Finding twin smooth integers
for isogeny-based cryptography

UCL InfoSec Seminar
Feb 11, 2021

Craig Costello
Microsoft Research

joint work with Michael Meyer and Michael Naehrig
https://eprint.iacr.org/2020/1283.pdf

1109496723119
1109496723120
1109496723121
1109496723122
1109496723123
1109496723124
1109496723125
1109496723126
1109496723127
1109496723128
1109496723129
1109496723130
1109496723131
1109496723132
1109496723133
1109496723134

$$
\begin{aligned}
1109496723119 &= 709 \cdot 1564875491 \\
1109496723120 &= 2^4 \cdot 3^2 \cdot 5 \cdot 1873 \cdot 822727 \\
1109496723121 &= 643 \cdot 1725500347 \\
1109496723122 &= 2 \cdot 79 \cdot 7022131159 \\
1109496723123 &= 3 \cdot 1153 \cdot 320756497 \\
1109496723124 &= 2^2 \cdot 89 \cdot 27953 \cdot 111493 \\
1109496723125 &= 5^4 \cdot 7 \cdot 17 \cdot 19^2 \cdot 31^2 \cdot 43 \\
1109496723126 &= 2 \cdot 3 \cdot 11^2 \cdot 23 \cdot 29^2 \cdot 41^2 \cdot 47 \\
1109496723127 &= 13 \cdot 467 \cdot 12401 \cdot 14737 \\
1109496723128 &= 2^3 \cdot 67 \cdot 8231 \cdot 251483 \\
1109496723129 &= 3^4 \cdot 2339 \cdot 5856131 \\
1109496723130 &= 2 \cdot 5 \cdot 110949672313 \\
1109496723131 &= 61 \cdot 18188470871 \\
1109496723132 &= 2^2 \cdot 3 \cdot 7^3 \cdot 691 \cdot 390097 \\
1109496723133 &= 1109496723133 \\
1109496723134 &= 2 \cdot 554748361567
\end{aligned}
$$

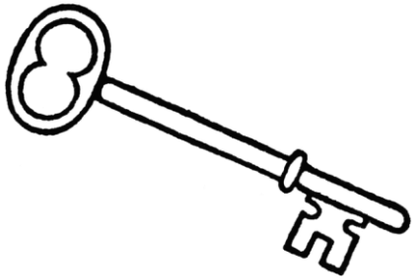
Outline

1. Why?

2. Twin smooths (and first attempts)

3. The PTE sieve

1. Why?

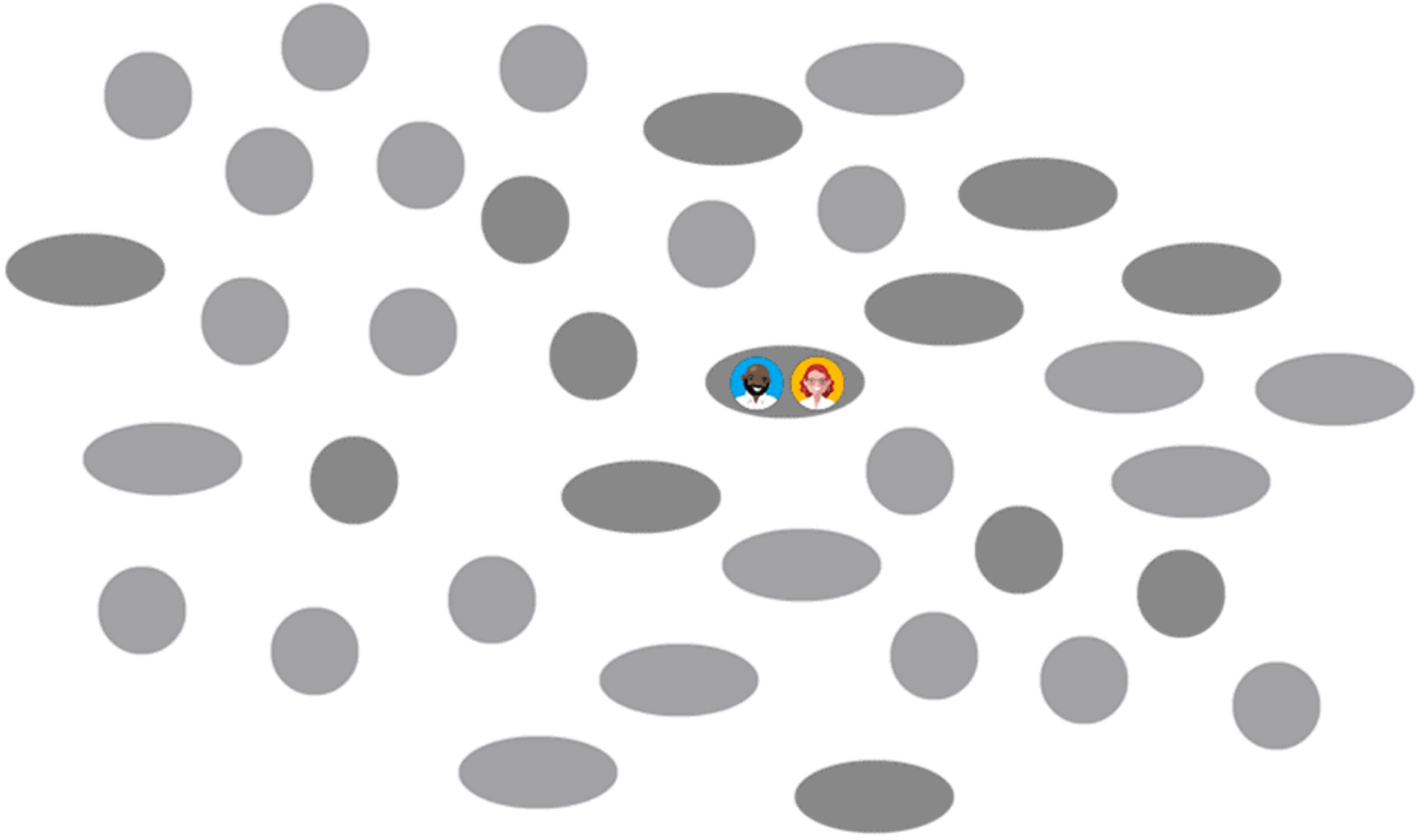


B-SIDH
Keys = 186B

SQI-Sign
(Keys, Sig) = (64B, 204B)

- Both schemes require prime $\boldsymbol{p = 2m + 1}$
- Performance of both depends on largest prime in $\boldsymbol{(m, m + 1)}$

