LUCAS'S THEOREM: A GREAT THEOREM

Douglas Smith

Department of Mathematics and Statistics
Miami University
Oxford, OH 45056

smithdr1@muohio.edu

Supervising Instructor: Professor David Kullman

Part I: INTRODUCTION

Combinatorics is the branch of mathematics studying the enumeration, combination, and permutation of sets of elements and the mathematical relations that characterize their properties. A major theorem in that field is Lucas's Theorem, which is often stated in the following way:

If p is a prime, $m = m_1m_2m_3...m_k$ in base p, and $n = n_1n_2n_3...n_k$ in base p, then

$$\binom{m}{n} \equiv \binom{m_1}{n_1} \bullet \binom{m_2}{n_2} \bullet \binom{m_3}{n_3} \bullet \ldots \bullet \binom{m_k}{n_k} \bmod p \text{ (Riddle).}$$

This paper will discuss Lucas's Theorem and some applications, as well as mathematical developments leading to Lucas's Theorem and the mathematical environment of Lucas's time.

Part II: LUCAS'S LIFE AND TIMES

François-Édouard-Anatole Lucas, always known as Édouard, was born the son of a laborer in Amiens, France in 1842 (Williams, p. 53). He grew up in very unsettled times. When Édouard was six years old, revolutions swept the world. Just before the 1848 revolution in France took place, Karl Marx and Friedrich Engels published their *Communist Manifesto* (Garraty, pp. 885-889). France participated in the Crimean War from 1854 to 1856, and China was engaged from 1851 to 1864 in the Taiping Rebellion, possibly the bloodiest civil war in history. Another kind of revolution started with Charles Darwin's publication of *The Origin of Species* in 1859 (Garraty, p. 31).

Because of his mathematical talents, starting in 1861 Édouard was educated at the *École polytechnique* and *École normale*, which were at that time the most prestigious institutions of higher learning in France, and graduated from the latter in 1864 (Williams, p. 53). He was first employed at the Paris Observatory as an assistant (Gridgeman). The

ongoing turmoil in Europe affected him directly. He became an artillery officer during the short-lived Franco-Prussian War (Gridgeman), which ended in defeat and a new government for the French in 1871 (Garraty, p. 914).

In 1872 Lucas became professor of mathematics at the *Lycée* of Moulins, and after that he taught at the *Lycées* of Paris Saint-Louis and Paris Charlemagne (Williams, p. 53). He was known for his boundless energy and broad range of interests (Williams, p. 53). Lucas's career was cut short by an accident in 1891, when a piece of a dropped plate flew up and gashed his cheek while he was attending a meeting of the French Association for the Advancement of Science in Marseilles (Williams, pp. 148-149). The wound became infected, and within a few days Lucas was dead of erysipelas (Gridgeman).

As the world changed socially during Lucas's lifetime, so did it change mathematically. The multifaceted activity was doubtlessly inspired by the genius of Carl Friedrich Gauss (1777-1855), the man often called the founder of modern mathematics (Dunnington). Ernst Eduard Kummer (1810-1893) developed the concept of algebraic integers and ideal numbers. His work extended the fundamental theorem of arithmetic, which states that every integer can be factored into a product of primes, to include complex number fields ("Kummer"). The field of logic developed during the Nineteenth Century, with Augustus De Morgan's (1806-1871) solution of the negation problem and George Boole's (1815-1864) creation of operator algebra and a system for logical expression (Suzuki, pp 700-701).

Euclidean geometry was turned on its head during Lucas's career, as many mathematicians studied and expanded the contributions of János Bolyai (l802-1860) and Nikolai Lobachevsky (1793-1856) in the first half of the Nineteenth Century. These two

men independently conceived of a geometric system in which Euclid's fifth postulate was replaced with the characteristic axiom of hyperbolic geometry (Chern). Lobachevsky published the first account of a non-Euclidean geometry in 1829 (Suzuki, p. 652). Eugenio Beltrami (1835-1900) investigated the mapping of abstract surfaces and developed theories about surfaces with constant curvature. Bernhard Riemann (1826-1866) unified the theories of complex and harmonic functions. His concept of the Riemann surface is an important part of fundamental complex function theory (Suzuki, p. 660). These mathematicians greatly expanded the bounds of mathematical thinking and investigation and initiated the development of topological theory, which has been a major area of mathematical research ever since. By the end of the Nineteenth Century projective geometry had been developed by Felix Klein (1849-1924) and others (Chern).

