Differential addition chains

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
Danmarks Tekniske Universitet
Alfred P. Sloan Foundation

Motivating problem:
Given elliptic curve E,
integer n, and point P on E,
compute nP on E
as quickly as possible.

Many variations of problem.
Some applications reuse one n
for many P's.
Some applications don't.
Some applications use secret n;
must not leak n through timing.
Some applications use public n.
Etc.

1987 Montgomery:

Focus on large-characteristic curves $y^2 = x^3 + ax^2 + x$ with small $a \in \{6, 10, 14, \ldots\}$.

Use pair (x, z) to represent point $P = (x/z, \ldots)$.

Computing $Q, R, Q - R \mapsto Q + R$ takes 6 mults.
Only 5 mults if $Q - R$ has small denominator.
Only 4 mults if $Q - R$ has small numerator and small denominator.
Only 4 mults if $Q = R$.

Given n, write $P \mapsto nP$

as composition of additions

$Q, R, Q - R \mapsto Q + R$.

e.g. $n = 10$: compute

P, P, $0 \mapsto 2P$ with 4 mults;

$2P$, $P, P \mapsto 3P$ with 6 mults;

$3P, 2P, P \mapsto 5P$ with 6 mults;

$5P, 5P$, $0 \mapsto 10P$ with 4 mults.

Overall 20 mults for $P \mapsto 10P$.

Only 18 mults

if P has small denominator.

Only 16 mults

if P has small numerator

and small denominator.

$0, P, 2P, 3P, 5P, 10P$ is a
differential addition chain
starting from $0, P$:
each subsequent term
is $Q + R$ for some
$Q, R, Q - R$ already in chain.

$0, 1, 2, 3, 5, 10$ is a
differential addition chain
starting from $0, 1$.

Question: Given n, how to find
short differential addition chain
starting from $0, 1$ and ending n?
Variations: measure shortness
by mults, CPU cycles, etc.

The binary method:

obtain $n, n+1$ from

$\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1$ using

one addition with difference 1,

one addition with difference 0.

e.g.

$13P, 13P, 0 \mapsto 26P$ with 4 mults;

$14P, 13P, P \mapsto 27P$ with 5 mults,

if P has small denominator.

Overall 9 mults

for each bit of n,

if P has small denominator.

1992 Montgomery,
1996 Bleichenbacher,
2001 Tsuruoka: Can do better!

Experiments for average 128-bit n find length ≈ 1.533 per bit, instead of 2 per bit.
Lower bound ≈ 1.440 per bit.

Count mults instead of length: ≈ 8.885 per bit, instead of 9 per bit.

Disadvantages: harder to find; no uniform structure; harder to avoid leaking n through timing.

Two-dimensional question:
Given m, n, how to find
short differential addition chain
starting from the vectors
$(0, 0), (1, 0), (0, 1), (1, -1)$
and ending (m, n)?

Motivating problem:
Given elliptic curve E,
integers m, n,
and points $P, Q, P - Q$,
compute $mP + nQ$ on E
as quickly as possible.

For average 128-bit exponents,
small $P, Q, P - Q$ denominators:

dim	method	mults per bit	unif
2	easy binary	19.000	yes
2	Schoenmakers	17.250	no
2	Akishita	14.250	no
2	new binary	14.000	yes
2	Montgomery	10.261	no
2	new ext gcd	9.918	no
1	easy binary	9.000	yes
1	standard	8.885	no
	Fibonacci case	8.643	

Easy dim-2 binary chain:

$$
\begin{tikzcd}
(0,0) \arrow[d, dashed] & (0,1) \arrow[d] & (1,0) \arrow[dll, dashed] \arrow[dl] \arrow[d, Rightarrow] \arrow[dr] & (1,-1) \\
(1,0) \arrow[d, dashed] & (1,1) \arrow[rr, bend left] \arrow[dl, dashed] \arrow[d, Rightarrow] \arrow[dr] \arrow[drr] & (2,0) \arrow[d] & (2,1) \arrow[d] \\
(2,1) \arrow[d] & (2,2) \arrow[dl] \arrow[d, Rightarrow] \arrow[dr] \arrow[drr] & (3,1) \arrow[d] & (3,2) \arrow[d] \\
(4,3) \arrow[d] & (4,4) \arrow[d] & (5,3) \arrow[d] & (5,4) \arrow[dlll] \arrow[dll] \arrow[dl] \arrow[d, Rightarrow] \\
(9,7) \arrow[d, Rightarrow] \arrow[dr] \arrow[drr] \arrow[drrr] & (9,8) \arrow[d] & (10,7) \arrow[d] & (10,8) \arrow[d] \\
(18,14) & (18,15) & (19,14) & (19,15)
\end{tikzcd}
$$

