

1109496723119

1109496723120

1109496723121

1109496723122

1109496723123

1109496723124

1109496723125

1109496723126

1109496723127

1109496723128

1109496723129

1109496723130

1109496723131

1109496723132

1109496723133

1109496723134

Finding twin smooth integers

Michael Naehrig
Microsoft Research

joint work with Craig Costello and Michael Meyer

Tutte Colloquium
Combinatorics and Optimization, University of Waterloo

2021-01-29

1109496723119

1109496723120

1109496723121

1109496723122

1109496723123

1109496723124

1109496723125

1109496723126

1109496723127

1109496723128

1109496723129

1109496723130

1109496723131

1109496723132

1109496723133

1109496723134

1109496723119 = 709 · 1564875491
1109496723120 = $2^4 \cdot 3^2 \cdot 5 \cdot 1873 \cdot 822727$
1109496723121 = 643 · 1725500347
1109496723122 = 2 · 79 · 7022131159
1109496723123 = 3 · 1153 · 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 · 467 · 12401 · 14737
1109496723128 = $2^3 \cdot 67 \cdot 8231 \cdot 251483$
1109496723129 = $3^4 \cdot 2339 \cdot 5856131$
1109496723130 = 2 · 5 · 110949672313
1109496723131 = 61 · 18188470871
1109496723132 = $2^2 \cdot 3 \cdot 7^3 \cdot 691 \cdot 390097$
1109496723133 = 1109496723133
1109496723134 = 2 · 554748361567

789985665896729546962271648201932479916708211432100206574984369714099006240
789985665896729546962271648201932479916708211432100206574984369714099006241

789985665896729546962271648201932479916708211432100206574984369714099006240
 $= 2^6 \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 23 \cdot 107 \cdot 149 \cdot 401 \cdot 503 \cdot 599 \cdot 727 \cdot 941 \cdot 977 \cdot 2351 \cdot 3469 \cdot 3779 \cdot 4273 \cdot$
 $5051 \cdot 6211 \cdot 9001 \cdot 11447 \cdot 12589 \cdot 14159 \cdot 14779 \cdot 24919$

789985665896729546962271648201932479916708211432100206574984369714099006241
 $= 19^6 \cdot 151^2 \cdot 601^2 \cdot 1009^2 \cdot 1103^2 \cdot 1427^2 \cdot 2011^2 \cdot 6599^2 \cdot 7321^2 \cdot 9091^2 \cdot 32191^2$

Smooth integers

$m \in \mathbb{Z}, B > 0$:

m is B -smooth

if for any prime divisor

$q \mid m$: $q \leq B$.

5-smooth:

$$m = 15 = 3 \cdot 5$$

$$m + 1 = 16 = 2^4$$

Twin smooth integers

$m \in \mathbb{Z}$, $B > 0$:

$(m, m + 1)$ are twin
 B -smooth integers

if m and $m + 1$ are
both B -smooth.

Twin 5-smooth:

$$m = 15 = 3 \cdot 5$$

$$m + 1 = 16 = 2^4$$

$$m = 24 = 2^3 \cdot 3$$

$$m + 1 = 25 = 5^2$$

$$m = 80 = 2^4 \cdot 5$$

$$m + 1 = 81 = 3^4$$

Twin smooth integers

All twin 5-smooth
integers:

$(m, m + 1)$	$m + (m + 1)$
(1,2)	3
(2,3)	5
(3,4)	7
(4,5)	9
(5,6)	11
(8,9)	17
(9,10)	19
(15,16)	31
(24,25)	49
(80,81)	161

Smooth integers

$$99999998 = 2 \cdot 49999999$$

$$99999999 = 3^2 \cdot 239 \cdot 4649$$

$$100000000 = 2^7 \cdot 5^7$$

$$100000001 = 11 \cdot 909091$$

$$100000002 = 2 \cdot 3 \cdot 47 \cdot 35461$$

$$100000003 = 13 \cdot 769231$$

$$100000004 = 2^2 \cdot 7 \cdot 19 \cdot 18797$$

$$100000005 = 3 \cdot 5 \cdot 666667$$

Smooth integers

$$9999998 = 2 \cdot 4999999$$

$$9999999 = 3^2 \cdot 239 \cdot 4649$$

$$10000000 = 2^7 \cdot 5^7$$

$$10000001 = 11 \cdot 909091$$

$$10000002 = 2 \cdot 3 \cdot 47 \cdot 35461$$

$$10000003 = 13 \cdot 769231$$

$$10000004 = 2^2 \cdot 7 \cdot 19 \cdot 18797$$

$$10000005 = 3 \cdot 5 \cdot 666667$$

$$10000006 = 2 \cdot 83 \cdot 107 \cdot 563$$

$$10000007 = 941 \cdot 10627$$

$$10000008 = 2^3 \cdot 3^2 \cdot 138889$$

$$10000009 = 23 \cdot 434783$$

$$10000010 = 2 \cdot 5 \cdot 101 \cdot 9901$$

$$10000011 = 3 \cdot 7 \cdot 31 \cdot 15361$$

$$10000012 = 2^2 \cdot 11 \cdot 17 \cdot 29 \cdot 461$$

$$10000013 = 421 \cdot 23753$$

$$10000014 = 2 \cdot 3 \cdot 179 \cdot 9311$$

$$10000015 = 5 \cdot 2000003$$

$$10000016 = 2^4 \cdot 13 \cdot 131 \cdot 367$$

$$10000017 = 3^4 \cdot 123457$$

$$10000018 = 2 \cdot 7^2 \cdot 67 \cdot 1523$$

$$10000019 = 10000019$$

$$10000020 = 2^2 \cdot 3 \cdot 5 \cdot 166667$$

$$10000021 = 97 \cdot 103093$$

$$10000022 = 2 \cdot 5000011$$

$$10000023 = 3 \cdot 11 \cdot 19 \cdot 41 \cdot 389$$

$$10000024 = 2^3 \cdot 1250003$$

$$10000025 = 5^2 \cdot 7 \cdot 57143$$

$$10000026 = 2 \cdot 3^2 \cdot 555557$$

$$10000027 = 37 \cdot 270271$$

$$10000028 = 2^2 \cdot 59 \cdot 42373$$

$$10000029 = 3 \cdot 13 \cdot 17 \cdot 15083$$

Twin smooth integers

$$11859205 = 5 \cdot 31 \cdot 76511$$

$$11859206 = 2 \cdot 83 \cdot 199 \cdot 359$$

$$11859207 = 3 \cdot 733 \cdot 5393$$

$$11859208 = 2^3 \cdot 149 \cdot 9949$$

$$11859209 = 41 \cdot 289249$$

$$11859210 = 2 \cdot 3^4 \cdot 5 \cdot 11^4$$

$$11859211 = 7 \cdot 13 \cdot 19^4$$

$$11859212 = 2^2 \cdot 383 \cdot 7741$$

The problem

Given B and N .

Find an integer $N/2 < m \leq N$ such that $(m, m + 1)$ are twin B -smooth.