Arthur Cayley (1821-1895) played an important role in developing modern linear and abstract algebra (Suzuki, p. 707). Throughout the second half of the Nineteenth Century there was a movement to arithmetize mathematics, encouraging the modern emphasis on algebraic rather than geometric reasoning (Boyer). Georg Cantor (1845-1918) proved several important foundations of set theory, including the fact that the rational numbers are countable, but the real numbers are uncountable (Suzuki, p. 681). He revolutionized the concept of infinity by showing that because the set of real numbers is not countable its cardinality is a "larger" infinity than that of the set of counting numbers ("Mathematics"). Richard Dedekind (1831-1916) advanced number theory and set theory to include irrational numbers, proving that the domain of the real numbers is continuous ("Mathematics"). In his book *The Foundations of Arithmetic* Gottlob Frege

(1848-1925) was the first to publish a theory of the natural numbers (Suzuki, pp. 677-678).

Lucas contributed to the flurry of mathematical development during the second half of the Nineteenth Century. He wrote papers about many subjects, including astronomy, weaving, analysis, combinatorics, calculating devices, geometry, and recreational mathematics (Williams, p. 53). He invented the still-popular game known as the Tower of Hanoi, in which *n* distinctive rings piled on one of three pegs on a board must be transferred, in single peg-to-peg steps, to one of the other pegs, with the final ordering of the rings remaining unchanged (Gridgeman). A version of one of Lucas' chessboard puzzles was adapted for the computer nearly a century after his death (Riamus). Lucas also published several volumes of mathematical recreations, which included a variety of chessboard and geometry problems, among many others (Ball, pp. 124-125). Certainly these games help to explain his known popularity as a teacher (Gridgeman).

Lucas's most famous research centered on number theory, particularly the testing for prime numbers. His most significant discovery was that it could be done without a large number of calculations (Williams, p.57). Lucas proposed any number of theorems concerning primality; among them was one discussing the Fermat numbers, which take the form $F_n = 2^{2^n} + 1$.

> Let $F_n = 2^r + 1$ ($r = 2^n$) and $T_1 = 3$. If we define the sequence $\{T_i\}$ by $T_{i+1} = 2T_i^2 - 1$ ($i = 1,2,3,\ldots$), then F_n is a prime if the first term of this sequence which is divisible by F_n is T_{r-1}. Also, F_n is composite if none of these terms up to and including T_{r-1} is divisible by F_n. Finally, if k [$< r$] denotes the rank of the first term which is divisible by F_n, the prime divisors of F_n must have the form $2^{k+1}q + 1$. (Williams, p. 99)

Lucas devised a theorem which provided the basis of the modern method of testing the primality of Mersenne numbers, which take the form $2^n - 1$ (Gridgeman). His version states:

> Let $M_n = 2^n - 1$, where $n \equiv 1 \pmod 4$. Form the sequence $r_1 = 4$, $r_2 = 14$, $r_3 = 194$, $r_4 = 37634,\ldots$, where $r_{i+1} = r_i^2 - 2$. The number M_n is composite if M_n [does not divide] r_k for $k = 1,2,3,\ldots, n-1$; M_n is prime if the least value α of k such that $M_n \mid r_k$ is such that $(n+1)/2 \le \alpha \le n$. If $\alpha < (n-1)/2$, then the prime divisors of M_n must have the form $2^{\alpha}m \pm 1$. [Lucas wrote $2^{\alpha}m + 1$, but this is clearly incorrect.] (Williams, p. 98)

Derrick Lehmer (1905-1991) expanded the theorem in 1930 to include all odd values of n. His work yielded the technique known as the Lucas-Lehmer test (Williams, p. 112), which is still commonly used today (Havil, p. 164). In 1876 Lucas used his own theorem to identify $2^{127} - 1$ as a prime. This was the first new Mersenne prime discovered in over a century, and was also the largest ever to be discovered without electronic help (Gridgeman).

PART III: MATHEMATICAL DEVELOPMENTS LEADING TO LUCAS'S THEOREM

Mathematical developments painting the background for Lucas's Theorem represent several separate fields: prime number theory, and the three areas that converge in Pascal's Triangle: figurative, or sequential, number theory; algebra; and combinatorics. Interestingly, the Chinese know Pascal's Triangle as Yang Hui's Triangle; the Iranians call it the Khayyam Triangle; and the Italians call it Tartaglia's Triangle (Pascal's Triangle Builder). The varied nomenclature demonstrates the disparate trails that led to Pascal's accomplishment of unifying various results into one figure.

