

F_{12} ECM

A PROGRAM FOR FINDING
THE FACTORS OF
THE TWELFTH FERMAT NUMBER

Elliptic Curve Method and Probabilities

Yves Gallot

September 20, 2021

F₁₂ECM is free source code, under the MIT license.

Copyright (c) 2021, Yves Gallot

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Chapter 1

Fermat numbers

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 [7]. 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 [12]. 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 [4]. 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 [10]. Finally R. P. Brent completely factored F_{10} in 1995 by ECM [4].

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 [14].

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

Chapter 2

Elliptic curves

2.1 Elliptic curves over $\mathbb{Z}/p\mathbb{Z}$

An elliptic curve over a field K is a set of points in K^2 on the curve

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

for some coefficients a_1, a_2, a_3, a_4 and a_6 in K and an additional point at infinity O .

If K has characteristic different from 2 and 3 then the curve can be transformed into

$$y^2 = x^3 + ax + b.$$

The condition $\Delta = -16(4a^3 + 27b^2) \neq 0$ ensures that the curve is non-singular.

Let $E : y^2 = x^3 + ax + b$ over $K = \mathbb{Z}/p\mathbb{Z}$ and $P = (x, y)$ be a point on E . The point $Q = (x, -y)$ is on the curve: $Q = -P$ is the point opposite of P . The curve has the property that if a non-vertical line intersects it at two points P and Q , then it will also have a third point R of intersection. The addition law is defined by $P + Q = -R$. If $P = Q$, the tangent of the curve at P is considered. If the line is vertical, we have $P + -P = O$. The points on an elliptic curve and the addition form an abelian group. O is the identity of the group: we have $P + O = O + P = P$.

Hasse's theorem on elliptic curves over finite fields provides an estimate of the number of points. If $\#E$ is the order of the group of an elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$ then

$$|\#E - (p + 1)| \leq 2\sqrt{p}.$$

Given a prime $p > 3$ and any integer n such that $|n - (p + 1)| \leq 2\sqrt{p}$, there exists a and b such that $|\#E(a, b)| = n$.

To avoid the time-consuming inversion over $\mathbb{Z}/p\mathbb{Z}$, projective coordinates are preferred for computations. X, Y, Z are integers such that $x = X/Z$ and $y = Y/Z$. If $P \neq O$ then $Z \neq 0$ and the coordinates of the identity O are $(0, Y, 0)$.

$y^2 = x^3 + ax + b$ is called the short Weierstrass form but there exist some alternative representations of elliptic curves. Some of them are faster for computations.

2.2 Montgomery curves

One of F_{12} ECM representations is the Montgomery curve

$$B y^2 = x^3 + A x^2 + x,$$

where $A \neq \pm 2$ and $B \neq 0$. The Montgomery curves are a subset of elliptic curves. The order of a Montgomery curve over $\mathbb{Z}/p\mathbb{Z}$ is always divisible by 4.

The j -invariant is $256(A^2 - 3)^3/(A^2 - 4)$. Because it is independent of B , the computation of y and B is not needed for the Elliptic Curve Method.

Montgomery coordinates are the two projective coordinates (X, Z) .

2.3 Edwards curves

The other representation of F_{12} ECM is the Edwards curve

$$x^2 + y^2 = 1 + d x^2 y^2,$$

where $d \notin \{0, 1\}$. It is equivalent to a Montgomery curve:

if $e = 1 - d$, $u = (1 + y)/(1 - y)$, $v = 2u/x$ then $(1/e)v^2 = u^3 + (4/e - 2)u^2 + u$ and the point $P = (0, 1)$ is mapped to the infinity O .

However, the Montgomery curve $B v^2 = u^3 + A u^2 + u$ is birationally equivalent to a twisted Edwards curve: if $a = (A + 2)/B$, $d = (A - 2)/B$, $x = u/v$, $y = (u - 1)(u + 1)$ then $a x^2 + y^2 = 1 + d x^2 y^2$. It can be written in Edwards form if a is a square.

2.4 Torsion groups

The Tate normal form of an elliptic curve is

$$E(b, c) : y_T^2 + (1 - c)x_T y_T - b y_T = x_T^3 - b x_T^2.$$

It is obtained from the Weierstrass normal form by imposing the conditions: $P = (0, 0)$ is a torsion point, the straight line $x_T = 0$ is a tangent to E at P and $\text{ord}(P) \neq 2, 3$.

If $P = (x_0, y_0)$ then $-P = (x_0, -y_0 - (1 - c)x_0 + b)$. Starting from $P = (0, 0)$, we can calculate $2P = (b, bc)$, $3P = (c, b - c)$, $4P = ((-bc + b^2)/c^2, (b^2 c^2 + b^2 c - b^3)/c^3)$. Define $r = b/c$, $s = c^2/(b - c)$, we have $x_{4P} = r(r - 1)$, $x_{5P} = rs(s - 1)$, etc.

We can remove the $x_T y_T$ term with the transform $x = x_T$ and $y = y_T + ((1 - c)x_T - b)/2$. We get

$$E'(b, c) : y^2 = x^3 + \frac{(c - 1)^2 - 4b}{4} x^2 + \frac{b(c - 1)}{2} x + \frac{b^2}{4}.$$

2.4.1 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over \mathbb{Q}

If $c = 0$ then $(0, 0)$ is a point of order 4 on the Tate normal form. Hence the equation is

$$y^2 = x^3 + \frac{1-4b}{4}x^2 - \frac{b}{2}x + \frac{b^2}{4}.$$

The subgroup of order 4 is $\{(0, -b/2); (b, 0); (0, b/2); O\}$.

If $2P = O$ then the y -coordinate of P is zero. The x -solutions are $b, (\pm\sqrt{16b+1}-1)/8$. Define $b = v^2 - 1/16$. The two new solutions are $(\pm 4v - 1)/8$. $\{(4v - 1)/8, 0); O\}$ is a new subgroup of order 2 and $((-4v - 1)/8, 0) = ((4v - 1)/8, 0) + (b, 0)$. We have

$$y^2 = \left(x - \left(v^2 - \frac{1}{16}\right)\right) \left(x - \frac{4v-1}{8}\right) \left(x - \frac{-4v-1}{8}\right),$$

and $P = ((4v - 1)/8, 0)$ is a point of order 2.

Define $z = x - (-4v - 1)/8$, we have

$$64y^2 = 64z^3 - 4(16v^2 + 24v + 1)z^2 + 4v(4v + 1)^2z.$$

Define $A = -((4v + 1)^2 + 16v)$ and $B = 16v(4v + 1)^2$. A coordinate transform leads to the curve

$$y^2 = x^3 + Ax^2 + Bx.$$

We search for x such that $x + A + B/x = u^2$. We take $x = 4v + 1$ then the condition is

$$48v^2 - 4v = u^2.$$

The curve has genus 0 and one solution is $v = 0, u = 0$. If $v = \alpha u$ then $u = 4\alpha/(48\alpha^2 - 1)$.

Theorem 2.1. *Let $\alpha \in \mathbb{Q} \setminus \{0, \pm 1/8\}$. Define $v = 4\alpha^2/(48\alpha^2 - 1)$, $A = -((4v + 1)^2 + 16v)$, $B = 16v(4v + 1)^2$. For any prime $p > 3$ the order of $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 8 and $(4v + 1, v(4v + 1)/\alpha)$ is a point of order greater than 8.*

2.4.2 Torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(i)$

We can extend the torsion group: we search for Q such that $2Q = P = ((4v - 1)/8, 0)$.

From [8, Theorem 4.2], $(4v - 1)/8 - (v^2 - 1/16) = -(4v - 1)^2/16$ and $(4v - 1)/8 - (-4v - 1)/8 = v$ must be squares. Then $v = w^2$, the field is $\mathbb{Q}(i)$ and the torsion group is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

The equation is $48w^4 - 4w^2 = u^2$. Let $s = 2w$ and $t = u/s$, the condition is

$$3s^2 - 1 = t^2.$$

The curve has genus 0 and $s = 0, t = i$ is a solution in $\mathbb{Q}(i)$. If $z = t - i$ and $s = \alpha z$ we have $z = 2i/(3\alpha^2 - 1)$ and $w = i\alpha/(3\alpha^2 - 1)$.