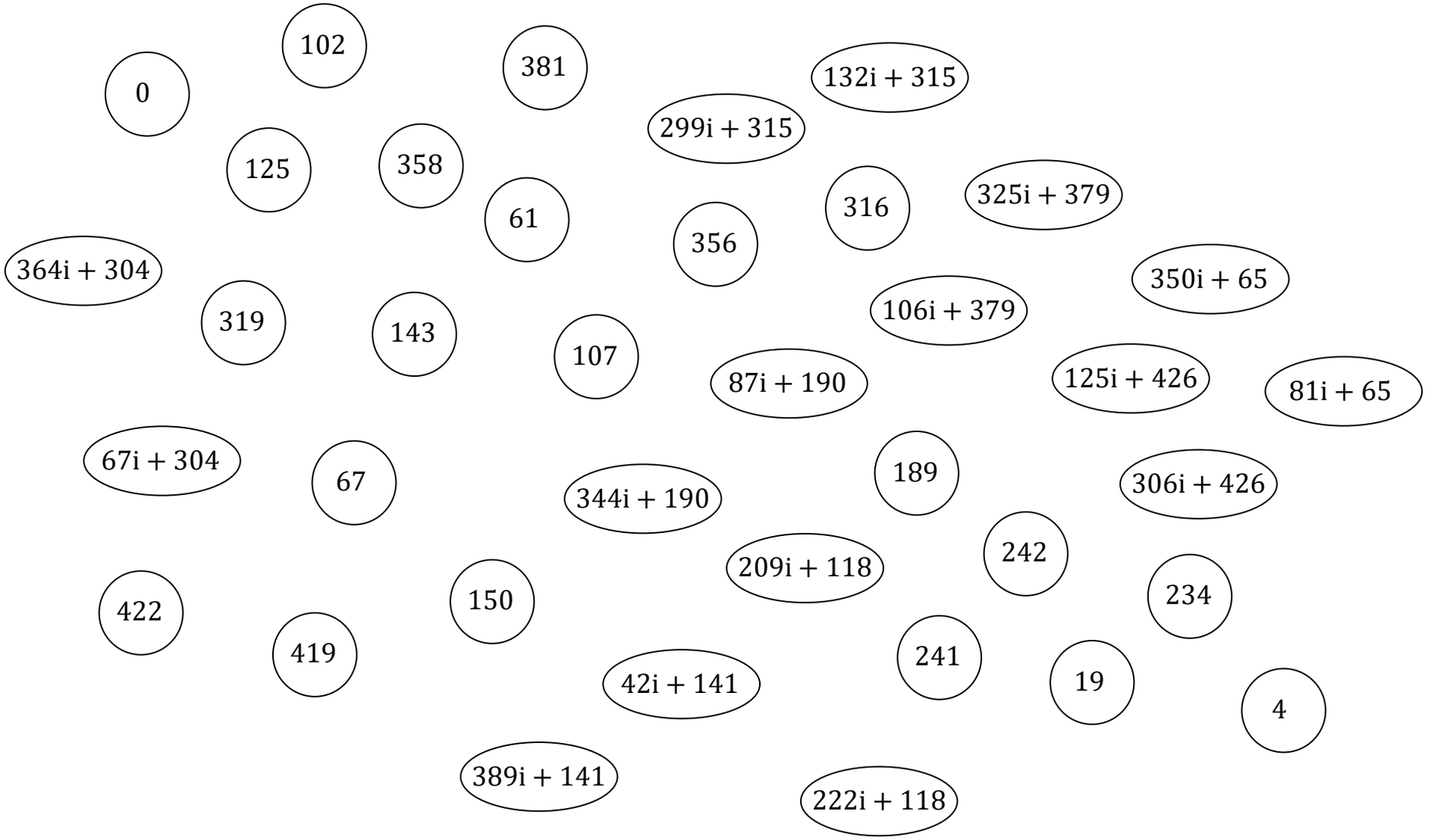
SIDH/SIKE



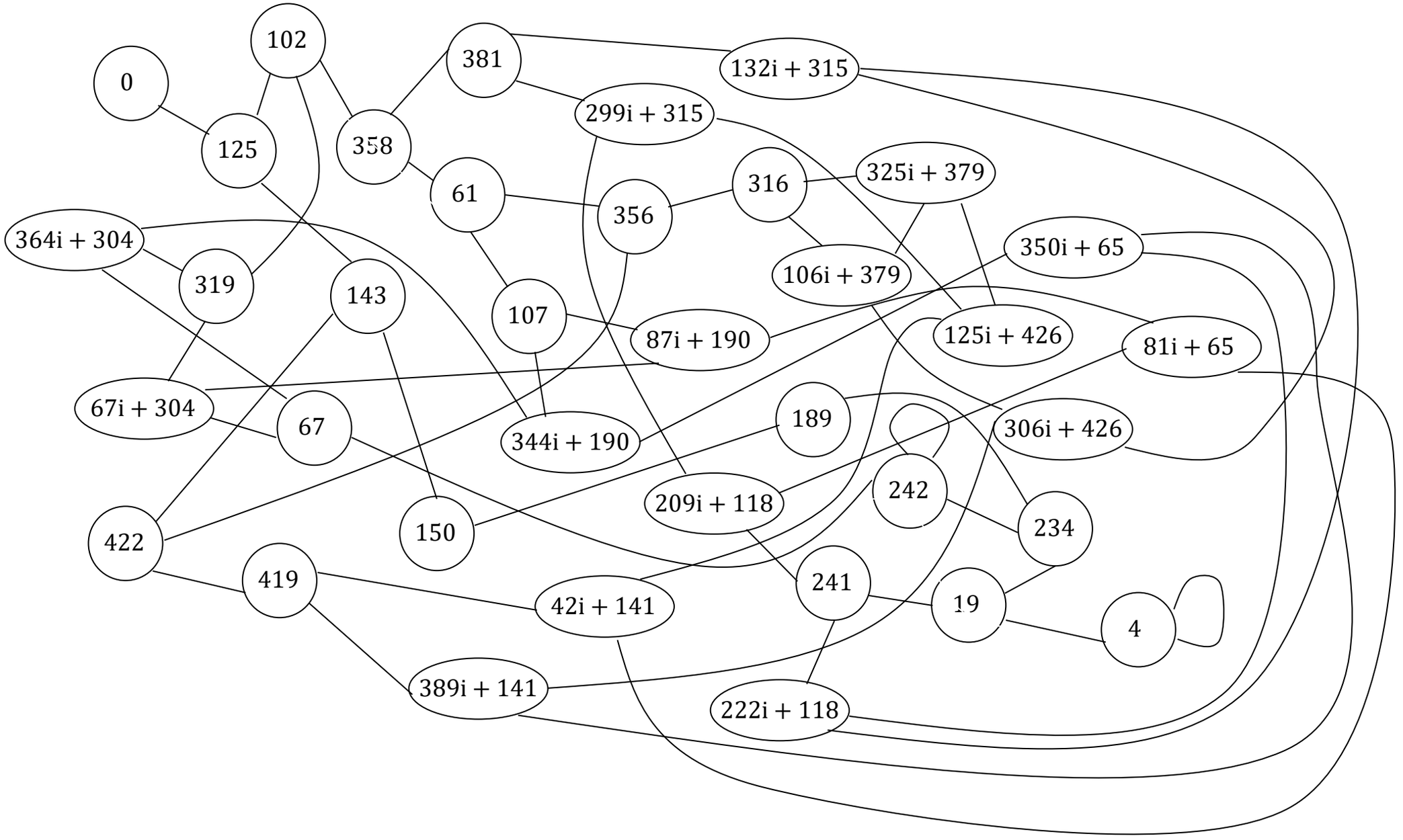
$$p = 431 = 2^4 3^3 - 1$$

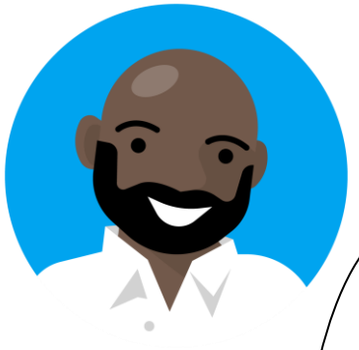
$\mathbb{F}_{p^2} = \mathbb{F}_p(i)$;

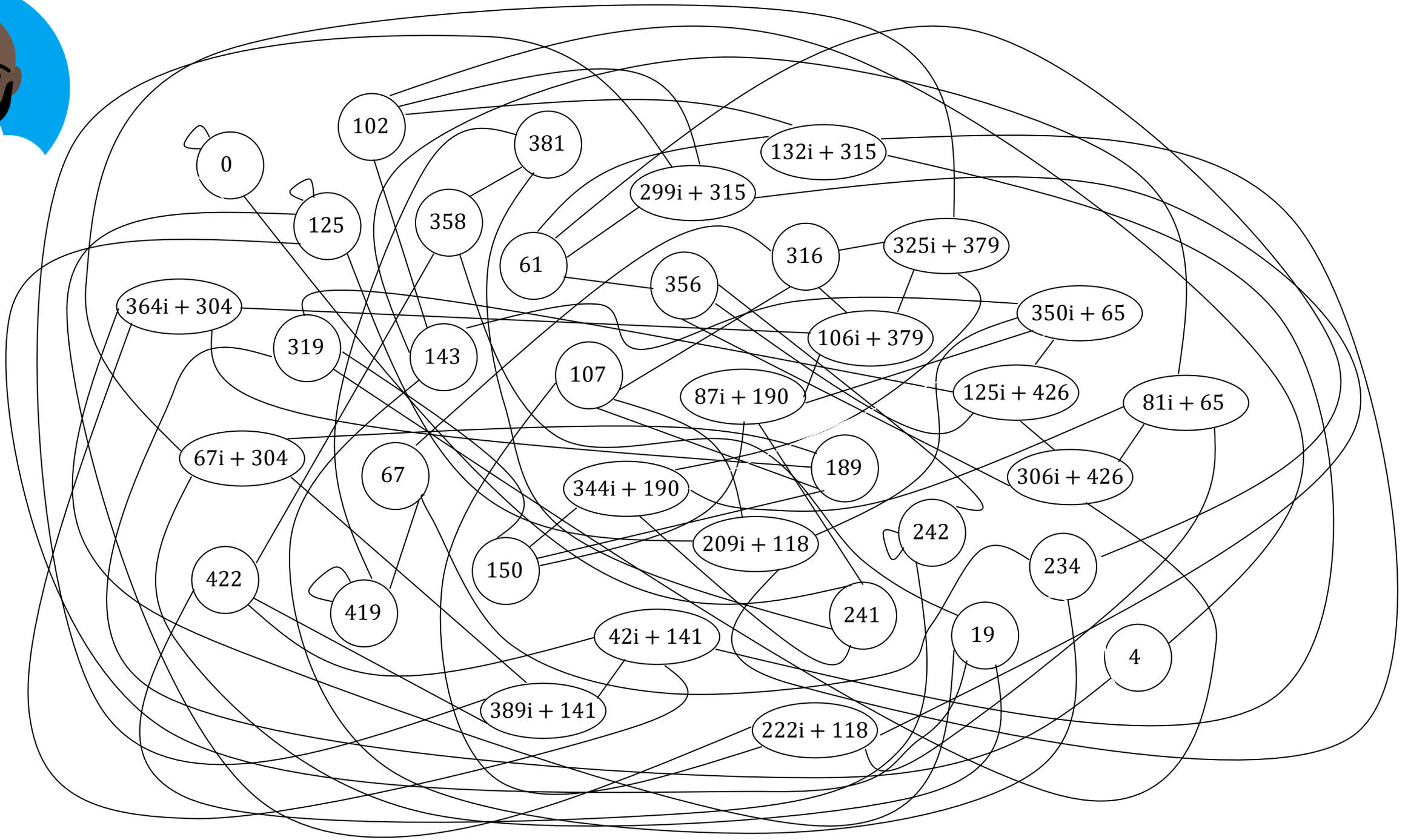
$i^2 + 1 = 0$



S:=SupersingularInvariants(431);


0
102
125
358
381
132i + 315
299i + 315
61
356
316
325i + 379
364i + 304
319
143
107
106i + 379
350i + 65
87i + 190
125i + 426
81i + 65
67i + 304
67
344i + 190
189
306i + 426
242
209i + 118
234
422
150
241
419
42i + 141
19
4
389i + 141
222i + 118




0
102
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
150
234
422
419
241
19
42i + 141
4
389i + 141
222i + 118

p plus-*and*-minus 1

- Security of SIDH/SIKE depends on degree of isogeny, not on p
- SIDH/SIKE takes $p = 2^a 3^b - 1$ to squeeze Alice and Bob *into* $p + 1$
- B-SIDH: But we can squeeze Alice into $p + 1$ and Bob into $p - 1$
- Take $p + 1 = 2M$ and $p - 1 = 2N$, so $\gcd(M, N) = 1$
- Alice computes M-isogenies, Bob computes N-isogenies
- Can have $M = 2^a$ and $N = 3^b$, but largest such prime is $p = 17$

2. Twin smooths (and first attempts)

Smoothness

Def^{n}: An integer is said to be B-smooth if it has no prime factors larger than B

Def^{n}: Two consecutive integers m and $m+1$ are B-smooth "twins" if
$m \cdot (m+1)$ is B-smooth

Twin smooths

Goal: find p where $p \pm 1$ both smooth
Equiv: find $(m, m+1)$ smooth with $2m+1$ prime

- Largest 3-smooth twins $(8,9)$.
- Largest 5-smooth twins $(80,81)$.

