F_{12}ECM

A PROGRAM FOR FINDING
THE FACTORS OF
THE 12^{TH} FERMAT NUMBER

Elliptic Curve Method and Probabilities

Yves Gallot

February 13, 2021

Chapter 1

Introduction

> Si je puis une fois tenir la raison fondamentale que 3, 5, 17, etc. sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière,
>
> *Fermat à Mersenne*
> *25 décembre 1640*

Pierre de Fermat conjectured that every number of the form $F_n = 2^{2^n} + 1$, where n is a non-negative integer, is prime [5]. Today these positive integers are named Fermat numbers. The first five Fermat numbers are prime, but Leonhard Euler proved in 1732 that 641 divides F_5.

F_6 was completely factored by T Clausen, F. Landry and H. Le Lasseur in 1855. In 1970, M. A. Morrison and J. Brillhart cracked F_7 by the Continued Fraction method [9]. In 1980, R. P. Brent and J. M. Pollard used a modification of Pollard's rho method to factor F_8. R. P. Brent completely factored F_{11} in 1988 by ECM [2]. In 1990, A. K. Lenstra, H. W. Lenstra, M. S. Manasse and J. M. Pollard organized a distributed computation on approximately 700 workstations around the world and factored F_9 by the Number Field Sieve [7]. Finally R. P. Brent completely factored F_{10} in 1995 by ECM [2].

The smallest Fermat number which is not completely factored is F_{12}. Six prime factors are known, the 54-digit factor was found by Michael Vang in 2010 using GMP–ECM [10].

$$
\begin{aligned}
F_5 &= 641 \cdot 6700417 \\
F_6 &= 274177 \cdot 67280421310721 \\
F_7 &= 59649589127497217 \cdot 5704689200685129054721 \\
F_8 &= 1238926361552897 \cdot P_{62} \\
F_9 &= 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99} \\
F_{10} &= 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252} \\
F_{11} &= 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564} \\
\\
F_{12} &= 114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot \\
& 568630647535356955169033410940867804839360742060818433 \cdot C_{1133}
\end{aligned}
$$

Chapter 2

Elliptic curves over finite fields

Chapter 3

Elliptic Curve Method

3.1 Implementation

3.2 Probabilities

Dickman [4] proved that the probability that a large integer n has no prime factor exceeding n^α approaches a limit $F(\alpha)$ as $n \to \infty$, where

$$F(\alpha) = \begin{cases} 1 - \int_\alpha^1 F(\frac{t}{1-t})\frac{dt}{t} & \text{if } 0 \leq \alpha < 1, \\ 1 & \text{if } \alpha \geq 1. \end{cases}$$

Let $u = 1/\alpha$. $F(1/u) = 1 - \int_{1/u}^1 F(\frac{t}{1-t})\frac{dt}{t}$. If $t' = 1/t$ we have $\frac{t}{1-t} = \frac{1}{t'-1}$ and $\frac{dt}{t} = -\frac{dt'}{t'}$ then $F(1/u) = 1 - \int_1^u F(\frac{1}{t'-1})\frac{dt'}{t'}$. The relation becomes

$$F(1/u) = \rho(u) = \begin{cases} 1 - \int_1^u \frac{\rho(t-1)}{t}\,dt & \text{if } u > 1, \\ 1 & \text{otherwise.} \end{cases}$$

ρ is the Dickman function used to estimate the proportion of smooth numbers up to a given bound.

Differentiating both sides of the definition of $\rho(u)$ for $u > 1$ gives $t\,\rho'(t) = -\rho(t-1)$. Integration by parts of $\rho(t)$ and t is $\int_1^u \rho(t)\,dt = [t\,\rho(t)]_1^u - \int_1^u t\,\rho'(t)\,dt$. Hence $\int_1^u \rho(t)\,dt = u\,\rho(u) - 1 + \int_0^{u-1} \rho(t)\,dt$. Since $\int_0^1 \rho(t)\,dt = 1$ we have

$$\rho(u) = \frac{1}{u}\int_{u-1}^u \rho(t)\,dt.$$

This relation can be used for the numerical computation of ρ by approximating the integral with the trapezoidal formula [8]. If $1 \leq u < 2$, $\rho(u) = 1 - \int_1^u \frac{dt}{t} = 1 - \log u$.

Knuth and Trabb Pardo [6] extended Dickman's theorem and shown that the probability that the k^{th} largest prime factor of a number n is at most n^α tends to a limiting distribution $F_k(\alpha)$ as $n \to \infty$, where $F_0(\alpha) = 0$ for all α by convention and for $k \geq 1$

$$F_k(\alpha) = \begin{cases} 1 - \int_\alpha^1 \left(F_k(\frac{t}{1-t}) - F_{k-1}(\frac{t}{1-t})\right) \frac{dt}{t} & \text{if } 0 \leq \alpha < 1, \\ 1 & \text{if } \alpha \geq 1. \end{cases}$$

We can define the generalized Dickman function $\rho_k(u) = F_k(1/u)$ and we have

$$\rho_k(u) = \begin{cases} 1 - \int_1^u (\rho_k(t-1) - \rho_{k-1}(t-1)) \frac{dt}{t} & \text{if } u > 1 \text{ and } k \geq 1, \\ 1 & \text{if } 0 < u \leq 1 \text{ and } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

The differential equation is $t\,\rho_k'(t) = -\rho_k(t-1) + \rho_{k-1}(t-1)$. Integrating by parts, we get

$$\rho_k(u) = \frac{1}{u}\left(\int_{u-1}^{u} \rho_k(t)\,dt + \int_0^{u-1} \rho_{k-1}(t)\,dt\right).$$

This relation can be used for the numerical computation of ρ_2.