Find **all** integers $N/2 < m \leq N \dots$

Find **enough** integers $N/2 < m \leq N \dots$

Identifying smooth integers

Given a single $m \in \mathbb{Z}$, $B > 0$:

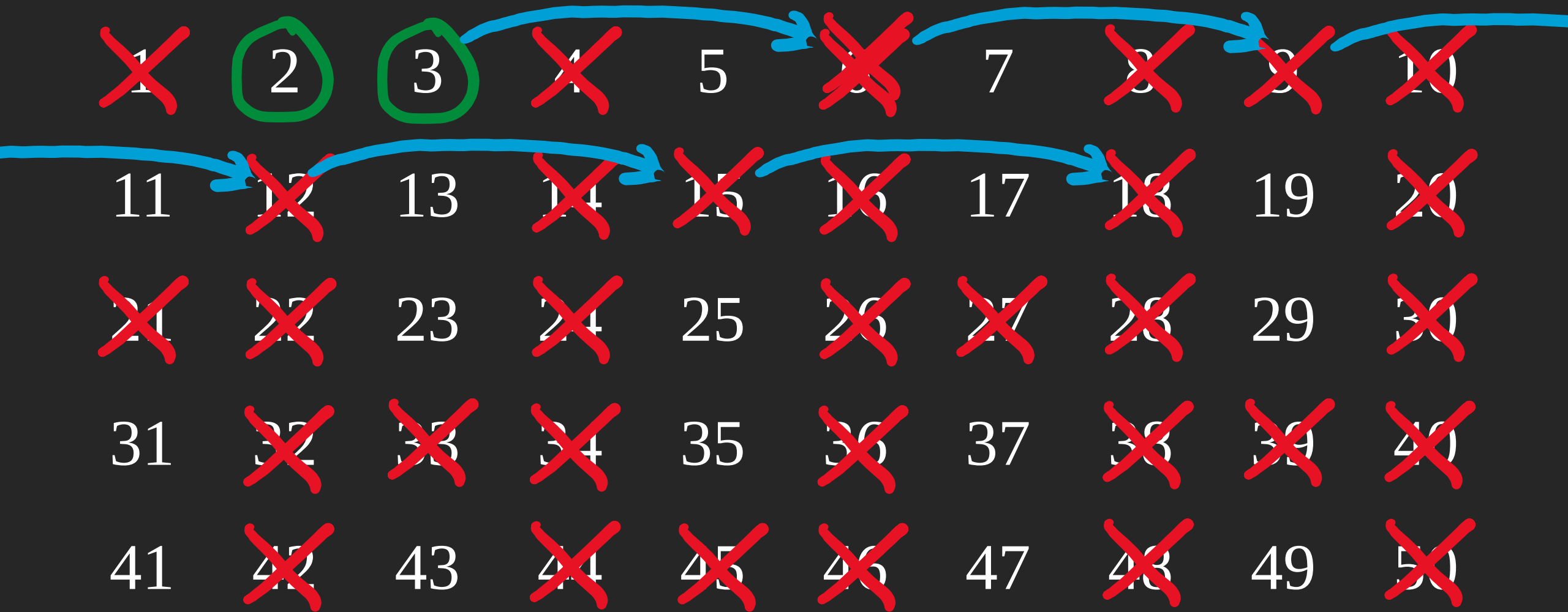
Factor m and check whether $q \leq B$ for its largest prime divisor q .

What are the B -smooths in an interval $[L, R] = \{L, L + 1, L + 2, \dots, R\}$?

The sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

The sieve of Eratosthenes



The sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

The sieve of Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

The sieve of Eratosthenes



Sieving for smooth numbers

$$B = 5$$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₁	3 ₁	4 ₁	5 ₁	6 ₁	7 ₁	8 ₁	9 ₁	10 ₁
11 ₁	12 ₁	13 ₁	14 ₁	15 ₁	16 ₁	17 ₁	18 ₁	19 ₁	20 ₁
21 ₁	22 ₁	23 ₁	24 ₁	25 ₁	26 ₁	27 ₁	28 ₁	29 ₁	30 ₁
31 ₁	32 ₁	33 ₁	34 ₁	35 ₁	36 ₁	37 ₁	38 ₁	39 ₁	40 ₁
41 ₁	42 ₁	43 ₁	44 ₁	45 ₁	46 ₁	47 ₁	48 ₁	49 ₁	50 ₁

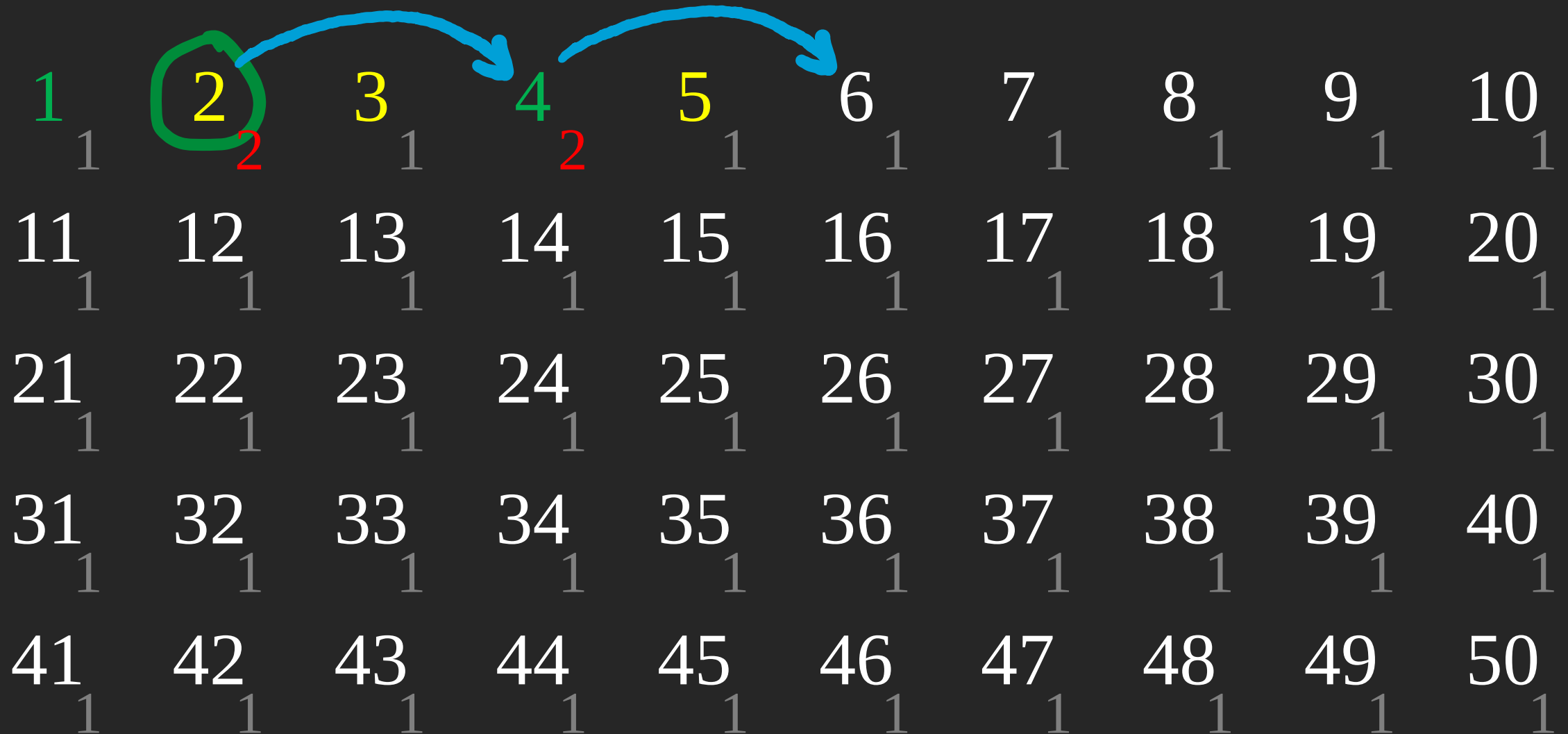
Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₁	5 ₁	6 ₁	7 ₁	8 ₁	9 ₁	10 ₁
11 ₁	12 ₁	13 ₁	14 ₁	15 ₁	16 ₁	17 ₁	18 ₁	19 ₁	20 ₁
21 ₁	22 ₁	23 ₁	24 ₁	25 ₁	26 ₁	27 ₁	28 ₁	29 ₁	30 ₁
31 ₁	32 ₁	33 ₁	34 ₁	35 ₁	36 ₁	37 ₁	38 ₁	39 ₁	40 ₁
41 ₁	42 ₁	43 ₁	44 ₁	45 ₁	46 ₁	47 ₁	48 ₁	49 ₁	50 ₁

Sieving for smooth numbers

$$B = 5$$



Sieving for smooth numbers

$$B = 5$$



1 ₁	2 ₂	3 ₁	4 ₂	5 ₁	6 ₂	7 ₁	8 ₁	9 ₁	10 ₁
11 ₁	12 ₁	13 ₁	14 ₁	15 ₁	16 ₁	17 ₁	18 ₁	19 ₁	20 ₁
21 ₁	22 ₁	23 ₁	24 ₁	25 ₁	26 ₁	27 ₁	28 ₁	29 ₁	30 ₁
31 ₁	32 ₁	33 ₁	34 ₁	35 ₁	36 ₁	37 ₁	38 ₁	39 ₁	40 ₁
41 ₁	42 ₁	43 ₁	44 ₁	45 ₁	46 ₁	47 ₁	48 ₁	49 ₁	50 ₁

