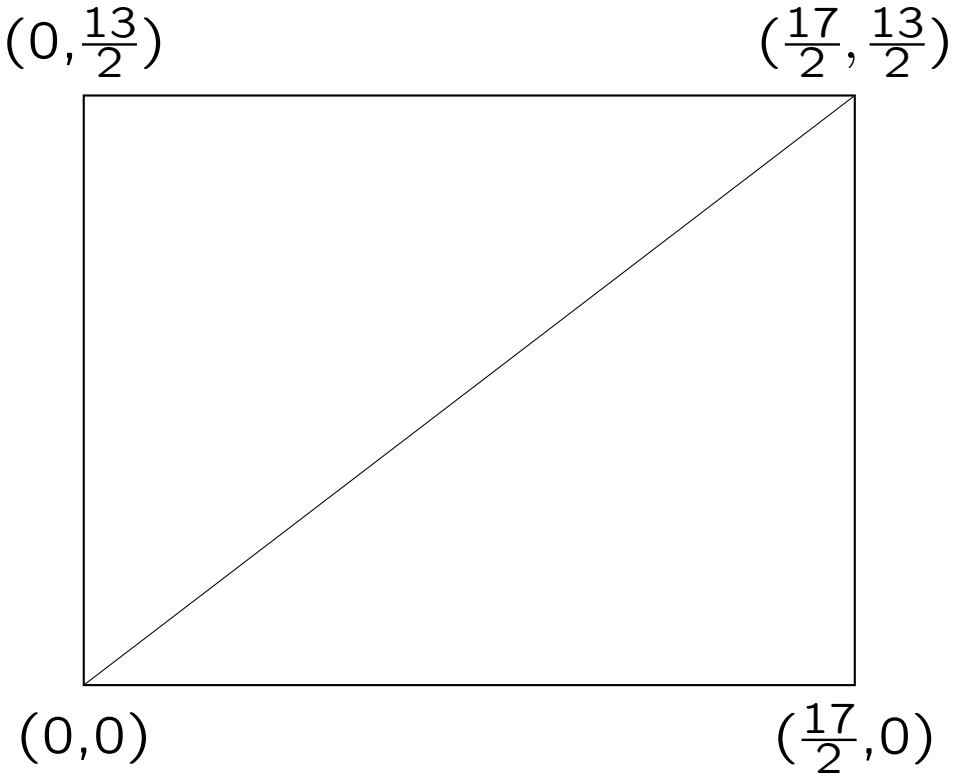
CANT 2020

June 1–5, 2020

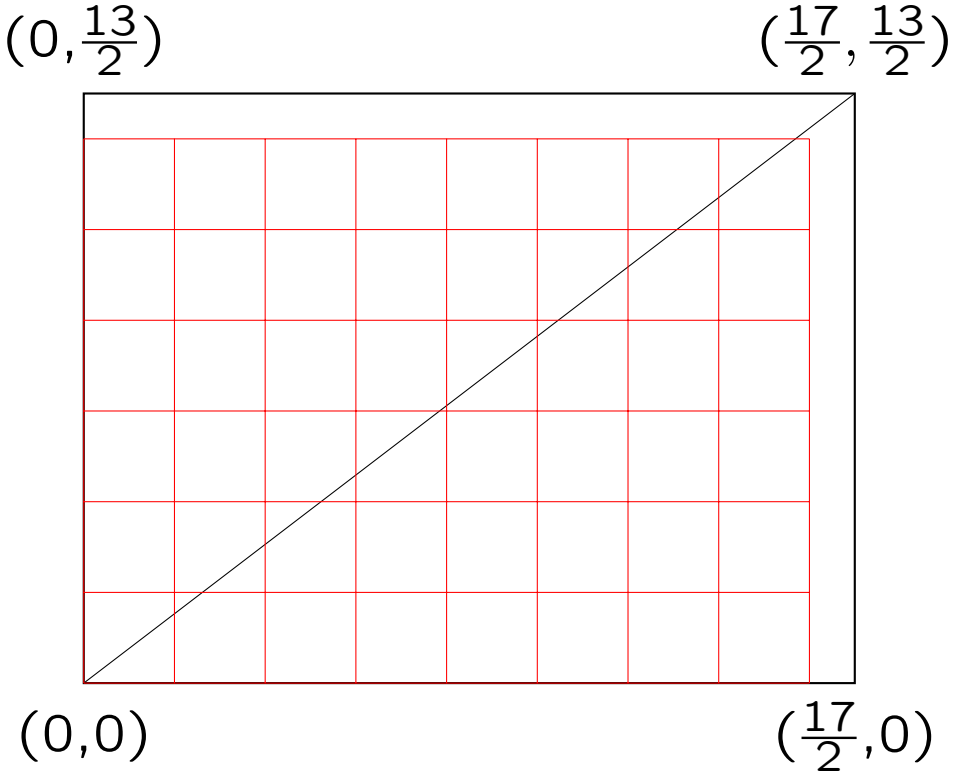
Symmetric primes

Carl Pomerance

Dartmouth College



Here is the $\frac{17}{2} \times \frac{13}{2}$ rectangle, with the diagonal drawn. We're interested in the interior lattice points.