⋮

- Largest 113-smooth twins have $m = 19316158377073923834000 \approx 2^{74}$
- Largest 113-smooth twins with prime sum $m = 759541500560601866624 \approx 2^{66}$

⋮

- Largest B-smooth twins requires solving $2^{\pi(B)}$ Pell equations (Störmer/Lehmer)

Smoothness probability

The probability that m is $m^{1/u}$-smooth is $\approx \rho(u)$ as $m \to \infty$

Suppose we take a random $m \in [0,2^{256})$

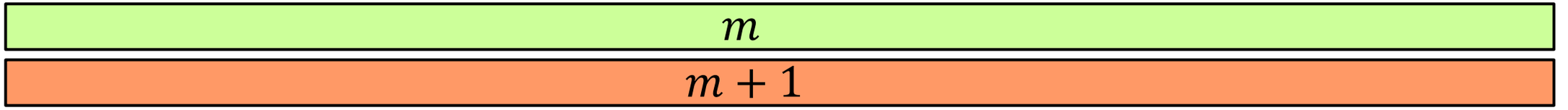
- The probability that m is 2^{128}-smooth is $\approx \rho(2) = 0.3069$
- The probability that m is 2^{64}-smooth is $\approx \rho(4) = 0.0049$
- The probability that m is 2^{32}-smooth is $\approx \rho(8) = 3.2 \cdot 10^{-8}$
- The probability that m is 2^{16}-smooth is $\approx \rho(16) = 1.1 \cdot 10^{-21}$

u	$\rho(u)$
1	1
2	3.0685282×10^{-1}
3	4.8608388×10^{-2}
4	4.9109256×10^{-3}
5	3.5472470×10^{-4}
6	1.9649696×10^{-5}
7	8.7456700×10^{-7}
8	3.2320693×10^{-8}
9	1.0162483×10^{-9}
10	$2.7701718 \times 10^{-11}$

Prior methods

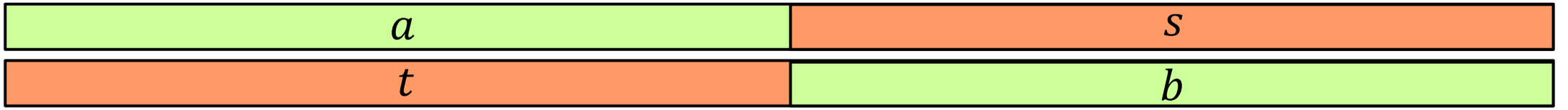
$m \approx 2^{256}$ $B = 2^{16}$

Method 1 (Naïve): search smooth $m \approx 2^{256}$, check $m \pm 1$



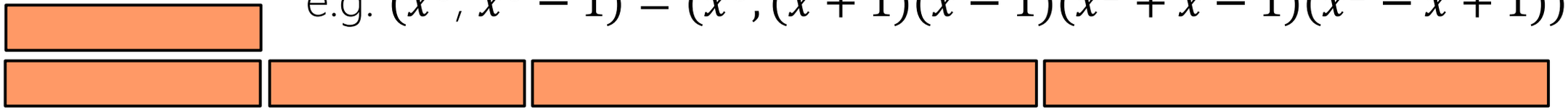
Pr(smooth) $\approx 2^{-70}$

Method 2 (XGCD): search smooth coprime $a, b \approx 2^{128}$ set $m = |as|$ and $m + 1 = |bt|$



Pr(smooth) $\approx 2^{-50}$

Method 3 (Power): search $(m, m-1) = (x^n, x^n - 1)$,
e.g. $(x^6, x^6 - 1) = (x^6, (x+1)(x-1)(x^2+x-1)(x^2-x+1))$

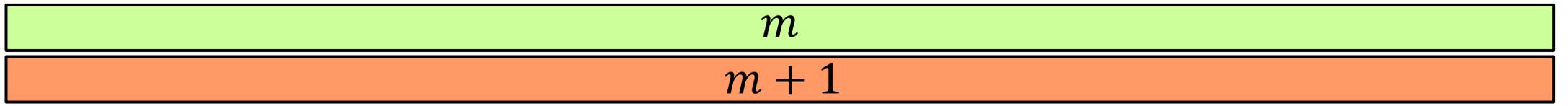


Pr(smooth) $\approx 2^{-36.2}$

Method 1: naïve $m \approx 2^{256}$ $B = 2^{16}$

Search smooth $m \approx 2^{256}$, check $m \pm 1$

The probability that $m + 1$ is 2^{16}-smooth is $\approx \rho(16) = 1.1 \cdot 10^{-21} \approx 2^{-70}$



Pr(smooth) $\approx 2^{-70}$

Method 2: XGCD

$m \approx 2^{256}$ $B = 2^{16}$

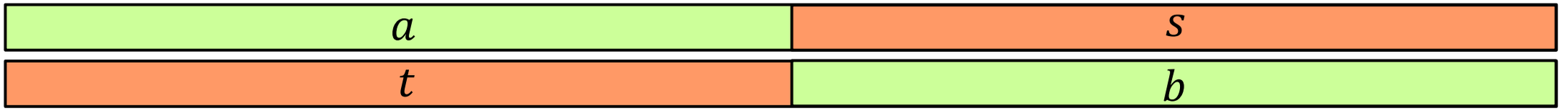
Recall that if $\mathbf{GCD}(a, b) = 1$, then $\exists\ s, t \in \mathbb{Z}$ such that

$$as + bt = 1$$

e.g. $a = 2^5 = 32$ and $b = 3^3 = 27$, then (extended Euclid) gives $(s, t) = (11, -13)$

$$m = 3^3 \cdot 13$$
$$m + 1 = 2^5 \cdot 11$$

search smooth coprime $a, b \approx 2^{128}$ set $m = |as|$ and $m + 1 = |bt|$



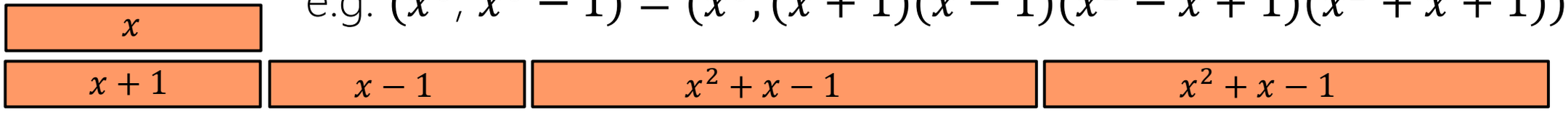
Pr(smooth) $\approx 2^{-50}$

Method 3: $(m+1, m) = (x^n, x^n - 1)$, $m \approx 2^{256}$

- Choose small $n \in \mathbb{N}$ such that $x^n - 1$ factors favorably…
- Larger n means smaller factors, but too large means not enough x to search over
- Sweet spot for $m \approx 2^{256}$ is $n \in \{4,6\}$

