Brun's Sieve

Joe Fields

November 8, 2007

Eratosthene's Sieve

- Start with $\mathbb{N}$.

Eratosthene's Sieve

- Start with $\mathbb{N}$.
- For each prime p, remove $p^2, p(p+1), p(p+2), p(p+3)\ldots$

Eratosthene's Sieve

- Start with $\mathbb{N}$.
- For each prime p, remove $p^2, p(p+1), p(p+2), p(p+3)\ldots$
- What's left behind?

Eratosthene's Sieve

- Start with $\mathbb{N}$.
- For each prime p, remove $p^2, p(p+1), p(p+2), p(p+3)\ldots$
- What's left behind?

Of course Eratosthene's sieve is used to find the primes so this may seem circular.

Brun's Sieve

- Start with $\mathbb{N}$.

Brun's Sieve

- Start with $\mathbb{N}$.
- For each prime p, remove one *or more* congruence classes mod p — from some specified point onward.

Brun's Sieve

- Start with $\mathbb{N}$.
- For each prime p, remove one *or more* congruence classes mod p — from some specified point onward.
- What's left behind?

Example of Brun's Sieve

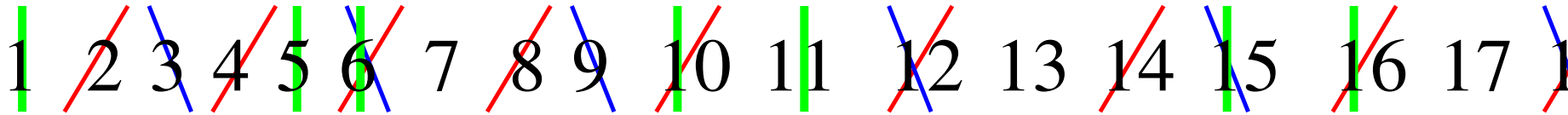
Consider removing the sequences

- $0 \pmod 2$
- $0 \pmod 3$
- $0, 1 \pmod 5$

Example of Brun's Sieve

Consider removing the sequences

- $0 \pmod 2$
- $0 \pmod 3$
- $0, 1 \pmod 5$



CRT

- CRT allows us to solve problems such as: Which values mod 35 are congruent to 1 (mod 5) and 3 (mod 7).

CRT

- CRT allows us to solve problems such as: Which values mod 35 are congruent to 1 (mod 5) and 3 (mod 7).

1					6	
	2					7
8		3				
	⋱		4			
				5		

CRT continued

1	16	31	11	26	6	21
22	2	17	32	12	27	7
8	23	3	18	33	13	28
29	9	24	4	19	34	14
15	30	10	25	5	20	35

CRT continued

1	16	**31**	11	26	6	21
22	2	17	32	12	27	7
8	23	3	18	33	13	28
29	9	24	4	19	34	14
15	30	10	25	5	20	35

Implications

- So long as no prime has *all* its congruence classes removed, something will survive the sieving.

Implications

- So long as no prime has *all* its congruence classes removed, something will survive the sieving.
- The survivors are roughly evenly distributed mod the product of the primes.

Implications

- So long as no prime has *all* its congruence classes removed, something will survive the sieving.
- The survivors are roughly evenly distributed mod the product of the primes.
- The number of survivors is (exactly) predictable mod the product of the primes.

Review of the Goldbach conjecture

- Goldbach's original conjecture:
  Every integer greater than 2 can be written as the sum of three primes.

Review of the Goldbach conjecture

- Goldbach's original conjecture:
  Every integer greater than 2 can be written as the sum of three primes.
- Goldbach thought 1 was a prime – a modern version is:
  Every integer greater than 5 can be written as the sum of three primes.

Review of the Goldbach conjecture

- Goldbach's original conjecture:
  Every integer greater than 2 can be written as the sum of three primes.
- Goldbach thought 1 was a prime – a modern version is:
  Every integer greater than 5 can be written as the sum of three primes.
- This is equivalent to what is now known as the Weak Goldbach Conjecture:
  Every odd number greater than 7 is the sum of three odd primes.

