The importance of factorization and primality testing

Luis Perez

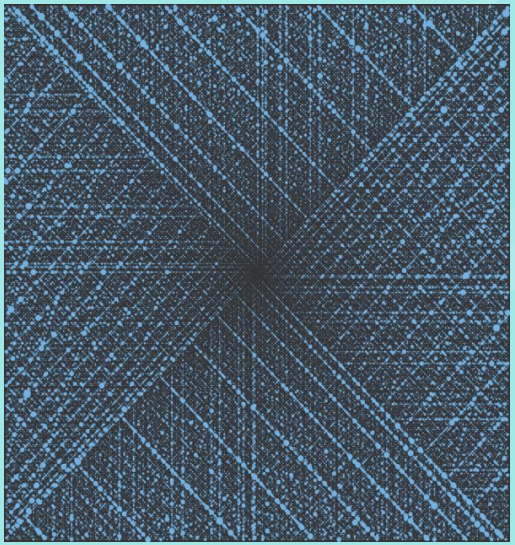
Nicholas Johnson

Prime numbers

- **What is so special about primes?**

  Since ancient times prime numbers have been the most extensively studied numbers. Primes very complex and intriguing properties and their applications in cryptology have elevated their status as modern methods of encryption rely on these properties.

Ulam's spiral



[1]

Discovered by Polish-American mathematician Stanislaw Ulam while doodling, this prime spiral consists of arranging the positive integers into a spiral and highlighting only the prime numbers, this work was the cover of the Scientific American magazine in 1964 [1].

Fundamental theorem of arithmetic

- **Are primes infinite?**

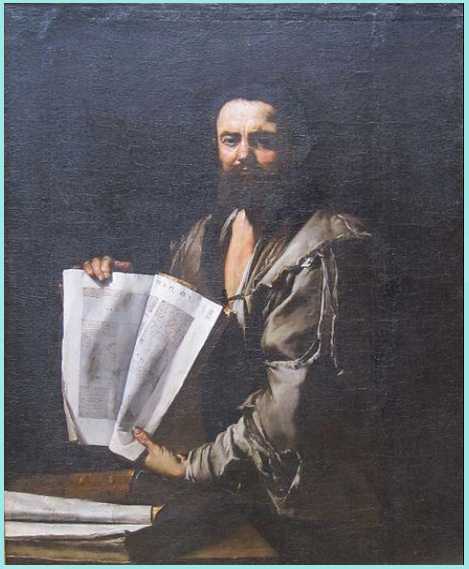
Yes primes are infinite, we can show this using the fundamental theorem of arithmetic via contradiction. This is the same way Euclid proved the infinitude of the primes .

The fundamental theorem of arithmetic can be expressed as the following if $n > 1 \in \mathbb{N}$, then $n = p_1 \cdot p_2 \cdot ... \cdot p_m, m \in \mathbb{N}$, where p_i is prime.

Theorem. There are infinitely many prime numbers.

Proof. We show there infinitely many primes by contradiction. Assume to the contrary that there are finitely many prime numbers, then quantity of primes is expressed as a finite integer n, then there exists a largest prime number call it p_n. Suppose there is a positive integer m that is a product of all primes up to and including p_n, then by the fundamental theorem of arithmetic $m = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n$. Let $N = m + 1$, then $p_i \nmid N$, hence N is prime or divisible by a prime integer larger than p_n, but since p_n is the largest prime, this means N is prime and $N > p_n$, but this is a contradiction since the supposition is p_n is the largest prime, therefore there are infinitely many primes. ■

Euclid



[2]

In his most influential work The Elements, Euclid proved the fundamental theorem of arithmetic and was the first to show the infinitude of the primes.

Factorization of semiprimes

- ## What is factorization of a semiprime?

Firstly, a semiprime is a product of two prime numbers, by factorization we mean given an arbitrary product of two primes, find the two primes that are the product of said semiprime. On March 11, 2020, an international team of computer scientists from France and the United States set a record for integer factorization of an 829-bit semiprime, this semiprime was issued by RSA laboratories as RSA-250. Each prime factor was 125 decimal digits long and in total took over 2700 years of combined computation which was distributed over thousands of machines that would compute the factors in a span of a few months.

