Finding twin smooth integers

for isogeny-based cryptography

RMIT Cybersecurity Seminar
March 29, 2023

Craig Costello
Microsoft Research
craigco@microsoft.com

⋮

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

⋮

$$\vdots$$

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

$$\vdots$$

Outline

- 1. Why?
- 2. Twin smooths and Störmer's theorem
- 3. First attempts

  https://eprint.iacr.org/2019/1145.pdf
  (C. AsiaCrypt 2020)
- 4. The PTE sieve

  https://eprint.iacr.org/2020/1283.pdf
  (C-Meyer-Naehrig. EuroCrypt 2021)
- 5. The CHM algorithm

  https://eprint.iacr.org/2022/1439.pdf
  (Bruno-Corte Real Santos-C-Eriksen-Meyer-Naehrig-Sterner. Preprint.)

1. Why?

Post-quantum cryptography


NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Post-Quantum Cryptography PQC

Overview

The Candidates to be Standardized and Round 4 Submissions were announced July 5, 2022. NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available.

PQC Seminars
Next Talk: April 4, 2023

New Call for Proposals:
Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

PQC License Summary & Excerpts

Background

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. **Full details can be found in the Post-Quantum Cryptography Standardization page.**

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against

PROJECT LINKS

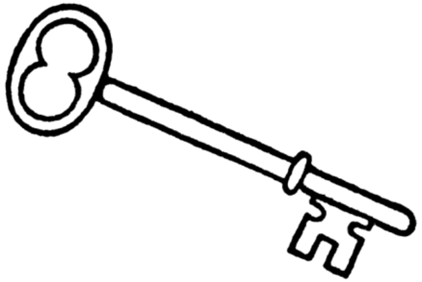
- Overview
- FAQs
- News & Updates
- Events
- Publications
- Presentations

ADDITIONAL PAGES

- Post-Quantum Cryptography Standardization
  - Call for Proposals
  - Example Files
  - Round 1 Submissions
  - Round 2 Submissions
  - Round 3 Submissions
    - *Round 3 Seminars*
- Round 4 Submissions
- Selected Algorithms 2022
- Workshops and Timeline

https://csrc.nist.gov/projects/post-quantum-cryptography

Compact post-quantum isogeny-based protocols



B-SIDH
Keys = 186B
https://eprint.iacr.org/2019/1145.pdf

SQI-Sign
(Keys, Sig) = (64B, 204B)
https://eprint.iacr.org/2020/1240.pdf

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

Smoothness is harder than primeness

- **Problem:** find a prime p where $p^2 - 1 = (p-1)(p+1)$ is as smooth as possible
- **Restated:** find large twins $(m, m+1)$ as smooth as possible, then hope that $2m+1 = p$, a prime
- **In practice:** find enough large smooth twins $(m, m+1)$ to ensure that prime sums are found
- **This talk:** find large $(\approx 2^{256})$ twins $(m, m+1)$ as smooth as possible

2. Twin smooths and Störmer’s theorem

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 2-smooth twins $(1,2)$.
- Largest 3-smooth twins $(8,9)$.
- Largest 5-smooth twins $(80,81)$.

$\vdots$

- Largest 113-smooth twins have $m = 19316158377073923834000 \approx 2^{74}$
- Largest 113-smooth twins with prime sum $m = 75954150056060186624 \approx 2^{66}$

$\vdots$

- Largest B-smooth twins requires solving $2^{\pi(B)}$ Pell equations (Störmer's theorem)

Limits of Störmer's theorem

Theorem: $x-1$ and $x+1$ both B-smooth iff (x,y) is a solution of the Pell equation

$$x^2 - Dy^2 = 1$$

where D and y are also B-smooth and D is square-free.

Sieving: search over $D = \prod q_i$, prime $q_i \le B$
if (x,y) is a solution and y is B-smooth, then test if x is prime

E.g.: $D = 5 \cdot 7 \cdot 29 \cdot 47 \cdot 59 \cdot 61 \cdot 73 \cdot 97 \cdot 103$, found with $B = 113$ $(\pi(B) = 30)$

Solution is (x,y) with $x = 38632316754147847668001$ and y being B −smooth

$$19316158377073923834000 = 2^4 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 23^2 \cdot 29 \cdot 47 \cdot 59 \cdot 61 \cdot 73 \cdot 97 \cdot 103,$$
$$19316158377073923834001 = 13^2 \cdot 31^2 \cdot 37^2 \cdot 43^4 \cdot 71^4.$$

These are largest ($\approx 2^{77}$) twins found by solving 2^{30} Pell equations ☹

Limits of Störmer's theorem

e.g. $D = 2 \cdot 3 \cdot 7 \cdot 139 \cdot 1021$ with $B = 2^{22}$

$$
\begin{aligned}
(x_2, y_2) = (&8006718886643889784645405164462767030834865080572754173440 1,\\
&327951532338700140691220177322040615230563635277339678 40)
\end{aligned}
$$

$$
\begin{aligned}
p - 1 &= 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 17^2 \cdot 41^2 \cdot 43^2 \cdot 53^2 \cdot 139 \cdot 523^2 \cdot 1021 \cdot 24547^2 \cdot 95651^2 \cdot 175061^2,\\
p + 1 &= 2 \cdot 11^2 \cdot 31^2 \cdot 2011^2 \cdot 7207^2 \cdot 22709^2 \cdot 23041^2 \cdot 42257^2 \cdot 1831021^2.
\end{aligned}
$$

