Large smooth twins from short lattice vectors

Bruno Sterner (*joint with Erik Mulder and Wessel van Woerden*)

Inria and LIX, Institut Polytechnique de Paris, Palaiseau, France

Season 7 Episode 1 of the "Isogeny Club"

Consecutive integers

$$\vdots \qquad \vdots \qquad \vdots$$

"smooth twin"

$$
\begin{aligned}
22529735146513345759959448571 &= 2137 \cdot 10542693096169090201197683\\
22529735146513345759959448572 &= 2^2 \cdot 3 \cdot 907 \cdot 39239 \cdot 70177 \cdot 751717782012361\\
22529735146513345759959448573 &= 97 \cdot 66533 \cdot 2653633 \cdot 1315547053747481\\
22529735146513345759959448574 &= 2 \cdot 8423 \cdot 296591 \cdot 4132577 \cdot 1091139724967\\
22529735146513345759959448575 &= 3^2 \cdot 5^2 \cdot 7^5 \cdot 11^3 \cdot 59 \cdot 71^2 \cdot 101 \cdot 127 \cdot 173^2 \cdot 197 \cdot 199\\
22529735146513345759959448576 &= 2^{10} \cdot 13 \cdot 17^2 \cdot 23 \cdot 37^2 \cdot 41 \cdot 47 \cdot 61 \cdot 79 \cdot 107^2 \cdot 113^2 \cdot 137\\
22529735146513345759959448577 &= 4515076051 \cdot 4989890511705435227\\
22529735146513345759959448578 &= 2 \cdot 3 \cdot 29 \cdot 10273 \cdot 12604033531997919868039\\
22529735146513345759959448579 &= 73 \cdot 308626508856347202191225323\\
22529735146513345759959448580 &= 2^2 \cdot 5 \cdot 499 \cdot 599623 \cdot 3764846397877672777
\end{aligned}
$$

$$\vdots \qquad \vdots \qquad \vdots$$

Motivation: “smooth sandwiches”

Cryptographic-sized primes p such that $p^2 - 1$ is smooth or has a large smooth factor

~~B-SIDH~~

POKE

$$\phi : E \to E'$$
$$\#E(\mathbb{F}_{p^2}) = (p-1)^2, (p+1)^2$$

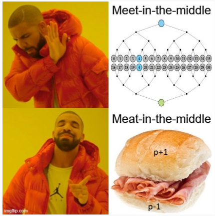
SQIsign1D

Fully smooth sandwich:

$(r, r+1)$ smooth twin and $p = 2r + 1$ prime $\rightsquigarrow$ $p^2 - 1 = 4r(r+1)$ smooth sandwich

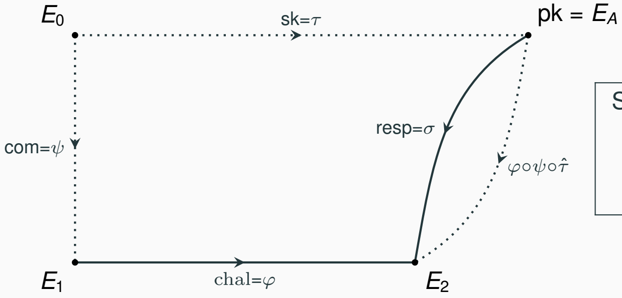
Lightly toasted sandwich: Sufficient for most isogeny-based applications

Finding large smooth twins & sandwiches with small smoothness bounds is *computationally challenging*



Signing with isogeny skies

SQIsign: Family of isogeny-based signatures based on the Deuring correspondence



SQIsign variants – σ is represented as a:

- long chain of 2-isogenies (1D)
- short chain of $(2, \cdots, 2)$-isogenies (HD)
- short chain of $(2, 2)$-isogenies (2D)

σ is a 1-dimensional isogeny between E_A and E_2 with an efficient "isogeny representation"

SQIsign1D parameters

Prime requirements

$$2^f T \mid p^2 - 1, \quad f \text{ is as large as possible}, \quad T \approx p^{5/4} \text{ is odd and smooth}$$

Signing: Compute $2\left\lceil \frac{15\log_2(p)}{4f} \right\rceil$ T-isogenies (difficult & annoying part to make efficient)

Verification: Compute a chain of 2^f-isogenies (easy part & more efficient for large f)