Method 3 (Power): search $(m+1, m) = (x^n, x^{n-1})$,

e.g. $(x^6, x^6 - 1) = (x^6, (x+1)(x-1)(x^2 - x + 1)(x^2 + x + 1))$



Pr(smooth) $\approx 2^{-36.2}$

Method 3: examples

$$m + 1 = x^6$$

$$m = (x+1)(x-1)(x^2 - x + 1)(x^2 + x + 1)$$

$B = 2^6$

$$\left(2^3 \cdot 3^4 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 53^2\right)^6$$

x^6

$B = 2^{20}$ (e.g. 6 of [B-SIDH])

$$(7 \cdot 13 \cdot 269 \cdot 439 \cdot 62753)$$
$$\cdot (881 \cdot 15803 \cdot 48437)$$
$$\cdot (43 \cdot 883 \cdot 20161 \cdot 24043 \cdot 34843 \cdot 709153)$$
$$\cdot (73 \cdot 103 \cdot 1321 \cdot 5479 \cdot 9181 \cdot 12541 \cdot 72577)$$

$$(x+1) \cdot (x-1) \cdot \left(x^2 - x + 1\right) \cdot (x^2 + x + 1)$$

$B = 2^{12}$

$$\left(5^3 \cdot 101 \cdot 211 \cdot 461 \cdot 2287\right)^6$$

x^6

$B = 2^{19}$ (e.g. 8 of [B-SIDH])

$$(2 \cdot 3 \cdot 109 \cdot 8821 \cdot 486839)$$
$$\cdot (2^3 \cdot 7 \cdot 37 \cdot 107 \cdot 1607 \cdot 7883)$$
$$\cdot (3 \cdot 79 \cdot 433 \cdot 487 \cdot 5701 \cdot 6199 \cdot 57037 \cdot 78301)$$
$$\cdot (13 \cdot 199 \cdot 349 \cdot 1993 \cdot 3067 \cdot 6373 \cdot 11497 \cdot 19507)$$

$$(x+1) \cdot (x-1) \cdot \left(x^2 - x + 1\right) \cdot (x^2 + x + 1)$$

3. The PTE sieve

- The problem with Method 3 was the higher degree terms

$$\text{e.g. } (x^6,\ x^6-1) = (x^6, (x+1)(x-1)(x^2-x+1)(x^2+x+1))$$

- With $x \in [0, 2^{42})$, the probability of x or $x-1$ or $x+1$ being B-smooth is far greater than that of x^2-x+1 or x^2+x-1

  e.g. with $B = 2^{14}$,

$$\Pr(x \text{ is smooth}) \approx \rho(3) \approx 0.0486 \qquad (\rho(3)^2 \approx 0.0023)$$
$$\Pr(x^2-x+1 \text{ is smooth}) \approx \rho(6) \approx 0.0000196$$

- IDEA: Can we find $(m+1, m) = (f(x), g(x))$ where $f(x)$ and $g(x)$ split completely into linear terms, like

$$f(x) = x^2 \quad \text{and} \quad g(x) = x^2 - 1 = (x+1)(x-1),$$

  but with larger degrees?

u	$\rho(u)$
1	1
2	3.0685282×10^{-1}
3	4.8608388×10^{-2}
4	4.9109256×10^{-3}
5	3.5472470×10^{-4}
6	1.9649696×10^{-5}
7	8.7456700×10^{-7}
8	3.2320693×10^{-8}
9	1.0162483×10^{-9}
10	$2.7701718 \times 10^{-11}$

Split polynomials in $\mathbb{Q}[x]$ with constant differences

$$f(x) = (x-1)(x-2)(x-9)(x-10)$$
$$= x^4 - 22x^3 + 149x^2 - 308x + 180$$
$$= g(x) + 180$$

$$g(x) = x(x-4)(x-7)(x-11)$$
$$= x^4 - 22x^3 + 149x^2 - 308x$$

$$(m+1, m) = (f(x)/180, g(x)/180)$$

($80/180$ of the residues give $f(x) \equiv g(x) \equiv 0 \bmod 180$)

Rather than searching m such that $m+1$ is smooth…

m
$m+1$

….search x such that $x-1$, $x-2$, …, $x-11$ are all smooth

x	$x-4$	$x-7$	$x-11$
$x-1$	$x-2$	$x-9$	$x-10$

The Prouhet-Tarry-Escott (PTE) problem

(Ideal) PTE problem: find disjoint multisets $\{a_1, \dots a_n\}$ and $\{b_1, \dots b_n\}$ with

$$\begin{aligned} a_1 + \cdots + a_n &= b_1 + \cdots + b_n \\ a_1^2 + \cdots + a_n^2 &= b_1^2 + \cdots + b_n^2 \\ &\vdots \\ a_1^{n-1} + \cdots + a_n^{n-1} &= b_1^{n-1} + \cdots + b_n^{n-1} \end{aligned}$$

e.g. $\{0,4,7,11\}$ and $\{1,2,9,10\}$, since

$$0 + 4 + 7 + 11 = 1 + 2 + 9 + 10 = 22$$

$$0^2 + 4^2 + 7^2 + 11^2 = 1^2 + 2^2 + 9^2 + 10^2 = 186$$

$$0^3 + 4^3 + 7^3 + 11^3 = 1^3 + 2^3 + 9^3 + 10^3 = 1738$$

The Prouhet-Tarry-Escott (PTE) problem

(Ideal) PTE problem: find disjoint multisets $\{a_1, \dots a_n\}$ and $\{b_1, \dots b_n\}$ with

$$\begin{aligned} a_1 + \cdots + a_n &= b_1 + \cdots + b_n \\ a_1^2 + \cdots + a_n^2 &= b_1^2 + \cdots + b_n^2 \\ &\vdots \\ a_1^{n-1} + \cdots + a_n^{n-1} &= b_1^{n-1} + \cdots + b_n^{n-1} \end{aligned}$$

e.g. $\{0,4,7,11\}$ and $\{1,2,9,10\}$, since

$$\begin{aligned} 0 + 4 + 7 + 11 = 1 + 2 + 9 + 10 &= 22 \\ 0^2 + 4^2 + 7^2 + 11^2 = 1^2 + 2^2 + 9^2 + 10^2 &= 186 \\ 0^3 + 4^3 + 7^3 + 11^3 = 1^3 + 2^3 + 9^3 + 10^3 &= 1738 \end{aligned}$$

PTE solutions $\leftrightarrow$ split $f(x), g(x) \in \mathbb{Z}[x]$ with $f - g \in \mathbb{Z}$

