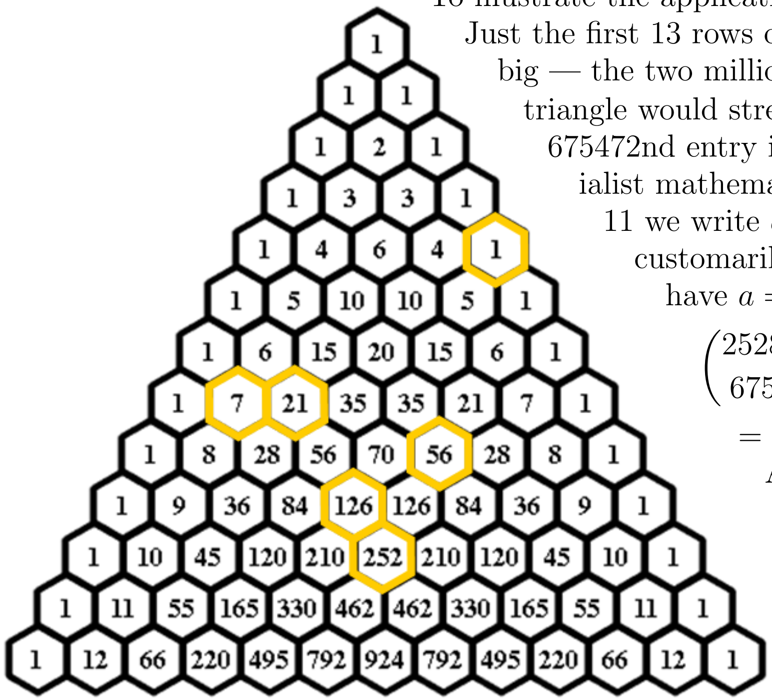
THEOREM OF THE DAY

Lucas' Theorem *Let p be a prime number and let a and b, $a \geq b$, be positive integers written in base p (say, $a = [a_s, a_{s-1}, \ldots, a_1, a_0], b = [b_t, b_{t-1}, \ldots, b_1, b_0]$, with $a = \sum a_i p^i$ and $b = \sum b_j p^j$ and $s \geq t$). Then*

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_{t-1}}{b_{t-1}}\binom{a_t}{b_t} \pmod{p}.$$



To illustrate the application of Lucas' theorem, we will consider the values $a = 2528646$ and $b = 675471$. Just the first 13 rows of Pascal's triangle are shown here (starting at row 0). The numbers get very big — the two millionth row contains almost a trillion digits (by which time, on this scale, the triangle would stretch beyond the moon!) So to calculate the precise value of $\binom{2528646}{675471}$, the 675472nd entry in the 2528647th row, is a big task, even for a computer running specialist mathematical software. But we can easily find its remainder, mod 11: in base 11 we write a=$147789A_{11}$ (in base conversions ≥ 10, the letters A, B, C, . . . , are customarily used to represent 10, 11, 12, . . .). In base 11, b=421545_{11}. So we have $a = [1, 4, 7, 7, 8, 9, 10]$ and $b = [4, 2, 1, 5, 4, 5]$ and, by Lucas' Theorem,

$$\binom{2528646}{675471} \equiv \binom{10}{5} \times \binom{9}{4} \times \binom{8}{5} \times \binom{7}{1} \times \binom{7}{2} \times \binom{4}{4} \pmod{11}$$

$= 252 \times 126 \times 56 \times 7 \times 21 \times 1 \pmod{11} = 261382464 \pmod{11}$.

A neat trick for extracting the remainder mod 11 is to alternately add and subtract digits in reverse order, which, for 261382464, gives us $4 - 6 + 4 - 2 + 8 - 3 + 1 - 6 + 2 = 19 - 17 = 2$. And, in a mere few minutes, we have discovered something about a number that has more digits than the number of seconds in an entire week!

Édouard Lucas (1842–1891) is remembered for his work on the Fibonacci numbers and for inventing the Towers of Hanoi puzzle. His theorem on the binomial coefficients can be used to derive many interesting properties of Pascal's triangle, for instance, $\binom{a}{b}$ is odd exactly when every 1 in the base 2 representation of b is also a 1 in the base 2 representation of a.

Web link: www.math.hmc.edu/funfacts/ffiles/30002.4-5.shtml; the image of Pascal's triangle is from mathforum.org.

Further reading: Pascal's Arithmetical Triangle by A.W.F. Edwards, Johns Hopkins University Press, 2002.