General boosting strategy: Find SQIsign1D parameters using $p_2(x) = 2x^2 - 1$

- Carefully choose $r = 2^a m$ and evaluate the polynomial to get $p = p_2(r) = 2r^2 - 1$
- The power of two in $p + 1$ is amplified by the squaring – i.e. $f = 2a + 1$
- The careful choice of r ensures p is prime and the conditions on T are met

Remark: $$f \leq \log_2(p)/4 \quad \Rightarrow \quad 2^f T \leq p^{3/2}$$

Boosting with a sieve

Sieve-and-boost: Do an exhaustive search of the form $r = 2^a 3^b m'$

- Apply the *sieve of Eratosthenes* to identify smooth integers in a large interval
- For each smooth integer m' compute $p = p_2(2^a 3^b m')$
- Output all candidate primes p that meet all conditions

This strategy was done by the NIST submission crew and found the following 254-bit prime

$$p = p_{1973} = 2r^2 - 1 \text{ with } r = 2^{37} \cdot 3^{18} \cdot 2053899652631121509:$$

$$p + 1 = 2^{75} \cdot 3^{36} \cdot 23^2 \cdot 59^2 \cdot 101^2 \cdot 109^2 \cdot 197^2 \cdot 491^2 \cdot 743^2 \cdot 1913^2, \text{ and}$$

$$p - 1 = 2 \cdot 7^4 \cdot 11 \cdot 13 \cdot 37 \cdot 89 \cdot 97 \cdot 107 \cdot 131 \cdot 137 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 499 \cdot 607 \cdot 1033$$
$$\cdot 1049 \cdot 1193 \cdot 1973 \cdot 32587069 \cdot 275446333 \cdot 1031359276391767$$

Boosting with a smooth twin

Twin-and-boost: Observe that for $p = p_2(r)$ we have

$$p^2 - 1 = 4r^2(r-1)(r+1),$$

if $(r, r+1)$ is a smooth twin we automatically get $p^{3/2}$ amount of smoothness in $p^2 - 1$

- Find a smooth twin $(r, r+1)$ with large (WLOG assume) $2^a \mid r$ and compute $p = p_2(r)$
- Output all primes p if: either $f = 2a + 1 \leq \log_2(p)/4$; or $r - 1$ has enough smooth factors for T

Difficult to instantiate this *smooth twin oracle* using $p_2(x)$

CHM algorithm: Using the polynomial $p_4(x) = 2x^4 - 1$ and the CHM algorithm, a relatively decent 253-bit prime was found (see S2E4 of the Isogeny Club)

"Not as good compared to the previous prime due to a smaller power of two"

Boosting with a smooth twin

Twin-and-boost: Observe that for $p = p_2(r)$ we have

$$p^2 - 1 = 4r^2(r-1)(r+1),$$

if $(r, r+1)$ is a smooth twin we automatically get $p^{3/2}$ amount of smoothness in $p^2 - 1$

- Find a smooth twin $(r, r+1)$ with large (WLOG assume) $2^a \mid r$ and compute $p = p_2(r)$
- Output all primes p if: either $f = 2a + 1 \leq \log_2(p)/4$; or $r - 1$ has enough smooth factors for T

Our algorithm: We can instantiate this oracle with $p_2(x)$ and showcase this 246-bit prime

$$p = p_{499} = 2r^2 - 1 \text{ with } r = 2^{31} \cdot 249349058236865954346624402 5:$$

$$p + 1 = 2^{63} \cdot 5^4 \cdot 23^4 \cdot 67^2 \cdot 71^2 \cdot 73^2 \cdot 89^2 \cdot 113^2 \cdot 137^4 \cdot 163^2 \cdot 229^2 \cdot 263^2 \cdot 293^2, \text{ and}$$

$$p - 1 = 2 \cdot 3 \cdot 7^2 \cdot 11 \cdot 13^2 \cdot 31 \cdot 47^2 \cdot 79^2 \cdot 103 \cdot 151 \cdot 241^2 \cdot 353 \cdot 367 \cdot 389 \cdot 449 \cdot 463 \cdot 499$$
$$\cdot 50355971 \cdot 1032403334060991048097384477$$

Smooth Twins

“Optimal” smooth twins

B-smooth twin: Consecutive integers $(r, r+1)$ with their product $r(r+1)$ being B-smooth