Greeks of Pythagoras' time as well as Egyptians as early as 300 B.C. were very interested in number patterns (Edwards, pp. 1-5). Leonardo of Pisa (1170-1250), also known as Fibonacci (Williams, p. 31), published the sequence of numbers named after him in 1202, to solve the question of how many descendants a pair of rabbits can produce in various periods of time (Phillips, p. 139).

Euclid expanded $(a + b)^2$ about 300 B.C. and Brahmagupta expanded $(a + b)^3$ about 628 A.D. Al-Karaji discovered the binomial triangle around 1000 A.D. A century later Omar Khayyam claimed to have raised binomials to the sixth power and higher. Yang Hui showed the coefficients of $(a + b)^n$ up to the sixth power about 1261 A.D., and Al-Kashi gave the general rule for positive integers about 1427 A.D. (Edwards, pp. 51-52) About 1544 the German mathematician Michael Stifel (1487-1567) utilized the figurate triangle to extract roots. He is considered the first in the western world to discover the identity of the binomial and figurate numbers according to the equation

$\binom{n}{r} = f_r^{n-r+1}$, where $f_k^l = f_k^{l-1} + f_{k-1}^l$; $f_k^1 = f_0^l = f_0^1 = 1$;

$l = 2,3,4,\ldots$; $k = 1,2,3,\ldots$; $f_k^l = \sum_{i=1}^{l} f_{k-1}^i$ (Edwards, pp. 5-7).

Combinatorics also has a long history, though Gottfried Leibniz (1646-1716) was the first to use the term in the modern sense. Well in the pre-Christian era the Indian mathematician Susruta systematically enumerated possibilities to arrive at the total number of potential outcomes (Edwards, p. 27). Around 310 A.D., when studying intersecting lines, Pappus derived a general rule for choosing 2 items from *n* different things, specifically that $f_2^{n-1} = \frac{n(n-1)}{2}$ (Edwards, p. 27). In about 1140, Rabbi Ben Ezra

(1092-1167), the inspiration for Robert Browning's famous poem bearing his name (Bradley, pp. 510-515), who was responsible for bringing much Eastern knowledge to Europe (O'Connor, 1999), used the Hindu method for finding the number of combinations of seven objects, in this case the then-known six planets and the sun, taken *r* at a time, which yielded the combinatorial numbers ${}^{7}C_{2}$, ${}^{7}C_{3}$,…,${}^{7}C_{7}$, or 21, 35, 35, 21, 7, and 1, for a total of 120.

Gambling was the impetus for much combinatorial study in the Middle Ages. During the Renaissance, Niccolo Tartaglia (1500-1557) created a general rule for determining the number of unordered throws of *n* dice. He also devised a general formula for solving cubic polynomials. It appears that both Tartaglia and his rival Girolamo Cardano (1501-1576), who published a combinatorial triangle which he related to the figurate triangle, understood that these two sets of numbers were connected to the binomial expansion (Edwards, pp. 34-43). In 1636 Marin Mersenne (1588-1648) published a collection of the rules of combinatorics. A young student named Blaise Pascal (1623-1662) knew Mersenne, and followed Mersenne's format when constructing his famous triangle (Edwards, p. 47).

Prime numbers have been studied since the earliest days of mathematics. Pythagoras understood the concept of primality (Valens, p. 18). Primes are a part of the fundamental theorem of arithmetic, which was deduced if not explicitly stated by Euclid (Suzuki, p. 126). Around 300 B.C. this great mathematician proved that the number of primes is infinite, and in so doing created the abstract theory of prime numbers (Crandall, p. 5). The Sieve of Eratosthenes, devised about 200 B.C., was an algorithm to calculate

primes. After this time there was a long period of apparent inactivity in research about primality.

In the Seventeenth Century Mersenne asserted that the number $2^n - 1$ is prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and for no other values of $n \leq 257$ (Phillips, p. 169). His work was the basis for much of Lucas's research, as was that of Pierre de Fermat (1601-1665), who claimed wrongly in 1637 that Fermat's numbers, as they became known, are always prime (Crandall, p. 24). Despite this often-cited error in a distinguished career, Fermat spurred interest in primality, and in his own work combined the concepts of prime number and probability theory (O'Connor, 2005), leading the way to combinatorics.

