Two Algorithms to Find Primes in Patterns*

Jonathan P. Sorenson
Computer Science and Software Engineering, Butler University
Indianapolis, IN 46208 USA
sorenson@butler.edu

Jonathan Webster
Mathematics, Statistics, and Actuarial Science, Butler University
Indianapolis, IN 46208 USA
jewebste@butler.edu

Prime Patterns

Mathematicians are interested in prime numbers, and how they can appear in patterns.

Twin Primes and Prime k-Tuples

- One example of a simple pattern is twin primes, which follow the pattern $(p, p+2)$.
- Zhang [20] recently showed that there exists a postive integer h where there are infinitely many primes in the pattern $(p, p+h)$.
- Generalizing this idea to more primes leads to **prime k-tuples** or **prime constellations**.

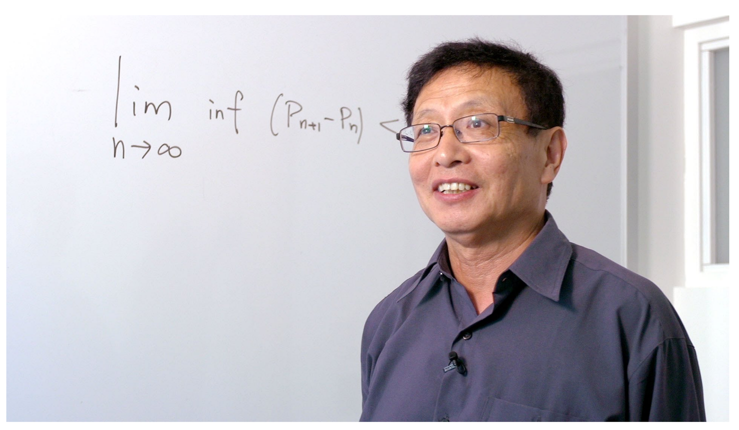
Sophie Germain Primes and Cunningham Chains

Sophie Germain was interested in the pattern $(p, 2p+1)$. Extending this idea leads to **Cunningham Chains**:

- Chains of the **first kind**: $(p, 2p+1, 4p+3, \ldots)$
- Chains of the **second kind**: $(p, 2p-1, 4p-3, \ldots)$.

Sophie Germain aos 14 anos, por Auguste Eugene Leray.

Sophie Germain



Yitang Zhang

Prime Pattern Definition

Let $k > 0$ be an integer. We define a **prime pattern** of size k as a list of linear polynomials over the integers with positive leading coefficients

$$(f_1(x), \ldots, f_k(x)).$$

Distribution of Primes in Patterns

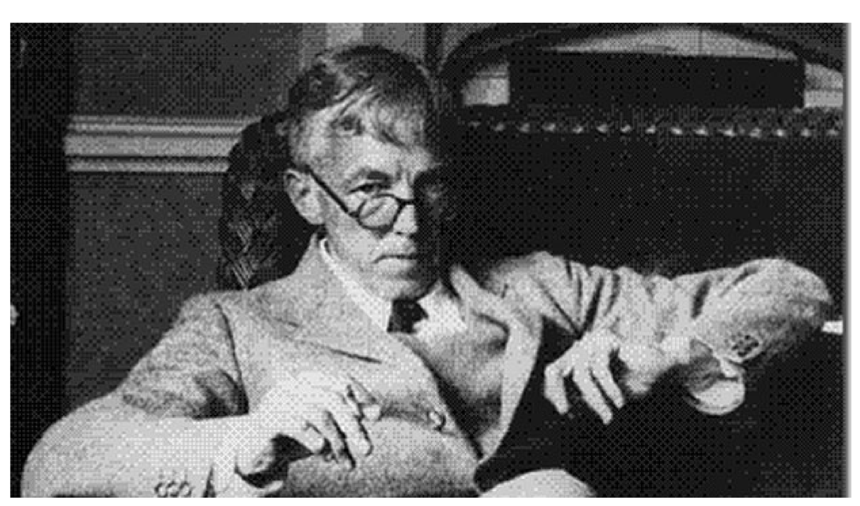
- **The Hardy-Littlewood k-tuple conjecture [9]** implies that each such pattern, with leading coefficient 1, that is **admissible**, will be satisfied by primes infinitely often.
- Further, the conjecture implies that the number of primes $\le n$ in such a pattern of length k is roughly proportional to

$$\frac{n}{(\log n)^k}.$$

- A pattern of size k is *admissible* if, for every prime $p \le k$, there is an integer x such that p does not divide any of the $f_i(x)$.
- Dickson [4] conjectured that there are infinitely many primes satisfying admissible patterns with arbitrary positive leading coefficients.
- Halberstam and Richert [8, Theorem 2.4] proved the upper bound

$$O\left(\frac{n}{(\log n)^k}\right)$$

for the number of primes $\le n$ that satisfy a pattern of length k.



G. H. Hardy

John Edensor Littlewood

The Algorithmic Problem

Given a pattern of length k, $(f_1(x), \ldots, f_k(x))$, and a bound n, find all positive integer values of x such that all the $f_i(x)$ are prime, and $\max\{f_i(x)\} \le n$.