$g(x) = x(x-4)(x-7)(x-11)$ $\qquad$ $f(x) = (x-1)(x-2)(x-9)(x-10)$

Known PTE solutions

For $m, m+1$ in $[0, 2^{256})$, $n = 6$ is a sweet spot!

```
25  # Solutions of size 6:
26  solutions['size-6'] = [
27  [[0, 3, 5, 11, 13, 16], [1, 1, 8, 8, 15, 15], 1] ,
28  [[0, 5, 6, 16, 17, 22], [1, 2, 10, 12, 20, 21], 1] ,
29  [[0, 4, 9, 17, 22, 26], [1, 2, 12, 14, 24, 25], 1] ,
30  [[0, 7, 7, 21, 21, 28], [1, 3, 12, 16, 25, 27], 1] ,
31  [[0, 7, 8, 22, 23, 30], [2, 2, 15, 15, 28, 28], 1] ,
32  [[0, 5, 13, 23, 31, 36], [1, 3, 16, 20, 33, 35], 1]
33  [[0, 8, 9, 25, 26, 34], [1, 4, 14, 20, 30, 33], 1] ,
34  [[0, 7, 11, 25, 29, 36], [1, 4, 15, 21, 32, 35], 1]
35  [[0, 9, 11, 29, 31, 40], [1, 5, 16, 24, 35, 39], 1]
36  [[0, 8, 11, 27, 30, 38], [2, 3, 18, 20, 35, 36], 1]
37  [[0, 5, 16, 26, 37, 42], [2, 2, 21, 21, 40, 40], 1]
```

⋮

```
521  [[0, 59, 104, 222, 267, 326], [2, 51, 114, 212, 275, 324], 1] ,
522  [[0, 37, 106, 180, 249, 286], [6, 25, 124, 162, 261, 280], 1] ,
523  [[0, 72, 89, 233, 250, 322], [2, 58, 105, 217, 264, 320], 1] ,
524  [[0, 44, 87, 175, 218, 262], [10, 22, 119, 143, 240, 252], 1] ,
525  [[0, 65, 123, 253, 311, 376], [1, 61, 128, 248, 315, 375], 1] ,
526  [[0, 46, 125, 217, 296, 342], [2, 41, 132, 210, 301, 340], 1] ,
527  [[0, 37, 127, 201, 291, 328], [3, 31, 136, 192, 297, 325], 1] ,
528  [[0, 24, 131, 179, 286, 310], [10, 11, 154, 156, 299, 300], 1] ,
529  [[0, 52, 117, 221, 286, 338], [2, 46, 125, 213, 292, 336], 1] ,
530  [[0, 21, 145, 187, 311, 332], [7, 12, 161, 171, 320, 325], 1] ,
531  [[0, 32, 129, 193, 290, 322], [4, 25, 140, 182, 297, 318], 1] ,
532  [[0, 66, 125, 257, 316, 382], [1, 62, 130, 252, 320, 381], 1]
```

⋮

n	$\lceil \log_2(C_{\min,n}) \rceil$	Bitlength of upper bound	# of solutions
5	13	50	49
6	14	50	2438
7	33	60	8
8	31	60	51
9	52	60	2
10	73	100	1
12	76	100	1

$$f(x) = (x-1)(x-2)(x-10)(x-12)(x-20)(x-21)$$
$$g(x) = x(x-5)(x-6)(x-16)(x-17)(x-22)$$

Pr(smooth) $\approx 2^{-41}$

$$f(x) = (x-2)^2(x-21)^2(x-40)^2$$
$$g(x) = x(x-5)(x-16)(x-26)(x-37)(x-42)$$

Pr(smooth) $\approx 2^{-31}$

$$B = 2^{16},\ x \approx 2^{43}$$

Identifying smooth numbers in an interval

$B = 7$

4350_{1}	4351_{1}	4352_{1}	4353_{1}	4354_{1}	4355_{1}	4356_{1}	4357_{1}	4358_{1}	4359_{1}
4360_{1}	4361_{1}	4362_{1}	4363_{1}	4364_{1}	4365_{1}	4366_{1}	4367_{1}	4368_{1}	4369_{1}
4370_{1}	4371_{1}	4372_{1}	4373_{1}	4374_{1}	4375_{1}	4376_{1}	4377_{1}	4378_{1}	4379_{1}
4380_{1}	4381_{1}	4382_{1}	4383_{1}	4384_{1}	4385_{1}	4386_{1}	4387_{1}	4388_{1}	4389_{1}
4390_{1}	4391_{1}	4392_{1}	4393_{1}	4394_{1}	4395_{1}	4396_{1}	4397_{1}	4398_{1}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of **2**

4350_{2}	4351_{1}	4352_{2}	4353_{1}	4354_{2}	4355_{1}	4356_{2}	4357_{1}	4358_{2}	4359_{1}
4360_{2}	4361_{1}	4362_{2}	4363_{1}	4364_{2}	4365_{1}	4366_{2}	4367_{1}	4368_{2}	4369_{1}
4370_{2}	4371_{1}	4372_{2}	4373_{1}	4374_{2}	4375_{1}	4376_{2}	4377_{1}	4378_{2}	4379_{1}
4380_{2}	4381_{1}	4382_{2}	4383_{1}	4384_{2}	4385_{1}	4386_{2}	4387_{1}	4388_{2}	4389_{1}
4390_{2}	4391_{1}	4392_{2}	4393_{1}	4394_{2}	4395_{1}	4396_{2}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $4 = 2^2$

4350_{2}	4351_{1}	4352_{4}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{4}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{4}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{4}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{4}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{4}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $8 = 2^3$

4350_{2}	4351_{1}	4352_{8}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{8}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{8}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $16 = 2^4$

4350_{2}	4351_{1}	4352_{16}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{16}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{16}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $32 = 2^5$

4350_{2}	4351_{1}	4352_{32}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{16}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{32}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $64 = 2^6$

4350_{2}	4351_{1}	4352_{64}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{16}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{32}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $128 = 2^7$

4350 2	4351 1	4352 128	4353 1	4354 2	4355 1	4356 4	4357 1	4358 2	4359 1
4360 8	4361 1	4362 2	4363 1	4364 4	4365 1	4366 2	4367 1	4368 16	4369 1
4370 2	4371 1	4372 4	4373 1	4374 2	4375 1	4376 8	4377 1	4378 2	4379 1
4380 4	4381 1	4382 2	4383 1	4384 32	4385 1	4386 2	4387 1	4388 4	4389 1
4390 2	4391 1	4392 8	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $256 = 2^8$

4350_{2}	4351_{1}	4352_{256}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{16}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{32}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $\mathbf{512 = 2^9}$

4350_{2}	4351_{1}	4352_{256}	4353_{1}	4354_{2}	4355_{1}	4356_{4}	4357_{1}	4358_{2}	4359_{1}
4360_{8}	4361_{1}	4362_{2}	4363_{1}	4364_{4}	4365_{1}	4366_{2}	4367_{1}	4368_{16}	4369_{1}
4370_{2}	4371_{1}	4372_{4}	4373_{1}	4374_{2}	4375_{1}	4376_{8}	4377_{1}	4378_{2}	4379_{1}
4380_{4}	4381_{1}	4382_{2}	4383_{1}	4384_{32}	4385_{1}	4386_{2}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{8}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of **3**

