The importance of Number Theory: A historical perspective

Sebastian Miles

Pure mathematics is the study of mathematical concepts independently of any application outside mathematics. This does not necessarily imply abundance of the field. In fact applications of great importance have appeared throughout history. Take the mathematical branch of number theory as an example, even though the field has been studied for thousands of years without primary intent of being applied to the real world, modern society is heavily dependent on applications such as cryptography, which is used for secure communications [7].

The earliest trace of number theoretic nature is the Babylonian clay tablet Plimpton 322 (ca 1800 BC) which contains a list of Pythagorean triples, that is positive integers a, b, c satisfying $a^2+b^2 = c^2$. It is believed, because of the sheer amount of tuples—that it was not constructed with brute force, but with a method [1]. Around 300 BC the ancient Greek mathematician and logician Euclid collected most of mathematics of the time and condensed it to a series of 13 books known as *Euclid's Elements*. The books are complete with postulates, propositions and definitions, with a high regard to rigour. The treatise dealt with geometry, number theory and conics. [8].
In book VII, Euclid presents an algorithm now called Euclid's algorithm. In a lecture given by Johan Jonasson at Chalmers University of Technology he introduces the algorithm as follows:
Let $d = \gcd(a, b)$ denote the greatest common divisor of the positive integers a, b.

Then by successively computing the quotients and remainders for the sequence

$$
\begin{aligned}
&a = q_1 b + r_1, \quad 0 < r_1 \leq b - 1 \\
&b = q_2 r_1 + r_2, \quad 0 < r_2 \leq r_1 - 1 \\
&r_1 = q_3 r_2 + r_3, \quad 0 < r_3 \leq r_2 - 1 \\
&\vdots \\
&r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n \leq r_{n-1} - 1 \\
&r_{n-1} = q_{n+1} r_n.
\end{aligned}
$$

until the remainder is zero, then the greatest common divisor is given by $r_n = \gcd(a, b)$ [5], see theorem 207 in [4] for a proof that the algorithm yields the greatest common divisor.
The algorithm terminates in less than $2\log_2 b + 1$ steps, the following is a proof sketch:

$$
\begin{cases}
r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad k > 1 \\
r_k = q_{k+2} r_{k+1} + r_{k+2}
\end{cases}
\implies r_{k-1} = q_{k+1}(q_{k+2} r_{k+1} + r_{k+2}) + r_{k+1}
$$

$$
> q_{k+1} q_{k+2} r_{k+1} + r_{k+1} > 2r_{k+1}
$$

Thus, we have the recursive relation $r_k > 2r_{k+2}$ for $k = 0, 1, \ldots, n$, where $b = r_0$. Let $i = \lfloor \frac{n}{2} \rfloor$, then

$$
\begin{aligned}
&b > 2r_2 > 4r_4 > \ldots > 2^i r_{2i} > 2^i \\
&\implies \log_2 b > i \geq \frac{n}{2}
\end{aligned}
$$

Thus $2\log_2 b$ is an upper bound for n.

In another lecture by Jonasson he continues talking about number theory. In particular he defines the Euler Totient function $\phi(n)$ which counts the numbers below n that are relatively prime to n, or formally

$$
\phi(n) = |\{0 < x < n \mid \gcd(x, n) = 1\}|.
$$

For this function the following three properties hold:

(a) If p is prime then $\phi(p) = p - 1$

(b) If $\gcd(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$

(c) If p, q are prime then $\phi(pq) = (p - 1)(q - 1)$

Furthermore, Jonasson explains and proves Euler's Theorem:
If $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

As the final part of the lecture, he explains the RSA (Rivest-Shamir-Adleman) cryptosystem as an application of number theory used for secure communications. For example, Amy wishes to send a message to Bob such that

(i) Nobody but Bob can read it.

(ii) Bob will know it was Amy who sent it.

(iii) Nobody can tamper with the message.

This is something RSA can achieve. Jonasson explains that each user must choose two very large distinct primes p, q and a natural number a such that

$$\gcd(a, \phi(pq)) = \gcd(a, (p - 1)(q - 1)) = 1$$

and then reveal pq and a (public key). It is unfeasible to find p and q given pq because prime number factorization is rather slow, thus finding $\phi(pq)$ also presents difficulty, Jonasson states. Suppose Amy wants to send a message to Bob, then, let x be an integer less than p, q, a and b where b is an integer satisfying $ab \equiv 1 \pmod{\phi(pq)}$.
Amy encrypts and sends

$$y = x^a \mod pq$$

and then Bob computes

$$x = y^b \mod pq$$

and thus the message has been decrypted. [6].

A theorem called the Prime Number Theorem (PNT) states that the prime counting function

$$\pi(x) = \#\text{ primes} \leq x$$

satisfies the equality

$$\lim_{x\to\infty} \pi(x) \cdot \frac{\ln x}{x} = 1.$$

or equivalently $\pi(x) = O\left(\frac{x}{\ln x}\right)$. This proposition was first proved in 1896 using complex analysis. In 1921 G.H Hardy wrote in a letter that he believes a proof of PNT not fundamentally relying on the theory of functions is extraordinary unlikely. However, in 1948 Paul Erdős and Atle Selberg proved PNT without complex analysis [3][2]. The proof was elementary per definition, but was in fact far more technical than previous proofs.

At a talk Christian Johansson, a mathematician and a lecturer at the University of Gothenburg and Chalmers Technical University talks about what mathematicians do and how the science is researched. Johansson studies number theory with algebraic structures, in particular Langlands theory.

Although number theory is a so called pure field of mathematics—meaning it is primarily researched for the sake of mathematics itself, it's applications are plentiful. Many applications lie in the field of computer science and cryptography. The RSA cryptosystem is today widely used in the modern world for secure connection and will likely continue to be used for years to come.

References

[1] Abdulrahman Ali Abdulaziz. The plimpton 322 tablet and the babylonian method of generating pythagorean triples. https://arxiv.org/abs/1004.0025, 2010.

[2] Tom M. Apostol. *Introduction to Analytic Number Theory.* Springer New York, Ny, 1 edition, 1976.

[3] D. Goldfeld. *The Elementary Proof of the Prime Number Theorem: An Historical Perspective*, pages 179–192. Springer New York, New York, NY, 2004.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford, fourth edition, 1975.

[5] Johan Jonasson. Heltalsaritmetik del 1. Eulers ϕ-funktion och RSA-krypto, November 2022.

[6] Johan Jonasson. Heltalsaritmetik del 2. Euklides algoritm och modulär aritmetik, November 2022.

[7] Ayad Barsoum Julius O. Olwenyi, Aby Tino Thomas. Cryptography in modern world. `https://cdn.stmarytx.edu/wp-content/uploads/2020/10/Cryptography-in-Modern-World.pdf`, 2020.

[8] B. L. Waerden. *Science Awakening I*. Springer Dordrecht, 1 edition, 1975.

[9] André Weil. *Number Theory: An approach through history From Hammurapi to Legendre*. Birkhäuser Boston, MA, 1 edition, 2001.