ECM -- Then and Now

- Joppe W. Bos, EPFL, Lausanne, Switzerland
- Thorsten Kleinjung, EPFL
- Arjen K. Lenstra, EPFL
- Peter L. Montgomery, Microsoft Research, Redmond, USA

- Presented at Workshop on Elliptic Curve Computations, Redmond, October 22, 2010.

Abstract

This talk has two parts. The first part lists the major factorization algorithms when the Elliptic Curve Method (ECM) was discovered in 1985, stressing similarities between ECM and $P \pm 1$. The last part describes the recent discoveries of six large Mersenne factors using ECM on a network of PlayStations.

What is Factorization?

- Express a given positive integer as a product of smaller ones. Repeat if possible.

- Example: $2010 = 10 \cdot 201 = 5 \cdot 2 \cdot 201$

$$= 5 \cdot 2 \cdot 3 \cdot 67$$

- The integers 2, 3, 5, 67 cannot be further decomposed and are **prime**.

Uniqueness of Factorization

- We might find the factors in a different order
- $2010 = 2 \cdot 1005 = 2 \cdot 3 \cdot 335 = 2 \cdot 3 \cdot 5 \cdot 67$.
- Output (2, 3, 5, 67) is same as earlier (5, 2, 3, 67) except for order.

Importance of Factorization

- Used to be primarily academic.
- Now RSA cryptosystem can be broken if factorization is easy.
- Interest in records -- how high can we go?

Major Factoring Methods when Elliptic Curve Method (ECM) was Born (1985)

- Assume we are factoring a composite integer N, with (unknown) prime factor $p > 2$.
- Assume N is not a perfect power.
- Some factoring methods take time depending primarily on product N.
- Others (including ECM) take time depending primarily on prime p.

Pre-1985 Methods Whose Time Depends Primarily on Size of *N*.

- Continued Fraction (Mike Morrison
- and John Brillhart)
- Quadratic Sieve (Carl Pomerance)

· Each finds several pairs (x, y) where $x^2 \equiv y \pmod{N}$ and y is smooth.

- Multiply congruences to get squares on both sides.

- Linear algebra mod 2 selects congruences to multiply.

Quadratic Sieve Example

$N = 1919 \quad f(x) = x^2 - N$

$f(15) = -1694 = -2 \cdot 7 \cdot 11^2$

- $f(27) = -1190 = -2 \cdot 5 \cdot 7 \cdot 17$
- $f(29) = -1078 = -2 \cdot 7^2 \cdot 11$
- $f(37) = -550 = -2 \cdot 5^2 \cdot 11$
- $f(43) = -70 = -2 \cdot 5 \cdot 7$
- $f(44) = 17$
- $f(48) = 385 = 5 \cdot 7 \cdot 11$

- Seven congruences found. Each right side is a product of powers of $-1, 2, 5, 7, 11, 17$.

Quadratic Sieve Example (cont.)

- Seven congruences on five primes and −1.
- Each right side is product of powers of −1, 2, 5, 7, 11, 17.

- One way to get a square on the right is
- $(-1078)(-550) = 770^2$.

- $770^2 = (-1078)(-550) = f(29)\, f(37) \equiv 29^2 \cdot 37^2 = 1073^2$
- $770^2 \equiv 1073^2 \pmod{N}$

GCD(770 − 1073, N) = GCD(−303, 1919) = 101 factors N.

Pre-1985 Methods Whose Time Depends Primarily on *p*

- Trial division

- Pollard Rho (John Pollard)
- P – 1 (John Pollard)
- P + 1 (Hugh Williams)

- Bottom three do some computations mod *N*, hoping to encounter a number divisible by *p* but not by *N*.
- Take a GCD.

