# On the myth of an ancient Chinese theorem about primality

Qi Han
Institute for the History of Natural Science
Chinese Academy of Sciences
Beijing, China
and

Man-Keung Siu
Department of Mathematics
University of Hong Kong
Hong Kong SAR, China

*On the 60th birthday of an esteemed scholar and friend, Professor Lih Ko-Wei*

In a letter to Bernhard Frenicle de Bessy, Pierre de Fermat wrote on 18 October, 1640 that

> "Given any prime $p$, and any geometric progression $1, a, a^2$, etc. [$p$ is not a divisor of $a$], $p$ must divide some number $a^n - 1$ for which $n$ divides $p - 1$; if then $N$ is any multiple of the smallest $n$ for which this is so, $p$ divides also $a^N - 1$." [16, p.56]

In particular, if $p$ is a prime which is not a divisor of $a$, then $p$ divides $a^{p-1} - 1$, or $a^{p-1} \equiv 1 \pmod{p}$. This has come to be known as Fermat's Little Theorem. To include the case when $p$ divides $a$ as well, we can phrase it as $a^p \equiv a \pmod{p}$. In particular, when $a = 2$, we have $2^p \equiv 2 \pmod{p}$ for any prime $p$. If the converse holds, i.e. an odd $n$ dividing $2^n - 2$ is prime, then this congruence becomes a criterion for primality. The myth that the ancient Chinese used this congruence as a criterion for primality has been passed on by many Western authors. For instance, Walter William Rouse Ball said in the classic [2, p.61]:

> "Fermat discovered (1640) and Euler proved (1736) that, if $p$ is

prime and $a$ is not divisible by $p$, then $a^{p-1}-1$ is divisible by $p$.
The case when $a=2$ was known to the Chinese as early as 500 B.C;
they stated also the converse proposition: if $N$ divides $2^{N-1}-1$,
then $N$ is a prime."

In another classic [6, p.59 and p.91] Leonard Eugene Dickson began Chapter 3 with:

"The Chinese seem to have known as early as 500 B.C. that
$2^p-2$ is divisible by the prime $p$."

About thirty pages later in the same book the author said:

"In a Chinese manuscript dating from the time of Confucius
it is stated erroneously that $2^{n-1}-1$ is not divisible by $n$ if
$n$ is not prime (Jeans)."

This is a blatantly incorrect ascription, because the notions of prime numbers and of factorization into prime numbers were completely foreign to ancient Chinese mathematics. These notions were first transmitted into China in the early 18th century when the Qing Emperor Kangxi commissioned the compilation of the monumental 53-volume mathematical encyclopedia *Shuli Jingyun* [Collected Basic Principles of Mathematics], which appeared in 1722 after a decade's work. However, it should be remarked that even though the ancient Chinese did not have the notions of prime numbers and of factorization into prime numbers as their Greek counterparts had, they were nonetheless well versed in the technique known to the West as the Euclidean algorithm. This was recorded in Chapter 1 of the most important mathematical classic in China, *Jiuzhang Suanshu* [Nine Chapters on the Mathematical Art], which is believed to have been compiled between 100 BC and AD 100 but whose content can be dated to much older time:

"If both numerators and denominators are divisible by two, then
halve them both. If they are not both divisible by two, then set
up the numbers for numerator and denominator, subtract
the smaller from the larger, continually and alternately, to seek
their equality [in order to obtain their greatest common divisor]."

According to Joseph Needham, this same passage may have contributed to the myth. In a footnote in Section (d) of Chapter 19 in [11, p.54] he admitted that he could not trace with certainty the origin of the myth but pointed out it is a copy of a "mysterious remark by J.H. Jeans in a note of 1897 (written while he was still an undergraduate)" that "a paper found among those of Sir Thomas Wade and dating from the time of Confucius contains this theorem and also states [wrongly] that it does not hold if $p$ is not a prime" [6, p.93]. Needham went on to point out that sinologists might have been misled into thinking so by such a passage in *Jiuzhang Suanshu*. But we do not know to what extent this is true, whether Jeans had actually read the passage, or whether Wade, a famed British diplomat and sinologist, already misquoted the story or misinterpreted the mathematical statement. In this article we will expose yet another incident which may have contributed to the myth. At the end we will touch upon some aspect on the social history of the incident but will leave a more detailed discussion to possibly another paper. Any possible interconnection between the incident and the story by Jeans (and Wade) is also a question awaiting further investigation. Part of the exposition on the historical part is lifted from [7]. Some mathematical information related to the converse of Fermat's Little Theorem is added for the interest of a readership of mathematicians.