3. First attempts…

Smoothness probability

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

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	$2.7701718 \times 10^{-11}$

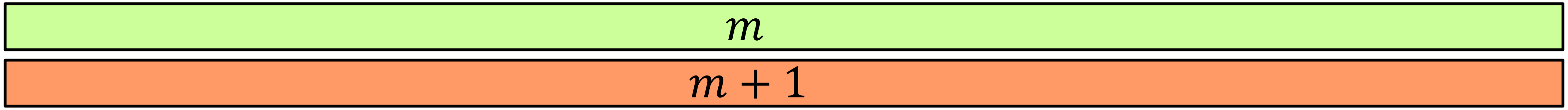
Suppose we take a random $m \in [0, 2^{256})$

- 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 $\approx \rho(16) = 1.1 \cdot 10^{-21}$

Prior methods

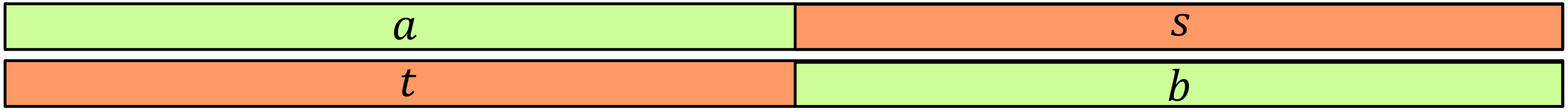
$m \approx 2^{256}$ $B = 2^{16}$

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



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

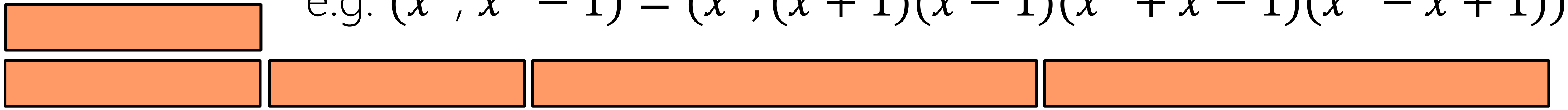
Method 2 (XGCD): search smooth coprime $a, b \approx 2^{128}$ set $m = |as|$ and $m + 1 = |bt|$



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 $\approx \rho(16) = 1.1 \cdot 10^{-21} \approx 2^{-70}$

m

$m + 1$

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

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

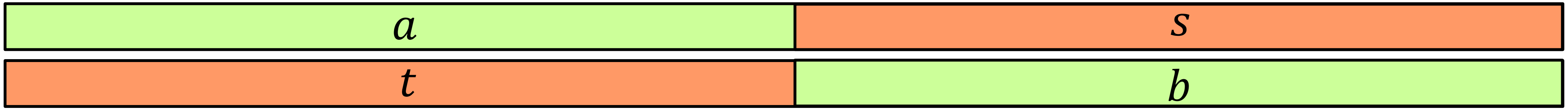
Recall that if $\mathbf{GCD}(a, b) = 1$, then $\exists\ s, t \in \mathbb{Z}$ such that

$$as + bt = 1$$

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 $m + 1 = |bt|$



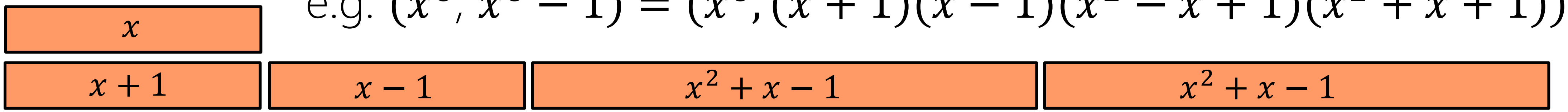
Pr(smooth) $\approx 2^{-50}$

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

$$m+1=x^6 \qquad m = (x+1)(x-1)(x^2-x+1)(x^2+x+1)$$

$m+1=x^6$	$m = (x+1)(x-1)(x^2-x+1)(x^2+x+1)$
$B=2^6$ $(2^3\cdot 3^4\cdot 17\cdot 19\cdot 31\cdot 37\cdot 53^2)^6$ $\boxed{x^6}$	$B=2^{20}$ $(7\cdot 13\cdot 269\cdot 439\cdot 62753)$ $\cdot(881\cdot 15803\cdot 48437)$ $\cdot(43\cdot 883\cdot 20161\cdot 24043\cdot 34843\cdot 709153)$ $\cdot(73\cdot 103\cdot 1321\cdot 5479\cdot 9181\cdot 12541\cdot 72577)$ $(x+1)\cdot(x-1)\cdot(x^2-x+1)\cdot(x^2+x+1)$
$B=2^{12}$ $(5^3\cdot 101\cdot 211\cdot 461\cdot 2287)^6$ $\boxed{x^6}$	$B=2^{19}$ $(2\cdot 3\cdot 109\cdot 8821\cdot 486839)$ $\cdot(2^3\cdot 7\cdot 37\cdot 107\cdot 1607\cdot 7883)$ $\cdot(3\cdot 79\cdot 433\cdot 487\cdot 5701\cdot 6199\cdot 57037\cdot 78301)$ $\cdot(13\cdot 199\cdot 349\cdot 1993\cdot 3067\cdot 6373\cdot 11497\cdot 19507)$ $(x+1)\cdot(x-1)\cdot(x^2-x+1)\cdot(x^2+x+1)$