P – 1 Method for Factoring *N*

- 1) Select an exponent $e > 0$ divisible by all prime powers below a bound B_1.
- 2) Select base b_0, where $\gcd(b_0, N) = 1$.
- 3) Form $b_1 = b_0^e \bmod N$.
- By Fermat's little theorem, if $(p - 1)$ divides e,
- then $b_1 \equiv 1 \pmod p$.
- 4) Test whether $\text{GCD}(b_1 - 1, N) > 1$.

$N = 2^{977} - 1$

- Mersenne number
- Part of Cunningham project
- Full factorization N = P6 · P7 · P19 · P32 · P62 · P171
  - P6 = 867577
  - P7 = 1813313
  - P19 =20696553747195772 73
  - P32=49858990580788430540126900788 41
  - P62 has 62 digits
  - P171 has 171 digits

P – 1 Tackles $N = 2^{977} - 1$

- $P6 - 1 = 2^3 \cdot 3 \cdot 37 \cdot 977$
- $P7 - 1 = 2^6 \cdot 29 \cdot 977$
- $P19 - 1 = 2^3 \cdot 977 \cdot 3469 \cdot 166471 \cdot 458533$
- $P32 - 1 = 2^3 \cdot 5 \cdot 13 \cdot 19 \cdot 977 \cdot 1231 \cdot 4643 \cdot 74941 \cdot 1045397 \cdot 11535449$
- With B1 = 1000, P – 1 finds P6 and P7 together since both have largest prime 977.
- If $B1 \geq 500000$, then P –1 finds P19.
- P32 – 1 has prime exceeding 10^7.

Step 2 of P−1

- Divide N by any factors found so far.
- Repeat GCD test until $\mathrm{GCD}(b_1 - 1, N) = 1$.

- Choose new bound $B_2 > B_1$.

- Hope for a prime q between B_1 and B_2 such that $(\mathbf{Z}/p\mathbf{Z})^*$ group order $(p - 1)$ divides qe.
- Then $b_1^q \equiv (b_0^e)^q \equiv 1 \pmod{p}$.

Step 2 of P−1

- Want to compare pairs of powers of b_1.
- Choose two disjoint sets S_1, S_2 of subscripts such that any q in range divides some $i - j$ with $i \in S_1$ and $j \in S_2$. Example: $S_1 = \{1, 3, 7, 9\}$ and $S_2 = \{10, 20, 30, 40, 50\}$ when $B_2 = 50$.
- Compute all $b_1^i \bmod N$ and all $b_1^j \bmod N$.
- Test each GCD($b_1^i - b_1^j$, N).

Improved Step 2

- Better to test GCD($b_1^i + b_1^{-i} - b_1^j - b_1^{-j}$, N).
- $b_1^i + b_1^{-i} - b_1^j - b_1^{-j} = b_1^{-i}(b_1^{i+j} - 1)(b_1^{i-j} - 1)$
- Each q should divide some $i+j$
  or some $i-j$, not necessarily $i - j$.

Step 2 of P−1 Finds P32

- Largest factors of P32 – 1 were 1045397 and 11535449.
- Output b_1 of step 1 has multiplicative mod P32 order dividing q = 11535449 if B_1 > 1.1 million.
- Two exponents on b_1 differ by multiple of q if $B_2 > q$.

- Found by Richard Brent in 1984.
- Was P – 1 record for several years.

Combining GCD's

- Instead of testing many GCD(x_i, N) with the same N, multiply the x_i mod N and do one GCD with N.

- If an intermediate product is zero mod N, backtrack.

- All but one GCD cost only a multiply mod N.

Lucas Functions V_n

- Integer polynomial degree $|n|$
- Formal identity: $V_n(X + 1/X) = X^n + X^{-n}$
- $V_0(Y) = 2$
- $V_1(Y) = Y$
- $V_2(Y) = Y^2 - 2$
- $V_3(Y) = Y^3 - 3Y$

Computing Lucas Functions

- $V_{m+n}(Y) = V_m(Y)\, V_n(Y) - V_{m-n}(Y)$
- $V_{mn}(Y) = V_m(V_n(Y))$
- Can compute $V_n(Y)$ mod N with O(log n) operations mod N.