Before we go to the incident itself, let us look at the mathematics arising from the converse of Fermat's Little Theorem. In 1819 F. Sarrus gave the first counter-example [6, p.92], namely

$$341 \mid 2^{341} - 2, \quad \text{but } 341 = 11 \times 31.$$

One may wonder whether Fermat thought about the converse of his result. If the converse were indeed true, then all the so-called "Fermat's numbers" (of the form $F_n = 2^{2^n} + 1$) would be prime as he conjectured [16, p.172]. This is because

$$F_n = 2^{2^n} + 1 = 2^k + 1 \text{ with } k = 2^n,$$

$$\begin{aligned} \text{so that} \quad 2^{F_n} - 2 &= 2(2^{F_n - 1} - 1) = 2(2^{2^k} - 1) \\ &= 2(2^{2^{k-1}} + 1)(2^{2^{k-1}} - 1) \\ &= 2(2^{2^{k-1}} + 1)(2^{2^{k-2}} + 1)(2^{2^{k-2}} - 1) \end{aligned}$$

$$= \cdots$$
$$= 2(2^{2^{k-1}}+1)(2^{2^{k-2}}+1)\cdots(2^k+1)\cdots 5\cdot 3\cdot 1$$

is divisible by $F_n = 2^k + 1$. Hence "$F_n$ is prime"! (This amusing vignette was offered by E. Bombieri and communicated via email by J. Propp in July 1998. Via email in January 1999 A. Schinzel drew our attention to the reference by T. Banachiewicz in 1909 [6, p.94].)

In the 1920s and 1930s P. Poulet investigated those composite numbers $N$ with $N \mid 2^N - 2$ and gave examples up to $10^8$ [13]. We now know that there are infinitely many "Poulet numbers". What about $N \mid a^N - a$ with $a$ not necessarily equal to 2? In 1899 A. Korselt investigated in [9] those composite numbers $N$ with $N \mid a^N - a$ for every positive integer $a$, which have come to be known as Carmichael numbers because of the work of Robert Daniel Carmichael [3, 4] in 1910-1912. Korselt gave a criterion for Carmichael numbers, namely $N$ is square free (and composite) and $p-1 \mid N-1$ for every prime divisor $p$ of $N$. For instance, $561 = 3 \times 11 \times 17$ is a Carmichael number, since its only prime divisors are 3, 11 and 17, while $2 \mid 560, 10 \mid 560$ and $16 \mid 560$. (Incidentally, the famous "taxicab number" in the story about Srinivasa Ramanujan recounted by Godfrey Harold Hardy is the third Carmichael number, namely $1729 = 7 \times 13 \times 19$.) In the books on prime numbers by Paulo Ribenboim [14, p.122; 15, p.102] one can find an account on the progress up to the late 1990s in discovering large Carmichael numbers. In 1992 W.R. Alford, A. Granville and C. Pomerance proved that there are infinitely many Carmichael numbers [1]. For more information on Carmichael numbers one can consult the excellent expository article by C. Pomerance [12].

Now let us go back to the old China in the middle of the 19th century. This was a time when China was forced into greater contact with Western nations through their expansion of interest in China backed up by strong military power. After being defeated by the British in the First Opium War of 1840-1842 and by the British and French in the Second Opium War of 1859, China was forced into signing a number of "unequal treaties" which extorted benefits from and imposed harsh conditions on the declining imperial empire. The sad irony was that this humiliation and suffering led to the