Theorem 2.2. *Let $\alpha \in \mathbb{Q} \setminus \{0, \pm 1/3, \pm 1\}$. Define $v = -\alpha^2/(3\alpha^2 - 1)^2$, $A = -((4v + 1)^2 + 16v)$, $B = 16v(4v + 1)^2$. For any prime $p \equiv 1 \pmod{4}$, the order of $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 16 and $(4v + 1, -2v(4v + 1)(3\alpha^2 + 1)/\alpha)$ is a point of order greater than 16.*

By the coordinate changes $x = \sqrt{B} x_M$, $y = \sqrt{B} y_M$, we get the Montgomery form

$$\frac{1}{\sqrt{B}} y_M^2 = x_M^3 + \frac{A}{\sqrt{B}} x_M^2 + x_M.$$

The equivalence with a twisted Edwards curve is the map $x_T = x_M/y_M$, $y_T = (x_M - 1)/(x_M + 1)$,

$$(A + 2\sqrt{B})x_T^2 + y_T^2 = 1 + (A - 2\sqrt{B})x_T^2 y_T^2.$$

We have $A \pm 2\sqrt{B} = -(4w^2 + 1 \mp 4w)^2 = -(2w \mp 1)^4$. Finally if $x_E = i(2w - 1)^2 x_T$, $y_E = y_T$, we get the Edwards form $x_E^2 + y_E^2 = 1 + \left(\frac{2w+1}{2w-1}\right)^4 x_E^2 y_E^2$.

Theorem 2.3. Let $\alpha \in \mathbb{Q} \setminus \{0, \pm 1/3, \pm 1\}$. Define

$$d = \left(\frac{3\alpha^2 + 2i\alpha - 1}{3\alpha^2 - 2i\alpha - 1} \right)^4, \quad x_P = \frac{i(3\alpha^2 - 2i\alpha - 1)^2}{2\alpha(3\alpha^2 + 1)}, \quad y_P = \frac{(\alpha - i)(3\alpha - i)}{(\alpha + i)(3\alpha + i)}.$$

For any prime $p \equiv 1 \pmod{4}$, the order of $x^2 + y^2 = 1 + d x^2 y^2$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 16 and (x_P, y_P) is a point of order greater than 16.

Note that for any divisor of F_{12} we have $i \equiv 2^{2^{11}} \pmod{p}$.

2.4.3 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over \mathbb{Q}

Let $P = (0, 0)$ be a point of order 8 on the Tate normal form. We must have $5P = -3P$, this implies $x_{3P} = x_{5P}$. If $b = cr$ and $c = s(r - 1)$, we have $x_{3P} = c$ and $x_{5P} = rs(s - 1)$. The condition is

$$b = cr = (r - 1)(2r - 1).$$

$x_{4P} = r(r - 1)$. Since $2(x_{4P}, y_{4P}) = O$, $y_{4P} = 0$. The curve is birationally equivalent to

$$A = \frac{8r^4 - 16r^3 + 16r^2 - 8r + 1}{4r^2}, \quad B = (r - 1)^4, \quad y^2 = x^3 + Ax^2 + Bx.$$

The discriminant is

$$\Delta = \frac{(r - 1)^8 (2r - 1)^4 (8r^2 - 8r + 1)}{r^4}.$$

It must be a square: the condition is $u^2 = 8r^2 - 8r + 1$. The curve has genus 0 and $r = 0$, $u = 1$ is a solution. If $u - 1 = \alpha r$ we have

$$r = (8 + 2\alpha)/(8 - \alpha^2).$$

P is a point of order 8 and $Q \neq 4P$ is a point of order 2 where

$$P = (-(r - 1)r, (r - 1)(2r - 1)/2), \quad Q = \left(-\frac{\alpha^4(4 + \alpha)^2}{16(8 - \alpha^2)^2}, 0 \right).$$

We search for x such that $x + A + B/x$ is a square. We take $x = -(2r - 1)/2 - r(r - 1)$ then the condition is $(1 - 2r)^4/(4r^2(1 - 2r^2)) = u^2$ and $1 - 2r^2 = (\alpha^4 - 24\alpha^2 - 64\alpha - 64)/(\alpha^2 - 8)^2$ must be a square. The equation

$$Y^2 = X^4 - 24X^2 - 64X - 64$$

is birationally equivalent to

$$T^2 = S^3 + 4S - 16, \quad X = (T + 8)/(S - 4), \quad Y = -X^2 + 2S + 4.$$

$(4, 8)$ is a point of infinite order $T^2 = S^3 + 4S - 16$.

Theorem 2.4. Let (s, t) be a multiple of $(4, 8)$ on the curve $t^2 = s^3 + 4s - 16$. If $s \neq 4$ define

$$\alpha = \frac{t+8}{s-4}, \quad r = \frac{8+2\alpha}{8-\alpha^2}, \quad A = \frac{8r^4 - 16r^3 + 16r^2 - 8r + 1}{4r^2}, \quad B = (r-1)^4.$$

For any prime $p > 3$, if $r \not\equiv 0, 1/2, 1 \pmod{p}$ then the order of $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 16 and $(1/2 - r^2, (2r-1)^2(\alpha^2 - 2s - 4)/(4r(8-\alpha^2)))$ is a point of order greater than 16.

The equivalence with a twisted Edwards curve is the map $x = \sqrt{B}x_M, y = \sqrt{B}y_M, x_T = x_M/y_M, y_T = (x_M - 1)/(x_M + 1)$,

$$(A + 2\sqrt{B})x_T^2 + y_T^2 = 1 + (A - 2\sqrt{B})x_T^2y_T^2.$$

We have $A + 2\sqrt{B} = (2r-1)^4/(4r^2)$ and $A - 2\sqrt{B} = (8r^2 - 8r + 1)/(4r^2)$. Finally if $x_E = \frac{(2r-1)^2}{2r}x_T, y_E = y_T$, we get the Edwards form $x_E^2 + y_E^2 = 1 + \frac{8r^2 - 8r + 1}{(2r-1)^4}x_E^2y_E^2$.

Theorem 2.5. Let (s, t) be a multiple of $(4, 8)$ on the curve $t^2 = s^3 + 4s - 16$. If $s \neq 4$ define

$$\alpha = \frac{t+8}{s-4}, \quad r = \frac{8+2\alpha}{8-\alpha^2}, \quad d = \frac{8r^2 - 8r + 1}{(2r-1)^4}, \quad x_P = \frac{(8-\alpha^2)(2r^2-1)}{2s-\alpha^2+4}, \quad y_P = \frac{(2r-1)^2}{4r-3}.$$

For any prime $p > 3$, if $d \not\equiv 0, \pm 1 \pmod{p}$ then the order of $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 16 and (x_P, y_P) is a point of order greater than 16.

2.4.4 Torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}(\zeta_8)$

We can try to extend the torsion group: we search for R such that $2R = Q = \left(-\frac{\alpha^4(4+\alpha)^2}{16(8-\alpha^2)^2}, 0\right)$ on the curve

$$y^2 = x \left(x - \frac{-\alpha^4(4+\alpha)^2}{16(8-\alpha^2)^2} \right) \left(x - \frac{-16(2+\alpha)^4}{(4+\alpha)^2(8-\alpha^2)^2} \right).$$

From [8, Theorem 4.2],

$$-\frac{\alpha^4(4+\alpha)^2}{16(8-\alpha^2)^2} \quad \text{and} \quad -\frac{\alpha^4(4+\alpha)^2}{16(8-\alpha^2)^2} - \frac{-16(2+\alpha)^4}{(4+\alpha)^2(8-\alpha^2)^2} = \frac{(\alpha^2 + 4\alpha + 8)^2(\alpha^2 + 8\alpha + 8)}{16(\alpha + 4)^2(8-\alpha^2)}$$

must be squares.

If the field is $\mathbb{Q}(i)$ the condition is $x^2 + 8x + 8 = y^2(x^2 - 8)$. If $Y = y(x^2 - 8)$ and $X = x + 2$ we have $Y^2 = X^4 - 24X^2 + 16$. This curve is birationally equivalent to $T^2 = S^3 - S$ via the formulas $X = 2T/(S-1)$ and $Y = -X^2 + 8S + 4$. Then the modular curve $X_1(4, 8)$ is over $\mathbb{Q}(i)$ the elliptic curve with Cremona label 32a2. Over $\mathbb{Q}(\zeta_8)$ its Mordell-Weil group structure is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. All the points generate a singular curve.

No elliptic curve over $\mathbb{Q}(\zeta_8)$ exists with a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

2.4.5 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over \mathbb{Q}

Let $P = (0, 0)$ be a point of order 6 on the Tate normal form. We must have $4P = -2P$, this implies $x_{4P} = x_{2P}$. If $b = cr$, we have $x_{2P} = b$ and $x_{4P} = r(r-1)$. The condition is $b = r(r-1)$ and then $c = r-1$. The equation is

$$y^2 = x^3 + \frac{4-3r^2}{4}x^2 + \frac{2r^3-6r^2+4r}{4}x + \frac{r^4-2r^3+r^2}{4}$$

and the subgroup of order 6 is $\{(0, -b/2); (b, bc/2); (c, 0); (b, -bc/2); (0, b/2); O\}$.