Sieving for smooth numbers

$B = 5$

1 ₁	2 ₂	3 ₁	4 ₂	5 ₁	6 ₂	7 ₁	8 ₂	9 ₁	10 ₂
11 ₁	12 ₁	13 ₁	14 ₁	15 ₁	16 ₁	17 ₁	18 ₁	19 ₁	20 ₁
21 ₁	22 ₁	23 ₁	24 ₁	25 ₁	26 ₁	27 ₁	28 ₁	29 ₁	30 ₁
31 ₁	32 ₁	33 ₁	34 ₁	35 ₁	36 ₁	37 ₁	38 ₁	39 ₁	40 ₁
41 ₁	42 ₁	43 ₁	44 ₁	45 ₁	46 ₁	47 ₁	48 ₁	49 ₁	50 ₁

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₂	5 ₁	6 ₂	7 ₁	8 ₂	9 ₁	10 ₂
11 ₁	12 ₂	13 ₁	14 ₂	15 ₁	16 ₂	17 ₁	18 ₂	19 ₁	20 ₂
21 ₁	22 ₂	23 ₁	24 ₂	25 ₁	26 ₂	27 ₁	28 ₂	29 ₁	30 ₂
31 ₁	32 ₂	33 ₁	34 ₂	35 ₁	36 ₂	37 ₁	38 ₂	39 ₁	40 ₂
41 ₁	42 ₂	43 ₁	44 ₂	45 ₁	46 ₂	47 ₁	48 ₂	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$



1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₂	9 ₁	10 ₂
11 ₁	12 ₂	13 ₁	14 ₂	15 ₁	16 ₂	17 ₁	18 ₂	19 ₁	20 ₂
21 ₁	22 ₂	23 ₁	24 ₂	25 ₁	26 ₂	27 ₁	28 ₂	29 ₁	30 ₂
31 ₁	32 ₂	33 ₁	34 ₂	35 ₁	36 ₂	37 ₁	38 ₂	39 ₁	40 ₂
41 ₁	42 ₂	43 ₁	44 ₂	45 ₁	46 ₂	47 ₁	48 ₂	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₄	9 ₁	10 ₂
11 ₁	12 ₂	13 ₁	14 ₂	15 ₁	16 ₂	17 ₁	18 ₂	19 ₁	20 ₂
21 ₁	22 ₂	23 ₁	24 ₂	25 ₁	26 ₂	27 ₁	28 ₂	29 ₁	30 ₂
31 ₁	32 ₂	33 ₁	34 ₂	35 ₁	36 ₂	37 ₁	38 ₂	39 ₁	40 ₂
41 ₁	42 ₂	43 ₁	44 ₂	45 ₁	46 ₂	47 ₁	48 ₂	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₄	9 ₁	10 ₂
11 ₁	12 ₄	13 ₁	14 ₂	15 ₁	16 ₂	17 ₁	18 ₂	19 ₁	20 ₂
21 ₁	22 ₂	23 ₁	24 ₂	25 ₁	26 ₂	27 ₁	28 ₂	29 ₁	30 ₂
31 ₁	32 ₂	33 ₁	34 ₂	35 ₁	36 ₂	37 ₁	38 ₂	39 ₁	40 ₂
41 ₁	42 ₂	43 ₁	44 ₂	45 ₁	46 ₂	47 ₁	48 ₂	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₄	9 ₁	10 ₂
11 ₁	12 ₄	13 ₁	14 ₂	15 ₁	16 ₄	17 ₁	18 ₂	19 ₁	20 ₄
21 ₁	22 ₂	23 ₁	24 ₄	25 ₁	26 ₂	27 ₁	28 ₄	29 ₁	30 ₂
31 ₁	32 ₄	33 ₁	34 ₂	35 ₁	36 ₄	37 ₁	38 ₂	39 ₁	40 ₄
41 ₁	42 ₂	43 ₁	44 ₄	45 ₁	46 ₂	47 ₁	48 ₄	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₈	9 ₁	10 ₂
11 ₁	12 ₄	13 ₁	14 ₂	15 ₁	16 ₈	17 ₁	18 ₂	19 ₁	20 ₄
21 ₁	22 ₂	23 ₁	24 ₈	25 ₁	26 ₂	27 ₁	28 ₄	29 ₁	30 ₂
31 ₁	32 ₈	33 ₁	34 ₂	35 ₁	36 ₄	37 ₁	38 ₂	39 ₁	40 ₈
41 ₁	42 ₂	43 ₁	44 ₄	45 ₁	46 ₂	47 ₁	48 ₈	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₈	9 ₁	10 ₂
11 ₁	12 ₄	13 ₁	14 ₂	15 ₁	16 ₁₆	17 ₁	18 ₂	19 ₁	20 ₄
21 ₁	22 ₂	23 ₁	24 ₈	25 ₁	26 ₂	27 ₁	28 ₄	29 ₁	30 ₂
31 ₁	32 ₁₆	33 ₁	34 ₂	35 ₁	36 ₄	37 ₁	38 ₂	39 ₁	40 ₈
41 ₁	42 ₂	43 ₁	44 ₄	45 ₁	46 ₂	47 ₁	48 ₁₆	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₁	4 ₄	5 ₁	6 ₂	7 ₁	8 ₈	9 ₁	10 ₂
11 ₁	12 ₄	13 ₁	14 ₂	15 ₁	16 ₁₆	17 ₁	18 ₂	19 ₁	20 ₄
21 ₁	22 ₂	23 ₁	24 ₈	25 ₁	26 ₂	27 ₁	28 ₄	29 ₁	30 ₂
31 ₁	32 ₃₂	33 ₁	34 ₂	35 ₁	36 ₄	37 ₁	38 ₂	39 ₁	40 ₈
41 ₁	42 ₂	43 ₁	44 ₄	45 ₁	46 ₂	47 ₁	48 ₁₆	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 1	4 4	5 1	6 2	7 1	8 8	9 1	10 2
11 1	12 4	13 1	14 2	15 1	16 16	17 1	18 2	19 1	20 4
21 1	22 2	23 1	24 8	25 1	26 2	27 1	28 4	29 1	30 2
31 1	32 32	33 1	34 2	35 1	36 4	37 1	38 2	39 1	40 8
41 1	42 2	43 1	44 4	45 1	46 2	47 1	48 16	49 1	50 2

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 3	4 4	5 1	6 6	7 1	8 8	9 3	10 2
11 1	12 12	13 1	14 2	15 3	16 16	17 1	18 6	19 1	20 4
21 3	22 2	23 1	24 24	25 1	26 2	27 3	28 4	29 1	30 6
31 1	32 32	33 3	34 2	35 1	36 12	37 1	38 2	39 3	40 8
41 1	42 6	43 1	44 4	45 3	46 2	47 1	48 48	49 1	50 2

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₃	4 ₄	5 ₁	6 ₆	7 ₁	8 ₈	9 ₉	10 ₂
11 ₁	12 ₁₂	13 ₁	14 ₂	15 ₃	16 ₁₆	17 ₁	18 ₁₈	19 ₁	20 ₄
21 ₃	22 ₂	23 ₁	24 ₂₄	25 ₁	26 ₂	27 ₉	28 ₄	29 ₁	30 ₆
31 ₁	32 ₃₂	33 ₃	34 ₂	35 ₁	36 ₃₆	37 ₁	38 ₂	39 ₃	40 ₈
41 ₁	42 ₆	43 ₁	44 ₄	45 ₉	46 ₂	47 ₁	48 ₄₈	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₃	4 ₄	5 ₁	6 ₆	7 ₁	8 ₈	9 ₉	10 ₂
11 ₁	12 ₁₂	13 ₁	14 ₂	15 ₃	16 ₁₆	17 ₁	18 ₁₈	19 ₁	20 ₄
21 ₃	22 ₂	23 ₁	24 ₂₄	25 ₁	26 ₂	27 ₂₇	28 ₄	29 ₁	30 ₆
31 ₁	32 ₃₂	33 ₃	34 ₂	35 ₁	36 ₃₆	37 ₁	38 ₂	39 ₃	40 ₈
41 ₁	42 ₆	43 ₁	44 ₄	45 ₉	46 ₂	47 ₁	48 ₄₈	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 ₁	2 ₂	3 ₃	4 ₄	5 ₁	6 ₆	7 ₁	8 ₈	9 ₉	10 ₂
11 ₁	12 ₁₂	13 ₁	14 ₂	15 ₃	16 ₁₆	17 ₁	18 ₁₈	19 ₁	20 ₄
21 ₃	22 ₂	23 ₁	24 ₂₄	25 ₁	26 ₂	27 ₂₇	28 ₄	29 ₁	30 ₆
31 ₁	32 ₃₂	33 ₃	34 ₂	35 ₁	36 ₃₆	37 ₁	38 ₂	39 ₃	40 ₈
41 ₁	42 ₆	43 ₁	44 ₄	45 ₉	46 ₂	47 ₁	48 ₄₈	49 ₁	50 ₂

