Abstract: Lucas’s Theorem is used to express the remainder of the binomial coefficient of any two integers \( m \) and \( n \) when divided by any prime integer \( p \). The remainder is equivalent to the product of the binomial coefficients of every digit of the base \( p \) expansion of \( m \) and \( n \), modulo \( p \). The well-known proof of this theorem cleverly incorporates the Binomial Theorem, but this result can be proven in a more straightforward manner through induction. We are going to explore this and some of the special cases that come with this proof.

Introduction: Édouard Lucas was a French mathematician born in 1842 who worked as a mathematics professor in Paris for most of his life. He is best known for his contributions to number theory through his work with sequences and primes. His study of the Fibonacci sequence led to his own Lucas sequence, and he is credited with proving the primality of a Mersenne prime that is still the largest known prime proven by hand. His interest in patterns and primes is what led him to the result of Lucas’s theorem in 1878. The theorem states that for any integers \( m \) and \( n \) and for any prime integer \( p \),

\[
\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod(p)
\]

where \( m_i \) and \( n_i \) are the base \( p \) expansions of \( m \) and \( n \) respectively.

The common proof arises from the Binomial Theorem expansion of \((1+x)^r\) and one significant lemma states that if any of the digits in the base \( p \) expansion of \( n \) are greater than the corresponding digit in the base \( p \) expansion of \( m \), then their binomial coefficient is divisible by \( p \). Recent research and generalization of the theorem has provided interesting findings, including yet another pattern that can be found in Pascal’s Triangle. Fine’s Theorem uses Lucas’s Theorem to state that for a prime \( p \) and an integer \( n \) such that \( n \geq 0 \), the number of nonzero entries, modulo \( p \), of row \( n \) is \( a_p(n) = \prod_{i=0}^{l} (n_i + 1) \).
Other research has attempted to expand the original theorem to powers of primes but the results are more complex and conditional. Regardless, it is an intriguing theorem that reasserts the beauty of numbers and provides an efficient way to check for divisors of large numbers.

**Body:**

We want to show that

\[
\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod(p)
\]

\[m = m_0 + m_1 p + m_2 p^2 + ... m_k p^k \text{ for } (0 \leq m_r < p)\]

and

\[n = n_0 + n_1 p + n_2 p^2 + ... n_k p^k \text{ for } (0 \leq n_r < p)\]

And through binomial expansion,

\[
\frac{m!}{n! (m-n)!} = \frac{(m_0 + m_1 p + m_2 p^2 + ... m_k p^k)(m_0 + m_1 p + m_2 p^2 + ... m_k p^k - 1) \cdots (m_0 + m_1 p + m_2 p^2 + ... m_k p^k - r)}{(n_0 + n_1 p + n_2 p^2 + ... n_k p^k)((m_0 - n_0) + p(m_1 - n_1) \cdots p^k(m_k - n_k))!}
\]

Which should then be equivalent to

\[
\frac{m_0!}{n_0!(m_0 - n_0)!} \times \frac{m_1!}{n_1!(m_1 - n_1)!} \times \cdots \frac{m_k!}{n_k!(m_k - n_k)!} \mod(p).
\]

This is far too messy to prove as is, so we will being with a base case and proceed from there.

Pick a prime number \(d\) and two positive integers \(a\) and \(b\), such that \(a, b < d\). Since \(a\) and \(b\) are both less than \(d\), their base \(d\) expansions are simply \(a\) and \(b\) respectively. Thus, it follows to no surprise that \(\binom{a}{b} \equiv \binom{a}{b_0} \mod(d)\). We have now shown that this theorem works for
a special case of integers, but we want to show that it works for all integers; we can begin by showing that if it works for \(a\) and \(b\), it must work for \(a\) and \(b\) multiplied by any power of \(d\).

Taking \(a \times d\) and \(b \times d\), we find that the base \(d\) expansions of these new numbers are \(a_1d + 0\) and \(b_1d + 0\) where \(a_1\) and \(b_1\) are simply just \(a\) and \(b\). Then \({\binom{ad}{bd}} = (a_1\binom{b_1}{d}) \times (0) \mod(d)\). Since \(0\) is just 1, \({\binom{ad}{bd}}\) is just \(\binom{a}{b}\) \mod(d). The proof of that is as follows:

By binomial expansion, the numerator of

\[
\binom{ad}{bd} = (a_1d)(a_1d - 1)(a_1d - 2) \cdots (a_1d - (d - 1))(a_1d - d) \cdots
\]

These terms will continue until our last term is 1, and from this expansion, we can extract \(d^a\) and here’s why: Our first \(d^a\) comes from the first term of the expansion, the second will come from \((a_1d - d)\), the third from \((a_1d - 2d)\) and so on. The last term we will be able to extract a \(d\) from will be \((a_1d - (a_1 - 1)d)\) since going beyond this would leave us with \((a_1d - (a_1)d)\) which is 0 and not a term in our expansion. Extracting a \(d^a\) also allows us to extract an \(a\)!

because factoring a \(d\) out of said terms leaves behind an \((a_1 - 1)\), an \((a_1 - 2)\), etc. all the way to \((a_1 - (a_1 - 1))\) which is simply 1. Of course, this does not take care of all of our terms. Our remaining terms include all terms of the form \((a_1d - r)\) where \(r\) is an integer not divisible by \(d\), meaning that \(r\) will encompass all integers ranging from 1 to \(d - 1\) modulo \(d\). Since \(d\) shows up \(a\)
times in our product, the numbers between \( d \) and the next multiple of \( d \), will each show up \( a \) times as well. So we will have \((d - 1)^a\) and \((d - 2)^a\), all the way to \((d - (d - 1))^a\), left over.