For instance, the following are 7 and 23-smooth twins (which are my favourite):

$$(4374, 4375) = (2 \cdot 3^7,\ 5^4 \cdot 7), \text{ and}$$
$$(4096575, 4096576) = (3^4 \cdot 5^2 \cdot 7 \cdot 17^2,\ 2^6 \cdot 11^2 \cdot 23^2)$$

Størmer (1897): For a fixed smoothness bound B, the set of B-smooth twins is *finite!*

B	2	3	5	7	11	...	40	...	100	...	113	......	200
# B-smooth twins	1	4	10	23	40	...	653	...	13,374	...	33,233	......	(conjectured) 348,865

Optimal smooth twins: The largest B-smooth twins for a fixed B (in this context we will call B the *optimal smoothness bound*)

Finding all B-smooth twins from Pell equations

Notation: Write $P_B \coloneqq \{p \leq B\} = \{2, 3, \cdots, q\}$ and $\pi(B) = \#P_B$

Pell equation characterisation: Smooth twins arise as solutions to a Pell equation

$$(r, r+1) \quad \longleftrightarrow \quad \mathcal{C}_D : x^2 - 4Dy^2 = 1$$

with $D = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot \cdots \cdot q^{\alpha_q}$ being squarefree (i.e. $\alpha_p \in \{0, 1\}$)

Complete set of twins: Solving all $2^{\pi(B)} - 1$ Pell equations finds all B-smooth twins

$B = 7$: Solve $\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_{10}, \mathcal{C}_{14}, \mathcal{C}_{15}, \mathcal{C}_{21}, \mathcal{C}_{30}, \mathcal{C}_{35}, \mathcal{C}_{42}, \mathcal{C}_{70}, \mathcal{C}_{105}, \mathcal{C}_{210}$

$B = 40$: **Lehmer (1964)**
$B = 100$: **Luca & Najman (2011)**
$B = 113$: **Costello (2020)**

Remark: When solely finding the *optimal twin* there is no advantage other than solving all Pell equations!

New characterisation – high-level idea

Lattice characterisation: Smooth twins arise as short vectors in a *prime number lattice*

$$\text{shortest vectors} \longleftrightarrow a, b \in \mathbb{Z} \text{ with } a, b \text{ smooth, coprime and } |a-b| \text{ small \& nonzero}$$

Optimal twins: The parameters of the lattice allows to target the largest twin — e.g. this 196-bit B-smooth twin with $B = 751$ was found (which we believe is optimal)

$$\begin{aligned} r &= 7^7 \cdot 11 \cdot 17 \cdot 29 \cdot 47 \cdot 59 \cdot 67 \cdot 83^2 \cdot 89 \cdot 151^3 \cdot 163 \cdot 173 \cdot 271 \cdot 347 \cdot 461 \cdot 491 \cdot 547 \cdot 587 \\ &\quad \cdot 619 \cdot 661 \cdot 683 \cdot 701, \text{ and} \\ r+1 &= 2 \cdot 3^9 \cdot 13^2 \cdot 19 \cdot 31 \cdot 41 \cdot 71 \cdot 73 \cdot 97 \cdot 157^2 \cdot 181^3 \cdot 191 \cdot 227 \cdot 241 \cdot 293 \cdot 307^3 \cdot 337 \cdot 557 \\ &\quad \cdot 617 \cdot 727 \cdot 751 \end{aligned}$$

More smooth twins: We found larger smooth twins than this one but it is not optimal; and also find new smaller twins which were not known before

- ➢ We conjecture that the exact number of 200-smooth twins is 348,865

Lattice preliminaries

Lattices, short vectors and the Gaussian heuristic

Lattices: Discrete subgroup $\mathcal{L}$ of $\mathbb{R}^n \longleftrightarrow \mathbb{Z}$-span of some linearly independent vectors

$$\mathcal{L} = \left\{ x_1 \boldsymbol{b}_1 + \cdots + x_k \boldsymbol{b}_k : x_i \in \mathbb{Z} \right\} = \left\{ \mathcal{B} \cdot \boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^k \right\}, \text{ where } \mathcal{B} = \begin{pmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k \end{pmatrix}$$

Short vectors and SVP: Non-zero vectors $\boldsymbol{v} \in \mathcal{L}$ with a small $\|\boldsymbol{v}\|$ — the shortest vector problem (SVP) finds the shortest non-zero vector in $\mathcal{L}$, whose norm we write as $\lambda_1(\mathcal{L})$

