2015

Large Numbers in Computing and Mathematics

Atkins, H.

Atkins, H., Coates, R., Hilditch, S., and Smith, L. (2015) 'Large Numbers in Computing and Mathematics', The Plymouth Student Scientist, 8(1), p. 114-122.
http://hdl.handle.net/10026.1/14087

The Plymouth Student Scientist
University of Plymouth

*The Plymouth Student Scientist, 2015, **8**, (1), 114-122*

Large Numbers in Computing and Mathematics

Hazel Atkins, Rebecca Coates, Sophie Hilditch and Lucy Smith

Project Advisor: Tom Heinzl, School of Computing and Mathematics, Plymouth University, Drake Circus, Plymouth, PL4 8AA

Abstract
We present an overview of large numbers within mathematics and computing. Particular emphasis is put on the problem of large number *notation* in the mathematical attempt to get closer to infinity.

1 A Brief History

In mathematics, the notion of 'large numbers' is associated with large positive integers that are not ordinarily used in everyday activities such as simple counting or monetary transactions [1].

In ancient times numbers were believed to have significant power, and naming large numbers was considered to be a mark of authority. This goes back to Greek philosophers from the school of Pythagoras (their motto was "all is a number") who identified numbers they considered to be linked with creation, thus representing building blocks of the universe. People believed that knowing the name of a large number gave you power over that number and then, in turn, gave you power over nature [2, p. 30–38].

According to Buddhist tradition, Gautama Buddha (583-483 BC) [3] named a whole series of numbers. He started with one million and worked upwards, reaching numbers comparable with the googol (1×10^{100}), numbers which in isolation have

little practical use, but demonstrated his command over the impossibly large [2, p. 30–38].

It is known that the ancient Indians had a passion for working with exceptionally large numbers, naming each of the powers of 10 up to 10^{62}. They also introduced the concept of infinity. An ancient Indian book, named Surya Prajnapti (dating back to 300-400 BC) contains definitions of how they classified all the real numbers [4]. There were three separate categories, one of them being infinite numbers. The latter were divided into nearly infinite, truly infinite and infinitely infinite [5].

2 The Sand-Reckoner

The earliest known application of large numbers was used in the calculation of the number of grains of sand on a beach by Archimedes in 287-212 BC, where he invented an equivalent to our use of powers of 10 for calculating large numbers. Archimedes named his paper "The Sand Reckoner", and in it he set out to determine the upper bound for the number of grains of sand that could fit into the 'known' universe [6].

2.1 Powers of 10

The ancient Greeks used a system based on a myriad, which is equal to 10,000. Their largest named number at the time was a myriad myriads, equal to 100,000,000, which is nowhere near large enough to calculate the grains of sand on a beach [4].

Archimedes denoted all numbers x less than or equal to a myriad myriads as being of 'first order':

$$x \leq \Omega = 10,000 \times 10,000 = 10^8. \tag{1}$$

Numbers of second order were therefore all x obeying:

$$x \leq \Omega^2 = 10^8 \times 10^8. \tag{2}$$

He continued this pattern up to the order of a myriad:

$$x \leq \Omega^{\Omega} = 10^{800,000,000}\ . \tag{3}$$

In general he stated:

"If there be any number of terms of a series in continued proportion, say A_1, A_2, A_3, ..., A_m, ..., A_n, ..., A_{m+n-1}, ... of which $A_1 = 1$, $A_2 = 10$ [so that the series forms the geometrical progression 1, 10^1, 10^2, ..., 10^{m-1}, ..., 10^{n-1}, ..., 10^{m+n-2}, ...], and if any two terms as A_m, A_n be taken and multiplied, the product $A_m \times A_n$ will be a term in the same series and will be as many terms distant from A_n, as A_m is distant from A_1; also it will be distant from A_1 by a number of terms less by one than the sum of the numbers of terms by which A_m and A_n, respectively are distant from A_1" [7].

2.2 Size of the Universe

Archimedes estimated the size of the universe by modelling it as a sphere whose centre is the centre of the earth and whose radius is equal to the straight line between the centre of the sun and the centre of the earth (nowadays called the astronomical unit). To be on the safe side, he then deliberately overestimated this size by using then known relationships between the size of the moon, the earth and the sun [8]. This was done to take into account views like those of Aristarchus, who believed the sun to be the centre of the universe and the universe to extend vastly beyond the astronomical unit [7].