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 3	4 4	5 5	6 6	7 1	8 8	9 9	10 10
11 1	12 12	13 1	14 2	15 15	16 16	17 1	18 18	19 1	20 20
21 3	22 2	23 1	24 24	25 5	26 2	27 27	28 4	29 1	30 30
31 1	32 32	33 3	34 2	35 5	36 36	37 1	38 2	39 3	40 40
41 1	42 6	43 1	44 4	45 45	46 2	47 1	48 48	49 1	50 10

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 3	4 4	5 5	6 6	7 1	8 8	9 9	10 10
11 1	12 12	13 1	14 2	15 15	16 16	17 1	18 18	19 1	20 20
21 3	22 2	23 1	24 24	25 25	26 2	27 27	28 4	29 1	30 30
31 1	32 32	33 3	34 2	35 5	36 36	37 1	38 2	39 3	40 40
41 1	42 6	43 1	44 4	45 45	46 2	47 1	48 48	49 1	50 50

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 3	4 4	5 5	6 6	7 1	8 8	9 9	10 10
11 1	12 12	13 1	14 2	15 15	16 16	17 1	18 18	19 1	20 20
21 3	22 2	23 1	24 24	25 25	26 2	27 27	28 4	29 1	30 30
31 1	32 32	33 3	34 2	35 5	36 36	37 1	38 2	39 3	40 40
41 1	42 6	43 1	44 4	45 45	46 2	47 1	48 48	49 1	50 50

Sieving for smooth numbers

$$B = 5$$

1 1	2 2	3 3	4 4	5 5	6 6	7 1	8 8	9 9	10 10
11 1	12 12	13 1	14 2	15 15	16 16	17 1	18 18	19 1	20 20
21 3	22 2	23 1	24 24	25 25	26 2	27 27	28 4	29 1	30 30
31 1	32 32	33 3	34 2	35 5	36 36	37 1	38 2	39 3	40 40
41 1	42 6	43 1	44 4	45 45	46 2	47 1	48 48	49 1	50 50

Sieving for smooth numbers

$$B = 5$$

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

Sieving for smooth numbers

$$B = 5$$

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

Sieving for smooth numbers

$$B = 5$$

1111101110100110101000110100101000100010000100101

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

2

51 ₁	52 ₁	53 ₁	54 ₁	55 ₁	56 ₁	57 ₁	58 ₁	59 ₁	60 ₁
61 ₁	62 ₁	63 ₁	64 ₁	65 ₁	66 ₁	67 ₁	68 ₁	69 ₁	70 ₁
71 ₁	72 ₁	73 ₁	74 ₁	75 ₁	76 ₁	77 ₁	78 ₁	79 ₁	80 ₁
81 ₁	82 ₁	83 ₁	84 ₁	85 ₁	86 ₁	87 ₁	88 ₁	89 ₁	90 ₁
91 ₁	92 ₁	93 ₁	94 ₁	95 ₁	96 ₁	97 ₁	98 ₁	99 ₁	100 ₁

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51	52	53	54	55	56	57	58	59	60
₁	₂	₁	₂	₁	₂	₁	₂	₁	₂
61	62	63	64	65	66	67	68	69	70
₁	₂	₁	₂	₁	₂	₁	₂	₁	₂
71	72	73	74	75	76	77	78	79	80
₁	₂	₁	₂	₁	₂	₁	₂	₁	₂
81	82	83	84	85	86	87	88	89	90
₁	₂	₁	₂	₁	₂	₁	₂	₁	₂
91	92	93	94	95	96	97	98	99	100
₁	₂	₁	₂	₁	₂	₁	₂	₁	₂

Sieving for smooth numbers

$\{2, 3, 5\}$

$$B = 5$$

8

51 ₁	52 ₄	53 ₁	54 ₂	55 ₁	56 ₄	57 ₁	58 ₂	59 ₁	60 ₄
61 ₁	62 ₂	63 ₁	64 ₄	65 ₁	66 ₂	67 ₁	68 ₄	69 ₁	70 ₂
71 ₁	72 ₄	73 ₁	74 ₂	75 ₁	76 ₄	77 ₁	78 ₂	79 ₁	80 ₄
81 ₁	82 ₂	83 ₁	84 ₄	85 ₁	86 ₂	87 ₁	88 ₄	89 ₁	90 ₂
91 ₁	92 ₄	93 ₁	94 ₂	95 ₁	96 ₄	97 ₁	98 ₂	99 ₁	100 ₄

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 1	52 4	53 1	54 2	55 1	56 8	57 1	58 2	59 1	60 4
61 1	62 2	63 1	64 8	65 1	66 2	67 1	68 4	69 1	70 2
71 1	72 8	73 1	74 2	75 1	76 4	77 1	78 2	79 1	80 8
81 1	82 2	83 1	84 4	85 1	86 2	87 1	88 8	89 1	90 2
91 1	92 4	93 1	94 2	95 1	96 8	97 1	98 2	99 1	100 4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 1	52 4	53 1	54 2	55 1	56 8	57 1	58 2	59 1	60 4
61 1	62 2	63 1	64 16	65 1	66 2	67 1	68 4	69 1	70 2
71 1	72 8	73 1	74 2	75 1	76 4	77 1	78 2	79 1	80 16
81 1	82 2	83 1	84 4	85 1	86 2	87 1	88 8	89 1	90 2
91 1	92 4	93 1	94 2	95 1	96 16	97 1	98 2	99 1	100 4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 1	52 4	53 1	54 2	55 1	56 8	57 1	58 2	59 1	60 4
61 1	62 2	63 1	64 32	65 1	66 2	67 1	68 4	69 1	70 2
71 1	72 8	73 1	74 2	75 1	76 4	77 1	78 2	79 1	80 16
81 1	82 2	83 1	84 4	85 1	86 2	87 1	88 8	89 1	90 2
91 1	92 4	93 1	94 2	95 1	96 32	97 1	98 2	99 1	100 4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

3

51

52
4

53
1

54
2

55
1

56
8

57
1

58
2

59
1

60
4

61
1

62
2

63
1

64
64

65
1

66
2

67
1

68
4

69
1

70
2

71
1

72
8

73
1

74
2

75
1

76
4

77
1

78
2

79
1

80
16

81
1

82
2

83
1

84
4

85
1

86
2

87
1

88
8

89
1

90
2

91
1

92
4

93
1

94
2

95
1

96
32

97
1

98
2

99
1

100
4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51	52	53	54	55	56	57	58	59	60
3	4	1	6	1	8	3	2	1	12
61	62	63	64	65	66	67	68	69	70
1	2	3	64	1	6	1	4	3	2
71	72	73	74	75	76	77	78	79	80
1	24	1	2	3	4	1	6	1	16
81	82	83	84	85	86	87	88	89	90
3	2	1	12	1	2	3	8	1	6
91	92	93	94	95	96	97	98	99	100
1	4	3	2	1	96	1	2	3	4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51	52	53	54	55	56	57	58	59	60
3	4	1	18	1	8	3	2	1	12
61	62	63	64	65	66	67	68	69	70
1	2	9	64	1	6	1	4	3	2
71	72	73	74	75	76	77	78	79	80
1	72	1	2	3	4	1	6	1	16
81	82	83	84	85	86	87	88	89	90
9	2	1	12	1	2	3	8	1	18
91	92	93	94	95	96	97	98	99	100
1	4	3	2	1	96	1	2	9	4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 3	52 4	53 1	54 54	55 1	56 8	57 3	58 2	59 1	60 12
61 1	62 2	63 9	64 64	65 1	66 6	67 1	68 4	69 3	70 2
71 1	72 72	73 1	74 2	75 3	76 4	77 1	78 6	79 1	80 16
81 27	82 2	83 1	84 12	85 1	86 2	87 3	88 8	89 1	90 18
91 1	92 4	93 3	94 2	95 1	96 96	97 1	98 2	99 9	100 4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