New dim-2 binary chain:

$$
\begin{tikzcd}
(0,0) & (1,0) \arrow[dl] \arrow[d, Rightarrow] \arrow[dr] & (0,1) \arrow[dll] & (1,-1) \\
(1,1) \arrow[rr, bend left=80] \arrow[d] \arrow[dr, Rightarrow] \arrow[drr] & (2,0) \arrow[dl] & (2,1) \arrow[d] & \\
(3,1) \arrow[d] & (2,2) \arrow[dl] \arrow[d, Rightarrow] \arrow[dr] & (3,2) \arrow[d] & \\
(5,3) \arrow[d] & (4,4) \arrow[dl] \arrow[dr] & (5,4) \arrow[dl, Rightarrow] \arrow[d] & \\
(9,7) \arrow[d] \arrow[dr, Rightarrow] \arrow[drr] & (10,8) \arrow[dl] & (9,8) \arrow[d] & \\
(19,15) & (18,14) & (18,15) &
\end{tikzcd}
$$

Line in easy binary chain has (a, b), $(a, b+1)$, $(a+1, b)$, $(a+1, b+1)$. Obtain next line by double-add-add-add.

New observation: can omit $(\text{even}, \text{odd})$ or $(\text{odd}, \text{even})$, chosen recursively so that next line can be obtained by double-add-add.
14 mults if $P, Q, P-Q$ have small denominators.

Intermediate results: 2000 Schoenmakers, 2001 Akishita.

How to do better than binary?
Don't worry about uniformity.

Critical idea for dim 1:
Build chain $0, 1, \ldots, n$
by choosing $r \approx n(\sqrt{5} - 1)/2$
and building chain
$0, 1, \ldots, r, n - r, n$.
Try many r's, keep best.

Some further choices here:
could build $\{r, n - r, n\}$
from $\{r, n - 2r, n - r\}$ or
from $\{n - r, 2r - n, r\}$ or
from $\{r, n/2 - r, n/2\}$ or $\ldots$.

e.g. $n = 100$, $r = 39$:

Build chain

$0, 1, 2, 3, 5, 7, 12, 17, 22, 39, 61, 100$

by building $\{39, 61, 100\}$

from $\{22, 39, 61\}$ etc.

What about dim 2?

Obvious adaptation of idea:

Build chain $\ldots, (m, n)$

by choosing (q, r)

and building chain

$\ldots, (q, r), (m - q, n - r), (m, n)$.

e.g. Work backwards from $(314, 271)$ and $(194, 167)$ to $(120, 104)$, then $(74, 63)$, then $(46, 41)$, then $(28, 22)$, then $(18, 19)$, then $(10, 3)$, then $(8, 16)$.

Hmmm, what's the endgame? How to build short chain with $\{(8, 16), (10, 3), (18, 19)\}$?

Several plausible approaches, but all of them scale badly. Normally this construction is abandoned.

New observation:
Simple endgames work well
if $rm - qn = \Delta$
with, e.g., $\Delta = \pm 2^a 3^b$.
Often find very good chains.

Easy to find (q, r)
given (m, n, Δ):
standard ext-gcd computation.

What if (m, n) not coprime?
Great! Exploit factor.

Try many good choices
for (Δ, q, r), keep best.

Example of new chain:

$(0,0)$, $(1,0)$, $(0,1)$, $(1,-1)$,
$(1,1)$, $(1,2)$, $(2,3)$, $(3,5)$,
$(4,7)$, $(5,9)$, $(9,16)$, $(14,25)$,
$(19,34)$, $(33,59)$, $(38,68)$,
$(66,118)$, $(71,127)$, $(61,109)$,
$(132,236)$, $(203,363)$, $(264,472)$,
$(325,581)$, $(528,944)$,
$(731,1307)$, $(1259,2251)$,
$(1787,3195)$, $(2518,4502)$,
$(3249,5809)$, $(5036,9004)$,
$(6823,12199)$, $(10072,18008)$,
$(16895,30207)$, $(26967,48215)$.