By taking the size of sand grains to be no larger than that of a poppy seed (equivalent to $1/40$ of a finger breadth), Archimedes showed that it would take, in modern notation, 8×10^{63} grains of sand to fill his model universe [8]. In doing so he also proved, of course, that there was an upper bound on the number of grains on a beach.

3 The Googolplex

In 1938, the nine year old nephew of mathematician E. Kasner described 10^{100} as looking like a 'googol' and this name stuck [2, p.13]. Later, the number "one followed by writing zeroes until you get tired" was more formally named a *googolplex* and, as "different people get tired at different times" [9], was given the value of

$$10^{\text{googol}} = 10^{10^{100}} = 1 \text{ googolplex} . \tag{4}$$

It is physically impossible to write down the number googolplex because it would require more space than is available in the known universe given that it contains about 10^{80} elementary particles. To do so would also take more time than the age of the universe. If one (naively) assumes that Moore's law (that computer power doubles every 18 months [10]) will continue to hold during the next few centuries, a computer will be able to store a googgolplex of bytes in about 500 years. As illustrated by this example, there is currently no specific use for the googolplex.

4 Prime Numbers in Computing and Cryptography

Although large numbers at first may seem rather useless, some of them have recently made an appearance in 'everyday life. These are the large prime numbers used for cryptography.

Recall that a prime number is any number greater than unity with the property of its only divisors being the number itself and one. The ancient Greeks already proved that there are an infinite number of primes, so there is no upper limit on their magnitude. Through the centuries mathematicians have been calculating larger and larger primes and continue to do so with the aid of modern computers. Any newly found

large prime might be of use for current and future encryption technology.

The distribution of prime numbers has occupied number theorists over the centuries and is still not too well understood. Many questions of prime number theory remain unanswered to this day, among them the famous Riemann conjecture [11]. As an example we show in Fig. 1 the pattern arising from highlighting the primes in a variant of Ulam's prime spiral [12] where all integers are successively aligned on a spiral emanating from the origin.

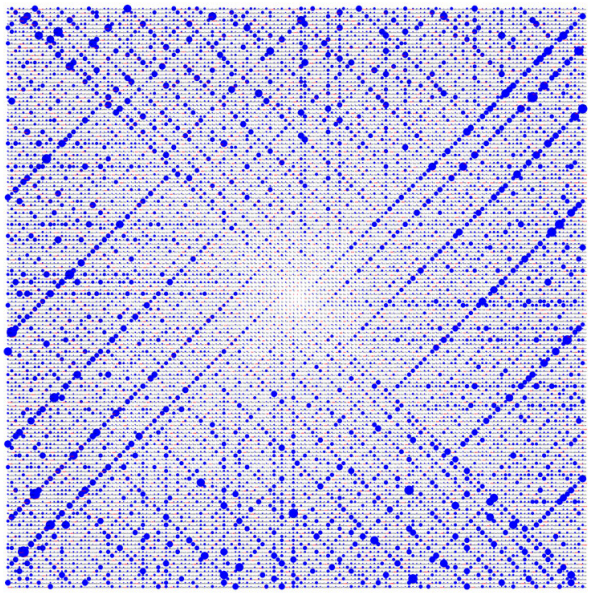

Figure 1: A variant of Ulam's prime spiral [12].

We said above that large primes are crucial for modern encryption. For example, when you log into your e-mail account via a browser, the "s" at the end of "https" in the web address stands for 'secure', which means that your emails are being encoded using SSL software. This uses public key encryption involving large prime numbers [13].

The basic idea for encryption with large primes relies on the fact that it is easy to multiply two numbers together but a lot harder to find the factors of a number. If we had a number that was 400 digits long, then two possible factors could each have about 200 digits. Assuming that a computer could test one million factorisations per second, then it could check 10^{24} possibilities in the time equivalent to the age of the universe. However, for a 400 digit number there are 10^{200} possibilities and this is where our large prime numbers come in handy.

The method is as follows: Two very large prime numbers p and q (each over 200 digits long) need to be picked to become the private key. They must be kept secure. The two primes are then multiplied together to get $N = pq$ and N is now the public key. This is the part that is given to anyone who wants to send a message. If the public

key was to be intercepted, it would be nearly impossible to find the private keys, p and q, from this one number because there is no known way of finding the factors of such a large number in reasonable time. The largest factored number to date is 232 digits long, so encryption with 200 digit factors should be safe.