The number of interior lattice points below the diagonal is

$$7+6+5+3+2+1=24$$

and the number above the diagonal is $8\times 6-24=24$.

However, doing this with the two primes 7 and 3, there are just 3 lattice points interior to the $\frac{7}{2} \times \frac{3}{2}$ rectangle, and so they are not split evenly above and below the diagonal.

A standard proof of quadratic reciprocity, counts the points above and below the diagonal in the $\frac{p}{2} \times \frac{q}{2}$ rectangle, and shows the two counts have opposite *parity* just for the case when $p \equiv q \equiv 3 \pmod 4$. When p or q is 1 (mod 4), it's the same parity.

But sometimes, not only are the counts of the same parity, they are exactly the same, as with 13 and 17. They are also exactly the same with 13 and 19, but not the same (but the same parity) with 13 and 23.

We say two odd primes p, q are a *symmetric pair* if the counts of the interior lattice points in the $\frac{p}{2} \times \frac{q}{2}$ rectangle nestled in the first quadrant, both above and below the main diagonal, are equal.

Say a prime is *symmetric* if it is a member of a symmetric pair, and otherwise say it is *asymmetric*.

The arithmetic condition for p, q to be a symmetric pair is that

$$|p - q| = \gcd(p - 1, q - 1).$$

A criterion: *A prime p is symmetric if and only if there is an even divisor d of $p - 1$ such that either $p - d$ or $p + d$ is prime.*

For example, 11 is symmetric because $11 + 2 = 13$ are a symmetric pair. (Any prime in a twin-prime pair is symmetric.)

And 23 is asymmetric since none of 23 ± 2, 23 ± 22 are prime.

It is natural to ask how the symmetric and asymmetric primes are distributed within the sequence of primes.

Some evidence:

Among the first 10^8 odd primes, more than 80% of them are symmetric, 80,112,625 to be precise.

A heuristic argument shows that the number of symmetric pairs of primes with one member below x is $\sim c\pi(x)$, for a positive constant c.

So, what would you conjecture for the number of symmetric primes below x?

Theorem (**Fletcher, Lindgren, Pomerance**, 1996): The number of symmetric primes below x is $O(\pi(x)/(\log x)^{0.027})$. In particular, asymptotically 100% of primes are asymmetric.

Left unsolved by this paper: Is this upper bound tight? Are there infinitely many symmetric primes?

Theorem (**Fletcher, Lindgren, Pomerance**, 1996): The number of symmetric primes below x is $O(\pi(x)/(\log x)^{0.027})$. In particular, asymptotically 100% of primes are asymmetric.

Left unsolved by this paper: Is this upper bound tight? Are there infinitely many symmetric primes?

Theorem (**Banks, Pollack, Pomerance**, 2019): The number of symmetric primes below x is $\leq \pi(x)/(\log x)^{\eta}(\log\log x)^{O(1)}$, where $\eta = 0.086\ldots$ is the Erdős–Ford–Tenenbaum constant $1 - (1 + \log\log 2)/\log 2$. In addition, there is a positive constant c with the count $> \pi(x)/(\log x)^{c}$; in particular, there are infinitely many.

Heuristically, the upper bound in the BPP theorem is tight.

The Erdős–Ford–Tenenbaum constant
$\eta = 1 - (1 + \log\log 2)/\log 2 = 0.086\ldots$**:**

So named because of the multiplication-table theorem: *The number of distinct entries in the* $N \times N$ *multiplication table is of magnitude* $N^2/(\log N)^\eta(\log\log N)^{3/2}$, proven by **Ford**, after earlier work by **Tenenbaum**, and still earlier work by **Erdős**.

The constant η pops up a lot in combinatorial number theory:

- The density of integers with a divisor between n and $2n$.
- The distribution of values of Carmichael's universal exponent function.
- The distribution of side lengths in Pythagorean triples with prime hypotenuse.
- The density of the integers divisible by a shifted prime $p - 1 > y$.
- Symmetric primes.

Not all occurrences are genuine. Recently **Guo** and **Weingartner** showed that the number of primes $p \le x$ with $p-1$ *practical* (that is, every integer up to $p-1$ is a subsum of divisors of $p-1$) is $\le \pi(x)/(\log x)^{\eta+o(1)}$. But in work-in-progress, **Weingartner** and I have replaced η with 1.