4. 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 $(m+1, m) = \big(f(x), g(x)\big)$ 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

$$\begin{aligned} f(x) &= (x-1)(x-2)(x-9)(x-10) \\ &= x^4 - 22x^3 + 149x^2 - 308x + 180 \\ &= g(x) + 180 \end{aligned}$$

$$\begin{aligned} g(x) &= x(x-4)(x-7)(x-11) \\ &= x^4 - 22x^3 + 149x^2 - 308x \end{aligned}$$

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

($80/180$ 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

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

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

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

The Prouhet-Tarry-Escott (PTE) problem

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

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

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

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

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!

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

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

⋮

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

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

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

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

$g(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$

$f(x) = (x-1)^2(x-8)^2(x-15)^2$

$\boxed{u = 5170314186755}$

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

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

$\boxed{p = 2m + 1 \text{ is prime!!!}}$

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

$\boxed{p = 2653194648913198538763028808847267222102564753030025033104122760223436801}$

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

5. The CHM algorithm

The Conrey-Holmstrom-McLaughin (CHM) algorithm

Start with $S^{(0)} = \{1, 2, \dots, B-1\}$

Test all distinct $r, s \in S^{(0)}$:

$$\frac{t}{t'} = \frac{r}{r+1} \cdot \frac{s+1}{s}$$

if $t' = t + 1$, then include t in next iteration $S^{(1)}$

Repeat until $S^{(d)} = S^{(d-1)}$

The CHM algorithm: example ($B = 5$)

$$S^{(0)} = \{1, 2, 3, 4\}$$

$$\boxed{\frac{8}{9} = \frac{2}{2+1} \cdot \frac{3+1}{3}} \qquad \boxed{\frac{5}{6} = \frac{2}{2+1} \cdot \frac{4+1}{4}} \qquad \boxed{\frac{15}{16} = \frac{3}{3+1} \cdot \frac{4+1}{4}}$$

$$S^{(1)} = \{1, 2, 3, 4, 5, 8, 15\}$$

$$S^{(2)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24\}$$

$$S^{(3)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24, 80\}$$

$$S^{(4)} = S^{(3)}.$$

CHM vs. Störmer

2011 - Luca and Najman (Störmer's theorem, Lehmer's algorithm)

- computed all 13,374 twins with $B = 100$
- solved all $2^{\pi(100)} = 2^{25}$ Pell equations
- 15 days on a quad-core 2.66 GHz
- largest pair 58 bits

$$166055401586083680 = 2^5 \cdot 3^3 \cdot 5 \cdot 11^3 \cdot 23 \cdot 43 \cdot 59 \cdot 67 \cdot 83 \cdot 89,$$
$$166055401586083681 = 7^2 \cdot 17^{10} \cdot 41^2.$$

2012 – Conrey-Holmstrom-McLaughlin algorithm

- computed 13,333 (all but 41 twins) in 20 minutes (same CPU)
- moved to $B = 200$ and found 346,192 pairs in 2 weeks
- largest pair 79 bits

$$\begin{aligned}589864439608716991201560 &= 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 \cdot 17 \cdot 31 \cdot 59^2 \cdot 83 \cdot 139^2 \\ &\quad \cdot 173 \cdot 181, \text{ and} \\ 589864439608716991201561 &= 13^2 \cdot 113^2 \cdot 127^2 \cdot 137^2 \cdot 151^2 \cdot 199^2.\end{aligned}$$

Cryptographic smooth neighbours

- A bunch of optimisations to CHM
- Ran to convergence $S^{(d)} = S^{(d-1)}$ up to $B = 547$ finding 82,026,426 pairs in a few weeks
- Störmer would have needed to solve 2^{101} Pell equations
- Largest pair still only 122 bits ☹

$$\begin{aligned} r &= 5^4 \cdot 7 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 29 \cdot 41 \cdot 109 \cdot 163 \cdot 173 \cdot 239 \cdot 241^2 \cdot 271 \cdot 283 \\ &\quad \cdot 499 \cdot 509, \qquad \text{and} \\ r + 1 &= 2^8 \cdot 3^2 \cdot 31^2 \cdot 43^2 \cdot 47^2 \cdot 83^2 \cdot 103^2 \cdot 311^2 \cdot 479^2 \cdot 523^2. \end{aligned}$$

- See paper for how these can be combined with the prior methods to find larger/secure SQISign parameters…

Future work

better methods / smoother twins? 🤷‍♂️