GMP-ECM: yet another implementation of the Elliptic Curve Method

(or how to find a 40-digit prime factor within $2 \cdot 10^{11}$ modular multiplications)

Paul Zimmermann

Inria Lorraine, Nancy, France

Abstract

This talk will describe how to combine Brent-Suyama's improvement and fast polynomial multipoint evaluation into the improved standard continuation of the Elliptic Curve Method. Some estimations of the success probability improvement, based on computer simulations, will be described. Those ideas were implemented in GMP-ECM, which is freely available at `http://www.loria.fr/ zimmerma/records/ecmnet.html`. Some nice factors found by GMP-ECM, as well as a comparison with other programs will be given.

ECM variants

Step 1: $K_1 \frac{B_1}{\log 2}$ modular multiplications

• affine coordinates: $K_1 = 11/2$ plus $3B_1/2$ inversions

• homogeneous coord.: $K_1 = 11$, or $K_1 = 10$ plus $\frac{B_1}{\log B_1}$ inversions

Step 2: $K_2 \frac{B_2}{\log B_2}$ modular multiplications, $1/2 \le K_2 \le 3$

• improved standard continuation (Montgomery 1987): check all primes up to B_2

• birthday paradox continuation (Brent 1985): check $\frac{B_2}{\log B_2}$ "random" numbers (with possibly several prime factors)

Efficiency of an ECM program

- algorithm used (success probability given step 1 and 2 limits)
- implementation (# of modular multiplications for given limits)
- underlying arithmetic (multiplication mod N, inversions)

Brent-Suyama's improvement

In step 2, instead of computing $(s-t)Q$, compute $(s^e - t^e)Q$ with $x^{2e} - y^{2e}$ having a lot of divisors.

e	1	2	3	6	12	18	24	30	60	90	120
$d(2e)$	2	3	4	6	8	9	10	12	16	18	20

If $2e = 2^{e_1} 3^{e_2} 5^{e_3} \cdots$, the success probability is conjectured to be in $(e_1+1)(e_2+1)(e_3+1)\cdots = d(2e)$.

Only used for birthday paradox continuation so far.

Details of GMP-ECM implementation

Uses Montgomery's form with group order divisible by 12:

$$by^2z = x^3 + ax^2z + xz^2$$

and starting point given from σ like Brent, Crandall, Woltman.

Step 1: homogeneous coord. with Montgomery's PRAC algorithm.

Step 2: improved standard continuation with affine coordinates using an idea of Gerhard Niklasch, Brent-Suyama's improvement, and fast multipoint polynomial evaluation

Details of GMP-ECM step 2

Choose m, K, D such that $mKD > B_2$, $K = 2^k$, $D = 6d$, $\phi(D) < 2K$.

A. Compute $S = \{i^e \cdot Q, 0 < i < D, i \equiv 1 \bmod 6, \gcd(i, D) = 1\}$

B. Compute $F(x) = \prod_{a \in S}(x - a)$

C. Compute $R(x) = \mathrm{Quo}(x^{2K-2}, F(x))$ using P.M.'s Recip algorithm

D. [m times] Compute $T_l = \{[(lK + j)D]^e Q, 0 \le j < K\}$

E. [m times] Compute $G_l(x) = \prod_{b \in T_l}(x - b)$

F. $[m - 1$ times$]$ Get $G_l(x) = G_{l-1}(x)G_l(x) \bmod F(x)$ using $R(x)$

Complexity analysis

Steps B and E cost each $M(K/2) + 2M(K/4) + 4M(K/8) + \cdots$ modular multiplications, i.e. $M(K)$ for $M(n) = O(n^{\frac{\log 2}{\log 3}})$.

Step C costs $3(M(\frac{K}{2}) + M(\frac{K}{4}) + \cdots)$ i.e. $3/2M(K)$ for Karatsuba.

Step F costs $3M(K)$.

The total is therefore $(4m - 1/2)M(K)$ for Karatsuba.