Gaussian heuristic: On average we expect $\lambda_1(\mathcal{L})$ to be approximately $\mathrm{gh}(\mathcal{L})$ where

$$\mathrm{gh}(\mathcal{L}) = \sqrt{\frac{n}{2\pi e}} \cdot \mathrm{vol}(\mathcal{L})^{1/n} = \sqrt{\frac{n}{2\pi e}} \cdot |\det(\mathcal{B})|^{1/n}$$

and the number of lattice vectors of norm $\leq \lambda$ is roughly $(\lambda / \mathrm{gh}(\mathcal{L}))^n$

Random lattices: This heuristic does not always hold which the lattice is fixed, but if you choose a *random* lattice then this heuristic should hold

Question: How do we solve SVP? In S5E6 we saw lattice reduction to find short vectors

Finding shortest vectors

Lattice sieving: An algorithm to find a set of short vectors of norm in an iterative manner

- From a large list L_i of $N = (4/3)^{k/2+o(k)}$ non-zero vectors with $R_i = \max_{\boldsymbol{v} \in L_i} \|\boldsymbol{v}\|$
- Construct a new list $L_{i+1} \coloneqq \{\boldsymbol{v} - \boldsymbol{w} : \boldsymbol{v}, \boldsymbol{w} \in L_i \mid \boldsymbol{v} \neq \boldsymbol{w} \text{ and } \|\boldsymbol{v} - \boldsymbol{w}\| \leq R_i\}$ of $\approx N$ vectors

Repeat this until $R_{i'} \leq \sqrt{4/3} \cdot \mathrm{gh}(\mathcal{L})$ (i.e. gives all $(4/3)^{k/2+o(k)}$ shortest vectors)

Advanced lattice sieving: Instead of checking all vectors in the L_{i+1}, one buckets vectors and only check pairs of vectors that lie in the same bucket

The runtime and memory of state-of-the-art lattice sieving is:

- Runtime: $O\left(2^{0.292k+o(k)}\right)$
- Memory: $O\left(2^{0.2075k+o(k)}\right)$

Jessica: All of this is implemented in the “general sieve kernel” (g6k)

Prime number lattice

Prime number lattice (or smooth rational lattice)

Notation: Let $P = \{p_i\} \subseteq P_B$ (with $p_i < p_{i+1}$), $n = \#P$ and $\alpha, \alpha_i \in \mathbb{R}$ for $i \in \{1, \cdots, n\}$

The *prime number lattice*, denoted $\mathcal{L}_{\alpha,\alpha_i,P} \coloneqq \{\mathcal{B}_{\alpha,\alpha_i,P} \cdot \boldsymbol{x} : \boldsymbol{v} \in \mathbb{Z}^n\}$, is the lattice with a generating matrix $\mathcal{B}_{\alpha,\alpha_i,P}$:

$$\mathcal{B} = \mathcal{B}_{\alpha,\alpha_i,P} = \begin{pmatrix} \alpha\log(p_1) & \alpha\log(p_2) & \cdots & \alpha\log(p_n) \\ \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix}$$

Remark: This lattice, with a choice of weights $\alpha_i = \log(p_i)$, has appeared in the context of factoring integers and computing discrete logarithms (**Schnorr 1993**)

Correspondence with smooth rationals

Lattice vectors: Let $\boldsymbol{x} = (x_1, \cdots, x_n)^T \in \mathbb{Z}^n$, then

$$\boldsymbol{v} = \mathcal{B} \cdot \boldsymbol{x} = \begin{pmatrix} \alpha x_1 \log(p_1) + \cdots + \alpha x_n \log(p_n) \\ \alpha_1 x_1 \\ \vdots \\ \alpha_n x_n \end{pmatrix} = \begin{pmatrix} \alpha \log(a/b) \\ \alpha_1 x_1 \\ \vdots \\ \alpha_n x_n \end{pmatrix} \in \mathcal{L}_{\alpha,\alpha_i,P},$$

where $a/b = \prod_{i=1}^n p_i^{x_i}$ is a P-smooth rational with a, b coprime (equivalently $x_i = \mathrm{val}_{p_i}(a/b)$)

Lemma

For all $\alpha, \alpha_i \in \mathbb{R}$, $\{$reduced P-smooth rationals $a/b\} \longleftrightarrow \{\mathbf{v} \in \mathcal{L}_{\alpha,\alpha_i,P}\}$ is a 1-1 corresp.