Review of the Goldbach conjecture

- Goldbach's original conjecture:
  Every integer greater than 2 can be written as the sum of three primes.
- Goldbach thought 1 was a prime – a modern version is:
  Every integer greater than 5 can be written as the sum of three primes.
- This is equivalent to what is now known as the Weak Goldbach Conjecture:
  Every odd number greater than 7 is the sum of three odd primes.
- The Strong version was framed by Euler:
  Every even number greater than 2 can be written as the sum of two primes.

Results to date

According to Wikipedia:

> *For small values of n, the strong Goldbach conjecture (and hence the weak Goldbach conjecture) can be verified directly. For instance, N. Pipping in 1938 laboriously verified the conjecture up to* $n \leq 10^5$. *With the advent of computers, many more small values of n have been checked; T. Oliveira e Silva is running a distributed computer search that has verified the conjecture up to* $n \leq 10^{18}$ *(as of April 2007).*
> *The weak Goldbach conjecture is fairly close to resolution.*
> *The strong Goldbach conjecture is much more difficult. . .*

More from Wikipedia

The work of Vinogradov in 1937 and Theodor Estermann (1902-1991) in 1938 showed that almost all even numbers can be written as the sum of two primes (in the sense that the fraction of even numbers which can be so written tends towards 1). In 1930, Lev Schnirelmann proved that every even number $n \geq 4$ can be written as the sum of at most 300,000 primes. This result was subsequently improved by many authors; currently, the best known result is due to Olivier Ramaré, who in 1995 showed that every even number $n \geq 4$ is the sum of at most six primes. In fact, resolving the weak Goldbach conjecture will also directly imply that every even number$n \geq 4$ is the sum of at most four primes.

Sieving to solve G.C.

Given an even integer, $2n$ we could use the Sieve of Eratosthenes to remove all composite numbers less than $2n$. This would require us to sieve with primes up to about $\sqrt{2n}$. If we also sieve out values of x such that $2n - x$ is composite we will be left with Goldbach pairs.

Example: Sieving to solve G.C.

- Consider the even number 36.

Example: Sieving to solve G.C.

- Consider the even number 36.
- Sieving to remove composites less than 36 will require us to remove $0 \pmod 2$ and $0 \pmod 3; x > 3$ and $0 \pmod 5; x > 5$.

Example: Sieving to solve G.C.

- Consider the even number 36.
- Sieving to remove composites less than 36 will require us to remove $0 \pmod 2$ and $0 \pmod 3$; $x > 3$ and $0 \pmod 5$; $x > 5$.
- We do not need to sieve-out $0 \pmod 7$.

Example: Sieving to solve G.C.

- Consider the even number 36.
- Sieving to remove composites less than 36 will require us to remove $0 \pmod 2$ and $0 \pmod 3$; $x > 3$ and $0 \pmod 5$; $x > 5$.
- We do not need to sieve-out $0 \pmod 7$.
- When x is even, so is $36 - x$.

Example: Sieving to solve G.C.

- Consider the even number 36.
- Sieving to remove composites less than 36 will require us to remove $0 \pmod 2$ and $0 \pmod 3$; $x > 3$ and $0 \pmod 5$; $x > 5$.
- We do not need to sieve-out $0 \pmod 7$.
- When x is even, so is $36 - x$.
- When $3 \mid x$, it also follows that $3 \mid (36 - x)$.

Example: Sieving to solve G.C.

- Consider the even number 36.
- Sieving to remove composites less than 36 will require us to remove $0 \pmod 2$ and $0 \pmod 3$; $x > 3$ and $0 \pmod 5$; $x > 5$.
- We do not need to sieve-out $0 \pmod 7$.
- When x is even, so is $36 - x$.
- When $3 \mid x$, it also follows that $3 \mid (36 - x)$.
- When $x \equiv 0 \pmod 5$ it is easy to see that $(36 - x) \equiv 1 \pmod 5$.