RSA-2048

```
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748804284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203 57
```

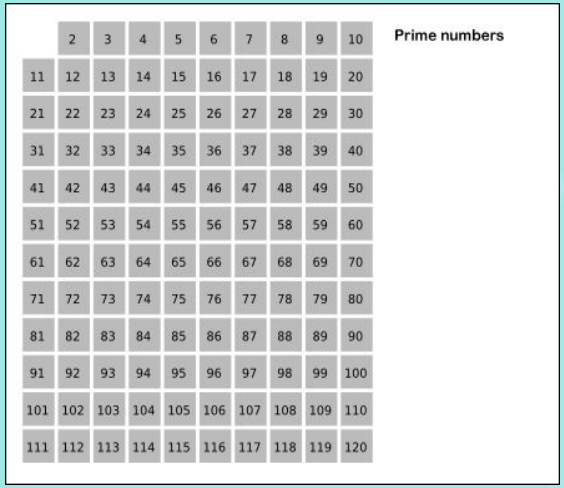
RSA-2048 was one the largest RSA number challenge issued by RSA laboratories. This semiprime is 2048 bit or 617 decimal digits long and had the largest price value of $200,00 for its factorization [2].

Methods of factorization

- **Trial division, the naive approach.**

  Consider an integer N trial division consists of dividing N by each integer less than the square root, N until there is an integer that divides without a remainder. If no integers other than 1, will divide N with no remainder, this means N is a prime number. Trivial division behaves as both a way to factor a product of primes but also test for primality, however, this method is very inefficient and can take a long to compute when numbers are large. However there is a distinction between factoring and primality testing, in terms of time complexity.

Sieve of Eratosthenes



[3]

A more efficient approach for trial division is to use the sieve of Eratosthenes to find all prime numbers less than the square root of N then check if any of those primes divide N with no remainder.

Methods of factorization

Pierre de Fermat

[4]

- **Fermat's Factorization method.**
  In this method, to find the prime factors for a product of primes N, we first take the square root of N and round it up to the nearest integer. Let a =⌈(N)^½⌉, let b^2 = a^2-N. If b is not an integer then N is not prime. If b is not an integer then the value of a is increased by one and the process is repeated. If no number is found then N is prime. If b is an integer then the factors are (a+b) and (a-b). This method can be less efficient than trial division if the prime factors of N are very far apart. For example a large number with 3 as a factor will be found very quickly with trial division but may take a long time using fermat's factorization method. however a combination of trial division and Fermat's factorization method is more efficient than either on their own .

In the margins of a book, Fermat wrote that he had discovered a proof for the equation $x^n+y^n=z^n$ has no integer solutions for $n>2$, $x,y,z \neq 0$, however Fermat did not provide a proof. This assertion became known as Fermat's last theorem and was proven by Andrew Wiles and Richard Taylor in 1994 [3].

Methods of primality testing

- ## Fermat's little theorem.

Fermat's little theorem states that if n is prime and $a \in \mathbb{Z}$, then $a^n \equiv a(\mod n)$ in other words $n \mid a^{n-1} - 1$ if and only if p is prime and $p \nmid a$. However there is a set of positive integers known as the Carmichael numbers that have this property. By definition a Carmichael number is an odd composite positive integer m, that satisfies Fermat's little theorem, where $m \mid a^{m-1} - 1$ for all positive integers a that are relatively prime to m [4]. The first three Carmichael numbers are 561, 1105, 1729, with largest ever found being 60351 digits long [4]. Suppose $C(n)$ is a function that approximates the quantity of Carmichael numbers less than n, for some sufficiently large n, then $C(n) > n^{2/7}$, this implies there exists infinitely many Carmichael numbers [4]. Fermat's little theorem can effectively demonstrate if a number is composite, however it cannot definitively show that a number is prime due to Carmichael numbers.

Leonhard Euler

[5]

In 1764 Leonhard Euler published what we know now as Euler's theorem. In his work Euler showed that Fermat's little theorem was a special case of his theorem, providing proof for what Fermat asserted.