Question: What are the short vectors? We have $\|\boldsymbol{v}\|^2 = (\alpha \log(a/b))^2 + \sum_{i=1}^n (\alpha_i x_i)^2$

Visualising short lattice vectors (small α)

Consider $\mathcal{L}_{\alpha,\log(p_i),P_7}$ for $P_7 = \{2,3,5,7\}$ – what are shortest vectors $\boldsymbol{v} = \mathcal{B} \cdot (x_1, x_2, x_3, x_4)^T$ and their corresponding smooth rationals a/b when we change α?

Small α: These are the shortest vectors with $\alpha = 2^8$:

(x_1, x_2, x_3, x_4)	$\lVert \boldsymbol{v} \rVert$	a/b	$\lvert a-b \rvert$
$(5, -2, -2, 1)$	5.6822	224/225	1
$(1, 2, -3, 1)$	6.0472	126/125	1
$(4, -4, 1, 0)$	6.3010	80/81	1
$(6, -2, 0, -1)$	6.4934	64/63	1
$(4, 1, 0, -2)$	7.2044	48/49	1
$(0, 5, -1, -2)$	7.2328	243/245	2
$(1, 0, 2, -2)$	7.2620	50/49	1
$(5, 3, -3, -1)$	7.7757	864/875	11
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Visualising short lattice vectors (larger α)

Consider $\mathcal{L}_{\alpha,\log(p_i),P_7}$ for $P_7 = \{2,3,5,7\}$ – what are shortest vectors $\boldsymbol{v} = \mathcal{B} \cdot (x_1, x_2, x_3, x_4)^T$ and their corresponding smooth rationals a/b when we change α?

Larger α: These are the shortest vectors with $\alpha = 2^{13}$:

(x_1, x_2, x_3, x_4)	$\|\boldsymbol{v}\|$	a/b	$\lvert a-b \rvert$
$(5, 1, 2, -4)$	9.7883	2400/2401	1
$(1, 7, -4, -1)$	10.4096	4374/4375	1
$(4, -6, 6, -3)$	13.4476	250000/250047	47
$(6, 8, -2, -5)$	15.0831	419904/420175	271
$(10, -9, -3, 4)$	16.2395	2458624/2460375	1751
$(15, -8, -1, 0)$	16.5349	32768/32805	37
$(11, -2, -7, 3)$	16.8324	702464/703125	661
$(16, -1, -5, -1)$	17.7861	65536/65625	89
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Visualising short lattice vectors (even larger α)

Consider $\mathcal{L}_{\alpha,\log(p_i),P_7}$ for $P_7 = \{2, 3, 5, 7\}$ – what are shortest vectors $\boldsymbol{v} = \mathcal{B} \cdot (x_1, x_2, x_3, x_4)^T$ and their corresponding smooth rationals a/b when we change α?

Even larger α: These are the shortest vectors with $\alpha = 2^{18}$:

(x_1, x_2, x_3, x_4)	$\|\boldsymbol{v}\|$	a/b	$\|a - b\|$
$(3, -13, 10, -2)$	24.4097	78125000/78121827	3173
$(4, -17, -1, 9)$	31.1775	645657712/645700815	43103
$(7, -30, 9, 7)$	39.3968	205885750000000/205891132094649	5382094649
$(1, -4, -11, 11)$	39.7948	3954653486/3955078125	424639
$(48, 0, -11, -8)$	41.7149	281474976710656/281484423828125	9447117469
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(1, 7, -4, -1)$	60.7940	4374/4375	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Visualising short lattice vectors (more primes)

For comparison consider $\mathcal{L}_{\alpha,\log(p_i),P_{19}}$ for $P_{19} = \{p \leq 19\}$ – what are shortest vectors $\boldsymbol{v} = \mathcal{B} \cdot \boldsymbol{x}$ and their corresponding smooth rationals a/b?