The curve is birationally equivalent to

$$A = -\frac{3r^2-12r+8}{4}, \quad B = -(r-1)^3, \quad y^2 = x^3 + Ax^2 + Bx$$

and if $2P = O$ then the y -coordinate of P is zero. The x -solutions are $0, -A/2 \pm r\sqrt{9r^2-8r}/8$. If $r = 8/(9-\alpha^2)$ then $\sqrt{9r^2-8r} = -\alpha r$.

P is a point of order 6 and $Q \neq 3P$ is a point of order 2 where

$$P = (1-r, r(1-r)/2), \quad Q = \left(\frac{(\alpha+1)^3}{(\alpha-3)(\alpha+3)^2}, 0 \right).$$

We search for x such that $x + A + B/x$ is a square. We take $x = 1 - 9/8r$ then $\frac{r^2(10r-9)}{8(9r-8)} = \frac{9\alpha^2-1}{\alpha^2(\alpha^2-9)^2}$ must be a square. If $\alpha = \frac{9+\beta^2}{3(9-\beta^2)}$ then $P = \left(x, \frac{81\beta(\beta^2+9)(\beta^2-9)^2}{(84\beta^2-45)^2(5\beta^2-36)^2} \right)$ is a point on the curve.

Theorem 2.6. Let $\beta \in \mathbb{Q} \setminus \{\pm 3\}$. Define

$$r = \frac{18(\beta^2-9)^2}{(4\beta^2-45)(5\beta^2-36)}, \quad A = -\frac{3r^2-12r+8}{4}, \quad B = -(r-1)^3.$$

For any prime $p > 3$ the order of $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 12 and $(1-9/8r, \beta(\beta^2+9)r^2/(32(\beta^2-9)^2))$ is a point of order greater than 12.

2.4.6 Barbulescu family of Suyama-11 curves

2.4.7 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-2})$

Let $P = (0, 0)$ be a point of order 10 on the Tate normal form. We must have $6P = -4P$, this implies $x_{4P} = x_{6P}$. If $b = cr$ and $c = s(r-1)$, we have $x_{4P} = r(r-1)$ and $x_{6P} = s(r-1)(r-s)/(s-1)^2$. The condition is

$$s^2 = (s-(s-1)^2)r.$$

$x_{5P} = rs(s-1)$. Since $2(x_{5P}, y_{5P}) = O$, $y_{5P} = 0$. The curve is birationally equivalent to

$$A = -\frac{(2s^2-2s+1)(4s^4-12s^3+6s^2+2s-1)}{4(s^2-3s+1)^2}, \quad B = \frac{(s-1)^5s^5}{(s^2-3s+1)^3}, \quad y^2 = x^3 + Ax^2 + Bx.$$

The discriminant is

$$\Delta = \frac{(s-1)^{10} s^{10} (2s-1)^5 (4s^2-2s-1)}{(s^2-3s+1)^{10}}.$$

It must be a square: the condition is $u^2 = (2s-1)(4s^2-2s-1)$. Define $t = 2s-1$, we have

$$A = -\frac{(t^2+1)(t^4-2t^3-6t^2+2t+1)}{2(t^2-4t-1)^2}, \quad B = \frac{(t-1)^5(t+1)^5}{16(t^2-4t-1)^3}.$$

$$\Delta = \frac{(t^2-1)^{10} t^4 u^2}{(t^2-4t-1)^{10}}, \quad u^2 = t^3 + t^2 - t.$$

P is a point of order 10 and $Q \neq 5P$ is a point of order 2 where

$$P = \left(\frac{(t-1)(t+1)^3}{4(t^2-4t-1)}, \frac{(t-1)t(t+1)^3}{2(t^2-4t-1)^2} \right), \quad Q = \left(\frac{8t^2u + t^6 - 2t^5 - 5t^4 - 5t^2 + 2t + 1}{4(t^2-4t-1)^2}, 0 \right).$$

The modular curve $X_1(2, 10)$ is the elliptic curve with Cremona label 20a2. $u^2 = t^3 + t^2 - t$ has six rational points $(-1, \pm 1)$, $(0, 0)$, $(1, \pm 1)$, O over \mathbb{Q} and all of them generate a singular curve. Over quadratic fields, we find the trivial solution $(-2, \sqrt{-2})$. It is a point of infinite order over $\mathbb{Q}(\sqrt{-2})$.

Theorem 2.7. *Let p be a prime such that $p \equiv 1, 3 \pmod{8}$ and (t, u) be a multiple of $(-2, \sqrt{-2})$ on the curve $u^2 = t^3 + t^2 - t$ over $\mathbb{Z}/p\mathbb{Z}$. Define*

$$A = -\frac{(t^2+1)(t^4-2t^3-6t^2+2t+1)}{2(t^2-4t-1)^2}, \quad B = \frac{(t-1)^5(t+1)^5}{16(t^2-4t-1)^3}.$$

The order of $y^2 = x^3 + Ax^2 + Bx$ over $\mathbb{Z}/p\mathbb{Z}$ is divisible by 20.

Note that for any divisor of F_{12} we have $\sqrt{i} \equiv 2^{2^{10}} \pmod{p}$ and $\sqrt{-2} = \sqrt{i} + \sqrt{i}^3$.

Chapter 3

Elliptic Curve Method

3.1 Algorithm

The elliptic curve factorization method (ECM) is an extension of Pollard's $p - 1$ algorithm [13].

Pollard's $p - 1$ algorithm finds the prime factors p such that $p - 1$ is B -smooth.

If $p > 2$ and e is a multiple of $p - 1$ then by Fermat's little theorem we have $2^e \equiv 1 \pmod{p}$. For a fixed bound B , $M = \prod_{\substack{p \leq B \\ p \text{ prime}}} p^{\lfloor \log_p B \rfloor}$ is computed modulo n and finally $g = \gcd(2^M - 1, n)$.

If n is a composite integer, $p \mid n$, $p - 1$ is B -powersmooth and $q \mid n$ but $q - 1$ is not B -powersmooth then $1 < g < n$ and g is a multiple of p .

In practice, a two-stage variant of the algorithm is implemented: instead of requiring that $p - 1$ has all its factors less than B , if all but one of them are less than B_1 and the remaining factor is less than B_2 then the range $]B_1; B_2]$ can be tested more quickly. M is computed for $B = B_1$ and the second stage is $M' = \prod_{\substack{B_1 < p \leq B_2 \\ p \text{ prime}}} ((2^M)^p - 1)$. If p_n and p_{n+1} are two consecutive prime numbers then

$A^{p_{n+1}} = A^{p_n} \cdot A^{d_n}$ where $d_n = p_{n+1} - p_n$. The d_n are relatively small then the values of A^2, A^4, A^6, \dots can be precomputed. Then $(2^M)^{p_n}$ is calculated with a single multiplication.

Fermat's little theorem can be extended to a group G such that each element of G is invertible. Pollard's $p - 1$ is based on $(\mathbb{Z}/p\mathbb{Z})^\times$. A finite field of order q exists if and only if $q = p^k$, where p is a prime number and k is a positive integer. The order of \mathbb{F}_q^\times is $p^k - 1$. A factor of $p^k - 1$ is sufficient for Pollard's method and the factors of $p^k - 1$ are the cyclotomic polynomials [1]. But in practice this algorithm is slower than ECM except $p + 1$.

Since the points on an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ forms an abelian group, Pollard's algorithm can be extended to this set. Because of Hasse's theorem, ECM is a " $p + 1 - a$ " algorithm. a is unknown and $a \in [-2\sqrt{p}, 2\sqrt{p}]$. With different curves, we can expect that a is a random number in a large range.

If \mathcal{P} is the probability that $p + 1 - a$ is B -smooth, with n curves the likelihood of success is $\mathcal{P}_n = 1 - (1 - \mathcal{P})^n$. If $\mathcal{P} \ll 1$ and $n \sim 1/\mathcal{P}$ then $\mathcal{P}_n = 1 - e^{-1} \approx 63.2\%$.

If \mathcal{P} is 1% with Pollard's $p - 1$, the likelihood of success with ECM is 63.2% with 100 curves and 99.99% with 1000 curves.

3.2 Largest prime factors

Dickman [6] proved that the probability that a large integer n has no prime factor exceeding n^α approaches a limit $F(\alpha)$ as $n \rightarrow \infty$, where

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

Let $u = 1/\alpha$. $F(1/u) = 1 - \int_{1/u}^1 F\left(\frac{t}{1-t}\right) \frac{dt}{t}$. If $t' = 1/t$ we have $\frac{t}{1-t} = \frac{1}{t'-1}$ and $\frac{dt}{t} = -\frac{dt'}{t'}$ then $F(1/u) = 1 - \int_1^u F\left(\frac{1}{t'-1}\right) \frac{dt'}{t'}$. 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 [11]. If $1 \leq u < 2$, $\rho(u) = 1 - \int_1^u \frac{dt}{t} = 1 - \log u$.