Example (continued)

Thus, we can find all Goldbach pairs that sum to 36 by applying Brun's sieve using

- $0 \pmod 2$
- $0 \pmod 3$
- $0, 1 \pmod 5$

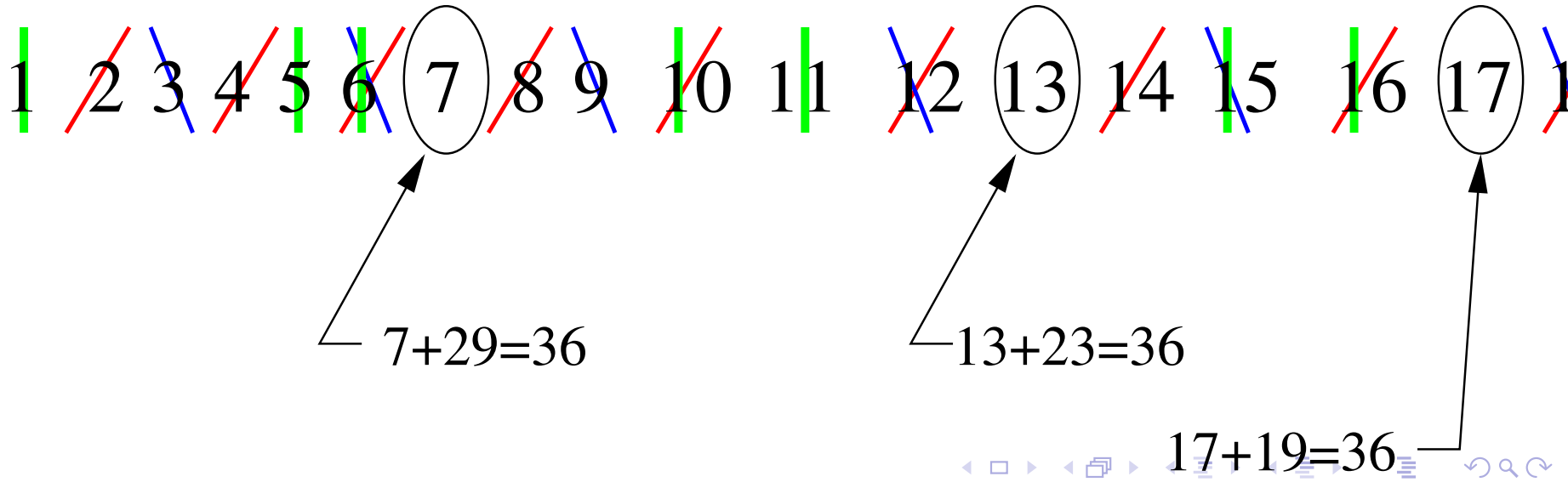
Haven't we seen this before?

Example (continued)

Thus, we can find all Goldbach pairs that sum to 36 by applying Brun's sieve using

- $0 \pmod 2$
- $0 \pmod 3$
- $0, 1 \pmod 5$

Haven't we seen this before?



What is the Twin Prime Conjecture?

A *twin prime* is a pair of prime numbers whose difference is 2. There is a unique triplet of primes $(3, 5, 7)$.

There seem to be many twin primes, for example $(3, 5)$, $(11, 13)$, $(311, 313)$ and

What is the Twin Prime Conjecture?

A *twin prime* is a pair of prime numbers whose difference is 2.
There is a unique triplet of primes $(3, 5, 7)$.
(Actually, prime triplets are defined to be triples $(p, p+2, p+6)$ or $(p, p+4, p+6)$ all of which are prime.)
There seem to be many twin primes, for example $(3, 5)$, $(11, 13)$, $(311, 313)$ and

What is the Twin Prime Conjecture?

A *twin prime* is a pair of prime numbers whose difference is 2.
There is a unique triplet of primes $(3, 5, 7)$.
(Actually, prime triplets are defined to be triples $(p, p+2, p+6)$ or $(p, p+4, p+6)$ all of which are prime.)
There seem to be many twin primes, for example $(3, 5)$, $(11, 13)$, $(311, 313)$ and
The current record holder
$(2003663613 \cdot 2^{195000} - 1, 2003663613 \cdot 2^{195000} + 1)$.

Really! What is the Twin Prime Conjecture?