Same α as before: These are the shortest vectors with $\alpha = 2^{18}$:

$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$	$\lVert\boldsymbol{v}\rVert$	a/b	$\lvert a-b\rvert$
$(5, 1, -4, 2, -1, -1, 0, 1)$	9.9705	89376/89375	1
$(9, -3, -3, -2, 0, 0, 1, 1)$	10.3657	165376/165375	1
$(6, -6, 2, 1, 1, -2, 0, 0)$	10.5588	123200/123201	1
$(4, -4, 1, -4, 1, 1, 1, 0)$	10.5994	194480/194481	1
$(5, 1, 1, 1, -2, 1, 0, -2)$	10.9485	43680/43681	1
$(2, -3, -1, 1, 3, -1, 1, -2)$	10.9712	633556/633555	1
$(4, -3, 3, 0, -2, -1, -1, 2)$	10.9821	722000/722007	7
$(4, 8, -2, 0, 0, -1, -1, -1)$	11.1716	104976/104975	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Choosing α to minimise the shortness of lattice vectors

Visual conclusion: α dominates the control on short vectors and correspond to $a/b \approx 1$

$$\alpha \log(a/b) \approx \alpha(a-b)/b$$

The shortest vectors have $\alpha \approx a/|a-b|$

Choosing α optimally: More precisely the following α minimises the shortness of the vector corresponding to $a/b \approx 1$

$$\alpha = \alpha_{\mathrm{opt}} \approx \sqrt{\frac{\beta_2}{(n-1)}} \frac{b}{|a-b|}$$

where $\beta_2 = \sum_{i=1}^{n} (x_i \alpha_i)^2$ – but this assumes we know the twin and its factorisations

Choosing α approximately: One does not need to choose α this exact – estimating this does not drastically change the shortness of the vector

Choosing α_i to actually get short vectors

Choosing α_i: Influences how large the x_i's can be for short vectors

- $\alpha_i = 1$;
- $\alpha_i = \sqrt{\log(p_i)}$;
- $\alpha_i = \log(p_i)$;
- $\alpha_i = \log(p_i)^e$

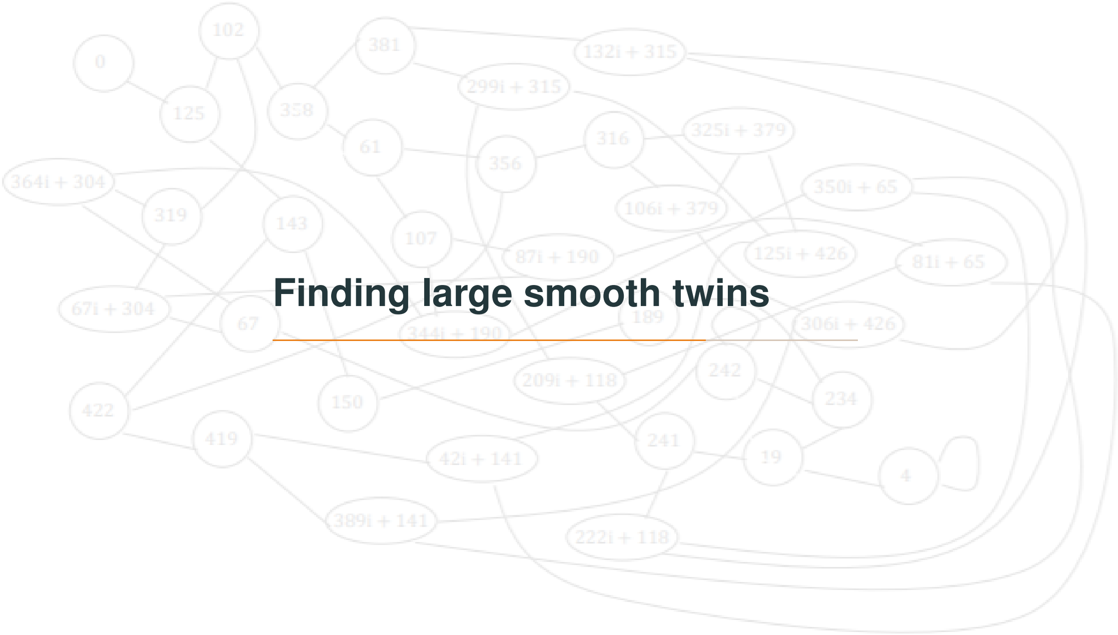
Theorem (Informal)

Under some heuristics, for optimal smooth twins and optimal $\alpha = \alpha_{\mathrm{opt}}$ and $\alpha_i = \log(p_i)$, the corresponding lattice vector is particularly short (and sometimes the shortest vector).