beginning of the modernization of China, but which was realized only after yet another hundred years of continual turmoil and further humiliation. Among the Chinese ports forced open by these treaties, Shanghai soon became an important city both for trade and for missionary activities. In 1847 the London Missionary Society sent Alexander Wylie (1815-1887), trained as a printer, to work in the Society's Press in Shanghai. Following the practice and tradition of the Jesuits in the early 17th century to the early 18th century, the British and American missionaries in the 19th century continued to pay much attention to transmitting Western science as a means of glorification of God. In 1852 a Chinese mathematician LI Shanlan (1811-1882) came to the Society's Press in Shanghai and became a good friend and collaborator of Wylie. Together they translated Euclid's *Elements* (the remaining nine books in the fifteen-book version after Book VI), de Morgan's *Elements of Algebra*, Loomis' *Elements of Analytical Geometry and of the Differential and Integral Calculus*, Herschel's *Outlines of Astronomy*, and an unfinished translation of Newton's *Mathematical Principles of Natural Philosophy*. For a more detailed account on the person and the works of LI Shanlan, readers are recommended to consult [8, 10].

Li was a very capable mathematician who was well versed since his youth in both the Chinese classic *Jiuzhang Suanshu* and the Western classic Euclid's *Elements* (through the translation of the first six books by XU Guang-qi and Matteo Ricci in 1607). Later he became interested in Western mathematics through the missionaries, while at the same time engaged in original research on his own. It was probably under this circumstance that he began investigation in number theory. The subject of number theory, in the form known to the ancient Greeks and to the European mathematicians of the 17th and 18th centuries, was completely foreign to indigenous mathematics of the time. We may guess that Li learnt about it while working on the translation of Books VII-IX of *The Elements*. One result obtained by Li must have impressed Wylie so much that he, not being a professional mathematician himself, publicized it in a short-lived journal (published from 1867 to 1870 in the newly established British colony of Hong Kong), *Notes And Queries On China and Japan*. The note bore the title "A Chinese Theorem"

and read:

> The theorem of which the following is a translation was jotted down in my notebook a few days ago, by Le Shen-lan [Li Shanlan], a native mathematician whose name has been more than once before the European public. I have no hesitation in saying that it is a purely independent discovery on his part, and as such, think it may be worth publicity in your pages. Some of your scientific readers will probably be able to say if an analogous rule is to be found in European books.
>
> To ascertain if any number is a prime number.
>
> "Multiply the given number by the logarithm of 2. Find the natural number of the resulting logarithm, and subtract 2 from the same. Divide the remainder by the given number. If there be no remainder, it is a prime number. If there be a remainder, it is not a prime. A. Wylie
>
> Hongkong, 10th May, 1869.

Three more notes appeared in the same journal in the wake of the announcement of this "Chinese Theorem". Those authors correctly pointed out that the result was questionable and that the rule was in want of a proof, and one referred to Fermat's Little Theorem. However, none of them seemed to understand the problem nor the work of Li well enough to make pertinent comments. Let us look at the three notes one by one.

The first note, relatively long for a note, was written by a British scholar (of German origin), Johannes von Gumpach (1818-1875), in Peking (Beijing) and dated 3 September, 1869: "It is manifest from Mr. Le's [Li Shanlan] mode of enunciation, that he has empirically deduced his rule from trials with some few low numbers; has not seized its principle; attaches an undue value to it; and was not justified in qualifying it as a theorem, without having demonstrated the mathematical necessity of its truth." He referred to Li's formulation as "Mr. Le's uncouth formula", and gave counter-examples

to other bases, for instance $4 \mid 4^4 - 4,\ 6 \mid 3^6 - 3$, etc. It must be admitted that the way Li phrased his result was indeed somewhat cumbersome:

> If $\quad [\text{antilog}\ (x \log 2) - 2]/x \quad$ is an integer,
>
> then $x$ is a prime number.

The expression was improved by von Gumpach to read $(2^x - 2)/x$. Based on the reliance on the logarithmic operation, von Gumpach concluded that Li checked the result only empirically, without any underlying theoretical principle. Since the terse note by Wylie did not mention how Li obtained his result, we cannot ascertain how Li arrived at it. However, we can surmise, from some other work of Li on series involving binomial coefficients, that he possessed theoretical understanding of the converse of the criterion (along the line explained in the next note by W. McGregor) but initially might have incorrectly thought that the converse held, after perhaps checking the divisibility of $2^n - 2$ by $n$ for a certain number of $n$. (Indeed, later Li gave $N = 341$ as a counterexample to the "theorem" [8, p.424].) Two years later, in the correspondence column of the Shanghai newspaper *North China Herald and Supreme Court and Consular Gazette* (June 9, 1871), another British scholar, John Fryer (1839-1928), who had worked in China for a number of years, had this to say in defence of his friend, "But either formula is almost impossible to be used in the case of high numbers, because there is no way of involving the number 2 to such high powers except by the laborious process of ordinary multiplication. The difficulty of using the latter formula led Mr. Li in a careless moment to think of employing logarithms to shorten the labour; and hence he gave his rule in the objectionable form in which Baron von Gumpach found it."