Previous Work

- **Algorithms:**
  Günter Löh [13] and Tony Forbes [5] published partial algorithm descriptions, and used their algorithms to find various primes in patterns.
- **Complexity:**
  As far as we are aware, no complexity analysis has been published.
  All primes $\le n$ can be found, and the resulting list scanned for patterns. This takes time $O(n/\log\log n)$ using $\sqrt{n}$ space, or $O(n)$ time using roughly $n^{1/3}$ space [1, 6].
- **Computational Results and Records:**
  Record computations can be found online here:
  – http://primerecords.dk, which is maintained by Jens Kruse Andersen.
  – *The Prime Pages* at primes.utm.edu has some as well.
  – The *Online Encyclopedia of Integer Sequences*, OEIS.org, has many entries related to primes in patterns, including A001359 (twin primes), A007530 (prime quadruplets), and A005602 and A109828 (Cunningham chains).

Our New Results

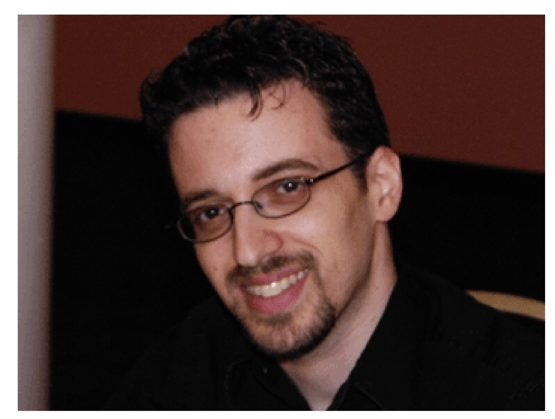
Theorem 1.

Given a pattern of length k with positive leading coefficients, and a search bound n, there is an algorithm to list all integers x such that $\max\{f_i(x)\} \le n$ and all the $f_i(x)$ are prime. This algorithm uses at most

$$O\left(\frac{nk}{(\log\log n)^k}\right) \text{ arithmetic operations (time) and } O(k\sqrt{n}) \text{ bits of space.}$$

- This algorithm extends the Atkin-Bernstein prime sieve [1] with the space-saving wheel sieve [17, 18, 19].

A. O. L. Atkin



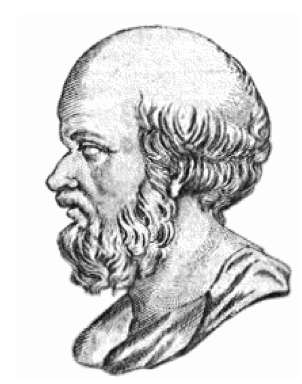
Daniel J. Bernstein

Theorem 2.

Let c be a constant with $0 < c < 1/2$. Given a pattern of length $k > 6$ with positive leading coefficients, and a search bound n, there is an algorithm to list all integers x such that $\max\{f_i(x)\} \le n$ and all the $f_i(x)$ are prime. This algorithm uses at most

$$O\left(\frac{nk}{(\log\log n)^{k-1}}\right) \text{ arithmetic operations (time) and } O(n^c) \text{ bits of space.}$$

- Due to the much smaller space use, this is a very practical algorithm.
- If we assume a conjecture due to Bach and Heulsbergen [2], we can take k as small as 3.
- This version uses the Sieve of Eratosthenes in place of the Atkin-Bernstein sieve, and supplements with base-2 pseudoprime tests [16] and the pseudosquares prime test of Lukes, Patterson, and Williams [14].



Eratosthenes of Cyrene

New Computational Results

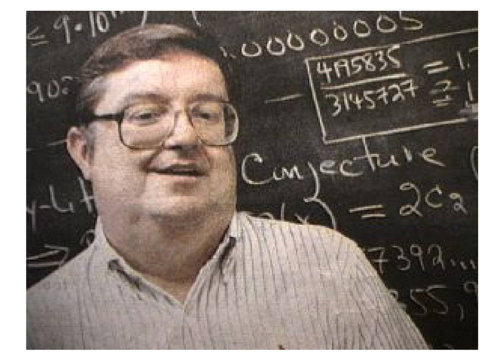
Twin Primes and Brun's Constant

Let $\pi_2(X)$ count the twin prime pairs $(p, p+2)$ with $p < X$ and $S_2(X)$ be the sum of their reciprocals. Thomas Nicely computed these functions up to $2 \cdot 10^{16}$ (See http://www.trnicely.net/#PI2X). We verified his computations and extended the results to $X = 10^{17}$.

$\pi_2(x)$ is known higher than 10^{17}, but the reciprocal sums are new.

X	$\pi_2(x)$	$S_2(X)$
$1 \cdot 10^{16}$	10304195697298	1.83048442465833932906
$2 \cdot 10^{16}$	19831847025792	1.83180806343237985727
$3 \cdot 10^{16}$	29096690339843	1.83255992186282759050
$4 \cdot 10^{16}$	38196843833352	1.83308370147757159450
$5 \cdot 10^{16}$	47177404870103	1.83348457901336613822
$6 \cdot 10^{16}$	56064358236032	1.83380868220200440399
$7 \cdot 10^{16}$	64874581322443	1.83408033035537994465
$8 \cdot 10^{16}$	73619911145552	1.83431390342560497644
$9 \cdot 10^{16}$	82309090712061	1.83451860315233433306
$10 \cdot 10^{16}$	90948839353159	1.83470066944140434160

In the last section of his PhD Thesis [12], Klyve describes how to use this information to derive bounds for Brun's constant.