The product of these “leftover” terms are equivalent to \(-1^a \mod(d)\). For any prime number \( j \), the product of all the integers between 1 and \( j - 1 \), modulo \( j \) is \(-1 \mod(j)\) and in our case, we have this \( a \) times.

Proceeding to the denominator of our expansion, we have \( bd!(ad - bd)! \). Generalizing our above findings, we can rewrite the denominator as \( (d^b(b)!(-1^b \mod(d))(d^{a-b}(a - b)!(-1^{a-b} \mod(d))) \).

Combining like terms, we can reduce that to \( p^a b!(a - b)!(-1^a \mod(d)) \). Putting together our numerator and denominator, we have \( \frac{d^{a!}(-1^a \mod(d))}{d^b!(−1^b \mod(d))d^{a-b}(a - b)!(-1^{a-b} \mod(d))} \) and

\( \frac{a!}{b!(a - b)!} \) which is \( \binom{a}{b} \). Thus, \( \binom{ad}{bd} \equiv \binom{a}{b} \mod(d) \), which is what we wanted. This result can be extended to any power of \( d \) and just that power of \( d \) will be factored out instead of \( d \) itself. We have successfully proven the theorem for cases when the integers we begin with are multiples of our prime.
This method, although applicable to all primes without loss of generality, does not necessarily cover all possible integers as the theorem claims. To do so, consider our previous result with a slight alteration. Say that instead of $\binom{ad}{bd}$, we have $\binom{ad+q}{bd+r}$ where $0 < q, r < d$. Using a similar method to the one above, expanding the numerator of the expansion gives

$$us \ (ad + q)(ad + q - 1)(ad + q - 2) \cdots (ad + q - q)(ad - 1) \cdots$$

Splitting this up, we have $(ad)(ad - 1) \cdots (ad - (ad - 1))$, which we already know is $d^a a!(-1^a \mod(d))$. With our leftover terms, we know that since $q < d$, we will not be able to factor a $d$ from any of them.

What we have instead is $(ad + q)(ad + q - 1) \cdots (ad + q - (q - 1))$ which is really $q! \mod(d)$. This can be generalized to the denominator as well, since $r < d$. When completely simplified, we have $\binom{ad+q}{bd+r} \equiv \frac{a!}{b!(a-b)!} \times \frac{q!}{r!(q-r)!} \mod(d)$ which is just $\binom{a}{b} \times \binom{q}{r} \mod(d)$. This is what we wanted, because the base $d$ representation of an integer of the form $ad + q$ is $aq$.

Using these two techniques, we can generalize the proof to apply to all integers. If in the second case, $q, r \geq d$, one of two things can happen. If either $q$ or $r$ are equal to $d$, we simply add 1 to $a$ or $b$, since we have another multiple of $d$. If either $q$ or $r$ are greater than $d$, we divide $q$ or $r$ by $d$,
add the quotient to $a$ or $b$, and the remainder takes the place of the initial $q/r$. If doing so causes $a$ or $b$ to be greater than or equal to $d$, we move them down and they simply become $ad^2$ and $bd^2$ and so on. If there was a case where one of our integers was of the form $a_2d^2 + 0d + 0$ to begin with, similar rules would apply but in this case, $q$ would have to be less than $d$, else it would add to $a$ and the previously described process simply repeats itself. This process may continue indefinitely and will work in the same manner because of basic base rules. Thus, we can conclude that the theorem works for all multiples of primes, as well as for all of the digits in between and we can rightfully claim, “QED”.

Conclusion: While simple, Lucas’s theorem is elegant and allows for both clever tricks and careful analysis when being proven. Although no significant discoveries were made in this paper, an old theorem was reevaluated through a different light. By proving this theorem this way, I managed to better convince myself of it’s result through such careful decomposition. I also managed to reaffirm why the modulo and base must be a prime number, otherwise terms would not factor the way they did and we could not have used the $−1 mod(p)$ that also cancels at the end.
In beginning the proof, I was quickly intimidated by the factorial expansions of undefined integers but I learned to use divisibility and modulo rules to my advantage to obtain the desired result. I also learned that it was important to look for things I could generalize so that my findings could be applied to future cases and then expanded upon rather than re-derived. Most importantly, I managed to fully convince myself of a result of a theorem that I was fascinated by but didn’t fully understand. I am still curious about what other Pascal’s triangle patterns might be present when using this theorem, and I can’t help but wonder how other modulo rules such as Fermat’s Little Theorem or the Chinese Remainder Theorem, would impact this result. Are there uses for such a theorem besides to check for divisibility, and what other special characters must $m$ and $n$ have in order for their binomial coefficient to be divisible by $p$?

**Bibliography:**

