



UNIVERSITY
OF BERGEN

Inria



UNIVERSITY OF
WATERLOO

PQSHIELD

Large smooth twins from short lattice vectors

Erik Mulder¹ **Bruno Sterner**^{2 3} Wessel van Woerden⁴

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

Talk at ANTS XVII

Smooth twin operator (made with ChatGPT)



Consecutive integers

⋮

⋮

⋮

“smooth twin”

$$22529735146513345759959448571 = 2137 \cdot 10542693096169090201197683$$

$$22529735146513345759959448572 = 2^2 \cdot 3 \cdot 907 \cdot 39239 \cdot 70177 \cdot 751717782012361$$

$$22529735146513345759959448573 = 97 \cdot 66533 \cdot 2653633 \cdot 1315547053747481$$

$$22529735146513345759959448574 = 2 \cdot 8423 \cdot 296591 \cdot 4132577 \cdot 1091139724967$$

$$22529735146513345759959448575 = 3^2 \cdot 5^2 \cdot 7^5 \cdot 11^3 \cdot 59 \cdot 71^2 \cdot 101 \cdot 127 \cdot 173^2 \cdot 197 \cdot 199$$

$$22529735146513345759959448576 = 2^{10} \cdot 13 \cdot 17^2 \cdot 23 \cdot 37^2 \cdot 41 \cdot 47 \cdot 61 \cdot 79 \cdot 107^2 \cdot 113^2 \cdot 137$$

$$22529735146513345759959448577 = 4515076051 \cdot 4989890511705435227$$

$$22529735146513345759959448578 = 2 \cdot 3 \cdot 29 \cdot 10273 \cdot 12604033531997919868039$$

$$22529735146513345759959448579 = 73 \cdot 308626508856347202191225323$$

$$22529735146513345759959448580 = 2^2 \cdot 5 \cdot 499 \cdot 599623 \cdot 3764846397877672777$$

⋮

⋮

⋮

“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		40		100		113		200
# B -smooth twins	1	4	10	23	40		653		13,374		33,233		348,865

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

Theorem

Under some heuristics, as $B \rightarrow \infty$, 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 $\mathbb{R}^m$



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

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

$$r = 2^2 \cdot 19 \cdot 37 \cdot 43^2 \cdot 47 \cdot 71 \cdot 149 \cdot 157 \cdot 173 \cdot 193 \cdot 229 \cdot 271 \cdot 317 \cdot 347^2 \cdot 353 \cdot 379 \cdot 397 \\ \cdot 439 \cdot 479 \cdot 499, \text{ and}$$

$$r + 1 = 3^2 \cdot 5 \cdot 11^2 \cdot 13^2 \cdot 31^4 \cdot 41^2 \cdot 73 \cdot 79 \cdot 103 \cdot 107 \cdot 127 \cdot 179 \cdot 199 \cdot 227 \cdot 263 \cdot 311 \cdot 337 \\ \cdot 373 \cdot 431 \cdot 433$$

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 $i \in \{1, \dots, n\}$

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

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

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

Correspondence with smooth rationals

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

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

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

Lemma

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

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

Visualising short lattice vectors (small α)

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

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

(x_1, x_2, x_3, x_4)	$\ \mathbf{v}\ $	a/b	$ a - b $
$(5, -2, -2, 1)$	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)

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

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

(x_1, x_2, x_3, x_4)	$\ \mathbf{v}\ $	a/b	$ a - b $
(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)

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

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

(x_1, x_2, x_3, x_4)	$\ \mathbf{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)

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

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

$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$	$\ \mathbf{v}\ $	a/b	$ a - b $
$(5, 1, -4, 2, -1, -1, 0, 1)$	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: 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 $\alpha \approx b/|a - b|$ (i.e. $\alpha \approx r$ for smooth twins)

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

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

Approximation: Estimating α_{opt} is sufficient and does not drastically change this trade-off

Choosing α_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 $\rightsquigarrow 2^{\pi(B)+o(\pi(B))}$

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

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

$B = 200$: $\alpha = 2^{96}$, $\alpha_i = \log(p_i) \rightarrow$ 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 $\mathcal{L}_{\alpha, \alpha_i, P_B} \rightsquigarrow 2^{0.292\pi(B)+o(\pi(B))}$

Optimal B -smooth twins (larger B)