Gauss explicated the concept of congruence with regard to residue classes. In his terminology, the expression $x \equiv u \pmod{n}$ indicates that x is congruent to u in terms of residue (Phillips, p.172). Shown below in Gaussian form, Fermat's Little Theorem, which is an important precursor to Lucas's Theorem, is clearer to the modern reader than it would be in the original version. Fermat's Little Theorem states that for any prime p and any positive integer a that is not divisible by p, $a^{p-1} \equiv 1 \pmod{p}$ (Phillips, p. 174). Joseph-Louis LaGrange (1736-1813) applied this theorem to polynomials, obtaining the result that, "given any prime p and a polynomial $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, where p does not divide a_0, then $f(x)$ is satisfied by at most n distinct residues modulo p" (Phillips, p. 179). Leonhard Euler (1707-1783) generalized Fermat's Little Theorem from just primes to all positive integers (Phillips, p. 177). Using these earlier results, themselves the outcomes of generations of mathematical study, Lucas was able to apply the patterns elucidated in Pascal's Triangle to create his theorem.

PART IV: LUCAS'S THEOREM, PROOFS, AND EXAMPLE OF USE

Lucas proposed his great theorem in 1878, in Section XXI of the massive journal article *Théorie des functions numériques simplement périodiques* (Lucas), without presenting an actual proof. A copy of the original version of this Section is in the Appendix. The following mathematical statements, through the theorem itself, are expressed using Lucas's notation, which, relative to today's notation, reversed the terms next to the *C*. He approached the statement of the theorem by first noting two fundamental formulas for determining the number of combinations of *m* objects taken from *n* objects one at a time:

$$C_m^n = \frac{m(m-1)....(m-n+1)}{1.2.3....n}, \qquad \text{and} \qquad C_m^n = C_{m-1}^n + C_{m-1}^{n-1},$$

and then specifying that when *p* is a prime number and *n* is an integer between 0 and *p* [exclusive], the congruence , $C_p^n \equiv 0$, (Mod. *p*) holds. For *n* between 0 and $p-1$ [exclusive], $C_{p-1}^n \equiv (-1)^n$, (Mod. *p*), and for *n* between 1 and *p* [exclusive], $C_{p+1}^n \equiv 0$, (Mod. *p*). Lucas then observed patterns in Pascal's Triangle and derived the general statement: $C_m^n \equiv C_{m_1}^{n_1} \times C_\mu^\nu$, (Mod. *p*), where μ and ν are the residues of *m* and *n*, respectively. Further, $C_{m_1}^{n_1} \equiv C_{m_2}^{n_2} \times C_{\mu_1}^{\nu_1}$, (Mod. *p*). These congruences led to Lucas's Theorem:

$$C_m^n \equiv C_{\mu_1}^{\nu_1} \times C_{\mu_2}^{\nu_2} \times C_{\mu_3}^{\nu_3} \times ..., \text{ (Mod. } p),$$

where $\mu_1, \mu_2, \mu_3, \ldots$ designate the residues of *m* and of the integers of $\frac{m}{p}, \frac{m}{p^2}, \frac{m}{p^3}, ...$, and the same for $\nu_1, \nu_2, \nu_3, \ldots$ with respect to *n* (Lucas).

One modern way of expressing Lucas's Theorem is to let *p* be prime and suppose

$r = r_k p^k + \ldots + r_1 p + r_0 \quad (0 \le r_i < p)$;

$c = c_k p^k + \ldots + c_1 p + c_0 \quad (0 \le c_i < p)$ (Evans). "Then

$$\binom{r}{c} \equiv \binom{r_k}{c_k} \ldots \binom{r_1}{c_1}\binom{r_0}{r_0} \pmod{p}$$" (Riddle).

The theorem can be used to calculate a number such as $\binom{105}{24}$ mod 3, as follows:

$105_{10} = 10220_3$, and $24_{10} = 220_3$; pairing the digits of these base 3 numbers yields

$$\binom{105}{24} \equiv \binom{1}{0}\binom{0}{0}\binom{2}{2}\binom{2}{2}\binom{0}{0} \bmod 3, \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \bmod 3 \equiv 1 \bmod 3,$$

and

therefore $\binom{105}{24} \equiv 1 \bmod 3$.

The several proofs offered for Lucas's Theorem are primarily of two types, algebraic and combinatorial. The following algebraic proof is based on the Binomial Theorem for expansion of $(1 + x)^r$. Let

$$\sum_{c=0}^{r}\binom{r}{c}x^c = (1+x)^r = \prod_{m=0}^{k}\left[(1+x)^{p^m}\right]^{r_m}$$

$$\equiv \prod_{m=0}^{k}(1+x^{p^m})^{r_m} \pmod{p}, \quad [\text{since } (1+x)^{p^m} \equiv 1 + x^{p^m} \pmod{p}]$$

$$\equiv \prod_{m=0}^{k}\left[\sum_{s_m=0}^{r_m}\binom{r_m}{s_m}x^{s_m p^m}\right] \pmod{p}$$