Knuth and Trabb Pardo [9] 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 $n \rightarrow \infty$, where $F_0(\alpha) = 0$ for all α by convention and for $k \geq 1$

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

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 .

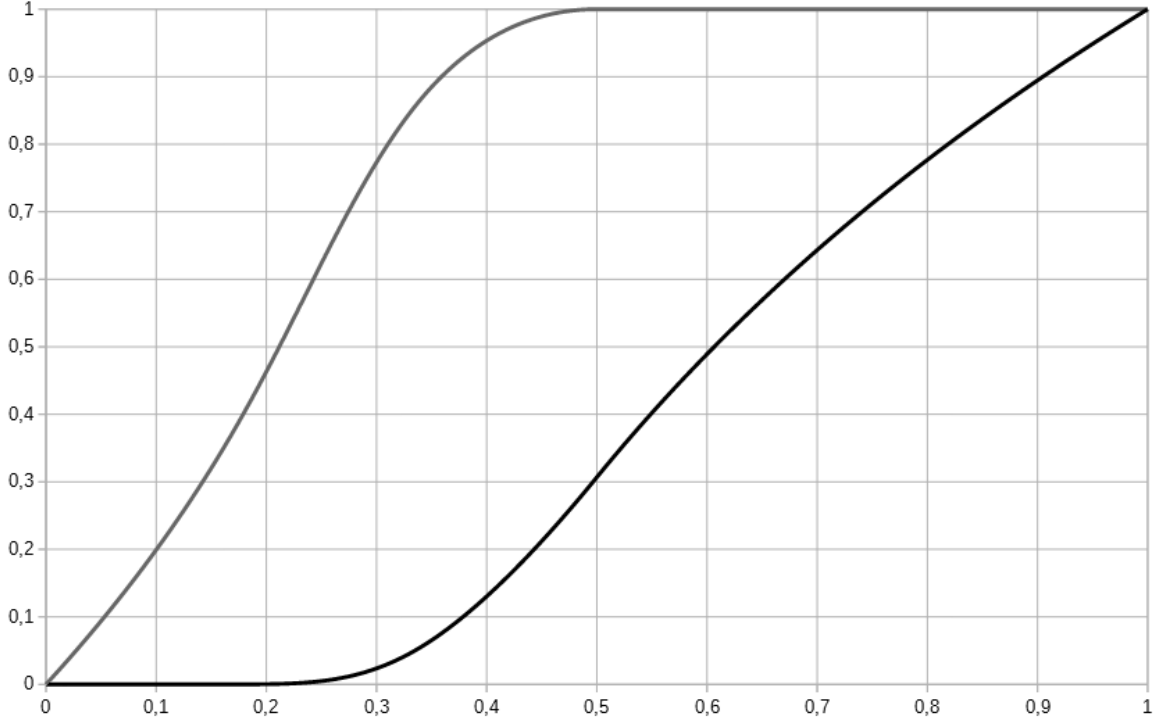


Figure 3.1: $F(\alpha)$ and $F_2(\alpha)$.

The sizes of the two largest prime factors are correlated: let $n \approx 10^{100}$ and $p \approx 10^{30}$ be the largest prime factor of n . We have $\alpha = 0.3$ and $F(\alpha) \approx 0.02365$. However $F_2(0.0131) \approx 0.02365$ and $n^{0.0131} \approx 20.4$. The probability that the largest prime factor of n is at most 10^{30} is equal to the probability that its second largest prime factor is at most 20.4. But this result cannot be used to set B_1 and B_2 . If the largest prime factor of n is a 30-digit prime, the second largest prime factor is certainly larger than 20.4 (see subsection 3.3.1).

3.3 Probabilities

Let B_1 and B_2 be the bounds of a two-stage ECM, n be the number of curves and p be a prime factor of F_{12} . $\mathcal{P}(B_1, B_2, n, p)$ is the chance for ECM to find p .

If ECM finds p , because of Hasse's theorem we have $\#E \approx p$. $F(\alpha)$ is the probability that the largest prime factor of $\#E$ is at most p^α . One must have $B_2 \gtrsim p^\alpha$. Let $P(B_2) = F(\log B_2 / \log p)$. If the second largest prime factor is larger than B_1 then the likelihood of success for ECM is $\mathcal{P}(B_2, B_2, n, p) = 1 - (1 - P(B_2))^n$.

Note that $\lim_{n \rightarrow \infty} (1 - x/n)^n = e^{-x}$. Hence, if $P(B_2) \ll 1$ we have $\mathcal{P}(B_2, B_2, n, p) \approx 1 - e^{-P(B_2)n}$. If $\mathcal{P}^*(B_2, B_2, n, p) = 1 - e^{-1} \approx 63.2\%$ is chosen as an acceptable likelihood of success, we have the condition $P(B_2)n = 1$.

The number of operations per curve is about $\log(B_1 \#) \sim B_1$ for stage 1 and about $B_2 / \log B_2$ for stage 2 if $B_1 \ll B_2$. Hence, computation time is proportional to $(B_1 + B_2 / \log B_2) n$. If $B_1 = K \cdot B_2 / \log B_2$

then $(B_2/\log B_2) n$ must be minimal.

Finally the conditions are B_2 is the maximum point of $P(B_2) \log B_2 / B_2$ and $n = 1/P(B_2)$.

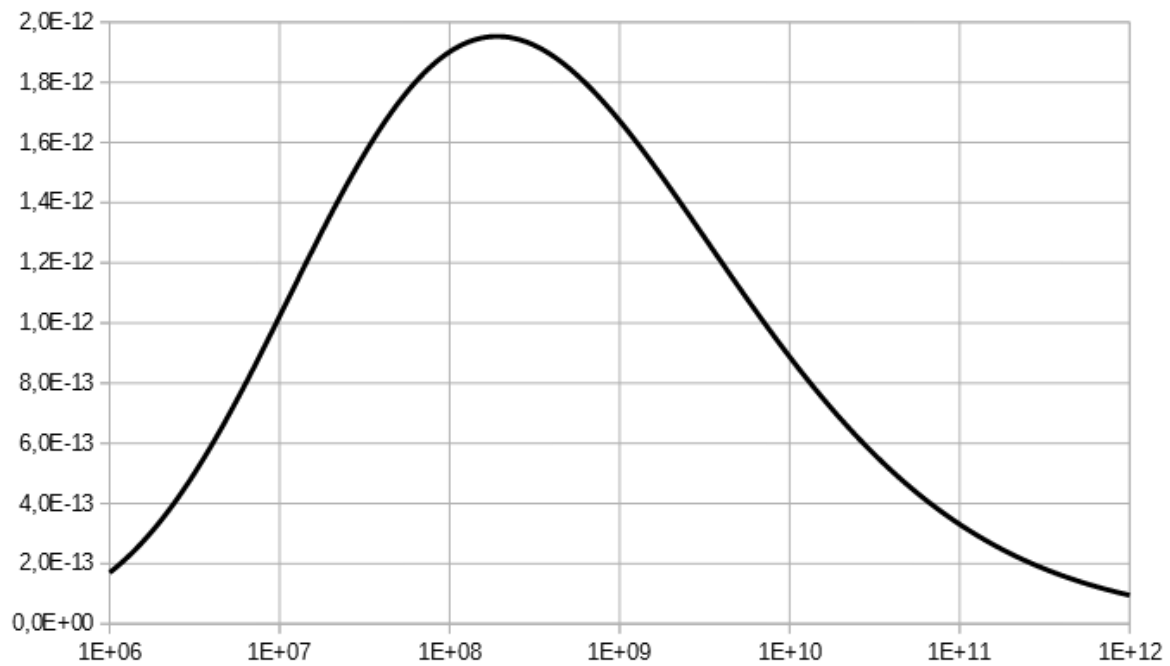


Figure 3.2: $P(B_2) \log B_2 / B_2$ for $p = 5 \cdot 10^{49}$.

Let $p = 5 \cdot 10^{49}$ be an average 50-digit prime. $P(B_2) \log B_2 / B_2$ is maximum at $B_2 \approx 1,9 \cdot 10^8$. We have $P(B_2) \approx 1,95 \cdot 10^{-5}$ and $n \approx 51400$.