P + 1 Method for Factoring N

- Select Y_0 and exponent e.
- Form $Y_1 = V_e(Y_0) \bmod N$.
- Test GCD($Y_1 - 2$, N) .

- Step 2 tests GCD($V_i(Y_1) - V_j(Y_1)$, N) for many i, j
- Like P – 1 step 2 if $Y_1 = b_1 + 1/b_1$.

P + 1 Analysis

- Fix Y_0 mod N. Let X_0 be a root of quadratic $X^2 - Y_0 X + 1$ in GF(p^2). Other root is $1/X_0$.

- X_0^p is a root – must equal one of the above.

- $Y_1 - 2 = V_e(Y_0) - 2 = V_e(X_0 + 1/X_0) - 2$
  $= X_0^e + X_0^{-e} - 2$
  $\equiv (X_0^e - 1)^2 / X_0^e$

More P + 1 Analysis

- If $X_0^p \equiv X_0 \pmod{p}$, then X_0 has multiplicative order dividing $p - 1$ so $X_0 \in \mathrm{GF}(p)$.
- We are lucky if $p-1$ divides our e (whence the order of X_0 divides e).
- Disguised P−1 run with $b_0 = X_0$.

- When $X_0^p \equiv 1/X_0 \bmod p$, we are are similarly lucky if $p+1$ divides e.
- Half the time we are lucky if $p - 1$ divides e.
- Half the time we are lucky if $p+1$ divides e.

P+1 Tackles $2^{977} - 1$

- $P6 + 1 = 2 \cdot 17^2 \cdot 19 \cdot 79$
- $P7 + 1 = 2 \cdot 3 \cdot 31 \cdot 9749$
- P19 + 1, P32 + 1, P62 + 1, P171 + 1
  have large factors.

With lucky Y_0, P + 1 finds P6 with B1 = 300.
Step 2 of P+1 might find P7.

P19, P32 found when running disguised P−1.

Primality Proof (Pocklington)

- Given N, try to prove that N is prime.
- If we can find an integer x such that
- 1) $x^{N-1} \equiv 1 \pmod{N}$;
- 2) If q is prime and q divides $N-1$ then $x^{(N-1)/q} \not\equiv 1 \pmod{N}$;

then N is prime.

The proof shows x has multiplicative order $N-1$ mod N.

Example: Show 67 is Prime

- $67 - 1 = 2 \cdot 3 \cdot 11$
- Assume we know 2, 3, 11 are prime.

- $x = 0$ and $x = 1$ fail. But $x = 2$ works.

- $2^{66} \equiv 1$ $\quad$ $2^{33} \equiv 66$
- $2^{22} \equiv 37$ $\quad$ $2^{6} \equiv 64$

- Since 37 has order 3 in $(\mathbf{Z}/67\mathbf{Z})^*$, group order must be divisible by 3, for example.

Lucas Sequences

- a, b distinct complex roots of $\lambda^2 - P\lambda + Q = 0$ where P, Q are integers.

- For $n \geq 0$, define $U_n = (a^n - b^n) / (a - b)$.

- All U_n are integers, easily computed.

Lucas Primality Proof

- Suppose $N + 1 = \text{product\_}j\ q_j^{\beta\_j}$ where the q_j are distinct primes. If there is a Lucas sequence U_n with

- 1) GCD($2Q(P^2 - 4Q)$, N) = 1;
- 2) GCD($U^{(N+1)/q\_j,}$ N) = 1 for all j;
- 3) $U_{N+1} \equiv 0 \pmod{N}$;

then N is prime.

Combined Primality Tests

- Pocklington primality proof needs full factorization of $N - 1$.
- Lucas primality proof needs full factorization of $N + 1$.
- Fancier pre-ECM primality proofs allow mixing factors of $N - 1$ and $N + 1$.
- Combined factorization size $N^{1/3}$ needed.

