reach $M = 21$ where we find $Q = 6700417$ in the interval Ω_{21}. In each interval Ω_ν, $\nu = 9, 10, 11, \ldots, 20$ the number of tests is $2^{\nu-8}$ (see equation (7)). Therefore up to Ω_{20}, $2^{9-8} + 2^{10-8} + 2^{11-8} + \ldots + 2^{20-8} = 2^{13} - 1$ tests are required. For $M = 21$, after 3298 tests, for $l = -1, 0, 1, \ldots, 3296$ we get $Q = 2^{23} + 1 - 5 \cdot 2^7 - 2^9 \cdot 3296 = 6700417$. Consequently, $2^{13} - 1 + 3298 = 11489$ tests are required to calculate $Q = 6700417$.

Finding $6700417 = 2^7 \cdot 52347 + 1$ from equation (1) requires $\dfrac{52347 - 1}{2} = 26173 > 11489$ tests. If we had done all the tests on set Ω_{21}, the required number of tests would be $2^{14} - 1 = 16383 < 26173$.

The algorithm has not been fully explored. An investigation concerns the replacement of parameters $2^{n+2}\cdot\lambda$, $2^{n+2}\cdot l$ in equations (2), (3) with $2^{n+2+x}\cdot\lambda$, $2^{n+2+y}\cdot l$, where x, y are positive integers. We give an example.

Example 2. To find the $Q=6700417$ factor of F_5 we use the equation

$$Q=2^{M+2}+1-5\cdot 2^7-2^{14}\cdot l \tag{8}$$

instead of the second of equations (6). Considering that Q belongs to the set Ω_M we get the following values of l,

$$l=-1,0,1,\ldots,2^{M-13}-2\,. \tag{9}$$

Therefore we have $M\geq 14$.

We give values $M=14,15,16..$ until we reach Ω_{21} where we find $Q=6700417$. In each interval Ω_ν, $\nu=14,15,16,\ldots,20$, $2^{\nu-13}$ tests are required (see equation (9)). Therefore the required tests are $2^{14-13}+2^{15-13}+2^{16-13}+\ldots+2^{20-13}=2^8-2=254$. For $M=21$, from equation (8) we get $Q=2^{23}+1-5\cdot 2^7-2^{14}\cdot l$ and from equation (9) we get $l=-1,0,1,\ldots,254$. After 105 tests, for $l=-1,0,1,\ldots,103$ we get $Q=2^{23}+1-5\cdot 2^7-2^{14}\cdot 103=6700417$. Therefore the tests required to find $Q=6700417$ are $254+105=359<<26171$.

Now let C be a composite factor of a Fermat number, $C-1=2^n\cdot K$. Then C has a factor of the form $Q=2^n\cdot K_1+1$ (see, [3] Corollary 3.1). Therefore, for the factorization of C, we know the parameter n in equations (2), (3).

References

[1] Grytczuk, A., M. Wójtowicz, and Florian Luca. "Another note on the greatest prime factors of Fermat numbers." *Southeast Asian Bulletin of Mathematics* 25 (2001): 111-115.

[2] Krizek, Michal, Florian Luca, and Lawrence Somer.*17 Lectures on Fermat numbers: from number theory to geometry*. Springer Science & Business Media, 2002.

[3] Manousos, E., **viXra:2103.0159**

[4] Nemron, Ikorong Anouk Gilbert. "Placed Near The Fermat Primes And The Fermat Composite Numbers." *International Journal Of Research In Mathematic And Apply Mathematical Sciences*14 (1)(2013): 72-82.

[5] Robinson, Raphael M. "A Report on Primes of the Form and On Factors of Fermat Numbers." *Proceedings of the American Mathematical Society* 9.5 (1958): 673-681.