Thomas Nicely

Prime Quads

A related sum involves the reciprocals of the prime tuple $(p, p+2, p+6, p+8)$. Let $\pi_4(X)$ count these tuplets up to X, and let $S_4(X)$ be the sum of their reciprocals. Thomas Nicely computed these functions up to $2 \cdot 10^{16}$. We extended this computation and partial results are in the table below. The first two lines are Thomas Nicely's own results, which we verified.

X	$\pi_4(x)$	$S_4(X)$
$1 \cdot 10^{16}$	25379433651	0.87047769123404594005
$2 \cdot 10^{16}$	46998268431	0.87048371094805250092
$3 \cdot 10^{16}$	67439513530	0.87048703104321483993
$4 \cdot 10^{16}$	87160212807	0.87048930200258802756
$5 \cdot 10^{16}$	106365371168	0.87049101694672496876
$6 \cdot 10^{16}$	125172360474	0.87049238890880442047
$7 \cdot 10^{16}$	143655957845	0.87049352884516002359
$8 \cdot 10^{16}$	161868188061	0.87049450175556017194
$9 \cdot 10^{16}$	179847459283	0.87049534891720052192
$10 \cdot 10^{16}$	197622677481	0.87049609811047504740

Cunningham Chains

We have two computational results for Cunningham chains.

- We found the smallest chain of length 15 of the first kind, and it begins with the prime

$$p = 90616\ 21195\ 84658\ 42219.$$

The next few chains of this length of the first kind are

1 13220 80067 50697 84839
1 13710 75635 40868 11919
1 23068 71734 48294 53339
1 40044 19781 72085 69169

- In 2008 Jaroslaw Wroblewski found a Cunningham Chain of length 17 of the first kind, starting with

$$p = 27\ 59832\ 93417\ 13865\ 93519,$$

and we were able to show that this is in fact the smallest such chain of that length.

References

[1] A. O. L. Atkin and D. J. Bernstein. Prime sieves using binary quadratic forms. *Mathematics of Computation*, 73:1023–1030, 2004.

[2] Eric Bach and Lorenz Huelsbergen. Statistical evidence for small generating sets. *Math. Comp.*, 61(203):69–82, 1993.

[3] Jack Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc.*, 45(4):269–274, 1939.

[4] L. E. Dickson. A new extension of Dirichlet's theorem on prime numbers. *Messenger of mathematics*, 33:155–161, 1904.

[5] Tony Forbes. Prime clusters and Cunningham chains. *Math. Comp.*, 68(228):1739–1747, 1999.

[6] William F. Galway. Dissecting a sieve to cut its need for space. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 297–312. Springer, Berlin, 2000.

[7] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[8] H. Halberstam and H.-E. Richert. *Sieve Methods*. Academic Press, 1974.

[9] G. H. Hardy and J. E. Littlewood. Some problems of 'partitio numerorum'; iii: On the expression of a number as a sum of primes. *Acta Mathematica*, 44(1):1–70, Dec 1923.

[10] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 5th edition, 1979.

[11] W. Kahan. Pracniques: Further remarks on reducing truncation errors. *Commun. ACM*, 8(1):40–, January 1965.

[12] Dominic Klyve. *Explicit Bounds on Twin Primes and Brun's Constant*. PhD in mathematics, Dartmouth College, Hanover, NH USA, 2007.

[13] Günter Löh. Long chains of nearly doubled primes. *Math. Comp.*, 53(188):751–759, 1989.

[14] R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Math. Comp.*, 65(213):361–372, S25–S27, 1996.

[15] T. Nicely. Enumeration to 10^{14} of the twin primes and Brun's constant. *Virginia J. Sci.*, 46:195–204, 1996.

[16] Carl Pomerance. On the distribution of pseudoprimes. *Math. Comp.*, 37(156):587–593, 1981.

[17] Jonathan Sorenson and Jonathan Webster. Strong pseudoprimes to twelve prime bases. *Math. Comp.*, 86(304):985–1003, 2017.

[18] Jonathan P. Sorenson. The pseudosquares prime sieve. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory (ANTS-VII)*, pages 193–207, Berlin, Germany, July 2006. Springer. LNCS 4076, ISBN 3-540-36075-1.

[19] Jonathan P. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. In Guillaume Hanrot, Francois Morain, and Emmanuel Thomé, editors, *Proceedings of the 9th International Symposium on Algorithmic Number Theory (ANTS-IX)*, pages 331–339, Nancy, France, July 2010. Springer. LNCS 6197, ISBN 978-3-642-14517-9.

[20] Yitang Zhang. Bounded gaps between primes. *Ann. of Math. (2)*, 179(3):1121–1174, 2014.

* Supported in part by a grant from the the Holcomb Awards Committee.