As of this writing, the largest known prime contains 17,425,170 digits and was found in February 2013 [14]. This special prime number is in the form of a Mersenne Prime ($M_n = 2^n - 1$) and takes the value of

$$M_{57,885,161} = 2^{57,885,161} - 1. \tag{5}$$

In what follows we will push the limits further and discuss numbers compared to which the large primes above are relatively small.

5 Ackermann's Function

Figure 2: Wilhelm Ackermann,1896-1962 [15].

In computability theory one defines primitive recursive functions as maps between non-negative integers employing only the operations of recursion and composition. For a more precise definition one requires the axioms that (i) the constant function $n \mapsto 0$, (ii) the successor function $n \mapsto n + 1$ and (iii) the projection $(1, \ldots, n) \mapsto i$ $(1 \leq i \leq n)$ are all primitive recursive [16].

In the 1920's Wilhelm Ackermann (Fig. 2), a German PhD student of David Hilbert, was studying the foundations of computation. In 1928, he published a paper with the title (translated into English) 'On Hilbert's Construction of the Real Numbers' [17] in which he introduced a function (now called Ackermann's function) that was not primitive recursive.

Ackermann's function is denoted $\varphi(a, b, n)$ and can be specified as follows [18]:

$$n = 0: \qquad \varphi(a, b, 0) = a + b\,, \tag{6}$$

$$n = 1: \qquad \varphi(a, b, 1) = a \times b\,, \tag{7}$$

$$n = 2: \qquad \varphi(a, b, 2) = a^b\,. \tag{8}$$

As n increases ($n \geq 2$), φ can be represented by the recursion

$$\varphi(a, b, n) = \varphi(a, \varphi(a, b-1, n), n-1) \; . \tag{9}$$

For $n > 2$ the Ackermann function rapidly becomes very hard to evaluate, so over time the original Ackermann function was replaced by simpler functions of two arguments. The most common modification is due to Péter and Robinson, often referred to as the Péter-Ackermann function and denoted $A(m, n)$ [18]. It is defined through the recursion

$$A(m, n) = \begin{cases} n+1 & \text{if } m = 0 \\ A(m-1, 1) & \text{if } m > 0 \text{ and } n = 0 \\ A(m-1, A(m, n-1)) & \text{if } m > 0 \text{ and } n > 0 \end{cases} \tag{10}$$

As this Ackermann function has a 2 variable argument, it can be represented in a table to display its rapid increase [18]:

$A(m, n)$ values				
m/n	**0**	**1**	**2**	**3**
0	1	2	3	4
1	2	3	5	5
2	3	5	7	9
3	5	13	29	61
4	$2^{2^2} - 3$	$2^{2^{2^2}} - 3$	$2^{2^{2^{2^2}}} - 3$	$2^{2^{2^{2^{2^2}}}} - 3$

To appreciate the rapid growth of $A(m, n)$ one notes that $A(4, 0) = 13$ and $A(4, 1) = 65,533$, while $A(4, 2)$ already has over 19,700 digits so is unprintable here.

Since only a few Ackermann numbers can be written in standard base-10 notation, new methods of notation had to be created in order to represent the higher values. An example is Knuth's up-arrow notation which is our next topic.

6 Knuth's up-arrow notation

In 1976, the American computer scientist Donald Knuth introduced his 'up-arrow' notation ($\uparrow$) as a method of writing extremely large numbers. The idea behind the notation is that multiplication can be seen as iterated addition,

$$a \times b = a + a + \ldots + a \; (b \text{ times}), \tag{11}$$

while powers can be seen as iterated multiplication,

$$a^b = a \times a \times \ldots \times a \; (b \text{ times}). \tag{12}$$

Hence the notation can be summarised by the recursion

$$a \uparrow^n b = \begin{cases} a \times b & \text{if } n = 0 \\ a^b & \text{if } n = 1 \\ 1 & \text{if } b = 0 \\ a \uparrow^{n-1} (a \uparrow^n (b-1)) & \text{otherwise.} \end{cases} \tag{13}$$

Here n is the number of arrows present and the notation is always right-associative [19]. The notation is closely linked to the Ackerman function and many discussions of the latter will include this notation. One finds, in particular [18],

$$A(m,n) = 2 \uparrow^{m-2} (n+3) - 3 \, . \tag{14}$$

To illustrate the use of Knuth's up-arrow notation we present a worked example:

$$\begin{aligned} 2 \uparrow\uparrow 3 = 2 \uparrow (2 \uparrow^2 2) &= 2 \uparrow (2 \uparrow\uparrow 2) \\ &= 2 \uparrow (2 \uparrow (2 \uparrow\uparrow 1)) \\ &= 2 \uparrow (2 \uparrow (2 \uparrow (2 \uparrow\uparrow 0))) \\ &= 2 \uparrow (2 \uparrow (2 \uparrow 1)) \\ &= 2 \uparrow (2 \uparrow 2) \\ &= 2 \uparrow 4 \\ &= 2^4 \end{aligned} \tag{15}$$