Optimal twins: For different $\alpha_i = \log(p_i)^e$ we experimentally show that vectors corresponding to optimal smooth twins in $\mathcal{L}_{\alpha_{\mathrm{opt}},\alpha_i,P_B}$ are also short

Smaller twins: Some but not all twins correspond to short vectors:

- There are more smaller twins than larger twins;
- Unusual large prime power, $p_i^{x_i} \mid r(r+1)$, giving a larger $(\alpha_i x_i)^2$ in the norm (e.g. $r = 107^6 - 1$)



Finding large smooth twins

Large smooth twins from short lattice vectors

Simple strategy: We find B-smooth twins as follows:

- Choose $\alpha = 2^\kappa$, $\alpha_i = \log(p_i)^e$ and work with $\mathcal{L} = \mathcal{L}_{\alpha,\alpha_i,P_B}$;
- Lattice sieving: find a large set of short vectors $\mathcal{L}_{\text{short}}$;
- For each $\boldsymbol{v} = \mathcal{B}_{\alpha,\alpha_i,P}\boldsymbol{x} \in \mathcal{L}_{\text{short}}$ compute $a = \prod_{i:x_i>0} p_i^{x_i}$ and $b = \prod_{i:x_i<0} p_i^{-x_i}$;
- Output the pairs (a, b) when $|a - b| = 1$.

Remark: The underlying operations in lattice sieving and CHM are the same (modulo the additive vs multiplicative subtly). The differences between them are:

- *Lattice sieving*: Start with large pairs that are far apart and reduce their difference;
- *CHM*: Start with small smooth twins and construct larger twins

Optimal B-smooth twins

Prior to this work: Only known for $B \leq 113$ – the largest of which is

$$r = 2^4 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 23^2 \cdot 29 \cdot 47 \cdot 59 \cdot 61 \cdot 73 \cdot 97 \cdot 103, \text{ and}$$
$$r + 1 = 13^2 \cdot 31^2 \cdot 37^2 \cdot 43^4 \cdot 71^4$$

Requires solving lots of Pell equations at a cost of $2^{\pi(B)+o\left(\pi(B)\right)}$

Lattice sieving: Purely solve SVP in $\mathcal{L}_{\alpha,\alpha_i,P_B}$ with a large enough α

$B = 103$: $\alpha = 2^{76} \longrightarrow$ the above 75-bit smooth is found ($\alpha_{\mathrm{opt}} \approx 2^{76.573325}$ when $\alpha_i = \log(p_i)$)

$B = 200$: $\alpha = 2^{97} \longrightarrow$ the 95-bit smooth twin mentioned at the start

$$r = 3^2 \cdot 5^2 \cdot 7^5 \cdot 11^3 \cdot 59 \cdot 71^2 \cdot 101 \cdot 127 \cdot 173^2 \cdot 197 \cdot 199, \text{ and}$$
$$r + 1 = 2^{10} \cdot 13 \cdot 17^2 \cdot 23 \cdot 37^2 \cdot 41 \cdot 47 \cdot 61 \cdot 79 \cdot 107^2 \cdot 113^2 \cdot 137$$

Computational cost of solving one SVP is $2^{0.292\pi(B)+o\left(\pi(B)\right)}$

Optimal B-smooth twins (much larger B)

$B = 500$: $\alpha = 2^{160} \longrightarrow$ this 157-bit smooth twin

$$\begin{aligned} r &= 2^2 \cdot 19 \cdot 37 \cdot 43^2 \cdot 47 \cdot 71 \cdot 149 \cdot 157 \cdot 173 \cdot 193 \cdot 229 \cdot 271 \cdot 317 \cdot 347^2 \cdot 353 \cdot 379 \cdot 397 \\ &\quad \cdot 439 \cdot 479 \cdot 499, \text{ and} \\ r+1 &= 3^2 \cdot 5 \cdot 11^2 \cdot 13^2 \cdot 31^4 \cdot 41^2 \cdot 73 \cdot 79 \cdot 103 \cdot 107 \cdot 127 \cdot 179 \cdot 199 \cdot 227 \cdot 263 \cdot 311 \cdot 337 \\ &\quad \cdot 373 \cdot 431 \cdot 433 \end{aligned}$$

