Binomial Coefficients and Prime Numbers: Legendre's, Kummer's and Lucas' Theorems

Mathematics AA Internal Assessment

Page count: 18

Introduction:

As a student who has been preparing for mathematical olympiads since 6th grade, I can say that number theory has always been my favorite branch of mathematics. In one of my olympiad classes, I came across this problem: *"What is* $\binom{2020}{1071}$ *congruent to in modulo 13?"* This question has led me into investigating the association between the prime numbers and binomial coefficients and I decided to write my IA on this topic. I worked on generalized binomial coefficients to first find out if they could be divided by a prime, and second if they couldn't be divided by that prime, what would their remainder be?

For this aim, I searched up many mathematicians' theorems and got fascinated by the variety of mathematical work. However, I decided to use the generalized ones which I thought would lead me to the intended solutions. In my IA I used and proved Legendre's theorem (1808), Kummer's theorem (1852) and Lucas' theorem (1878). Writing the proofs, I tried to point out the motivations leading to these proofs.

For my investigation, I got help of the rules of binomial distribution which is commonly used in mathematics. The other main topic I used was modular arithmetic as well as number bases and prime numbers. Although some of these topics were not included in my HL Analysis and Approaches Mathematics curriculum, I was quite familiar with them from my math olympiad classes.

Foreknowledge:

Before starting my investigation, I wanted to give the definitions of some mathematical concepts that the IB curriculum didn't include.

Modular arithmetic, is a system in mathematics that works with remainders in a division (*Modular Arithmetic | Britannica*). In modular arithmetic, if $x - y$ can be divided by a $m \in \mathbb{N}$, the real numbers x and y are "congruent" in modulo m. We can denote this as $x \equiv y \ (mod\ m)$. This would also mean that x and y should give the same remainder when divided by m (Özdemir, *Matematik Olimpiyatlarına Hazırlık 3* 147). So, this notation and modular arithmetic in general is useful for working with remainders.

Number bases, allow us to represent values using different notations. For example, the most common number base is "base 10" which we use all day and it can contain the numbers $0,1,2,\dots,9$ as digits to denote values. If we take a number with $k \in \mathbb{Z}^+$ digits where $a_0, a_1, \dots, a_{k-1}$ are from the set $\{0,1,2,\dots,9\}$, its value would be:

$$(a_{k-1}a_{k-2}\dots a_0) = a_0 \times 10^0 + a_1 \times 10^1 + \cdots + a_{k-1} \times 10^{k-1}$$

However, there are other number bases too, for example in base 5, all numbers are written using the digits $0,1,2,3,4$. In general, we can denote a number (with $k \in \mathbb{N}$ digits) written in base $t \in \mathbb{Z}^+$ as $(a_{k-1}a_{k-2}\dots a_0)_t$. ($a_i \in \mathbb{Z}$ for $\forall i \in \{0,1,2,\dots,k-1\}$)

Rule 1: All values in all bases can be converted to each other, so each number in base 10 can be written in any base t and the reverse is also true (Virnuls; Özdemir, *Matematik Olimpiyatlarına Hazirlik 1*):

$$(a_{k-1}a_{k-2}\dots a_0)_t = a_{k-1}t^{k-1} + a_{k-2}t^{k-2} + \cdots + a_0t^0$$

Body of Investigation:

Binomial coefficients refer to a mathematical expression consisting of factorials. So, when investigating their behavior modulo a prime, it is effective to use these factorials' behavior. My first strategy for analyzing $\binom{2020}{1071} = \frac{2020!}{1071! \times 949!}$ modulo 13 was to see if 13 actually divided this number.

In order to generalize the problem, let's take a binomial coefficient. It is evident that all binomial coefficients can be written in the form of $\binom{n+m}{n}$ where n and m are non-negative integers (and both not being equal to 0 at the same time). We investigate this modulo a prime, p.

$$\binom{n+m}{n} = \frac{(n+m)!}{n! \times m!}$$

In a fraction, if denominator is relatively prime with a prime number p and conversely p divides the numerator; the prime also divides the fraction itself. This would make the problem really simple; however, many binomial coefficients do not fit to this case. So, the number of the factor p in both the denominator and the numerator should be calculated independently and the fraction should be simplified accordingly.