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 12	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 3	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	4374 6	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 3	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 3	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $9 = 3^2$

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 36	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 9	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	4374 18	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 9	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $27 = 3^3$

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 36	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 9	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	4374 54	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 9	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $81 = 3^4$

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 36	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 9	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	4374 162	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 9	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $243 = 3^5$

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 36	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 9	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	4374 486	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 9	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $729 = 3^6$

4350_{6}	4351_{1}	4352_{64}	4353_{3}	4354_{2}	4355_{1}	4356_{36}	4357_{1}	4358_{2}	4359_{3}
4360_{8}	4361_{1}	4362_{6}	4363_{1}	4364_{4}	4365_{9}	4366_{2}	4367_{1}	4368_{48}	4369_{1}
4370_{2}	4371_{3}	4372_{4}	4373_{1}	4374_{1458}	4375_{1}	4376_{8}	4377_{3}	4378_{2}	4379_{1}
4380_{12}	4381_{1}	4382_{2}	4383_{9}	4384_{32}	4385_{1}	4386_{6}	4387_{1}	4388_{4}	4389_{1}
4390_{2}	4391_{1}	4392_{24}	4393_{1}	4394_{2}	4395_{1}	4396_{4}	4397_{1}	4398_{2}	4399_{1}

Identifying smooth numbers in an interval

$B = 7$

multiples of $\mathbf{2187 = 3^7}$

4350 6	4351 1	4352 64	4353 3	4354 2	4355 1	4356 36	4357 1	4358 2	4359 3
4360 8	4361 1	4362 6	4363 1	4364 4	4365 9	4366 2	4367 1	4368 48	4369 1
4370 2	4371 3	4372 4	4373 1	**4374** 4374	4375 1	4376 8	4377 3	4378 2	4379 1
4380 12	4381 1	4382 2	4383 9	4384 32	4385 1	4386 6	4387 1	4388 4	4389 1
4390 2	4391 1	4392 24	4393 1	4394 2	4395 1	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of **5**

4350 30	4351 1	4352 64	4353 3	4354 2	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 1	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 48	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 5	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 2	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 1
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $25 = 5^2$

4350 150	4351 1	4352 64	4353 3	4354 2	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 1	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 48	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 25	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 2	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 1
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $125 = 5^3$

4350 150	4351 1	4352 64	4353 3	4354 2	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 1	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 48	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 125	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 2	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 1
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $625 = 5^4$

4350 150	4351 1	4352 64	4353 3	4354 2	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 1	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 48	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 625	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 2	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 1
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $3125 = 5^5$

4350 150	4351 1	4352 64	4353 3	4354 2	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 1	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 48	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 625	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 2	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 1
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 4	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of **7**

4350 150	4351 1	4352 64	4353 3	**4354** 14	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	**4361** 7	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	**4368** 336	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	**4375** 4375	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	**4382** 14	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	**4389** 7
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	**4396** 28	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $49 = 7^2$

4350 150	4351 1	4352 64	4353 3	4354 14	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 49	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 336	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 4375	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 14	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 7
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 28	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

multiples of $\mathbf{343 = 7^3}$

4350 150	4351 1	4352 64	4353 3	4354 14	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 49	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 336	4369 1
4370 10	4371 3	4372 4	4373 1	4374 4374	4375 4375	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 14	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 7
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 28	4397 1	4398 2	4399 1

Identifying smooth numbers in an interval

$B = 7$

index $\stackrel{?}{=}$ number

4350 150	4351 1	4352 64	4353 3	4354 14	4355 5	4356 36	4357 1	4358 2	4359 3
4360 40	4361 49	4362 6	4363 1	4364 4	4365 45	4366 2	4367 1	4368 336	4369 1
4370 10	4371 3	4372 4	4373 1	**4374** 4374	**4375** 4375	4376 8	4377 3	4378 2	4379 1
4380 60	4381 1	4382 14	4383 9	4384 32	4385 5	4386 6	4387 1	4388 4	4389 7
4390 10	4391 1	4392 24	4393 1	4394 2	4395 5	4396 28	4397 1	4398 2	4399 1

$$4374 = 2 \cdot 3^7$$

$$4375 = 5^4 \cdot 7$$

Identifying smooth numbers in an interval

0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

Sieving optimisations

- Use logarithms and replace all $\times$'s with $+$'s
- Approximations
- Skip small primes

…many many more…

The PTE sieve

- Phase 1: process intervals (size depending on memory) of numbers into bitstrings using primes $\{2,3,\ldots,p\}$, $p \leq B$
- Phase 2: check PTE solution(s) to align with 1's

(perfectly parallelizable)

PTE sieve: example $B = 2^{15}$

5170314186730 5170314186731 5170314186732 5170314186733 5170314186734 5170314186735 5170314186736 5170314186737 5170314186738 5170314186739

5170314186740 5170314186741 5170314186742 5170314186743 5170314186744 5170314186745 5170314186746 5170314186747 5170314186748 5170314186749

5170314186750 5170314186751 5170314186752 5170314186753 5170314186754 5170314186755 5170314186756 5170314186757 5170314186758 5170314186759

5170314186760 5170314186761 5170314186762 5170314186763 5170314186764 5170314186765 5170314186766 5170314186767 5170314186768 5170314186769

5170314186770 5170314186771 5170314186772 5170314186773 5170314186774 5170314186775 5170314186776 5170314186777 5170314186778 5170314186779

Step 1: sieve interval with prime (powers) in $\{2, 3, 5, 7, \dots, 32719, 32749\}$

PTE sieve: example $B = 2^{15}$

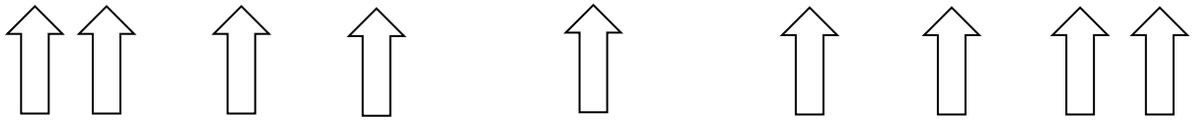
5170314186730	5170314186731	5170314186732	5170314186733	5170314186734	5170314186735	5170314186736	5170314186737	5170314186738	5170314186739
1	0	0	0	0	0	0	0	1	1
5170314186740	5170314186741	5170314186742	5170314186743	5170314186744	5170314186745	5170314186746	5170314186747	5170314186748	5170314186749
1	0	1	0	1	0	0	1	0	0
5170314186750	5170314186751	5170314186752	5170314186753	5170314186754	5170314186755	5170314186756	5170314186757	5170314186758	5170314186759
1	0	1	0	1	1	0	0	0	0
5170314186760	5170314186761	5170314186762	5170314186763	5170314186764	5170314186765	5170314186766	5170314186767	5170314186768	5170314186769
0	0	0	0	0	0	0	0	0	0
5170314186770	5170314186771	5170314186772	5170314186773	5170314186774	5170314186775	5170314186776	5170314186777	5170314186778	5170314186779
0	0	0	0	0	0	0	0	0	0