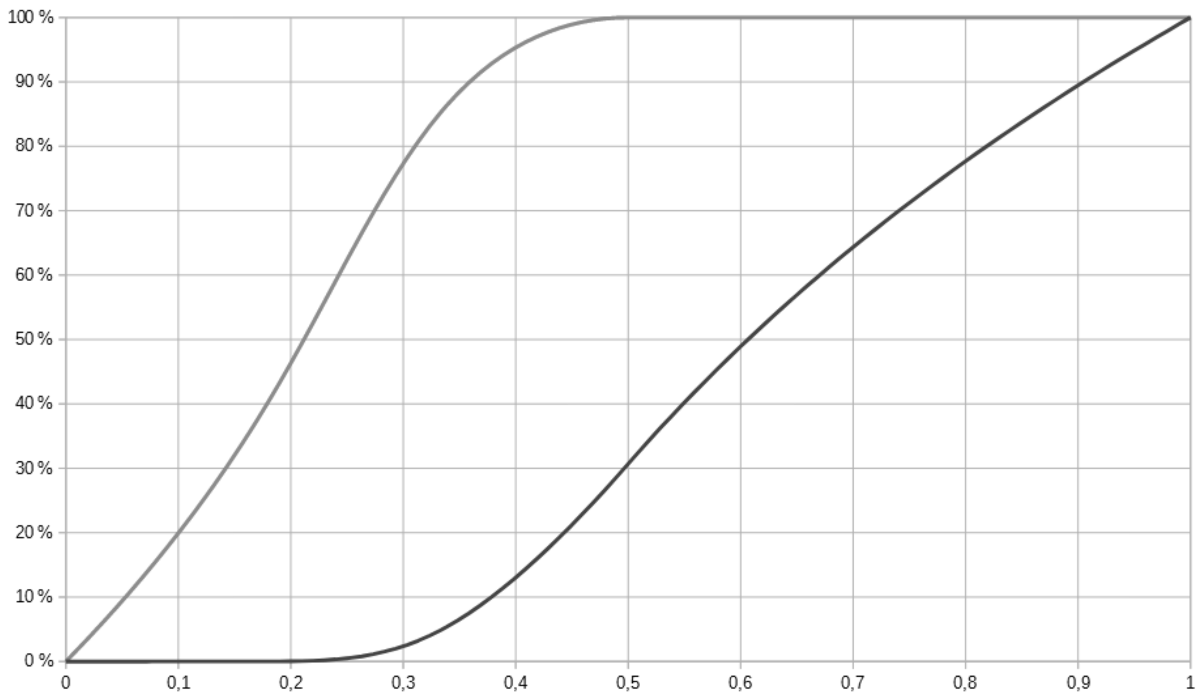

Figure 3.1: $F(\alpha)$ and $F_2(\alpha)$.

Bibliography

[1] Richard P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), 429–451, DOI: https://doi.org/10.1090/S0025-5718-99-00992-8.

[2] Richard P. Brent, *Factorization of the tenth and eleventh Fermat numbers*, Report TR-CS-96-02, Computer Sciences Laboratory, Australian National Univ., Canberra, Feb. 1996, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.6415&rep=rep1&type=pdf.

[3] Richard P. Brent and John M. Pollard, *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), 627–630, DOI: https://doi.org/10.1090/S0025-5718-1981-0606520-5.

[4] Karl Dickman, *On the Frequency of Numbers Containing Prime Factors of a Certain Relative Magnitude*, Arkiv för Mat., Astron. och Fys. 22A, 1-14, 1930.

[5] Pierre de Fermat, *Lettre à Marin Mersenne*, https://www.archive.org/stream/oeuvresdefermat942ferm#page/212/mode/2up.

[6] Donald E. Knuth and Luis Trabb Pardo, *Analysis of a simple factorization algorithm*, Theoretical Computer Science, Volume 3, Issue 3, December 1976, Pages 321–348, DOI: https://doi.org/10.1016/0304-3975(76)90050-5.

[7] A. K. Lenstra, H. W. Lenstra, M. S. Manasse and J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349, DOI: https://doi.org/10.1090/S0025-5718-1993-1182953-4.

[8] J. van de Lune and E. Wattel, *On the numerical solution of a differential-difference equation arising in analytic number theory*, Math. Comp. **23** (1969), 417–421, DOI: https://doi.org/10.1090/S0025-5718-1969-0247789-3.

[9] Michael A. Morrison and John Brillhart, *A method of factoring and the factorization of F_7*, Math. Comp. **29** (1975), 183–205, DOI: https://doi.org/10.1090/S0025-5718-1975-0371800-5.

[10] https://caramel.loria.fr/f12.txt.