$$\equiv \sum_{c=0}^{r}\left[\sum\prod_{m=0}^{k}\binom{r_m}{s_m}\right]x^c \pmod{p},$$

where for each value of c, the inner sum in the last sum is taken over all the sets $(s_0,s_1,s_2,\ldots,s_k)$ such that $0 \le s_m \le c_m < p$ and $\sum_{m=0}^{k} s_m p^m = c$. But there is at most one such set of coefficients, given by $s_m = c_m$ if every $c_m \le r_m$ (since there is a unique representation for the p-ary form of c.) If $c_m > r_m$ for some m,

then the inner sum is zero. In either case, the theorem follows by equating coefficients of x^c for each $0 \le c \le r$. (Riddle)

Anderson *et al*. have presented a longer, combinatorial proof of Lucas's Theorem (Anderson).

Lucas's Theorem can be used to solve very difficult problems in combinatorics and probability. For example, in a computer security algorithm, each employee's identification number can be made to be congruent mod 23, and is constructed using choose notation, *i.e*., $\binom{1000}{50}$. To access a file, the employee would enter the number 10000050. Clearly, the larger the modulus the more secure the system. All assigned identification numbers are congruent to 11 mod 23. If someone types in the identification number 22340197, it is critically important for the computer to tell if $\binom{2234}{197}$ is congruent to 11 mod 23. The number $\binom{2234}{197}$ is so large that it would cause an overflow error in almost any computer system. With Lucas's Theorem the calculation becomes manageable: in base 23, 2234 is 453, and 197 is 8(13) (13 is a single digit in base 23), so $\binom{2234}{197}$ is congruent to $\binom{4}{0}\binom{5}{8}\binom{3}{13} = 1 \times 0 \times 0 = 0$ mod 23. This is not congruent to 11 mod 23, so the person trying to login is either a hacker or a poor typist.

PART V: EXTENSIONS AND GENERALIZATIONS OF LUCAS'S THEOREM

Even today, Lucas's Theorem is being studied widely, and has been both extended and generalized, particularly in the area of binomial coefficients. Richard Bollinger and Charles Burchard applied the theorem to Pascal's Triangle, proving given

that p is a prime, and that $n = n_0 + n_1p + \ldots + n_rp^r$, $0 \le n_i < p$, and $k = k_0 + k_1p + \ldots + k_tp^t$, $0 \le k_i < p$, $0 \le k \le (m-1)n$, that "$C_m(n,k) \equiv \sum_{(s_0,\ldots,s_r)} \prod_{i=0}^{r} C_m(n_i, s_i) \pmod{p}$ where the sum is taken over all $(r+1)$-tuples $(s_0,s_1,\ldots,s_r)$ such that i) $s_0 + s_1p + \ldots + s_rp^r = k$, and *ii*) $0 \le s_i \le (m-1)n_i$; if k is not representable in this form then certainly $C_m(n,k) \equiv 0 \pmod{p}$" (Bollinger).

In the same area of research, Alexis Bès generalized Lucas's Theorem to mod prime powers. This accomplishment obviously serves to improve the security of cryptographic applications (Bès).

Jacques Boulanger and Jean-Luc Chabert have recently extended Lucas' Theorem to linear algebra and even topology.

> Let V be a discrete valuation domain with finite residue field. Denote by K the quotient field of V, by v the corresponding valuation of K, by m the maximal ideal of V, and by q the cardinality of the residue field V/m.
>
> We denote by $\hat{K}$, $\hat{V}$, and $\hat{m}$ the completions of K, V, and m with respect to the m-adic topology and we still denote by v the extension of v to $\hat{K}$ ….
> The polynomials $C_n(X)$ form a basis of the V-module Int(V)….
> If $n = n_0 + n_1q + \ldots + n_kq^k$ is the q-adic expansion of a positive integer n, and if $x = x_0 + x_1t + \ldots + x_jt^j + \ldots$ is the t-adic expansion of an element x of $\hat{V}$, then $C_n(x) \equiv C_{n_0}(x_0)C_{n_1}(x_1)\ldots C_{n_k}(x_k) \pmod{\hat{m}}$. (Boulanger)

In a related field, Neyamat Zaheer generalized Lucas's Theorem to vector-valued abstract polynomials in vector spaces (Zaheer).