A second note was written by W. McGregor in Amoy on 25 November, 1869. He said, "The law of numbers on which the approximate accuracy of the rule depends, although not given in books, is readily deduced from the well known theorem in elementary algebra that $2^n$ = sum of the coefficients in the expansion of $(1 + x)^n$." At the end he concluded not without a tinge of contempt that "it is simply an algebraical exercise, such as might be set in a school or college examination paper." What he referred to is the converse of the criterion, namely

$2^x = (1+1)^x$

$= 1 + x + x(x-1)/2! + \cdots + x(x-1)\cdots(x-s+1)/s! + \cdots + x + 1,$

each term except the first and last being divisible by $x$ if $x$ is a prime;

hence $x$ divides $2^x - 2$.

Finally a third note was written by R.A.J. (believed to be R.A. Jamieson, a British journalist who worked in China) in Hankow. Dated 27 November, 1869, it said: "After all the formidable symbols and figures that have intruded into your columns your readers will be surprised to learn that Le's rule is merely a particular, very narrow, and imperfectly developed case of a theorem which is as old as the seventeenth century, and which (until I read Mr. von Gumpach's paper) I thought was known to every senior schoolboy. It is referred to as "Fermat's Theorem," $\cdots$ " Jamieson seemed to be better informed mathematically than the other two authors, but he was confused about the criterion and Fermat's Little Theorem when he concluded that: "Le's rule is therefore merely reproduced from some elementary work on Algebra, and spoiled in the reproducing. With the condition above attached to $n$ it does detect prime numbers."

In his note von Gumpach mentioned that he had met Li in Peking when Li took up a professorship in mathematics at the Tung Wen Kuan (Tong Wen Guan, also known as the Peking College, an establishment originally set up in 1862 as part of the "Foreign Affairs Movement" to promote study of Western languages and translations, later extended to include science and mathematics in 1866). According to von Gumpach, Li submitted the "Chinese Theorem" to him a day or two before he wrote his note. Apparently von Gumpach conveyed to Li his doubts about the theorem which Li apparently accepted. In his book *Kao Shu Gen Fa* [Methods to Examine Primality] of 1872, Li did not include the incorrect criterion but further analysed the factors of $N$ if $N \mid a^N - a$. However, a younger mathematician HUA Hengfang (1833-1902), who looked upon Li as his mentor, was not aware of this error and included the incorrect criterion in his book *Shu Gen Shu Jie* [Explanation on the Methods to Examine Primality], which appeared in 1882 as part of a larger collected works. He wrote:

"Mr. Li Qiuren [Shanlan] proposes a quick check on primality:

find the number whose logarithm is the original number
multiplied by the logarithm of 2, subtract 2 from this number
and see if it is divisible by the original number. If it is, then
the original number is prime, and not a prime otherwise."

A mathematically interesting point is that Hua went further to say that for large $N$ it is not easy to check the congruence $2^N \equiv 2 \pmod{N}$ by direct multiplication, and proposed a method referred to by Fryer in the aforementioned note of 9 June, 1871. It read:

Translation of Mr. Hwa's [Hua Hengfang] Rule

"To discover if any given number be prime or not: — Subtract 1
from the given number and thus obtain an even number. Successively
halve this, and if an odd number occurs subtract 1 and halve as
before, stopping or reaching the number 1.
Then working backwards and commencing from the number 2, square
it once for every time of having divided by 2, and multiply by 2
for every time of having subtracted 1. Whenever the resulting
number is large enough, divide it by the given number, and proceed
with the remainder. From the last number so obtained subtract 2.
If nothing is left the given number is a prime number."