Methods of primality testing

- **Primality testing using Wilson's theorem.**

  Wilson's theorem states that M is prime if and only if $(M-1)!+1$ is divisible by M. Suppose $M=5$, then $(5-1)!=24$, and $24+1=25$, $5 \mid 25$, since $5 \cdot 5 = 25$, thus M is primes. If $M=6$, $(6-1)!=120$, and $120+1=121$, $6 \nmid 121$, since there is no positive integer value that satisfies the following equation $6 \cdot x = 121$, thus M is not prime. Now how about $M=173$, so we need to compute $172!$, but notice that for most calculators $172!$ is computed as infinity since this number is to large to be stored in memory. The limitations of computer memory required for storing and calculating $(M-1)!$ is why Wilson's theorem is a very inefficient primality test but nevertheless interesting.

John Wilson

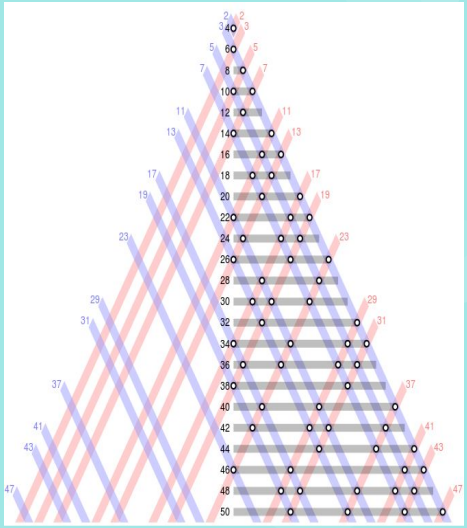
[6]

John Wilson was an English mathematician and Lawyer. He began teaching at Cambridge University in 1764. Although Wilson did not provide proof for his assertion, this theorem is forever linked to him [5].

Conclusion

- **Discussion on the algorithms presented and conjectures on the primes.**
  The naive approach of the trial division algorithm is one example of both factoring and testing for primality. Fermat's factorization method is fastest some cases where p, q the factors of a semiprime are closer apart. Wilson's theorem for primality testing needs to calculate $(N-1)!$ which is very memory intensive for large numbers N. As we have seen primes have astonishing properties, that make them truly unique. But as we investigate further into the primes we begin to ask more questions about the primes such as ; are there infinitely many primes that are evenly spaced out by two, can every even integer greater than two be expressed as the sum of primes, does there always exist a prime between n^2 and $(n+1)^2$ and so much more, we are only grasping the tip of the Iceberg of the world of primes.

Goldbach's Conjecture



[7]

Conjectured in 1742 in a letter written to Euler, Chirstian Goldbach stated that every even number greater than two could be expressed as the sum of two primes. This conjecture has been checked to hold for all $n < 4 \times 10^{1}$ [6].

Image references

[1] https://commons.wikimedia.org/wiki/File:Ulam_Spiral_Divisors_100000.png

[2] https://commons.wikimedia.org/wiki/File:Euclid_by_Jusepe_de_Ribera,_Getty_Center.JPG

[3] https://commons.wikimedia.org/wiki/File:Animation_Sieve_of_Eratosth.gif

[4] https://en.wikipedia.org/wiki/File:Pierre_de_Fermat.jpg

[5] https://commons.wikimedia.org/wiki/File:Leonhard_Euler.jpg

[6] https://en.wikipedia.org/wiki/File:John_Wilson_(Mathematician).jpeg

[7] https://commons.wikimedia.org/wiki/File:Goldbach_partitions_of_the_even_integers_from_4_to_50_rev2.svg

References

[1] Weisstein, Eric W. "Prime Spiral." From *MathWorld*--A Wolfram Web Resource. https://mathworld.wolfram.com/PrimeSpiral.html

[2] https://web.archive.org/web/20130921041734/http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-challenge-numbers.htm

[3] Weisstein, Eric W. "Fermat's Last Theorem." From *MathWorld*--A Wolfram Web Resource. https://mathworld.wolfram.com/FermatsLastTheorem.html

[4] Weisstein, Eric W. "Carmichael Number." From *MathWorld*--A Wolfram Web Resource. https://mathworld.wolfram.com/CarmichaelNumber.html

[5] https://mathshistory.st-andrews.ac.uk/Biographies/Wilson_John/

[6] Weisstein, Eric W. "Goldbach Conjecture." From *MathWorld*--A Wolfram Web Resource. https://mathworld.wolfram.com/GoldbachConjecture.html