To formulate a divisibility theorem, Tyler Evans applied Lucas's Theorem to Euler's φ function. "For $n \ge 1$, $m = Mn + m_0$, $r = Rn + r_0$, $0 \le m_0, r_0 < n$

$$\sum_{d/n} \varphi\left(\frac{n}{d}\right) \sum_{j=-(d-1)}^{d-1} \sum_{\substack{\|\alpha\|_d = \\ R-(j/d)}} \binom{M}{\alpha_1} \ \ldots \ \binom{M}{\alpha_d} \binom{m_0}{r_0 + (n/d)j} \equiv 0 \pmod{n}$$ " (Evans).

The breadth and longevity of research applying Lucas's Theorem to new areas of mathematics demonstrate the significance of this theorem. Last summer the author, under the direction of Professor Daniel Pritikin, extended Lucas's Theorem to determine how many entries in a given row of Pascal's Triangle are equivalent to a given number modulo 3 or 5. In the simpler case, mod 3, the number of entries with remainder 1 in row n was calculated to be

$$f_1(n) = 2^{c_1(n)} \bullet [3^{c_2(n)} + 1]/2,$$

and the number of entries with remainder 2 in row n was calculated to be

$$f_2(n) = 2^{c_1(n)} \bullet [3^{c_2(n)} - 1]/2,$$

where $c_1(n)$ is the number of 1's in the base 3 expansion of n and $c_2(n)$ is the number of 2's in the base 3 expansion of n (Smith).

Clearly, in the author's opinion, Lucas's Theorem is great. It amalgamates centuries of mathematical work, it is a useful tool on its own, and it also has been a building block of significant developments in diverse areas of mathematics in the decades since its exposition.

WORKS CITED

Anderson, Peter G., Arthur T. Benjamin, and Jeremy A. Rouse (2005). Combinatorial Proofs of Fermat's, Lucas's, and Wilson's Theorems. *The American Mathematical Monthly*, 112, 266-268.

Ball, W. W. Rouse and H. S. M. Coxeter (1974). *Mathematical Recreations and Essays*. Toronto: University of Toronto Press.

Bès, Alexis (1997). On Pascal Triangles Modulo a Prime Power. *Annals of Pure and Applied Logic*, 89, 17-35.

Bollinger, Richard and Charles Burchard (1990). Lucas' Theorem and Some Related Results for Extended Pascal Triangles. *American Mathematical Monthly*, 97, 198-204.

Boulanger, Jacques and Jean-Luc Chabert (2001). An Extension of the Lucas Theorem. *Acta Arithmetica*, XCVI, 303-312.

Boyer, Carl and Otto Neugebauer (1965). Mathematics, History of. *Encyclopaedia Britannica*, vol. 14, 1101-1107.

Bradley, Nella (1932). *The Standard Book of British and American Verse*. Garden City, New York: The Garden City Publishing Company.

Chern, Shiing Shen (1965). Geometry, Non-Euclidean. *Encyclopaedia Britannica*, vol. 10, 195-196. Chicago: Encyclopaedia Britannica, Inc.

Crandall, Richard and Carl Pomerance (2001). *Prime Numbers: A Computational Perspective*. New York: Springer-Verlag.

Dunnington, G. Waldo (1965). Gauss, (Johann) Carl Friedrich. *Encyclopaedia Britannica*, vol. 10, 35-36. Chicago: Encyclopaedia Britannica, Inc.

Edwards, A. W. F. (1987). *Pascal's Arithmetical Triangle*. London: Charles Griffin and Company.

Evans, Tyler J. (2005). On Some Generalizations of Fermat's, Lucas's and Wilson's Theorems. *Ars Combinatoria*, 79, 189-194.

Garraty, John A. and Peter Gay (eds.) (1986). *The Columbia History of the World*. New York: Harper & Row.

Gridgeman, Norman T. (1970-1990). Lucas, François-Édouard-Anatole. Gillispie, C. C. (ed.). *Dictionary of Scientific Biography*, vol. VIII. 531-532. New York: Scribners.

Havil, Julian (2003). *Gamma: Exploring Euler's Constant*. Princeton: Princeton University Press.

"Kummer" (2006). Encyclopaedia Britannica Online. www.britannica.com/eb/article-9046414. Available 30 September 2006.

Lucas, Édouard (1878). *Théorie des functions numériques simplement périodiques. Amer. J. Math.*, 1, 184-240, 289-321.

"Mathematics" (2006). Encyclopaedia Britannica Online. www.britannica.com/eb/article/66015 through www.britannica.com/eb/article/66033. Available 30 September 2006.

O'Connor, J. J. and E. F. Robertson (1999). Abraham ben Meir ibn Ezra. http://www-history.mcs.st-andrews.ac.uk/Biographies/Ezra.html. Available 6 October 2006.