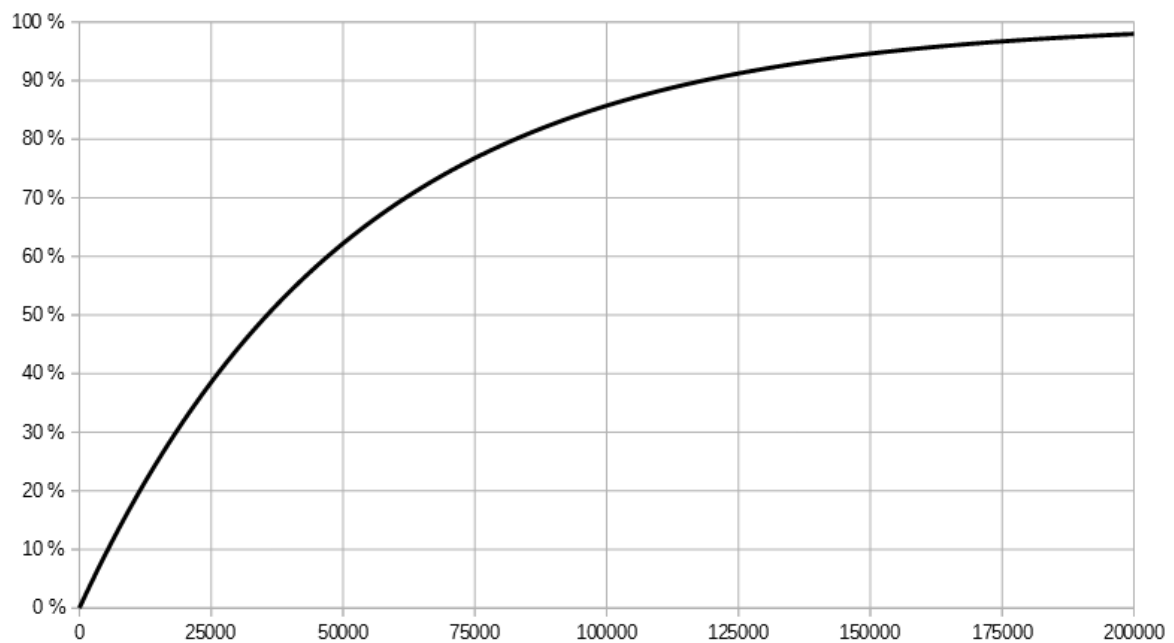


Figure 3.3: Probability of success for n curves, $p = 5 \cdot 10^{49}$ and $B_2 = 1,9 \cdot 10^8$.

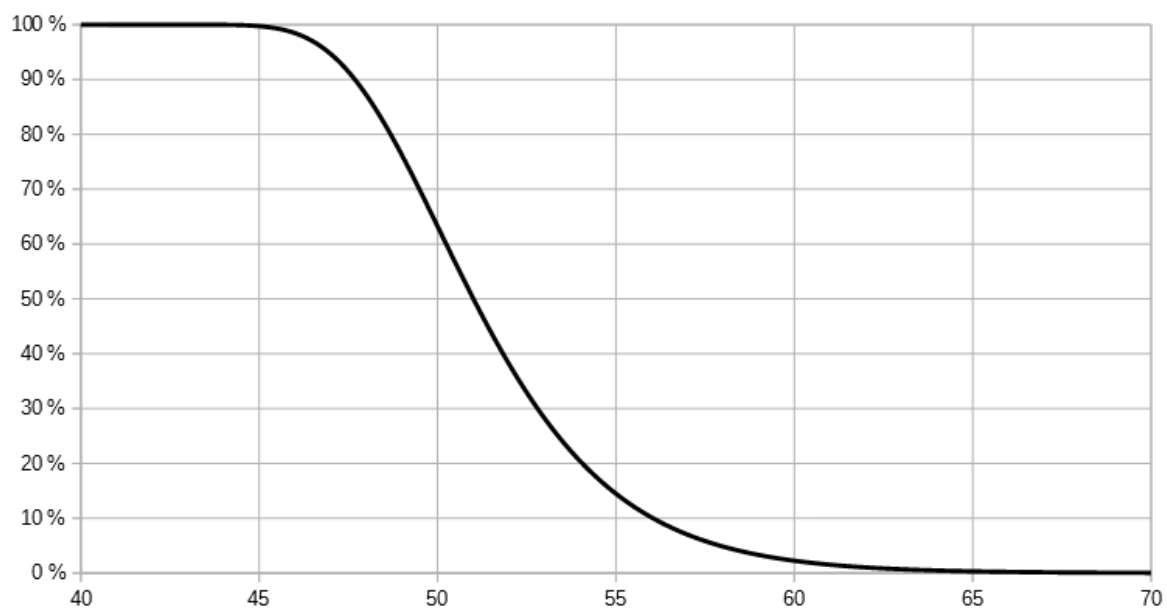


Figure 3.4: Chance to find a x -digit factor, $B_2 = 190 \cdot 10^6$ and $n = 51400$.

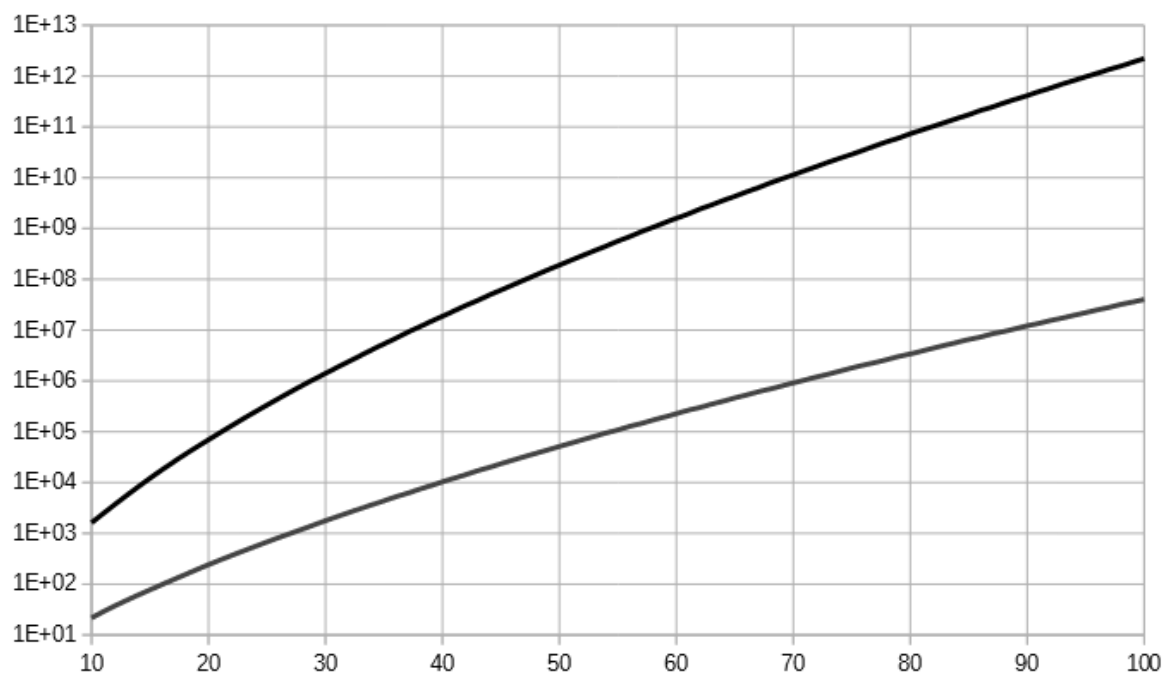


Figure 3.5: Optimal B_2 and number of curves as a function of the number of digits.

3.3.1 The ratio B_2/B_1

The generalized Dickman function F_2 cannot be used to compute B_1 as a function of B_2 (see section 3.2). Let $G(\alpha, \beta)$ be the probability that the largest prime factor of a number n is at most n^α and that the second largest prime factor of n is at most n^β . Following Knuth and Trabb Pardo [9] heuristic derivation, we have:

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

If $\beta \leq \alpha$ we have $G(\alpha, \beta) = F(\beta) + \int_\beta^\alpha \rho\left(\frac{1-t}{\beta}\right) \frac{dt}{t}$ and $G(1/u, 1/v) = \rho(v) + \int_{1/v}^{1/u} \rho((1-t)v) \frac{dt}{t}$.

Let $t' = (1-t)v + 1$. We have $t = (v+1-t')/v$, $dt = -dt'/v$ and $\frac{dt}{t} = -\frac{dt'}{v+1-t'}$. Hence,

$$G(1/u, 1/v) = \sigma(u, v) = \rho(v) + \int_{v+1-v/u}^v \frac{\rho(t-1) dt}{v+1-t}.$$

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

$P(B_2) = F(\log B_2 / \log p)$ can be replaced with $P(B_2, B_1) = G(\log B_2 / \log p, \log B_1 / \log p)$. Now the likelihood of success for ECM is $\mathcal{P}(B_2, B_1, n, p) = 1 - (1 - P(B_2, B_1))^n$.