Questions From Early 1980's

- The P ± 1 algorithms require one of $p \pm 1$ be smooth. Can we
- Mix $p + 1$ and $p - 1$ factors?

- Find P ± 2 algorithms?

- Find a step 3 which allows a prime beyond B_2?

Elliptic Curves to the Rescue

- Field K in which $6 \neq 0$.
- (E) Weierstrass equation $y^2 = x^3 + ax + b$
  where $a, b \in K$ and $-4\,a^3 - 27\,b^2 \neq 0$.
- Points on (E) form abelian group when we include infinity.
- When K = GF(p) is a prime field, the group order
- is $p + 1 - t$ for some integer t with $t < \text{sqrt}(4p)$. (Hasse)
- Group order varies with a and b. Many more possibilities than just $p-1$ and $p+1$.

Group Addition Law

- To add two general points (x_1, y_1) and (x_2, y_2) on the curve (E), find third point (x_3, y_3) on (E) where line through (x_1, y_1) and (x_2, y_2) intersects curve.
- Use tangent line while adding a point to itself.
- Output $(x_3, -y_3)$, the negative of (x_3, y_3).
- No square root. Arithmetic valid over commutative ring unless a division fails (while computing a slope).

Example Group Addition

- Add (0, 2) and (−2, 0) on $y^2 = x^3 - 2x + 4$.
- Line $y = x + 2$ intersects curve where
  $(x + 2)^2 = x^3 - 2x + 4$.
- Sum of roots is 1^2. Two roots are 0 and −2.
- Third root is 3. Sum of points is (3, −5).

Elliptic Curve Method for Factoring N (Hendrik W. Lenstra Jr., 1985)

1) Pretend N is prime. Find a curve (E) over ($\mathbf{Z}$/N$\mathbf{Z}$) and an initial point P_0 on (E).
2) Select B_1 and e.
3) Form $P_1 = [e]P_0$, the sum of e copies of P_0.
4) If P_1 computation attempts to divide by a nonzero, non-invertible, element of ($\mathbf{Z}$/$N\mathbf{Z}$)*, we are successful. If P_1 is infinite, reduce e. If P_1 is finite, proceed to 1) above (new curve).

Step 2 of ECM

- H. Lenstra did not specify a Step 2 for ECM.
- Richard Brent suggested a Step 2 based on the birthday paradox.
- Montgomery adapted his P ± 1 Step 2.

- Assume group order of (E) over GF(p) divides qe where q is prime, between B_1 and B_2.

- $P_1 = [e]P_0$ has order q.

- Compare x-coordinates $x([i]P_1)$ and $x([j]P_1)$ for many i, j.

- Need each potential q to divide some nonzero $i \pm j$.

Cunningham Tables

- Factors of $b^n \pm 1$ for b = 2, 3, 5, 6, 7, 10, 11, 12 and moderate n.
- Maintained by Samuel S. Wagstaff Jr.

- http://homes.cerias.purdue.edu/~ssw/cun/

- "Page" with recently found factors issued every few months.

- Demonstrate new algorithms by contributing to this table.

Algorithm Usage Frequencies

	Page 30 Spring, 1985	Page 31 Summer, 1985	Page 116 Summer, 2010
CFRAC	3	0	0
ECM	10	22.5*	4
NFS	0	0	28
P – 1	35	9	0
P + 1	4	9	0
Pollard Rho	10	6	0
Quadratic Sieve	0	35	0
Other	0	0.5	0
Totals	62	82	32

- *= Fractional counts when same factorization found multiple ways.