O'Connor, J. J. and E. F. Robertson (2005). Prime Numbers. http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html. Available 3 October 2006.

"Pascal's Triangle Builder" (unknown). Archimedes Laboratory. http://www.archimedes-lab.org/pascaltriangle.html#. Available 3 October 2006.

Phillips, George M. (2000). *Two Millenia of Mathematics*. New York: Springer-Verlag.

Riamus (2005). Lucas' Problem. http://www.mobygames.com/game/lucass-problem. Available 8 October 2006.

Riddle, Larry (2006). Proof of Lucas's Theorem. http://ecademy.agnesscott.edu/~lriddle/ifs/siertri/LucasProof.htm. Available 20 September 2006.

Smith, Douglas and Daniel Pritikin (2006). Unpublished work presented at Pi Mu Epsilon Session #1, Mathfest 2006, Knoxville, TN, August 10, 2006.

Suzuki, Jeff (2002). *A History of Mathematics*. Upper Saddle River, N.J.: Prentice-Hall.

Valens, Evans (1964). *The Number of Things*. New York: E. P Dutton and Co.

Williams, Hugh C. (1998). *Édouard Lucas and Primality Testing*. New York: John Wiley and Sons.

Zaheer, Neyamat (1993). A Generalization of Lucas' Theorem to Vector Spaces. *Int. J. Math. Math. Sci.*, 16, 267-276.

APPENDIX

et, par suite,

$$U_{91} = -7 \times 712711 \times 770041.$$

Ces deux derniers facteurs sont premiers; il n'y a que deux diviseurs à essayer. On comprend ainsi comment il est possible d'appliquer le théorème précédent, à la recherche directe de très-grands nombres premiers, par la considération des séries de troisième espèce.

SECTION XXI.

Sur les congruences du Triangle Arithmétique de PASCAL, *et sur une généralisation du théorème de* FERMAT.

En désignant par C_m^n le nombre des combinaisons de m objets pris n à n, on a les deux formules fondamentales

$$C_m^n = \frac{m\,(m-1)\,\ldots\,(m-n+1)}{1\,.\,2\,.\,3\,\ldots\,n}$$

$$C_m^n = C_{m-1}^n + C_{m-1}^{n-1};$$

par conséquent, lorsque p est premier, on a pour n entier compris entre 0 et p, la congruence

$$C_p^n \equiv 0, \quad (\text{Mod. } p); \tag{134}$$

pour n compris entre 0 et $p-1$,

$$C_{p-1}^n \equiv (-1)^n, \quad (\text{Mod. } p); \tag{135}$$

pour n compris entre 1 et p

$$C_{p+1}^n = 0, \quad (\text{Mod. } p). \tag{136}$$

En d'autres termes, dans le triangle arithmétique de PASCAL, tous les nombres de la $p^{ième}$ ligne sont, pour p premier, divisibles par p, à l'exception des coefficients extrêmes égaux à l'unité; les coefficients de la $(p-1)^{ième}$ ligne donnent alternativement pour résidus $+1$ et -1; ceux de la $(p+1)^{ième}$ ligne sont divisibles par p, en exceptant les quatre coefficients extrêmes, égaux à l'unité.

Si l'on continue la formation du triangle arithmétique, en ne conservant que les résidus suivant le module p, on reforme deux fois le triangle arithmétique des $(p-1)$ premières lignes; puis, à partir de la $(2p)^{ième}$ ligne, on le reforme trois fois; mais les résidus du triangle intermédiaire sont multipliés par 2; à partir de la $(3p)^{ième}$ ligne, le triangle des résidus est reproduit quatre

fois, mais les nombres de ces triangles sont respectivement multipliés par les coefficients 1, 3, 3, 1 de la troisième puissance du binôme, et ainsi de suite.

On a donc, en général,

$$C_m^n \equiv C_{m_0}^{n_0} \times C_\mu^\nu , \quad (\text{Mod. } p) ,$$

m, et n_1 désignant les entiers de $\frac{m}{p}$ et de $\frac{n}{p}$, et μ et ν les résidus de m et de n. On a, de même

$$C_{m_1}^{n_1} \equiv C_{m_2}^{n_2} \times C_{\mu_1}^{\nu_1} , \quad (\text{Mod. } p) ,$$

et, par suite,

$$C_m^n \equiv C_{\mu_1}^{\nu_1} \times C_{\mu_2}^{\nu_2} \times C_{\mu_3}^{\nu_3} \times \dots , \quad (\text{Mod. } p) , \tag{137}$$

$\mu_1, \mu_2, \mu_3, \dots$ désignant les résidus de m et des entiers de $\frac{m}{p}, \frac{m}{p^2}, \frac{m}{p^3}, \dots$, et de même pour $\nu_1, \nu_2, \nu_3, \dots$.