Output of step 1: $\mathbf{1000000011101010010010101100\ldots00}$

PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

$$1000000011101010010010101011000 \ldots 0$$

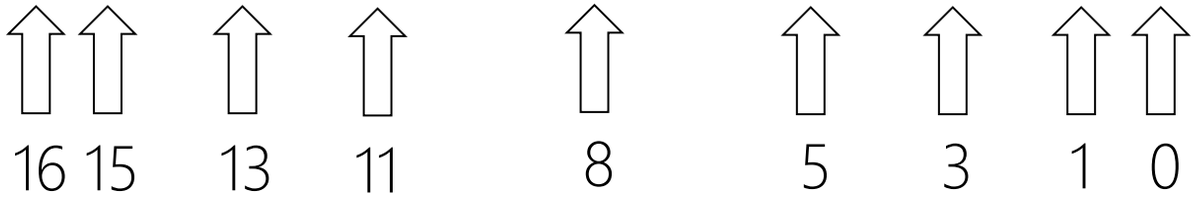


Step 2: check PTE solution(s) against bitstring…

PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

$$1000000011101010010010101011000 \ldots 0$$

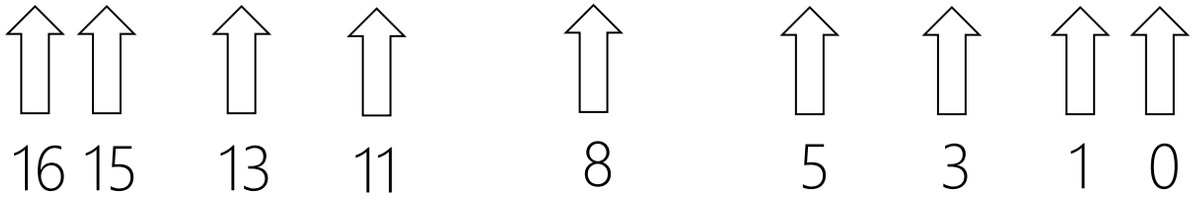


Step 2: check PTE solution(s) against bitstring…

PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

$$1000000011101010010010101011000 \ldots 0$$

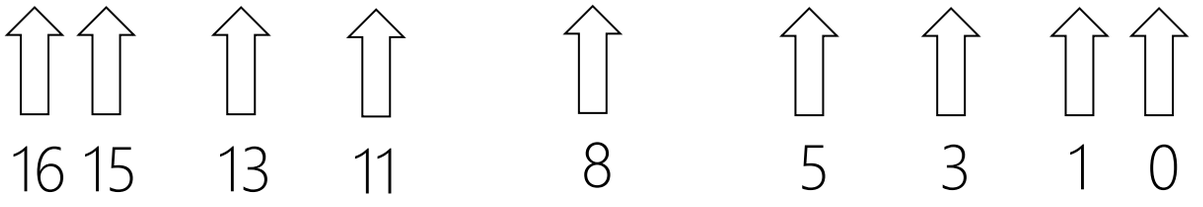


Step 2: check PTE solution(s) against bitstring…

PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

$$1000000011101010010010101011000 \ldots 0$$

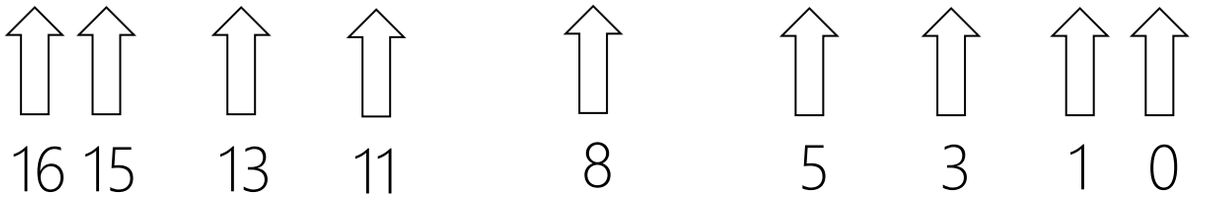


Step 2: check PTE solution(s) against bitstring…

PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

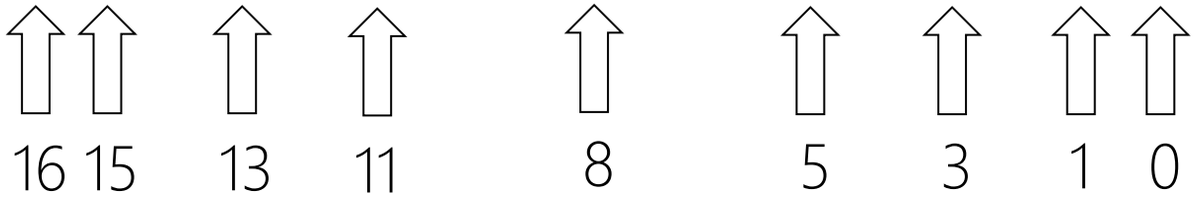
$$1000000011101010010010110110000 \ldots 0$$



PTE sieve: example $B = 2^{15}$

PTE soln: $\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$

$$1000000011101010010010110110000 \ldots 0$$



$u = 5170314186755$

PTE sieve: example $B = 2^{15}$

$$\{0,3,5,11,13,16\} =_5 \{1,1,8,8,15,15\}$$

$g(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$ $\qquad$ $f(x) = (x-1)^2(x-8)^2(x-15)^2$

$u = 5170314186755$

$f(x) - g(x) = 14400$ and $f(u) \equiv g(u) \equiv 0 \bmod 14400$

$m = g(u)/14400$ and $m + 1 = f(u)/14400$

$p = 2m + 1$ is prime!!!

$$p + 1 = 2 \cdot 3^2 \cdot 23^2 \cdot 41^2 \cdot 71^2 \cdot 83^2 \cdot 919^2 \cdot 1117^2 \cdot 1163^2 \cdot 1237^2 \cdot 6571^2 \cdot 11927^2 \cdot 18637^2 \cdot 32029^2$$

$p = 265319464891319853876302880884726722210256475303002503310412276022343680 1$

$$p - 1 = 2^{12} \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 29 \cdot 31 \cdot 43 \cdot 53 \cdot 103 \cdot 113 \cdot 181 \cdot 191 \cdot 211 \cdot 277 \cdot 557 \cdot 1093 \cdot 2663 \cdot 2897 \cdot 3347 \cdot 4783 \cdot 7963 \cdot 8623 \cdot 9787 \cdot 19841 \cdot 31489$$

Future work

Better methods / smoother twins 

C-Meyer-Naehrig. Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem. EUROCRYPT 2021, to appear. https://eprint.iacr.org/2020/1283.pdf