5

51 3	52 4	53 1	54 54	55 1	56 8	57 3	58 2	59 1	60 12
61 1	62 2	63 9	64 64	65 1	66 6	67 1	68 4	69 3	70 2
71 1	72 72	73 1	74 2	75 3	76 4	77 1	78 6	79 1	80 16
81 81	82 2	83 1	84 12	85 1	86 2	87 3	88 8	89 1	90 18
91 1	92 4	93 3	94 2	95 1	96 96	97 1	98 2	99 9	100 4

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 3	52 4	53 1	54 54	55 5	56 8	57 3	58 2	59 1	60 60
61 1	62 2	63 9	64 64	65 5	66 6	67 1	68 4	69 3	70 10
71 1	72 72	73 1	74 2	75 15	76 4	77 1	78 6	79 1	80 80
81 81	82 2	83 1	84 12	85 5	86 2	87 3	88 8	89 1	90 90
91 1	92 4	93 3	94 2	95 5	96 96	97 1	98 2	99 9	100 20

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 3	52 4	53 1	54 54	55 5	56 8	57 3	58 2	59 1	60 60
61 1	62 2	63 9	64 64	65 5	66 6	67 1	68 4	69 3	70 10
71 1	72 72	73 1	74 2	75 75	76 4	77 1	78 6	79 1	80 80
81 81	82 2	83 1	84 12	85 5	86 2	87 3	88 8	89 1	90 90
91 1	92 4	93 3	94 2	95 5	96 96	97 1	98 2	99 9	100 100

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 3	52 4	53 1	54 54	55 5	56 8	57 3	58 2	59 1	60 60
61 1	62 2	63 9	64 64	65 5	66 6	67 1	68 4	69 3	70 10
71 1	72 72	73 1	74 2	75 75	76 4	77 1	78 6	79 1	80 80
81 81	82 2	83 1	84 12	85 5	86 2	87 3	88 8	89 1	90 90
91 1	92 4	93 3	94 2	95 5	96 96	97 1	98 2	99 9	100 100

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

51 3	52 4	53 1	54 54	55 5	56 8	57 3	58 2	59 1	60 60
61 1	62 2	63 9	64 64	65 5	66 6	67 1	68 4	69 3	70 10
71 1	72 72	73 1	74 2	75 75	76 4	77 1	78 6	79 1	80 80
81 81	82 2	83 1	84 12	85 5	86 2	87 3	88 8	89 1	90 90
91 1	92 4	93 3	94 2	95 5	96 96	97 1	98 2	99 9	100 100

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

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

Sieving for smooth numbers

$\{2, 3, 5\}$

$B = 5$

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

Sieving for smooth numbers

$$B = 5$$

11111101110100110101000110100101000100010000100101
00010000010001000000010010000110000000010000010001

Sieving for smooth numbers

$$B = 5$$

(15,16)

(24,25)

11111101110100110101000110100101000100010000100101
00010000010001000000010010000110000000010000010001

(80,81)

Log-

Sieving for smooth numbers $\{2, 3, 5\}$

$$B = 5$$

$$\{[\log(2)], [\log(3)], [\log(5)]\}$$

51 0	52 0	53 0	54 0	55 0	56 0	57 0	58 0	59 0	60 0
61 0	62 0	63 0	64 0	65 0	66 0	67 0	68 0	69 0	70 0
71 0	72 0	73 0	74 0	75 0	76 0	77 0	78 0	79 0	80 0
81 0	82 0	83 0	84 0	85 0	86 0	87 0	88 0	89 0	90 0
91 0	92 0	93 0	94 0	95 0	96 0	97 0	98 0	99 0	100 0

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

2

51 0	52 0	53 0	54 0	55 0	56 0	57 0	58 0	59 0	60 0
61 0	62 0	63 0	64 0	65 0	66 0	67 0	68 0	69 0	70 0
71 0	72 0	73 0	74 0	75 0	76 0	77 0	78 0	79 0	80 0
81 0	82 0	83 0	84 0	85 0	86 0	87 0	88 0	89 0	90 0
91 0	92 0	93 0	94 0	95 0	96 0	97 0	98 0	99 0	100 0

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

4

51 0	52 1	53 0	54 1	55 0	56 1	57 0	58 1	59 0	60 1
61 0	62 1	63 0	64 1	65 0	66 1	67 0	68 1	69 0	70 1
71 0	72 1	73 0	74 1	75 0	76 1	77 0	78 1	79 0	80 1
81 0	82 1	83 0	84 1	85 0	86 1	87 0	88 1	89 0	90 1
91 0	92 1	93 0	94 1	95 0	96 1	97 0	98 1	99 0	100 1

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

8

51 0	52 2	53 0	54 1	55 0	56 2	57 0	58 1	59 0	60 2
61 0	62 1	63 0	64 2	65 0	66 1	67 0	68 2	69 0	70 1
71 0	72 2	73 0	74 1	75 0	76 2	77 0	78 1	79 0	80 2
81 0	82 1	83 0	84 2	85 0	86 1	87 0	88 2	89 0	90 1
91 0	92 2	93 0	94 1	95 0	96 2	97 0	98 1	99 0	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 0	52 2	53 0	54 1	55 0	56 3	57 0	58 1	59 0	60 2
61 0	62 1	63 0	64 3	65 0	66 1	67 0	68 2	69 0	70 1
71 0	72 3	73 0	74 1	75 0	76 2	77 0	78 1	79 0	80 3
81 0	82 1	83 0	84 2	85 0	86 1	87 0	88 3	89 0	90 1
91 0	92 2	93 0	94 1	95 0	96 3	97 0	98 1	99 0	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 0	52 2	53 0	54 1	55 0	56 3	57 0	58 1	59 0	60 2
61 0	62 1	63 0	64 4	65 0	66 1	67 0	68 2	69 0	70 1
71 0	72 3	73 0	74 1	75 0	76 2	77 0	78 1	79 0	80 4
81 0	82 1	83 0	84 2	85 0	86 1	87 0	88 3	89 0	90 1
91 0	92 2	93 0	94 1	95 0	96 4	97 0	98 1	99 0	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 0	52 2	53 0	54 1	55 0	56 3	57 0	58 1	59 0	60 2
61 0	62 1	63 0	64 5	65 0	66 1	67 0	68 2	69 0	70 1
71 0	72 3	73 0	74 1	75 0	76 2	77 0	78 1	79 0	80 4
81 0	82 1	83 0	84 2	85 0	86 1	87 0	88 3	89 0	90 1
91 0	92 2	93 0	94 1	95 0	96 5	97 0	98 1	99 0	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

3

51

52
2

53
0

54
1

55
0

56
3

57
0

58
1

59
0

60
2

61
0

62
1

63
0

64
6

65
0

66
1

67
0

68
2

69
0

70
1

71
0

72
3

73
0

74
1

75
0

76
2

77
0

78
1

79
0

80
4

81
0

82
1

83
0

84
2

85
0

86
1

87
0

88
3

89
0

90
1

91
0

92
2

93
0

94
1

95
0

96
5

97
0

98
1

99
0

100
2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

9

51 2	52 2	53 0	54 3	55 0	56 3	57 2	58 1	59 0	60 4
61 0	62 1	63 2	64 6	65 0	66 3	67 0	68 2	69 2	70 1
71 0	72 5	73 0	74 1	75 2	76 2	77 0	78 3	79 0	80 4
81 2	82 1	83 0	84 4	85 0	86 1	87 2	88 3	89 0	90 3
91 0	92 2	93 2	94 1	95 0	96 7	97 0	98 1	99 2	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51	52	53	54	55	56	57	58	59	60
2	2	0	5	0	3	2	1	0	4
61	62	63	64	65	66	67	68	69	70
0	1	4	6	0	3	0	2	2	1
71	72	73	74	75	76	77	78	79	80
0	7	0	1	2	2	0	3	0	4
81	82	83	84	85	86	87	88	89	90
4	1	0	4	0	1	2	3	0	5
91	92	93	94	95	96	97	98	99	100
0	2	2	1	0	7	0	1	4	2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 2	52 2	53 0	54 7	55 0	56 3	57 2	58 1	59 0	60 4
61 0	62 1	63 4	64 6	65 0	66 3	67 0	68 2	69 2	70 1
71 0	72 7	73 0	74 1	75 2	76 2	77 0	78 3	79 0	80 4
81 6	82 1	83 0	84 4	85 0	86 1	87 2	88 3	89 0	90 5
91 0	92 2	93 2	94 1	95 0	96 7	97 0	98 1	99 4	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