The computation time is proportional to $(K \cdot B_1 + B_2 / \log B_2) n$, where $K \approx 5.6$ depends on the implementation. Hence, $(B_2; B_1)$ must be the maximum point of the function

$$\frac{P(B_2, B_1)}{K \cdot B_1 + B_2 / \log B_2}.$$

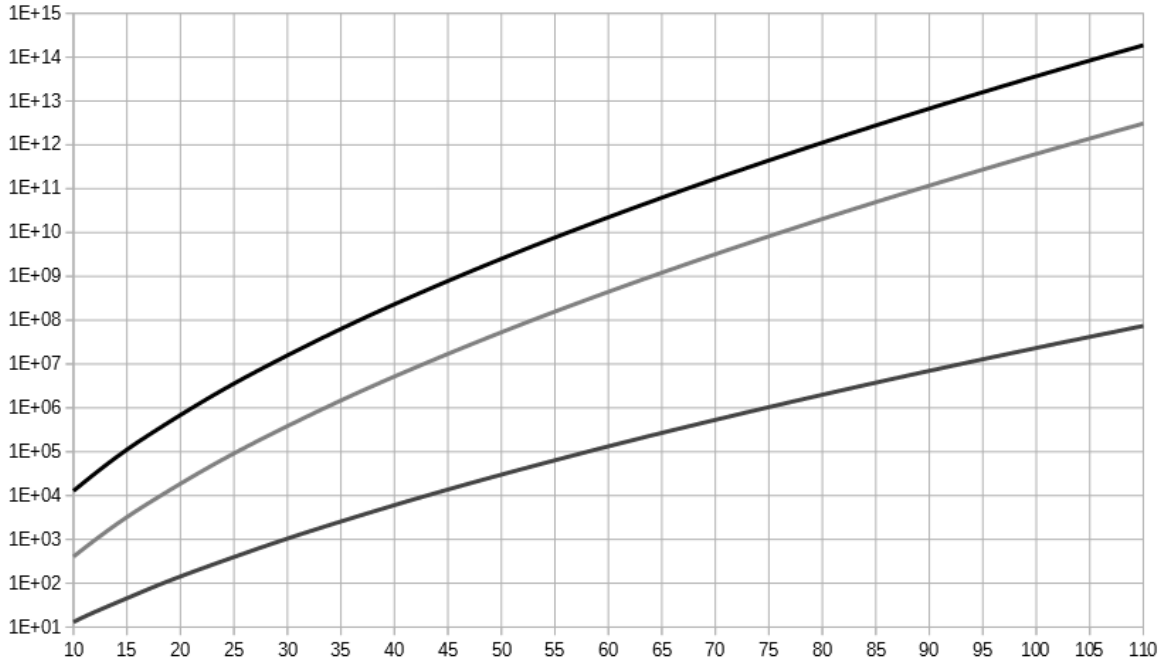


Figure 3.6: Optimal B_2, B_1 and number of curves as a function of the number of digits.

3.3.2 Smoothness of the number of points of elliptic curves over $\mathbb{Z}/p\mathbb{Z}$

All families of elliptic curves are not equivalent for ECM. The *quality* depends on the proportion of primes for which $\#E$ is B -smooth.

Let $\mathcal{E}(p)$ be a family of curve over $\mathbb{Z}/p\mathbb{Z}$ and $R(p) = [p-2\sqrt{p}; p+2\sqrt{p}]$. If $E \in \mathcal{E}(p)$ then $\#E \in R(p)$. In that range we can count the proportion \mathcal{P} of curves such that $\#E$ is B -smooth. This value is not equal to the proportion of B -smooth integers in the range (because almost all elliptic curves have surjective Galois image at all primes). But it is conjectured that there exists a factor $f(\mathcal{E}, p, B)$ such that if $n = f(\mathcal{E}, p, B)p$ then \mathcal{P} is equal to the proportion of B -smooth integers in $R(n)$ [2, § 5]. It is also conjectured that $f(\mathcal{E}, p, B)$ converges uniformly to $f(\mathcal{E}, p)$ when B go to infinity. We have

$$\text{Prob}(\#E \text{ is } B\text{-smooth} \mid \#E \in \mathcal{E}(p)) \approx \text{Prob}(n \text{ is } B\text{-smooth} \mid n \sim f(\mathcal{E}, p)p).$$

Let q be a prime number, we define the average valuation at q of $\mathcal{E}(p)$ by

$$\overline{\text{val}}_q(\mathcal{E}(p)) = \sum_{n \geq 1} n \cdot \text{Prob}(\text{val}_q(\#E) = n \mid E \in \mathcal{E}(p)).$$

The average valuation of an integer is

$$\overline{\text{val}}_q(\mathbb{N}) = \sum_{n \geq 1} n \cdot \text{Prob}(\text{val}_q(m) = n \mid m \in \mathbb{N}) = \sum_{n \geq 1} n \cdot \frac{q^{-n}}{q-1} = \frac{1}{q-1}.$$

Hence

$$f(\mathcal{E}, p) = \prod_{q \text{ prime}} \frac{q^{\overline{\text{val}}_q(\mathbb{N})}}{q^{\overline{\text{val}}_q(\mathcal{E}(p))}} = \prod_{q \text{ prime}} q^{1/(q-1) - \overline{\text{val}}_q(\mathcal{E}(p))}.$$

Note that $\overline{\text{val}}_q(\mathcal{E}(p))$ depends on the prime factors of $p-1$. For example, let $p > 1728$, $\mathcal{E}_j(p)$ be the curves over $\mathbb{Z}/p\mathbb{Z}$:

$$y^2 = \begin{cases} x^3 - 1 & \text{if } j = 0, \\ x^3 - x & \text{if } j = 1728, \\ x^3 - 3cx + 2c^2 & c = j/(j-1728) \text{ otherwise.} \end{cases}$$

Define

$$P_q(n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \text{Prob}(\text{val}_q(\mathcal{E}_j(p_i)) = n, \mid p_i \not\equiv 1 \pmod{2q}),$$

$$Q_q(n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \text{Prob}(\text{val}_q(\mathcal{E}_j(p_i)) = n, \mid p_i \equiv 1 \pmod{2q}).$$

We have $P_2(0) = Q_2(0) = 1/3$, $P_2(1) = Q_2(1) = 1/4$, $P_2(2) = 1/6$, $Q_2(2) = 5/24$ and if $n \geq 3$ then $P_2(n) = 1/2^n$ and $Q_2(n) = (2^n - 2)/4^n$. For $q \geq 3$ we have $P_q(0) = 1 - 1/(q-1)$, $Q_q(0) = 1 - q/(q^2 - 1)$ and if $n \geq 1$ then $P_q(n) = 1/q^n$ and $Q_q(n) = (q^n - 1)/q^{2n}$.

If $p \not\equiv 1 \pmod{4}$ then $\overline{\text{val}}_2(\mathcal{E}_j(p)) = 1/4 + 1/3 + \sum_{n \geq 3} n/2^n = 19/12$ and if $p \equiv 1 \pmod{4}$ then $\overline{\text{val}}_2(\mathcal{E}_j(p)) = 1/4 + 5/12 + \sum_{n \geq 3} n(2^{n-1} - 1)/2^{2n-1} = 55/36$.

For $q \geq 3$ if $p \not\equiv 1 \pmod{q}$ then $\overline{\text{val}}_q(\mathcal{E}_j(p)) = \sum_{n \geq 1} n/q^n = q/(q-1)^2$ and if $p \equiv 1 \pmod{q}$ then $\overline{\text{val}}_q(\mathcal{E}_j(p)) = \sum_{n \geq 1} n(q^n - 1)/q^{2n} = q(q^2 + q + 1)/(q^2 - 1)^2$.

We define

$$\overline{\text{val}}_q(\mathcal{E}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \overline{\text{val}}_q(\mathcal{E}(p_i)).$$

If $R_q(n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \text{Prob}(\text{val}_q(\mathcal{E}_j(p_i)) = n)$, for $n \geq 1$, we have $R_q(n) = \frac{(q-1)q^n-1}{(q-1)q^{2n}}$. Then $\overline{\text{val}}_q(\mathcal{E}_j) = \sum_{n \geq 1} n R_q(n) = \frac{q(q^3+q^2-2q-1)}{(q-1)(q^2-1)^2}$.

The first values are $\overline{\text{val}}_2(\mathcal{E}_j) = 14/9$, $\overline{\text{val}}_3(\mathcal{E}_j) = 87/128$ and $\overline{\text{val}}_5(\mathcal{E}_j) = 695/2304$.