Par conséquent, si l'on veut trouver le reste de la division de C_m^n par un nombre premier, il suffit d'appliquer la formule précédente, jusqu'à ce qu'on ait ramené les deux indices de C à des nombres inférieurs à p.

Nous venons de voir que les coefficients de la puissance p du binôme sont entiers et divisibles par p, lorsque p désigne un nombre premier, en exceptant toutefois les coefficients des puissances $p^{ième}$. En désignant par $\alpha, \beta, \gamma, \dots \lambda$, des entiers quelconques, en nombre n, on a donc

$$[\alpha + \beta + \gamma + \dots + \lambda]^p - [\alpha^p + \beta^p + \gamma^p + \dots + \lambda^p] \equiv 0, \quad (\text{Mod. } p),$$

et, pour $\alpha = \beta = \gamma = \dots = \lambda = 1$, on obtient

$$n^p - n \equiv 0, \quad (\text{Mod. } p) .$$

C'est dans cette congruence que consiste le théorème de FERMAT, que l'on peut généraliser de la manière suivante, différente de celle que l'on doit à EULER. Si $\alpha, \beta, \gamma, \dots \lambda$ désignent les puissances $q^{ièmes}$ des racines d'une équation à coefficients entiers, et S_q leur somme, le premier membre de la congruence précédente représente le produit par p d'une fonction symétrique, entière et à coefficients entiers, des racines, et, par conséquent, des coefficients de l'équation proposée. On a donc

$$S_{q^p} \equiv S_q^p , \quad (\text{Mod. } p) ,$$

et, par l'application du théorème de FERMAT,

$$S_{q^p} \equiv S_q , \quad (\text{Mod. } p) . \tag{138}$$

L'étude des diviseurs premiers de la fonction numérique S_q et de quelques autres analogues est très-importante ; on a, en particulier, pour $n = 1$ et $S_1 = 0$, comme dans l'équation

$$x^3 = x + 1 ,$$

la congruence

$$S_p \equiv 0\,, \quad (\text{Mod. } p)\,;$$

on en déduit inversement que *si, dans le cas de* $S_i = 0$, *on a* S_n *divisible par* p, *pour* $n = p$, *et non auparavant, le nombre* p *est un nombre premier*. En effet, supposons p égal, par exemple, au produit de deux nombres premiers g et h. On a

$$S_{gh} \equiv S_h\,, \quad (\text{Mod. } g)$$
$$S_{gh} \equiv S_g\,, \quad (\text{Mod. } h)\,;$$

par conséquent, si l'on a trouvé

$$S_{gh} \equiv 0\,, \quad (\text{Mod. } gh)\,,$$

on aura aussi

$$S_g \equiv 0\,, \quad (\text{Mod. } h)\,,$$
$$S_h \equiv 0\,, \quad (\text{Mod. } g)\,,$$

et, par le théorème démontré,

$$S_g \equiv S_h \equiv 0\,, \quad (\text{Mod. } gh)\,.$$

Ainsi S_{gh} ne serait pas le premier des nombres S_n divisible par gh.

On peut obtenir, de cette façon, un grand nombre de théorèmes servant, comme celui de WILSON, à vérifier les nombres premiers. Nous laisserons de côté, pour l'instant, les développements curieux et nouveaux que nous avons ainsi trouvés, pour ne considérer que ceux que l'on tire des fonctions numériques simplement périodiques.

SECTION XXII.

Sur la théorie des nombres premiers dans leurs rapports avec les progressions arithmétiques.

La doctrine des nombres premiers a été ébauchée par EUCLIDE et ERATOSTHÈNE. On doit à EUCLIDE la théorie des diviseurs et des multiples communs de deux ou plusieurs nombres donnés, la représentation des nombres composés à l'aide de leurs facteurs, et la démonstration de l'infinité des nombres premiers, que l'on peut étendre facilement à la preuve de l'infinité des nombres premiers appartenant aux formes linéaires $4x + 3$ et $6x + 5$. Nous donnerons, dans la Section XXIV, une démonstration élémentaire concernant l'infinité des nombres premiers de la forme $ax + 1$, quelle que soit la valeur de a. On sait d'ailleurs que, par l'emploi des séries infinies, LEJEUNE-DIRICHLET est parvenu à démontrer l'infinité des nombres premiers de la