Apparently this goes back to Euclid.
Flushed with the success of his proof that there are an infinite number of primes, he turned his attention to the twin primes.
The conjecture is simply that there are an infinite number of them.

More from our friends at the Wikipedia

Using his celebrated sieve method, Viggo Brun showed that the number of twin primes less than x is $<< x/(logx)^2$. This result implies that the sum of the reciprocals of all twin primes converges (see Brun's constant and Brun's theorem). This is in contrast to the sum of the reciprocals of all primes, which diverges. He also showed that every even number can be represented in infinitely many ways as a difference of two numbers both having at most 9 prime factors. Chen Jingrun's well known theorem states that for any m even, there are infinitely many primes that differ by m from a number having at most two prime factors. (Before Brun attacked the twin prime problem, Jean Merlin (1876-1914) had also attempted to solve this problem using the sieve method. He was killed in World War I.)

Using Brun's Sieve to find Twin Prime Centers

Define a *twin prime center* (TPC) to be the integer between a pair of (twin) primes. It's easy to see that every TPC is even. Every TPC after 4 is also divisible by 3. Thus "most" TPC's are of the form $6k$.

Using Brun's Sieve to find Twin Prime Centers

Define a *twin prime center* (TPC) to be the integer between a pair of (twin) primes. It's easy to see that every TPC is even. Every TPC after 4 is also divisible by 3. Thus "most" TPC's are of the form $6k$.
Indeed, the first several TPC's are 6, 12, 18, 24 ...

Using Brun's Sieve to find Twin Prime Centers

Define a *twin prime center* (TPC) to be the integer between a pair of (twin) primes. It's easy to see that every TPC is even. Every TPC after 4 is also divisible by 3. Thus "most" TPC's are of the form $6k$.
Indeed, the first several TPC's are 6, 12, 18, 24 . . .
Well. . . There seems to be something wrong here. . .

Using Brun's Sieve to find Twin Prime Centers

Define a *twin prime center* (TPC) to be the integer between a pair of (twin) primes. It's easy to see that every TPC is even. Every TPC after 4 is also divisible by 3. Thus "most" TPC's are of the form $6k$.
Indeed, the first several TPC's are 6, 12, 18, 24 . . .
Well. . . There seems to be something wrong here. . .
Ummmh. . . Yes, 24 lies intermediate between 23 and 25.

Using Brun's Sieve to find Twin Prime Centers

Define a *twin prime center* (TPC) to be the integer between a pair of (twin) primes. It's easy to see that every TPC is even. Every TPC after 4 is also divisible by 3. Thus "most" TPC's are of the form $6k$.
Indeed, the first several TPC's are 6, 12, 18, 24 . . .
Well. . . There seems to be something wrong here. . .
Ummmh. . . Yes, 24 lies intermediate between 23 and 25.
It should get sieved out when we do something to reject "primes" that are divisible by 5.

The sieve that finds TPC's

- Remove $x \equiv 1 \pmod 2; x \geq 1$.
- Remove $x \equiv \pm 1 \pmod 3; x \geq 8$.
- Remove $x \equiv \pm 1 \pmod 5; x \geq 24$.

In general, for each prime p, we remove the congruence classes ± 1 modulo p from $p^2 - 1$ onward.

Well, I'm not really sure...

The sieve of Eratosthenes can be used (along with the inclusion/exclusion principle and the Möbius function) to derive asymptotic bounds for $\pi(n)$ — the function that gives the number of primes less than or equal to n.

It seems hopeful that similar bounds for the number of twin primes could be obtained using Brun's sieve.

Limitations

As I've presented the topic, Brun's sieve is a tool for actually solving instances of the Goldbach conjecture (finding all the Goldbach pairs) or the Twin Prime Conjecture (finding all the TPC's up to some limit.)

Of course, to actually settle these conjectures we need to know that, in general, there will always be un-sieved values within the range of applicability of the sieve.

Limitations

Because of the CRT picture we know that the pattern of sieved/un-sieved values repeats mod $p\#$. Where $p\#$ is the so-called "primorial" function – the product of all primes less than or equal to p.

The sieves are applicable up to about p^2, which grows much more slowly than $p\#$.