Algorithm Report Cards (Wagstaff)

- From cover letter for p. 29: (Wagstaff):
- *``During the past few months I have received new factors somewhat more slowly than in the previous few years.''*
- Two pages later:
- *``It is clear from Page 31 that the multiple polynomial quadratic sieve (mp-qs) and the elliptic curve method (ecm) have enjoyed great success lately. Eighteen of the 28 factorizations on the "wanted" lists of Update # 3 have been done. Silverman did six of the Ten Most Wanted and 7 of the Eighteen More Wanted. Montgomery did four of the More Wanted. Atkin and Rickert did two Most and two More Wanted numbers. Some of these numbers were factored twice by different methods. The first "holes" of many tables were filled in. …''*

Post-1985 Hardware Trends Affecting ECM Performance

- 64-bit hardware arithmetic, including
  64 x 64 -> 128-bit integer product.
- Multicore
- Large shared memories.
  - 1985 -- 8 megabyte SPARC workstation;
  - 2010 -- 8 gigabyte x86 workstation.
- "Free" cycles widely available.

Allocating Today's Hardware

- Step 1 is low memory. Multiple curves can run on separate cores.
- Most of the memory can go to Step 2, on a few core.
- Large memories enable fast polynomial algorithms, such as evaluating a degree-*m* polynomial at *n* points.

Choice of Coordinate System

- Weierstrass $y^2 = x^3 + ax + b$ needs an inversion over $(\mathbf{Z}/n\mathbf{Z})$ for each elliptic curve addition.

- Montgomery coordinates $By^2 = x^3 + Ax^2 + x$ avoid these inversions and avoid computing y-coordinates. But we need x-coordinates of P, Q, $P - Q$ to get that of $P + Q$.

- Twisted Edwards coordinates $ax^2 + y^2 = 1 + dx^2 y^2$ (due to Daniel Bernstein et al) cut costs, esp. doubling cost.

ECM Finishes $2^{977} - 1$

- P−1 algorithm found P6, P7, P19, P32 factors of $2^{977} - 1$ but not P62 or P171.
- November, 2007 – After many trials, Bruce Dodson finds a lucky curve using Zimmermann's **gmpecm**. Group order over GF(P62):
  - $2^3 \cdot 3 \cdot 47 \cdot 127 \cdot 6073 \cdot 44963 \cdot 1510933 \cdot$
  - $4035517 \cdot 25660097 \cdot 40014391 \cdot 43782913 \cdot$
  - 2222473077901
- All but one factor of group order is below B_1 = 110 million. Last is near 2222 billion.
- Cofactor P171 is prime.

Massive Search for Mersenne Factors

- 2007 Mersenne number M1039 = $2^{1039} - 1$
  factored by SNFS
- 2009 RSA-768 factored by GNFS
- It's almost time to run SNFS on another Mersenne number, larger than M1039. Desire
  - In Cunningham table range (exponent < 1200);
  - Enough ECM work done to avoid "easy" factors.

SIMD Architectures

- Single Instruction, Multiple Data
  - Same operation applied to different data on different elements;
  - Like soldiers marching in formation;
  - Avoid branches unless all elements branch the same way;
  - Example: SSE (Streaming SIMD Extensions) on recent X86 systems.
  - A 128-bit entity might represent a 4-tuple of 32-bit items.
  - SIMD instructions act componentwise, such as adding two
  - 4-tuples.

SONY Playstation 3

- Uses Cell processor
- Each has six Synergistic Processing Elements (SPEs) available to users.
- Each SPE has 128 128-bit registers.
- View each 128-bit entity as a 4-tuple of 32-bit items.
- A 4-tuple has 32 bits of data foreach of four curves.
- Many SIMD instructions do same operation on each component of two input tuples.

Playstations and ECM

- B_1 = 3 billion. Exponent *e* chosen offline.
- Each Playstation runs 24 curves at a time.
- 215 Playstations at EPFL Switzerland run 5160 instances of Step 1 of ECM on same *N*.
- Step 2 run elsewhere.

Large Mersenne Factors Found

- M Old $2^M - 1$ status New status
- 1051 c310 p63·c248
- 1073 c281 p66·p215
- 1139 c313 p68·p246
- 1163 c318 p73·p246
- 1181 c291 p73·p218
- 1187 c266 p63·p204
- January-October, 2010. The two p73 are records.