This may be illustrated by the congruence $2^{101} \equiv ? \pmod{101}$:

$$101 \to 101 - 1 = 100 \to 100/2 = 50 \to 50/2 = 25 \to 25 - 1 = 24$$
$$\to 24/2 = 12 \to 12/2 = 6 \to 6/2 = 3 \to 3 - 1 = 2 \to 2/2 = 1.$$

Reversing the path, we obtain:

$$2^2 = 4 \to 2 \times 4 = 8 \to 8^2 = 64 \to 64^2 = 4096 \equiv 56 \to 56^2 = 3136 \equiv 5$$
$$\to 2 \times 5 = 10 \to 10^2 = 100 \to 100^2 = 1000 \equiv 1 \to 2 \times 1 = 2$$

Hence the answer is $2^{101} \equiv 2 \pmod{101}$. This method is none other than what in today's textbooks is called the fast modular exponentiation algorithm which computes $a^b \pmod{n}$ by exploiting the binary representation of $b$ [5, pp.829-830].

What is even more interesting, from the viewpoint of the social history of science, is a series of letters to the editor in the *North China Herald and Supreme Court and Consular Gazette* between Fryer and von Gumpach from March to June of 1871. This exchange of correspondence, which occurred more than one year after the announcement of the "Chinese Theorem" by Wylie, developed into a rather unpleasant exchange with personal attacks on both sides. It came to an end only because the editor published a note on 23 June, 1871 saying: "This subject has now been quite fully discussed, and we must decline to insert any further correspondence upon it." The episode also reveals the polarized attitudes different foreigners took towards Chinese science and mathematics, and Chinese efforts to learn from the West during the latter half of the 19th century, when China was forced to respond to the West through the so-called "Self-Strengthening Movement" following the two Opium Wars. More research and thinking need be put into the analysis of this complicated issue embedded in a complicated cultural-socio-political context.

## References


[1] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers, *Annals Math.*, **139** (1994), 703-722.

[2] W.W Rouse Ball (and H.S.M. Coxeter), *Mathematical Recreations and Essays*, 13th edition, Dover, New York 1987; first edition published in 1892.

[3] R.D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.*, **16** (1910), 232-238.

[4] R.D. Carmichael, On composite numbers $P$ which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, *Amer. Math. Monthly*, **19** (1912), 22-27.

[5] T.H. Cormen, C.E. Leiserson, R.L. Rivest, *Introduction to Algorithms*, MIT Press, Cambridge, 1990.

[6] L.E. Dickson, *History of the Theory of Numbers, Vol. I: Divisibility and Primality*, Carnegie Institute of Washington, 1919; reprinted by Chelsea Publ. Co. New York, 1971.

[7] Q. Han, Li Shanlan "Zhongguo Dingli" zhi youlei ji qi fanxiang [Origins and repurcussions of Li Shanlan's "Chinese Theorem"], *Ziran Kexueshi Yanjiu* [Studies in the History of Natural Sciences], **18** (1) (1999), 7-13.

[8] W.S. Horng, *Li Shanlan: The Impact of Western Mathematics in China During the Late 19th Century*, PhD thesis, City University of New York, New York, 1991.

[9] A. Korselt, Problème chinois, *L'intermédiare des mathématiciens*, **6** (1899), 142-143.

[10] J.C. Martzloff, Li Shanlan (1811-1882) and Chinese traditional mathematics, *Mathematical Intelligencer*, **14** (4) (1992), 32-37.

[11] J. Needham (with the collaboration of L. Wang), *Science and Civilization in China, Vol. 3: Mathematics and the Sciences of the Heavens and the Earth*, Cambridge University Press, Cambridge, 1959.

[12] C. Pomerance, Carmichael numbers, *Nieuw Archief Voor Wiskunde*, **11** (1) (1993), 199-209.

[13] P. Poulet, Table des nombres composés vérifiant le théorème de Fermat pour le module 2, jusqu'à 100.000.000, *Sphinx*, **8** (1938), 52; corrections in *Math. Comp.*, **25**(1971), 944-945; **26** (1972), 814.

[14] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, Heidelberg-New York, 1996.

[15] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd edition, Springer-Verlag, Heidelberg-New York, 2004.

[16] A. Weil, *Number Theory: An Approach Through History From Hammurapi To Legendre*, Birkhäuser, Boston-Basel-Stuttgart, 1984.