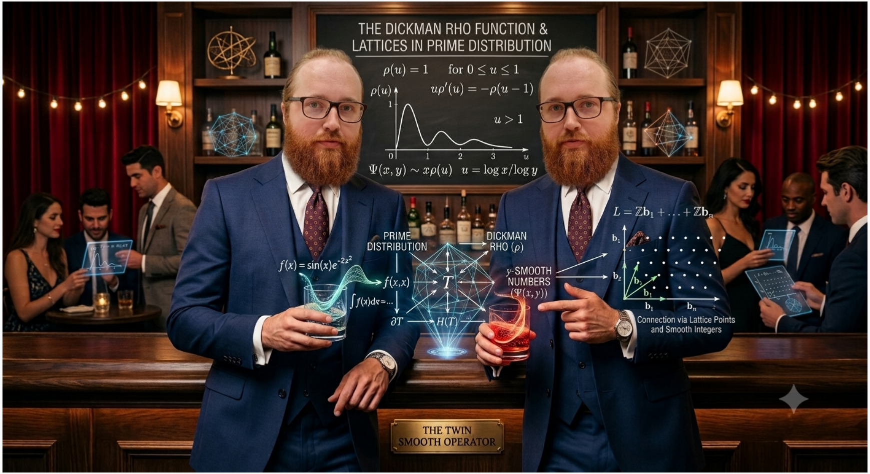
# Large smooth twins from short lattice vectors

Erik Mulder [1] ***Bruno Sterner*** [2] [3] Wessel van Woerden [4]

[1]University of Bergen, [2]Inria & Laboratoire d'Informatique de l'École polytechnique, [3]University of Waterloo, [4]PQShield

*Talk at* ANTS XVII

# Smooth twin operator (made with ChatGPT)



# Consecutive integers

$$
\begin{array}{ccc}
\vdots & & \vdots \\
2252973514651334575995944 8571 & = & 2137 \cdot 1054269309616909020 1197683 \\
2252973514651334575995944 8572 & = & 2^2 \cdot 3 \cdot 907 \cdot 39239 \cdot 70177 \cdot 751717782012361 \\
2252973514651334575995944 8573 & = & 97 \cdot 66533 \cdot 2653633 \cdot 1315547053747481 \\
2252973514651334575995944 8574 & = & 2 \cdot 8423 \cdot 296591 \cdot 4132577 \cdot 1091139724967 \\
2252973514651334575995944 8575 & = & 3^2 \cdot 5^2 \cdot 7^5 \cdot 11^3 \cdot 59 \cdot 71^2 \cdot 101 \cdot 127 \cdot 173^2 \cdot 197 \cdot 199 \\
2252973514651334575995944 8576 & = & 2^{10} \cdot 13 \cdot 17^2 \cdot 23 \cdot 37^2 \cdot 41 \cdot 47 \cdot 61 \cdot 79 \cdot 107^2 \cdot 113^2 \cdot 137 \\
2252973514651334575995944 8577 & = & 4515076051 \cdot 498989051170543 5227 \\
2252973514651334575995944 8578 & = & 2 \cdot 3 \cdot 29 \cdot 10273 \cdot 126040335319979198 68039 \\
2252973514651334575995944 8579 & = & 73 \cdot 3086265088563472021 91225323 \\
2252973514651334575995944 8580 & = & 2^2 \cdot 5 \cdot 499 \cdot 599623 \cdot 37648463978776727 77 \\
\vdots & & \vdots
\end{array}
$$

*"smooth twin"*

# "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):

$$(4374, 4375) = (2 \cdot 3^7,\ 5^4 \cdot 7), \text{ and}$$
$$(4096575, 4096576) = (3^4 \cdot 5^2 \cdot 7 \cdot 17^2,\ 2^6 \cdot 11^2 \cdot 23^2) = (2023 \cdot 2025, 2024^2)$$

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

| $B$ | 2 | 3 | 5 | 7 | 11 | $\cdots$ | 40 | $\cdots$ | 100 | $\cdots$ | 113 | $\cdots\cdots$ | 200 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # $B$-smooth twins | 1 | 4 | 10 | 23 | 40 | $\cdots$ | 653 | $\cdots$ | 13,374 | $\cdots$ | 33,233 | $\cdots\cdots$ | 348,865 |