7 Graham's Number

Alongside the Ackermann function, Knuth's up-arrow notation has also been used to represent Graham's number G [20], which we want to discuss briefly as a final extreme. Graham's number is unimaginably bigger than all other numbers we have discussed so far including the googolplex (10^{googol}). To express Graham's number in words, it is simply a power tower of three's 7,625,597,484,987 stages high. It is physically impossible to have a digital representation of Graham's number because the observable universe is too small to hold its digits – even if one was 'written' into every Planck cell in the universe. However, it can be described using Knuth's up-arrow notation in the form

$$G = 3 \uparrow\uparrow \ldots \uparrow 3 \tag{16}$$

It remains to represent the number of up-arrows. This can be done as follows using

'layers' [20]:

$$G = \left.\begin{array}{c} 3\underbrace{\uparrow\uparrow \ldots\ldots \uparrow}3 \\ 3\underbrace{\uparrow\uparrow \ldots.. \uparrow}3 \\ 3\underbrace{\uparrow\uparrow \ldots. \uparrow}3 \\ 3\underbrace{\uparrow\uparrow .. \uparrow}3 \\ 3 \uparrow\uparrow\uparrow\uparrow 3 \end{array}\right\} 64 \text{ Layers} \tag{17}$$

A simple recursion for this is $G = g_{64}$ with $g_1 = 3 \uparrow\uparrow\uparrow\uparrow 3$ and $g_n = 3 \uparrow^{g_n - 1} 3$.

8 Discussion and Conclusion

This report has explored a range of notations and uses for large numbers within mathematics and computing. We have followed the development of large number notation from the first powers of ten used by Archimedes' sand-reckoner to Knuth's up-arrow notation.

While finding or describing large numbers today commands less respect than in ancient times, it still remains a worthwhile enterprise. Large primes, once thought to be completely irrelevant for practical applications, have become a tool for modern encryption. It may very well be that large numbers such as Ackermanns' or Graham's will find similar uses in digital, or other, environments.

References

[1] http://en.wikipedia.org/wiki/Large_numbers, accessed 10-02-2014.

[2] Brian. Clegg, *A Brief History of Infinity, The Quest to Think the Unthinkable*, Robinson, London, 2003.

[3] http://www.thenagain.info/webchron/india/Buddha.html, accessed 10-02-2014

[4] http://en.wikipedia.org/wiki/History_of_large_numbersl, accessed 10-02-2014

[5] http://en.wikipedia.org/wiki/Infinity, accessed 10-02-2014

[6] http://www.numericana.com/answer/archimedes.htm#text, accesses 10-02-2014

[7] http://www.sacred-texts.com/cla/archim/sand/sandreck.html, accessed 10-02-2014

[8] http://en.wikipedia.org/wiki/The_Sand_Reckoner, accessed 10-02-2014

[9] http://en.wikipedia.org/wiki/Googolplex, accessed 10-02-2014

[10] http://whatis.techtarget.com/definition/Moores-Law, accessed 10-02-2014

[11] http://en.wikipedia.org/wiki/Prime_numbers, accessed 10-02-2014

[12] http://en.wikipedia.org/wiki/Ulam_spiral, accessed 10-02-2014

[13] http://www.ecommerce-web-hosting-guide.com/what-does-http-stand-for.html,accessed 10-02-2014

[14] http://primes.utm.edu/top20/page.php?id=3, accessed 10-02-2014

[15] http://en.wikipedia.org/wiki/Wilhelm_Ackermann, accessed 10-02-2014

[16] http://en.wikipedia.org/wiki/Primitive_recursive_function, accessed 10-02-2014

[17] http://iteror.org/big/Source/Ackermann/OnHilbertsConstructionOfReals.html, accessed 10-02-2014

[18] http://en.wikipedia.org/wiki/Ackermann_function, accessed 10-02-2014

[19] http://en.wikipedia.org/wiki/Knuth%27s_up-arrow_notation, accessed 10-02-2014

[20] http://en.wikipedia.org/wiki/Graham's_number, accessed 10-02-2014