5

51 2	52 2	53 0	54 7	55 0	56 3	57 2	58 1	59 0	60 4
61 0	62 1	63 4	64 6	65 0	66 3	67 0	68 2	69 2	70 1
71 0	72 7	73 0	74 1	75 2	76 2	77 0	78 3	79 0	80 4
81 8	82 1	83 0	84 4	85 0	86 1	87 2	88 3	89 0	90 5
91 0	92 2	93 2	94 1	95 0	96 7	97 0	98 1	99 4	100 2

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 2	52 2	53 0	54 7	55 2	56 3	57 2	58 1	59 0	60 6
61 0	62 1	63 4	64 6	65 2	66 3	67 0	68 2	69 2	70 3
71 0	72 7	73 0	74 1	75 4	76 2	77 0	78 3	79 0	80 6
81 8	82 1	83 0	84 4	85 2	86 1	87 2	88 3	89 0	90 7
91 0	92 2	93 2	94 1	95 2	96 7	97 0	98 1	99 4	100 4

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 2	52 2	53 0	54 7	55 2	56 3	57 2	58 1	59 0	60 6
61 0	62 1	63 4	64 6	65 2	66 3	67 0	68 2	69 2	70 3
71 0	72 7	73 0	74 1	75 6	76 2	77 0	78 3	79 0	80 6
81 8	82 1	83 0	84 4	85 2	86 1	87 2	88 3	89 0	90 7
91 0	92 2	93 2	94 1	95 2	96 7	97 0	98 1	99 4	100 6

Log-

Sieving for smooth numbers

{2, 3, 5}

{1, 2, 2}

$B = 5$

51 ⁶ 2	52 ⁶ 2	53 ⁶ 0	54 ⁶ 7	55 ⁶ 2	56 ⁶ 3	57 ⁶ 2	58 ⁶ 1	59 ⁶ 0	60 ⁶ 6
61 ⁶ 0	62 ⁶ 1	63 ⁶ 4	64 ⁶ 6	65 ⁶ 2	66 ⁶ 3	67 ⁶ 0	68 ⁶ 2	69 ⁶ 2	70 ⁶ 3
71 ⁶ 0	72 ⁶ 7	73 ⁶ 0	74 ⁶ 1	75 ⁶ 6	76 ⁶ 2	77 ⁶ 0	78 ⁶ 3	79 ⁶ 0	80 ⁶ 6
81 ⁶ 8	82 ⁶ 1	83 ⁶ 0	84 ⁶ 4	85 ⁶ 2	86 ⁶ 1	87 ⁶ 2	88 ⁶ 3	89 ⁶ 0	90 ⁶ 7
91 ⁷ 0	92 ⁷ 2	93 ⁷ 2	94 ⁷ 1	95 ⁷ 2	96 ⁷ 7	97 ⁷ 0	98 ⁷ 1	99 ⁷ 4	100 ⁷ 6

Log-

Sieving for smooth numbers

$\{2, 3, 5\}$

$\{1, 2, 2\}$

$B = 5$

51 ⁶ 2	52 ⁶ 2	53 ⁶ 0	54 ⁶ 7	55 ⁶ 2	56 ⁶ 3	57 ⁶ 2	58 ⁶ 1	59 ⁶ 0	60 ⁶ 6
61 ⁶ 0	62 ⁶ 1	63 ⁶ 4	64 ⁶ 6	65 ⁶ 2	66 ⁶ 3	67 ⁶ 0	68 ⁶ 2	69 ⁶ 2	70 ⁶ 3
71 ⁶ 0	72 ⁶ 7	73 ⁶ 0	74 ⁶ 1	75 ⁶ 6	76 ⁶ 2	77 ⁶ 0	78 ⁶ 3	79 ⁶ 0	80 ⁶ 6
81 ⁶ 8	82 ⁶ 1	83 ⁶ 0	84 ⁶ 4	85 ⁶ 2	86 ⁶ 1	87 ⁶ 2	88 ⁶ 3	89 ⁶ 0	90 ⁶ 7
91 ⁷ 0	92 ⁷ 2	93 ⁷ 2	94 ⁷ 1	95 ⁷ 2	96 ⁷ 7	97 ⁷ 0	98 ⁷ 1	99 ⁷ 4	100 ⁷ 6

Log-

Sieving for smooth numbers

Complexity:

$$O(L \cdot \ln \ln B)$$

for interval of length L and smoothness bound B

For each prime p do $\approx L/p$

- additions of p
- additions of $\lfloor \log p \rfloor$

$$\sum_{p \leq B} (1/p) \approx \ln \ln B$$

Counting smooth numbers

$$\Psi(x, y) = \#\{1 \leq m \leq x : m \text{ is } y\text{-smooth}\}$$

$$\Psi(x, x^{1/u}) \approx x \cdot \rho(u) \text{ as } x \rightarrow \infty \text{ for fixed } u \geq 1$$

ρ : Dickman-De Bruijn function

Smoothness probability

$$\frac{\Psi(x, x^{1/u})}{x} \approx \rho(u)$$

Approximate probability for $m < N$ to be B -smooth.

$$x = N \text{ and } x^{1/u} = B \Leftrightarrow N^{1/u} = B$$

$$\Leftrightarrow u = \log(N)/\log(B)$$

Smoothness probability

$$\frac{\Psi(N, B)}{N} \approx \rho(\log(N)/\log(B)) \text{ as } N \rightarrow \infty$$

$\Pr(m \leftarrow [0, 2^{256}), 2^{15}\text{-smooth}):$

$$\frac{\Psi(2^{256}, 2^{15})}{2^{256}} \approx \rho(256/15) < 2^{-76}$$

Hopeless to find twin smooths.

Smoothness probability

- $\Pr(m \leftarrow [0, 2^{43}) \text{ is } 2^{15}\text{-smooth})$
 $\approx \rho(43/15) \approx 2^{-3.96}$
- Use products of several smaller 2^{15} -smooths
 $m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 \cdot m_5 \cdot m_6 \in [0, 2^{258})$
- For **twin-smooths** need two products differing by 1

The Prouhet-Tarry-Escott problem

Given size n , degree k , find multisets of integers

$$A = \{a_1, a_2, \dots, a_n\} \neq B = \{b_1, b_2, \dots, b_n\} \text{ s.t.}$$

$$a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_n$$

$$a_1^2 + a_2^2 + \dots + a_n^2 = b_1^2 + b_2^2 + \dots + b_n^2$$

$$a_1^3 + a_2^3 + \dots + a_n^3 = b_1^3 + b_2^3 + \dots + b_n^3$$

$$\vdots$$
$$\vdots$$

$$a_1^k + a_2^k + \dots + a_n^k = b_1^k + b_2^k + \dots + b_n^k$$

The Prouhet-Tarry-Escott problem

Given size n , degree k , find multisets of integers

$$A = \{a_1, a_2, \dots, a_n\} \neq B = \{b_1, b_2, \dots, b_n\} \text{ s.t.}$$

$$\sum_{i=1}^n a_i^j = \sum_{i=1}^n b_i^j \text{ for all } 1 \leq j \leq k$$

$$\text{Write } [a_1, a_2, \dots, a_n] =_k [b_1, b_2, \dots, b_n].$$

The Prouhet-Tarry-Escott problem

$$n = 6, k = 5$$

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = b_1 + b_2 + b_3 + b_4 + b_5 + b_6$$