The cardinality of an elliptic curve has more chances of being smooth than a random integer of the same size: $f(\mathcal{E}_j) = \prod_{q \text{ prime}} q^{1/(q-1)-\overline{\text{val}}_q(\mathcal{E}_j)} \approx 0.44397$.

Note that $f(\mathcal{E}_j | p \equiv 1 \pmod{4}) = 2^{1/36} \cdot f(\mathcal{E}_j) \approx 0.45260$.

We can compute $f(\mathcal{E}_d)$ for the Edwards curves $\mathcal{E}_d : x^2 + y^2 = 1 + d x^2 y^2$. We have $P_2(1) = Q_2(1) = 0$, $P_2(2) = Q_2(2) = 1/4$ and if $n \geq 3$ then $P_2(n) = 3/2^n$ and $Q_2(n) = (5 \cdot 2^n - 24)/4^n$. Then $R_2(1) = 0$, $R_2(2) = 1/4$ and if $n \geq 3$ then $R_2(n) = (2^n - 3)/4^{n-1}$ and $\overline{\text{val}}_2(\mathcal{E}_d) = 11/3$. Since $\overline{\text{val}}_2(\mathcal{E}_j) = 14/9$ and for $q \geq 3$, $\overline{\text{val}}_q(\mathcal{E}_d) = \overline{\text{val}}_q(\mathcal{E}_j)$ we have $f(\mathcal{E}_d) = 2^{14/9-11/3} \cdot f(\mathcal{E}_j) \approx 0.102765$.

Let $\mathcal{E}_{4 \times 4}$ be the Edwards curves defined by Theorem 2.3. If $n < 4$ then $Q_2(n) = 0$ else $Q_2(n) = 3(2^n - 8)/4^{n-1}$. We have $\overline{\text{val}}_2(\mathcal{E}_{4 \times 4}) = 16/3$. Then $f(\mathcal{E}_{4 \times 4}) = 2^{14/9-16/3} \cdot f(\mathcal{E}_j) \approx 0.032369$.

Let $\mathcal{E}_{2 \times 8}$ be the Edwards curves defined by Theorem 2.5. If $n < 4$ then $R_2(n) = 0$ else $R_2(n) = 3(2^n - 8)/4^{n-1}$. We also have $\overline{\text{val}}_2(\mathcal{E}_{2 \times 8}) = 16/3$ and $f(\mathcal{E}_{2 \times 8}) = f(\mathcal{E}_{4 \times 4})$.

Let $\mathcal{E}_{2 \times 6}$ be the Edwards curves defined by Theorem 2.6. If $n < 2$ then $R_2(n) = 0$ else $R_2(n) = 3(2^n - 2)/4^n$ then $\overline{\text{val}}_2(\mathcal{E}_{2 \times 6}) = 10/3$. $R_3(0) = 0$ and for $n > 0$ we have $R_3(n) = (3^{n+1} - 4)/9^n$ and then $\overline{\text{val}}_3(\mathcal{E}_{2 \times 6}) = 27/16$. Finally $f(\mathcal{E}_{2 \times 6}) = 2^{14/9-10/3} \cdot 3^{87/128-27/16} \cdot f(\mathcal{E}_j) \approx 0.042790$.

Let $\mathcal{E}_{2 \times 10}$ be the curves defined by Theorem 2.7 and $S_q(n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \text{Prob}(\text{val}_q(\mathcal{E}_{2 \times 10}(p_i)) = n, |p_i \equiv 1 \pmod{8})$. We have $S_2(0) = S_2(1) = 0$, $S_2(2) = 1/2$, $S_2(3) = 3/16$, $S_2(4) = 5/32$ and for $n \geq 5$, $S_2(n) = 3(2^n - 8)/4^n$ then $\overline{\text{val}}_2(\mathcal{E}_{2 \times 10}) = 151/48$. $S_5(1) = 73/96$ and for $n \geq 2$, $S_5(n) = (4 \cdot 5^{n-1} - 1)/(4 \cdot 25^{n-1})$ then $\overline{\text{val}}_5(\mathcal{E}_{2 \times 10}) = 2999/2304$. Finally $f(\mathcal{E}_{2 \times 10}) = 2^{14/9-151/48} \cdot 5^{695/2304-2999/2304} \cdot f(\mathcal{E}_j) \approx 0.029489$.

In summary, if $g_T = f(\mathcal{E}_T)/f(\mathcal{E}_j)$, we have

g_j	g_d	$g_{4 \times 4}$	$g_{2 \times 8}$	$g_{2 \times 6}$	$g_{2 \times 10}$
1	0.231469	0.072908	0.072908	0.096380	0.066422

3.3.3 ECM and F_{12}

The present status is

$$F_{12} = P_6 \cdot P_8 \cdot P_8 \cdot P_{12} \cdot P_{16} \cdot P_{54} \cdot C_{1133}.$$

The size of the next prime factor is unknown and we can't set B_1 and B_2 as a function of its number of digits. The number of curves needed to find a new factor is unknown but it is a variable that will increase over time. We can set the size of the searched prime factor as a function of the index of the curve.

The number of digits, B_1 and B_2 can be computed as a function of the number of curves with subsection 3.3.1. However the value of p must be replaced by $n = f(\mathcal{E} \mid p \equiv 1 \pmod{2^{14}})p$. The results of subsection 3.3.2 are slightly modified by the condition $p \equiv 1 \pmod{2^{14}}$.

If $h_T = f(\mathcal{E}_T \mid p \equiv 1 \pmod{2^{14}}) / f(\mathcal{E}_j)$, we have

$$\begin{aligned}
h_j &= 2^{14/9-55/36} &= 2^{1/36}, \\
h_d &= 2^{14/9-91/24} &= 2^{-161/72}, \\
h_{4 \times 4} &= 2^{14/9-31/6} &= 2^{-65/18}, \\
h_{2 \times 8} &= 2^{14/9-139/24} &= 2^{-305/72}, \\
h_{2 \times 6} &= 2^{14/9-22/7} \cdot 3^{87/128-27/16} &= 2^{-100/63} \cdot 3^{-129/128}, \\
h_{2 \times 10} &= 2^{14/9-151/48} \cdot 5^{695/2304-2999/2304} &= 2^{-229/144} \cdot 5^{-1}.
\end{aligned}$$

In summary,

h_j	h_d	$h_{4 \times 4}$	$h_{2 \times 8}$	$h_{2 \times 6}$	$h_{2 \times 10}$
1.019441	0.212258	0.081837	0.053064	0.109983	0.066422

It is interesting to calculate the ratio h_T/g_T :

h_j/g_j	h_d/g_d	$h_{4 \times 4}/g_{4 \times 4}$	$h_{2 \times 8}/g_{2 \times 8}$	$h_{2 \times 6}/g_{2 \times 6}$	$h_{2 \times 10}/g_{2 \times 10}$
1.019441	0.917004	1.122462	0.727827	1.141140	1

$\mathcal{E}_{4 \times 4}$ and $\mathcal{E}_{2 \times 8}$ are equivalent if the factors of p are unknown but if p is a factor F_{12} is then $\mathcal{E}_{2 \times 8}$ is clearly more efficient.

Now we don't check n curves with a fixed set of parameters but the i^{th} curve is tested with different settings $B_1(i)$ and $B_2(i)$.

However subsection 3.3.1 can be the starting point. For integer values of $\log p$, $n(\lfloor \log p \rfloor)$ is calculated. If n curves are tested for each value of $\lfloor \log p \rfloor$, the probability of success is larger than $1 - e^{-1}$ because $n(\lfloor \log p \rfloor - 1), n(\lfloor \log p \rfloor - 2), \dots$ have already been tested. If $n(\lfloor \log p \rfloor) - n(\lfloor \log p \rfloor - 1)$ curves are tested then the probability is smaller than $1 - e^{-1}$ because $B_1(\lfloor \log p \rfloor - 1) < B_1(\lfloor \log p \rfloor)$ and $B_2(\lfloor \log p \rfloor - 1) < B_2(\lfloor \log p \rfloor)$.

We search for λ such that if $n'(\lfloor \log p \rfloor) = n(\lfloor \log p \rfloor) - \lambda \cdot n(\lfloor \log p \rfloor - 1)$ then the probability remains constant and equal to $1 - e^{-1}$. $\lambda \approx 0.92$ is suitable. By inverting this function, for each index an estimate of $\log p$ is computed and then $B_1(\log p)$ and $B_2(\log p)$.