Estimation of the success probability

For a prime factor of 40 digits (4668127 random tries):

B_1	B_2	e	hits	muls	curves	tot. muls	speedup
3e6	3e8	1	870+0	5.29e7	5366	2.84e11	1
3e6	8.0e8	12	1089+235	5.44e7	3526	1.92e11	1.48
3e6	8.0e8	18	1089+250	5.54e7	3486	1.93e11	1.47
3e6	8.0e8	30	1089+303	5.74e7	3354	1.93e11	1.47

With Dickson polynomials:

e	12	18	30
hits	+258	+268	+321

Number of modular multiplications

B_1	$m \times K \times D = B_2$	x^e	step 1 (K_1)	step 2 (K_2)
1e6	$6 \times 2048 \times 19110 = 2.3e8$	x^{12}	1.3e7 (9.0)	6.3e6 (0.52)
3e6	$5 \times 4096 \times 39270 = 8e8$	x^{30}	3.9e7 (9.0)	1.8e7 (0.47)
11e6	$6 \times 8192 \times 79170 = 3.9e9$	x^{60}	1.4e8 (9.1)	6.9e7 (0.39)
36e6	$6 \times 16384 \times 159390 = 1.6e10$	x^{120}	4.7e8 (9.1)	2.3e8 (0.35)

Underlying arithmetic (155 digits)

On 366Mhz PC/Linux: 39070093 modular multiplications: mul(248)+mod(289)=537s (step1=601s), 18348603 modular multiplications: mul(116)+mod(136)=252s (step2=383s)

On 195Mhz SGI R10000: 39070093 modular multiplications: mul(204)+mod(217)=421s (step1=484s), 18348603 modular multiplications: mul(96)+mod(102)=197s (step2=389s)

On 500Mhz Alpha 21264: 39070093 modular multiplications: mul(45)+mod(52)=97s (step1=117s), 18348603 modular multiplications: mul(21)+mod(24)=45s (step2=101s)

Nice factors found so far

p49=7612068647760892587567279171698469451260170146501 M. Quercia

p48=552044274610152692854436856453869841728449076617 S. Wagstaff

p45=106124644646629262293671146508062271116589169 P. Leyland

p37=8745075387933004096394385246656921347 T. Granlund

p37b=1408323592065265621229603282020508687 T. Charron

p36=108418776698113814016172668034087889 P. Zimmermann

factor	from	B_1	g_1	g_1/B_1	x^e
p49	$6^{250}+1$ c126	3,000,000	37,762,327	13	x^1
p48	$6^{726}+1$ c125	1,000,000	$< 10^8$	< 100	x^1
p45	Cullen(423) c129	3,000,000	1795043	0.60	x^1
p37	$10^{359}-1$ c312	3,224,000	2,731,091,911	847	x^5
p37b	$3^{509}-1$ c182	3,000,000	29,973,883,579	9991	x^3
p36	$2^{2074}+1$ c267	3,000,000	9,173,740,909	3058	x^6

Comparison with other programs

Machine: 500Mhz Alpha 21264 `leon5.medicis.polytechnique.fr`

On 500Mhz Alpha 21264, 155 digits, $B_1 = 3,000,000$:

	variant	B2	time
Magma V2.4-6	BP	?	614s
Pari/GP 2.0.14	SC	3.3e8	1411s
GMP-ECM 4a	SC+Kara	8e8 x^{30}	218s

Remark: for Pari/GP, extrapolated from $B_1 = 43000$ (64 curves performed at a time).

On 195Mhz R10000, 120 digits, $B_1 = 8,000,000$:

	variant	B2	time
GMP-ECM 4a	SC+Kara	2.6e9 x^{60}	1020+
ecmfft	B.P.+FFT	2.7e10	1824s

On 450Mhz PC, $2^{727} - 1$ c219, $B_1 = 3,000,000$:

	variant	B2	time
GMP-ECM 4a	SC+Kara	8e8 x^{30}	
mprime	SC	3e8	208s

References

Bosma, W., Lenstra, A.K. (1995). *An Implementation of the Elliptic Curve Integer Factorization Method.* In: W. Bosma, A. van der Poorten (eds), Computational Algebra and Number Theory. (Proceedings of CANT, Sydney, 1992.) Dordrecht: Kluwer.

Brent, R.P. (1999). *Factorization of the tenth Fermat number.* Mathematics of Computation 68 (225), pages 429–451.

Montgomery, P.L. (1992). *Evaluating Recurrences of Form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas Chains.*

Montgomery, P.L. (1992). *An FFT Extension of the Elliptic Curve Method of Factorization.* PhD dissertation, UCLA.