**Optimal smooth twins:** The largest $B$-smooth twins for a fixed $B$

**Theorem**

*Under some heuristics, as $B \to \infty$, the optimal $B$-smooth twin asymptotically grows as $r \sim e^{2e\sqrt{B}}$.*

# High-level overview

**Lattices:** $\mathbb{Z}$-span of linearly independent vectors in $\mathbb{R}^m$

$$\mathcal{L} = \left\{ x_1 \boldsymbol{b}_1 + \cdots + x_n \boldsymbol{b}_n : x_i \in \mathbb{Z} \right\} = \left\{ \boldsymbol{Bx} : \boldsymbol{x} \in \mathbb{Z}^n \right\} \subseteq \mathbb{R}^m, \text{ where } \boldsymbol{B} = \begin{pmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_n \end{pmatrix}$$

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

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

Solving the *shortest vector problem* (SVP) in this lattice can find such smooth twins

**Optimal twins:** This 157-bit $B$-smooth twin with $B = 500$ was found

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

# Prime number lattice

**Notation:**

- *Factor base*: $P = \{p_i\} \subseteq P_B := \{p \leq B\}$ (with $p_i < p_{i+1}$) and $n = \#P \leq \pi(B)$;
- *Scaling and weights*: $\alpha, \alpha_i \in \mathbb{R}$ for $i \in \{1, \cdots, n\}$

**Prime number lattice**: $\mathcal{L}_{\alpha,\alpha_i,P} := \{\boldsymbol{B}_{\alpha,\alpha_i,P}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\} \subseteq \mathbb{R}^{n+1}$ with a basis $\boldsymbol{B}_{\alpha,\alpha_i,P}$:

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

*Remark:* $\mathcal{L}_{\alpha,\log(p_i),P}$ has appeared in factoring integers and DLP (**Schnorr 1993**)

# Correspondence with smooth rationals

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

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

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

**Lemma**

*For all $\alpha, \alpha_i \in \mathbb{R}$, $\{$reduced $P$-smooth rationals $a/b\} \longleftrightarrow \{\boldsymbol{v} \in \mathcal{L}_{\alpha,\alpha_i,P}\}$ 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 $\alpha$)

$\mathcal{L}_{\alpha,\log(p_i),P_7}$ — what are shortest vectors $\boldsymbol{v} = \boldsymbol{B}(x_1, x_2, x_3, x_4)^T$ when we change $\alpha$?

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

| $(x_1, x_2, x_3, x_4)$ | $\|\boldsymbol{v}\|$ | $a/b$ | $\lvert a - b \rvert$ |
|---|---|---|---|
| $(5, -2, -2, 1)$ | 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 $\alpha$)

$\mathcal{L}_{\alpha,\log(p_i),P_7}$ — what are shortest vectors $\boldsymbol{v} = \boldsymbol{B}(x_1, x_2, x_3, x_4)^T$ when we change $\alpha$?

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

| $(x_1, x_2, x_3, x_4)$ | $\lVert\boldsymbol{v}\rVert$ | $a/b$ | $\lvert a-b\rvert$ |
|---|---|---|---|
| $(5, 1, 2, -4)$ | 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 $\alpha$)

$\mathcal{L}_{\alpha,\log(p_i),P_7}$ — what are shortest vectors $\boldsymbol{v} = \boldsymbol{B}(x_1, x_2, x_3, x_4)^T$ when we change $\alpha$?

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

| $(x_1, x_2, x_3, x_4)$ | $\lVert \boldsymbol{v} \rVert$ | $a/b$ | $\lvert a-b \rvert$ |
|---|---|---|---|
| $(3, -13, 10, -2)$ | 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)

$\mathcal{L}_{\alpha,\log(p_i),P_{19}}$ (more primes in the factor base) — shortest vectors $\boldsymbol{v} = \boldsymbol{B}\boldsymbol{x}$

**Same $\alpha$ 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 |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

# Optimising the choice of scaling and weight factors

**Visual conclusion:** $\alpha$ 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 $\alpha \approx b/|a-b|$ (i.e. $\alpha \approx r$ for smooth twins)