$B = 751$: $\alpha = 2^{198} \longrightarrow$ this 196-bit smooth twin

$$\begin{aligned} r &= 7^7 \cdot 11 \cdot 17 \cdot 29 \cdot 47 \cdot 59 \cdot 67 \cdot 83^2 \cdot 89 \cdot 151^3 \cdot 163 \cdot 173 \cdot 271 \cdot 347 \cdot 461 \cdot 491 \cdot 547 \cdot 587 \\ &\quad \cdot 619 \cdot 661 \cdot 683 \cdot 701, \text{ and} \\ r+1 &= 2 \cdot 3^9 \cdot 13^2 \cdot 19 \cdot 31 \cdot 41 \cdot 71 \cdot 73 \cdot 97 \cdot 157^2 \cdot 181^3 \cdot 191 \cdot 227 \cdot 241 \cdot 293 \cdot 307^3 \cdot 337 \cdot 557 \\ &\quad \cdot 617 \cdot 727 \cdot 751 \end{aligned}$$

These are conjectured to be optimal based on results we prove (based on heuristics)

Larger (not optimal) smooth twins

Tradeoffs for larger B: We can incorporate one or both of the following:

- *Lifting*: Use *dimension for free* tricks for solving (approx)SVP (**Ducas (2018)**);
- *Guessing*: Replace P_B with $P = P_B \setminus Q$ for a small set of primes $Q \subseteq P_B$ and work in $\mathcal{L}_{\alpha,\alpha_i,P}$

$B = 1000$: Using both dimension for free and guessing we found this 213-bit smooth twin

$$\begin{aligned} r &= 19^2 \cdot 41 \cdot 43^2 \cdot 53 \cdot 59^2 \cdot 73^2 \cdot 83 \cdot 173 \cdot 227 \cdot 241 \cdot 281 \cdot 337 \cdot 397^2 \cdot 433 \cdot 541 \cdot 577 \cdot 593 \\ &\quad \cdot 787 \cdot 821 \cdot 839 \cdot 857^2 \cdot 967 \\ r + 1 &= 2^2 \cdot 3 \cdot 5^2 \cdot 13^3 \cdot 23 \cdot 37 \cdot 47 \cdot 79 \cdot 107 \cdot 127 \cdot 131 \cdot 151 \cdot 157 \cdot 167 \cdot 179 \cdot 181^2 \cdot 193 \cdot 223 \\ &\quad \cdot 283 \cdot 317 \cdot 367 \cdot 379 \cdot 601 \cdot 709^2 \cdot 743 \cdot 941 \cdot 997 \end{aligned}$$

Remark: Optimal B-smooth twins for this B should have $\approx$ 227-bits

More smooth twins

Cryptographic smooth twins: This is more-or-less the limit of our experiments and cannot find 256-bit B-smooth twins (which should exist with $B \approx 1250$)

Would require more lifting and guessing $\Rightarrow$ smaller chance of finding such twins

SQIsign twins: Want smooth twins with a large $2^a \mid r(r+1)$ for the twin-and-boost method

Two tricks can be included to help find them:

- Either replace $p_1 = 2$ with $p_1 = 2^a$ in the factor base;
- Or modify the weights, e.g. $\alpha_1 = \log(p_1)/\eta$ for some $\eta \geq 1$ and $\alpha_i = \log(p_i)$ for $i \geq 2$

E.g. p_{499} was easily found with $\alpha_1 = \log(p_1)/5$ and lattice sieving in the full lattice

Complete set of twins: We conjecture to have the complete set of 200-smooth twins

Start with a known and large list of B-smooth twins (e.g. from CHM) and find new twins

Summary

Summary

Smooth twins: We found smooth twins from short vectors in the prime number lattice

$$\begin{pmatrix} \alpha \log(p_1) & \alpha \log(p_2) & \cdots & \alpha \log(p_n) \\ \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix}$$

Thanks for listening!

Optimal twins: Significantly improved finding the *largest* B-smooth twin:

- *Pell equations:* Largest 113-smooth twin has 75-bits
- *Lattice sieving:* Largest 751-smooth twin has 196-bits

SQIsign1D: Able to apply the algorithm for isogeny-based purposes

Silly extra slide: my favourite smooth twin??

$$\begin{aligned} 2023 &= 45^2 - 2 = 7 \cdot 17^2 \\ 2024 &= 45^2 - 1 = 2^3 \cdot 11 \cdot 23 \\ 2025 &= 45^2 \qquad\;\; = 3^4 \cdot 5^2 \end{aligned}$$

How do I choose the best out of these two smooth twins??

Even better: $(2023, 2024, 2025) \longrightarrow (4096575, 4096576) = (2023 \cdot 2025, 2024^2)$

"This has to be my *favourite* smooth twin!"