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 = b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2$$

$$a_1^3 + a_2^3 + a_3^3 + a_4^3 + a_5^3 + a_6^3 = b_1^3 + b_2^3 + b_3^3 + b_4^3 + b_5^3 + b_6^3$$

$$a_1^4 + a_2^4 + a_3^4 + a_4^4 + a_5^4 + a_6^4 = b_1^4 + b_2^4 + b_3^4 + b_4^4 + b_5^4 + b_6^4$$

$$a_1^5 + a_2^5 + a_3^5 + a_4^5 + a_5^5 + a_6^5 = b_1^5 + b_2^5 + b_3^5 + b_4^5 + b_5^5 + b_6^5$$

The Prouhet-Tarry-Escott problem

$$n = 6, k = 5: [0, 5, 6, 16, 17, 22] =_5 [1, 2, 10, 12, 20, 21]$$

$$0 + 5 + 6 + 16 + 17 + 22 = 1 + 2 + 10 + 12 + 20 + 21$$

$$0^2 + 5^2 + 6^2 + 16^2 + 17^2 + 22^2 = 1^2 + 2^2 + 10^2 + 12^2 + 20^2 + 21^2$$

$$0^3 + 5^3 + 6^3 + 16^3 + 17^3 + 22^3 = 1^3 + 2^3 + 10^3 + 12^3 + 20^3 + 21^3$$

$$0^4 + 5^4 + 6^4 + 16^4 + 17^4 + 22^4 = 1^4 + 2^4 + 10^4 + 12^4 + 20^4 + 21^4$$

$$0^5 + 5^5 + 6^5 + 16^5 + 17^5 + 22^5 = 1^5 + 2^5 + 10^5 + 12^5 + 20^5 + 21^5$$

The Prouhet-Tarry-Escott problem

$$n = 6, k = 5: [0, 5, 6, 16, 17, 22] =_5 [1, 2, 10, 12, 20, 21]$$

$$0 + 5 + 6 + 16 + 17 + 22 = 66 = 1 + 2 + 10 + 12 + 20 + 21$$

$$0^2 + 5^2 + 6^2 + 16^2 + 17^2 + 22^2 = 1090 = 1^2 + 2^2 + 10^2 + 12^2 + 20^2 + 21^2$$

$$0^3 + 5^3 + 6^3 + 16^3 + 17^3 + 22^3 = 19998 = 1^3 + 2^3 + 10^3 + 12^3 + 20^3 + 21^3$$

$$0^4 + 5^4 + 6^4 + 16^4 + 17^4 + 22^4 = 385234 = 1^4 + 2^4 + 10^4 + 12^4 + 20^4 + 21^4$$

$$0^5 + 5^5 + 6^5 + 16^5 + 17^5 + 22^5 = 7632966 = 1^5 + 2^5 + 10^5 + 12^5 + 20^5 + 21^5$$

The Prouhet-Tarry-Escott problem

$$n = 6, k = 5: [1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$$

$$1 + 1 + 8 + 8 + 15 + 15 = 0 + 3 + 5 + 11 + 13 + 16$$

$$1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2 = 0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2$$

$$1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3 = 0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3$$

$$1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4 = 0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4$$

$$1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5 = 0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5$$

The Prouhet-Tarry-Escott problem

$$n = 6, k = 5: [1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$$

$$1 + 1 + 8 + 8 + 15 + 15 = 48 = 0 + 3 + 5 + 11 + 13 + 16$$

$$1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2 = 580 = 0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2$$

$$1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3 = 7776 = 0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3$$

$$1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4 = 109444 = 0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4$$

$$1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5 = 1584288 = 0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5$$

The Prouhet-Tarry-Escott problem

$$\sum_{i=1}^n a_i^j = \sum_{i=1}^n b_i^j \text{ for all } 1 \leq j \leq k$$

if and only if

$$\deg(\prod_{i=1}^n (x - a_i) - \prod_{i=1}^n (x - b_i)) \leq n - 1 - k$$

The Prouhet-Tarry-Escott problem

$$(x - a_1)(x - a_2)(x - a_3) - (x - b_1)(x - b_2)(x - b_3)$$

$$= ((b_1 + b_2 + b_3) - (a_1 + a_2 + a_3)) \cdot x^2$$

$$\begin{aligned} & \left((a_1 + a_2 + a_3)^2 - (b_1 + b_2 + b_3)^2 \right. \\ & \left. - (a_1^2 + a_2^2 + a_3^2) + (b_1^2 + b_2^2 + b_3^2) \right) / 2 \cdot x \end{aligned}$$

$$+ b_1 b_2 b_3 - a_1 a_2 a_3$$

Ideal PTE solutions

Solutions for $k = n - 1$ are *ideal solutions*

$$[a_1, a_2, \dots, a_n] =_{n-1} [b_1, b_2, \dots, b_n]$$

Ideal solutions are known only for
 $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.

Ideal PTE solutions

Solutions for $k = n - 1$ are *ideal solutions*

$$[a_1, a_2, \dots, a_n] =_{n-1} [b_1, b_2, \dots, b_n]$$

$$\sum_{i=1}^n a_i^j = \sum_{i=1}^n b_i^j \text{ for all } 1 \leq j \leq n - 1$$

$$\Leftrightarrow \prod_{i=1}^n (x - a_i) = \prod_{i=1}^n (x - b_i) + c$$

Ideal PTE solutions

$$[0,5,6,16,17,22] =_5 [1,2,10,12,20,21]$$

$$\begin{aligned} & x(x-5)(x-6)(x-16)(x-17)(x-22) + 100800 \\ &= (x-1)(x-2)(x-10)(x-12)(x-20)(x-21) \end{aligned}$$

$$[1,1,8,8,15,15] =_5 [0,3,5,11,13,16]$$

$$\begin{aligned} & x(x-3)(x-5)(x-11)(x-13)(x-16) \\ &= (x-1)^2 (x-8)^2 (x-15)^2 - 14400 \end{aligned}$$