Maybe the same will happen with symmetric primes, though I don't think so. It would contradict the Hardy–Littlewood form of the prime k-tuples conjecture.

Here is the idea of the upper bound proof:

We first show that we may focus attention on those primes $p \le x$ where $p-1$ has a prime factor $r > x^{1/\log\log x}$ and $\Omega(p-1) \le L$, where Ω counts the number of prime factors with multiplicity, and $L = \lfloor \frac{1}{\log 2} \log\log x \rfloor$.

Assume p is symmetric and write $p-1 = ar$. Then there is some factorization $a = dm$ with at least one of $p \pm d,\ p \pm dr$ prime. Fix d, m. By the sieve, the number of primes r such $dmr \le x$, $dmr + 1 = p$ is prime, and one of $p \pm d,\ p \pm dr$ is prime is $\le x/(dm \log^3 x)(\log\log x)^{O(1)}$. We now sum $1/dm$ with $\Omega(dm) \le L$ and $dm \le x^{1-1/\log\log x} \le x$.

Let E denote the reciprocal sum of all primes and prime powers at most x, so that $E = \log\log x + O(1)$. Also, let $\omega(n)$ denote the number of distinct primes dividing n. We have

$$\begin{aligned}\sum_{\substack{dm\le x\\ \Omega(dm)\le L}} \frac{1}{dm} &\le \sum_{i+j\le L} \sum_{\substack{d\le x\\ \omega(d)=i}} \frac{1}{d} \sum_{\substack{m\le x\\ \omega(m)=j}} \frac{1}{m}\\ &\le \sum_{i+j\le L} \frac{1}{i!}E^i \frac{1}{j!}E^j\\ &= \sum_{k\le L} \frac{1}{k!}(E+E)^k \ll \frac{1}{L!}(2E)^L\\ &= (\log x)^{2-\eta}(\log\log x)^{O(1)}.\end{aligned}$$

Since our count is $\le \sum_{d,m} \frac{x}{dm\log^3 x}(\log\log x)^{O(1)}$, the upper bound argument is complete.

Towards a lower bound:

Assuming the quantitative form of the prime k-tuples conjecture, one can see that our sieve-derived upper bounds are essentially correct. And re-doing the argument for those primes p with at least two factorizations $p-1 = dmr = d'm'r$ giving a symmetric pair, using just the sieve upper bound, we get approximately the same count. So, assuming strong k-tuples, the upper bound is tight.

How can we obtain a rigorous lower bound?

By a result of **Heath-Brown**, for any k there are integers $a_1, \dots, a_k$ such that each $|a_i - a_j| = \gcd(a_i, a_j)$.

And by a famous result of **Maynard–Tao**, if m is given and k is large enough depending on m, then $\{a_1, \dots, a_k\}$ contains a subset $\{a_{i_1}, \dots, a_{i_m}\}$ such that $a_{i_1} n + 1, \dots a_{i_m} n + 1$ are simultaneously prime for infinitely many n. But then these primes are such that each pair of them is symmetric.

Looking at a quantitative version of this result when $m = 2$ we get that there are $\gg x/\log^{50} x$ symmetric primes up to x.

So now we're haggling over exponents: $\pi(x)/\log^{49} x$ for the lower bound and $\pi(x)/\log^{\eta} x$ for the upper bound.

Consider the **symmetry graph** on the odd primes, where two primes are connected by an edge if they are a symmetric pair. So our proof shows that for each m, there is a K_m (complete graph on m vertices) embedded in the graph.

For example: 13, 17, 19 are pairwise symmetric, as are 661, 881, 991, 1321.

In fact, applying a consequence of the **Maynard–Tao** result due to **Banks, Freiberg, & Turnage-Butterbaugh**, one can show that for any m there are infintely many m-tuples of *consecutive* primes that are pairwise symmetric.

So, the K_m can be made of consecutive primes.

Throwing out the asymmetric primes, which correspond to isolated vertices in the graph, one can ask how many connected components there are which include a prime up to x.
Presumably this tends to infinity, but how fast?

Is there an infinite connected component?

Is the component containing 3 infinite?

In a recent paper **Kalmynin** has shown that 3343 and 4457 are a symmetric pair of primes that's isolated in the symmetry graph. That is, they comprise a connected component of the graph.

In particular, he showed that 3343 is the smallest symmetric prime that is not in the component of the symmetry graph that contains 3.

He's shown, assuming the strong form of the prime k-tuples conjecture, that any finite connected graph is contained as a connected component infinitely often in the symmetry graph.

Perhaps there's some hope to prove this rigorously using the **Maynard–Tao** circle of ideas.

Thank You