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

$$r = 2^2 \cdot 19 \cdot 37 \cdot 43^2 \cdot 47 \cdot 71 \cdot 149 \cdot 157 \cdot 173 \cdot 193 \cdot 229 \cdot 271 \cdot 317 \cdot 347^2 \cdot 353 \cdot 379 \cdot 397 \\ \cdot 439 \cdot 479 \cdot 499, \text{ and}$$

$$r + 1 = 3^2 \cdot 5 \cdot 11^2 \cdot 13^2 \cdot 31^4 \cdot 41^2 \cdot 73 \cdot 79 \cdot 103 \cdot 107 \cdot 127 \cdot 179 \cdot 199 \cdot 227 \cdot 263 \cdot 311 \cdot 337 \\ \cdot 373 \cdot 431 \cdot 433$$

$B = 751$: $\alpha = 2^{198}$, $\alpha_i = \log(p_i) \longrightarrow$ this 196-bit smooth twin

$$r = 7^7 \cdot 11 \cdot 17 \cdot 29 \cdot 47 \cdot 59 \cdot 67 \cdot 83^2 \cdot 89 \cdot 151^3 \cdot 163 \cdot 173 \cdot 271 \cdot 347 \cdot 461 \cdot 491 \cdot 547 \cdot 587 \\ \cdot 619 \cdot 661 \cdot 683 \cdot 701, \text{ and}$$

$$r + 1 = 2 \cdot 3^9 \cdot 13^2 \cdot 19 \cdot 31 \cdot 41 \cdot 71 \cdot 73 \cdot 97 \cdot 157^2 \cdot 181^3 \cdot 191 \cdot 227 \cdot 241 \cdot 293 \cdot 307^3 \cdot 337 \cdot 557 \\ \cdot 617 \cdot 727 \cdot 751$$

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>

```
(gik-env) (base) brunosterner@act2gyp1:~$ python3 experiment.py 400 -a 128
Factor base: [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397]
Leaving out: []
# primes in factor base = 78
# lifting dimensions = 0
sieving dimension = 78
Trying log(alpha) = 128.0
Constructing basis matrix
Start pre-workout on Lattice of dimension 78
53: f 53 i 45 T: 1.116765, TT: 1.116895, q: 2.28514 r0/gh: 2.69661
481: f 60 i 61 T: 3.858365, TT: 4.967195, q: 1.28241 r0/gh: 1.06208
Start final csp call
78: f 78
Process 23869 vectors
Found 38 solutions
-----
Index      f          s          s + r      B      2^r      log2(r)      nrm/gh
-----
36      4851355181687302179614549804476285879489      4851355181687302179614549804476285879489      1      397      2^1      131.83      1.054
74      38924311231847441519886512142865253375      38924311231847441519886512142865253375      1      367      2^10      124.87      1.064
213      66834945589413027815586136021688768624      66834945589413027815586136021688768624      1      249      2^14      123.43      1.062
246      69281585447203469465555407049418136287      69281585447203469465555407049418136288      1      383      2^5      125.78      1.084
415      2962687424156577591337228563485181874      2962687424156577591337228563485181875      1      373      2^1      124.48      1.093
858      262515470598814877081614779767134975      262515470598814877081614779767134976      1      389      2^15      124.38      1.102
1376      31677812585262189144035946052158485999      31677812585262189144035946052158485999      1      397      2^4      124.58      1.118
5199      235998892977848317862728678186844412      235998892977848317862728678186844413      1      397      2^2      124.15      1.131
6111      67586162159239239231254665179781856148      67586162159239239231254665179781856149      1      367      2^2      120.99      1.134
2465      2319676227762163642439423364246832      23196762277621636424394233642468313      1      397      2^18      124.13      1.166
-----
SIEVING TIME:      28.4159681188065      seconds
POST-PROCESSING TIME:  0.2413987201538      seconds
TOTAL TIME:      29.65735289891187      seconds
(gik-env) (base) brunosterner@act2gyp1:~$
```



[Communities](#) [My dashboard](#)

[Dataset](#) [Open](#)

Smooth Twins

Mulder, Erik¹ · Sterner, Bruno² · van Woerden, Wessel³

[Show affiliations](#)

This dataset belongs to the paper

Large smooth twins from short lattice vectors, by Erik Mulder, Bruno Sterner and Wessel van Woerden.

Available at [arXiv](#):

A B-smooth twin (r+1) are two consecutive positive numbers r and r+1 whose prime factors are of size at most B.

This dataset contains the following files:

- all200twins.txt - Conjectured complete set of all 200-smooth twins.
- newtwins_sort_by_B_200.txt - The new 200-smooth twins found in the paper.
- newtwins_largest_collect.txt - Collection of largest known (strictly) B-smooth twins for all smoothness bounds B < 950 and a selection of smoothness bounds 550 < B < 1100.

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

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

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



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

SQLsign1D: Able to apply this for isogeny-based cryptographic purposes