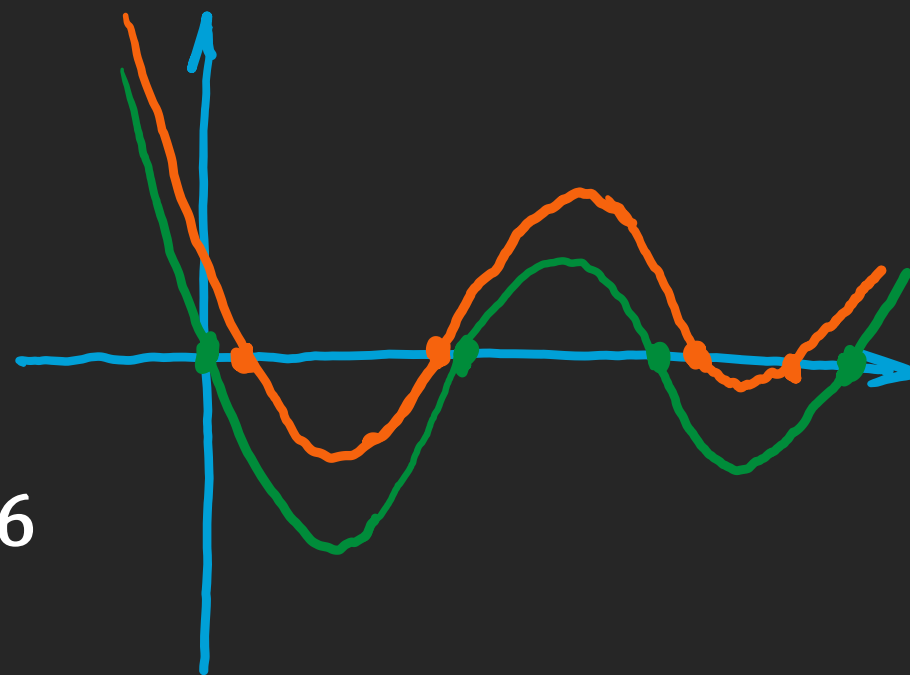
Ideal PTE solutions

$$[0,5,6,16,17,22] =_5 [1,2,10,12,20,21]$$

a_i	0			5	6		16	17		22
b_i		1	2			10	12		20	21

$$[1,1,8,8,15,15] =_5 [0,3,5,11,13,16]$$

a_i		1			8		15
b_i	0		3	5		11	13
						16	



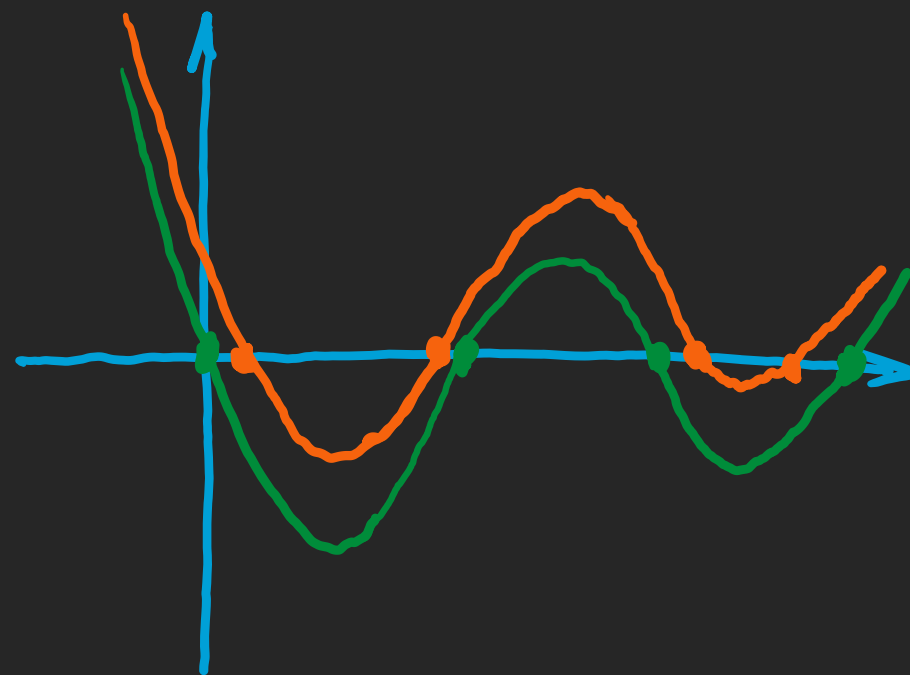
Ideal PTE solutions

$$[-11, -6, -5, 5, 6, 11] =_5 [-10, -9, -1, 1, 9, 10]$$

a_i	-11			-6	-5			5	6			11
b_i		-10	-9				-1	1			9	10

$$[-7, -7, 0, 0, 7, 7] =_5 [-8, -5, -3, 3, 5, 8]$$

a_i		-7			0			7				
b_i	-8		-5	-3			3	5		8		



Twin smooths from ideal PTE solutions

$$[1,1,8,8,15,15] =_5 [0,3,5,11,13,16]$$

$$\begin{aligned} & x(x-3)(x-5)(x-11)(x-13)(x-16) \\ &= (x-1)^2 (x-8)^2 (x-15)^2 - 14400 \end{aligned}$$

$$\begin{aligned} m &= \frac{1}{14400} x(x-3)(x-5)(x-11)(x-13)(x-16) \\ m+1 &= \frac{1}{14400} (x-1)^2 (x-8)^2 (x-15)^2 \end{aligned}$$

Sieving with PTE solutions

$$\begin{aligned} m &= \frac{1}{14400} x(x-3)(x-5)(x-11)(x-13)(x-16) \\ m+1 &= \frac{1}{14400} (x-1)^2(x-8)^2(x-15)^2 \end{aligned}$$

- Find an integer x such that all 9 terms $x, x-1, x-3, x-5, x-8, x-11, x-13, x-15, x-16$ are B -smooth.

Sieving with PTE solutions

$$m = \frac{1}{14400} x(x-3)(x-5)(x-11)(x-13)(x-16)$$

$$m+1 = \frac{1}{14400} (x-1)^2(x-8)^2(x-15)^2$$

00001000000**11010100100101011**00000000001000000000000000

$x-16$... $x-8$... x

11 1 1 1 1 1 11

- Prob(**11 1 1 1 1 1 11** in $[0, 2^{43})$ **2^{15}** -smooth) $\approx$ **$2^{-35.67}$**

Sieving with PTE solutions

- Python implementation calling a fast sieve in C (Thanks, Patrick Longa!)
- Checks multiple PTE solutions at once
- Covered interval $x \in [2^{40}, 2^{45} + \epsilon]$
- Found twin 2^{16} -smooth integers $(m, m + 1)$ with prime sum $p = m + (m + 1)$ of size 240, 241, ..., 250, 252, 253, 255 bits.

Example: 250 bits

$$B = 2^{15}$$

$$x = 36144284257450$$

$$C = 2822400 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2$$

$$p = m + (m + 1) = 2m + 1$$

$$= 1/1411200 \cdot (x - 2)^2 (x - 21)^2 (x - 40)^2 - 1 \quad (2^{249} < p < 2^{250})$$

$$p + 1 = 2 \cdot 19^6 \cdot 151^2 \cdot 601^2 \cdot 1009^2 \cdot 1103^2 \cdot 1427^2 \cdot 2011^2 \cdot 6599^2 \cdot 7321^2 \\ \cdot 9091^2 \cdot 32191^2$$

$$p - 1 = 2^6 \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 23 \cdot 107 \cdot 149 \cdot 401 \cdot 503 \cdot 599 \cdot 727 \cdot 941 \cdot 977 \\ \cdot 2351 \cdot 3469 \cdot 3779 \cdot 4273 \cdot 5051 \cdot 6211 \cdot 9001 \cdot 11447 \cdot 12589 \\ \cdot 14159 \cdot 14779 \cdot 24919$$

$$p = 1579971331793459093924543296403864959833416422864200413149968739428198012481$$

Example: 376 bits

$$B = 2^{22}$$

$$x = 73787785579919686280$$

$$C = 2822400 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2$$

$$p = m + (m + 1) = 2m + 1$$

$$= 1/1411200 \cdot (x - 2)^2(x - 21)^2(x - 40)^2 - 1 \quad (2^{375} < p < 2^{376})$$

$$p + 1 = 2^5 \cdot 7^2 \cdot 37^2 \cdot 41^2 \cdot 67^2 \cdot 83^2 \cdot 101^2 \cdot 223^2 \cdot 509^2 \cdot 4363^2 \cdot 19841^2 \\ \cdot 70949^2 \cdot 124981^2 \cdot 187193^2 \cdot 257611^2 \cdot 1058807^2 \cdot 2253169^2$$

$$p - 1 = 2 \cdot 3^2 \cdot 5 \cdot 11^2 \cdot 13 \cdot 19 \cdot 23 \cdot 103 \cdot 191 \cdot 283 \cdot 367 \cdot 677 \cdot 1291 \cdot 1607 \cdot 4933 \\ \cdot 8419 \cdot 13591 \cdot 22739 \cdot 27479 \cdot 34543 \cdot 68473 \cdot 69011 \cdot 174773 \cdot 244997 \\ \cdot 335213 \cdot 511153 \cdot 589859 \cdot 678499 \cdot 730757 \cdot 1649677 \cdot 3161131$$

$$p = 114371625799274949201834631580976454544194613164755104902272495273254249107363381979593080821748133417996625660191$$

Applications in isogeny-based crypto

B-SIDH (Costello 2019):

isogeny-based key exchange similar to SIDH

- SIDH/SIKE
 - uncompressed PK size (SIKEp434): 330B
 - compressed PK size (SIKEp434): 197B
- B-SIDH PK size (250-bit prime): 188B

Applications in isogeny-based crypto

B-SIDH (Costello 2019):

isogeny-based key exchange similar to SIDH

- Uses supersingular elliptic curves $E_{\mathbb{F}_{p^2}}: y^2 = x^3 + Ax + x$
- SIDH requires a prime p s.t. $p + 1$ or $p - 1$ smooth:
$$p = 2^e 3^f - 1$$

B-SIDH requires p such that $p + 1$ and $p - 1$ are smooth

The smaller B , the more efficient is B-SIDH

<https://eprint.iacr.org/2020/1283> (to appear @ Eurocrypt 2021)