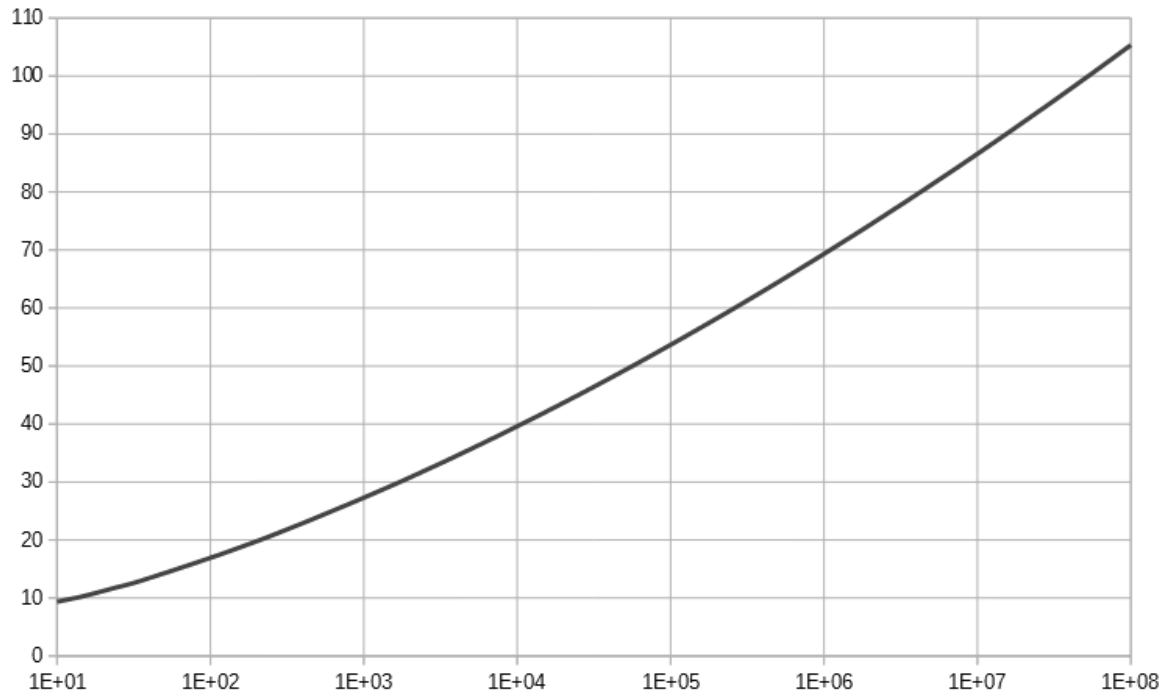


Figure 3.7: Expected number of digits as a function of the index of the curve.

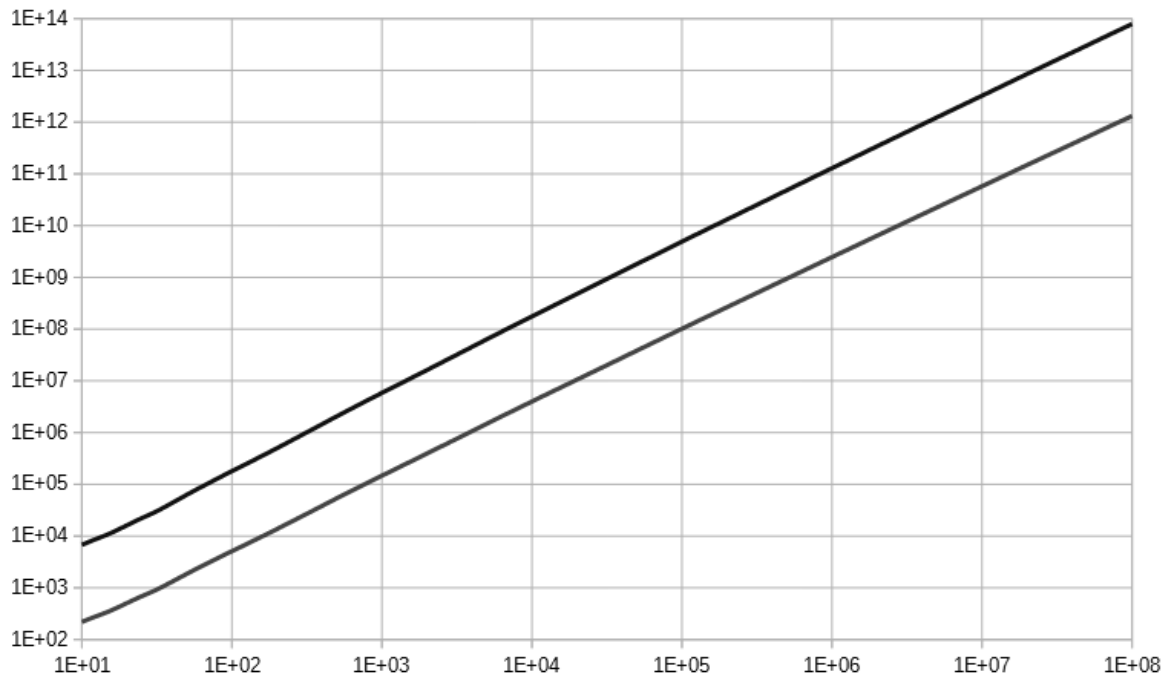


Figure 3.8: B_2 and B_1 as a function of the index of the curve.

$\log B_2 = f(\log i)$ where i is the i^{th} curve is close to a linear function. The error of the estimate $B_2 = 400 i^{\sqrt{2}}$ is less than 5% for $10^4 \leq i \leq 10^8$. The ratio of $B_2 / B_1 = 26 + 1.8 \log i$ is always slightly larger than the optimal value. Finally we have $\log p \approx (3 + 1.3 \log i)^{5/3}$.

The following parameters are applied: let i be the i^{th} curve and d be the expected number of digits of the prime factor, then

$$B_2 = 400 i^{\sqrt{2}},$$

$$B_1 = B_2 / (26 + 1.8 \log i),$$

$$d = (1.8 + 0.79 \log i)^{5/3}.$$

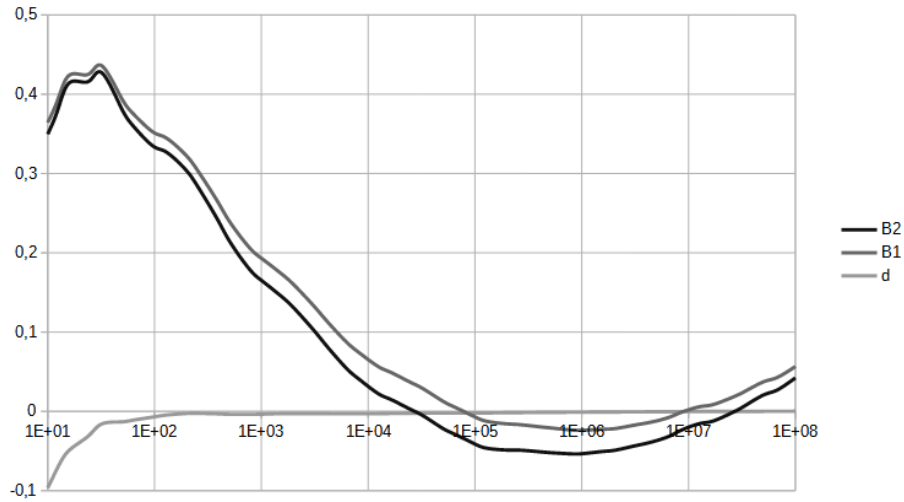


Figure 3.9: Relative error with applied parameters as a function of the index of the curve.

3.3.4 Test of the probabilistic model

Chapter 4

Implementation

Bibliography

- [1] Eric Bach and Jeffrey Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), 201–219, DOI: <https://doi.org/10.1090/S0025-5718-1989-0947467-1>.
- [2] Razvan Barbulescu and Sudarshan Shinde, *A classification of ECM-friendly families using modular curves*, intégré à la thèse de doctorat de Sudarshan Shinde, Sorbonne Université, 10 juillet 2020, <https://hal.archives-ouvertes.fr/hal-01822144v2>.
- [3] 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>.
- [4] 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>.
- [5] 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>.
- [6] 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.
- [7] Pierre de Fermat, *Lettre à Marin Mersenne*, <https://www.archive.org/stream/oeuvresdeferma942ferm#page/212/mode/2up>.
- [8] Anthony W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.
- [9] 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](https://doi.org/10.1016/0304-3975(76)90050-5).
- [10] 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>.
- [11] 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>.
- [12] 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>.

- [13] J. M. Pollard, *Theorems on factorization and primality testing*, Mathematical Proceedings of the Cambridge Philosophical Society, Volume 76, Issue 3, November 1974, pp. 521 - 528, DOI: <https://doi.org/10.1017/S0305004100049252>.
- [14] <https://caramel.loria.fr/f12.txt>.