**Choosing $\alpha$ optimally:** More precisely, under heuristic modelling, one should choose $\alpha$ slightly larger than $r$ for the best length/density trade-off

$$\alpha = \alpha_{\mathrm{opt}} \approx \sqrt{\frac{\sum_{i=1}^{n}(x_i\alpha_i)^2}{(n-1)}}\frac{b}{|a-b|}$$

*Approximation:* Estimating $\alpha_{\mathrm{opt}}$ is sufficient and does not drastically change this trade-off

**Choosing $\alpha_i$:** Many choices can be made, e.g. $\alpha_i = \log(p_i)$ or $\alpha_i = \log(p_i)^e$ or others

# Optimal $B$-smooth twins

**Prior to this work:** Only known for $B \leq 113$ – the largest of which has 75-bits

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

*Computational cost*: Solve exponentially many Pell equations $\rightsquigarrow 2^{\pi(B)+o\left(\pi(B)\right)}$

**This work:** Choose appropriate parameters $\alpha, \alpha_i$ and work with $\mathcal{L}_{\alpha,\alpha_i,P_B}$

$B = 103$: $\alpha = 2^{76}$, $\alpha_i = \log(p_i) \longrightarrow$ get the above smooth twin ($\alpha_{\mathrm{opt}} \approx 2^{76.573325}$)

$B = 200$: $\alpha = 2^{96}$, $\alpha_i = \log(p_i) \longrightarrow$ this 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*: Solve one SVP (with lattice sieving) in $\mathcal{L}_{\alpha,\alpha_i,P_B} \rightsquigarrow 2^{0.292\pi(B)+o\left(\pi(B)\right)}$

# Optimal $B$-smooth twins (larger $B$)

$B = 500$: $\alpha = 2^{159}$, $\alpha_i = \log(p_i) \longrightarrow$ this 157-bit smooth twin

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

$B = 751$: $\alpha = 2^{198}$, $\alpha_i = \log(p_i) \longrightarrow$ 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 (in accordance with $r \sim e^{2e\sqrt{B}}$ and its approximation)

# Larger and more twins

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

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

$B = 1000$ : Using both guessing and lifting we found this (non-optimal) 213-bit smooth twin

$$r = 19^2 \cdot 41 \cdot 43^2 \cdot 53 \cdot 59^2 \cdot 73^2 \cdot 83 \cdot 173 \cdot 227 \cdot 241 \cdot 281 \cdot 337 \cdot 397^2 \cdot 433 \cdot 541 \cdot 577 \cdot 593 \cdot 787 \cdot 821 \cdot 839 \cdot 857^2 \cdot 967$$

$$r + 1 = 2^2 \cdot 3 \cdot 5^2 \cdot 13^3 \cdot 23 \cdot 37 \cdot 47 \cdot 79 \cdot 107 \cdot 127 \cdot 131 \cdot 151 \cdot 157 \cdot 167 \cdot 179 \cdot 181^2 \cdot 193 \cdot 223 \cdot 283 \cdot 317 \cdot 367 \cdot 379 \cdot 601 \cdot 709^2 \cdot 743 \cdot 941 \cdot 997$$

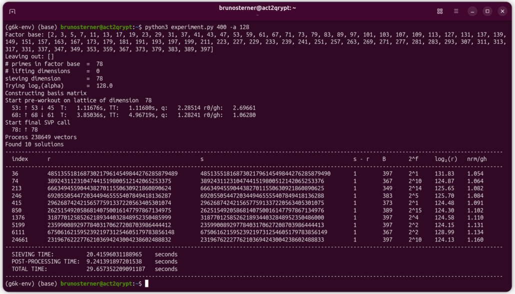
**Finding all twins:** We conjecture that there are exactly 348,865 many 200-smooth twins

CHM (348,840 twins) + Lattice sieving (25 twins) + Going above and beyond

# Code and dataset

http://github.com/WvanWoerden/SmoothTwins

https://zenodo.org/records/18234089




# Wrap-up: prime number lattice $\rightsquigarrow$ smooth twins

**Summary:** We found large smooth twins from short vectors in the prime number lattice

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

***Bedankt voor het luisteren***

**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

**Complete set of twins**: We conjecture to have all 200-smooth twins

**SQIsign1D**: Able to apply this for isogeny-based cryptographic purposes