For the sake of a cleaner notation, let's define $v_p(x)$ (where p is a prime and x is a positive integer) as the highest power of p which divides x. For example, $v_2(20) = v_2(2^2 \times 5) = 2$ and $v_5(250) = v_5(2 \times 5^3) = 3$. As mentioned earlier, the $v_p(denominator)$ and $v_p(nominator)$ should be observed to see if $p|\binom{n+m}{n}$. It is clear that there are A_1, A_2, A_3 integers such that $p \nmid A_1, A_2, A_3$, which satisfy these equations:

$$(n+m)! = p^{v_p((n+m)!)} \times A_1$$

$$n! = p^{v_p(n!)} \times A_2$$

$$m! = p^{v_p(m!)} \times A_3$$

Then we get:

$$\binom{n+m}{n} = \frac{(n+m)!}{n! \times m!} = \frac{p^{v_p((n+m)!)} \times A_1}{p^{v_p(n!)} \times A_2 \times p^{v_p(m!)} \times A_3} = p^{v_p((n+m)!)-v_p(n!)-v_p(m!)} \frac{A_1}{A_2 \times A_3}$$

$\frac{A_1}{A_2 \times A_3}$ must be an integer since $\binom{n+m}{n}$ is an integer.

Moreover since $\left(\frac{A_1}{A_2 \times A_3}, p\right) = 1$;

$$v_p\left(\binom{n+m}{n}\right) = v_p((n+m)!) - v_p(n!) - v_p(m!) \geq 1 \Leftrightarrow p \mid \binom{n+m}{n} \qquad (1)$$

This gives the mathematical relationship between the number of p factors in the binomial coefficient, and the number of p factors in each individual factorial. Now we aim to find the number of p factors in a factorial.

For some simplicity, I initiated my investigation using my original binomial coefficient $\binom{2020}{1071}$. Let's start with $2020! = 2020 \times 2019 \times ... \times 2 \times 1$. At this point we will observe each factor in this factorial (the numbers from 1 to 2020) to count $v_{13}(2020!)$. It is evident that the numbers $13, 26, 39 ..., 2015$ will provide a factor of 13 each; hence, there is at least $2015/13 = 155$ factors of 13 in the factorial. However, then we can realize that multiples of $13^2 = 169$ in this factorial, will include one more factor of 13 each. So, we have to count the numbers $169, 338, ... 1859$ again, which will lead to $1859 \,/\, 169 = 11$ additional factors. If we do the same logical process, we see that we should count multiples of 13^3 in this factorial; 2197 is the only number which satisfies these conditions. Since $13^4 > 2020$, we can conclude with that every factor of 13 has been counted:

$$\frac{2015}{13} + \frac{1859}{13^2} + \frac{2197}{13^3} = 155 + 11 + 1 = 167 = v_{13}(2020!)$$

Although this is a logical and valid process to find the intended value, we have to generalize these calculations to come up with a formula. We should find a way to count the multiples of $13, 13^2$ and 13^3. "Floor function" which is gives the outcome of the "greatest integer that is less than or equal at the input" seems to be helpful here. For example, we can use $\frac{2015}{13} = \left\lfloor \frac{2020}{13} \right\rfloor = 155$. Using this function, will help us more for in the process of generalizing these calculations for any $n!$ ($n \in \mathbb{Z}^+$).

At this point, it is obvious that we can state the intended value as an infinite sum of floor functions:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \qquad (2)$$

Let's try to write this formula in a more simplified way, for this aim we can use number base rules that I mentioned in the foreknowledge part. Because of Rule 1, we can write n in base p, let that be $(a_0 a_1 a_2 \ldots a_k)_p$.

$$n = a_0 p^k + a_1 p^{k-1} + \cdots + a_{k-1} p + a_k \qquad (3)$$

(a_i are nonnegative integers for $\forall i \in \{0,1,2, \ldots, k\}$ and $0 \leq a_i \leq p-1$)

Let's substitute (3) in (2):

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor$$

$$= (a_0 p^{k-1} + a_1 p^{k-2} + \cdots + a_{k-1}) + (a_0 p^{k-2} + a_1 p^{k-3} + \cdots + a_{k-2}) + \cdots + (a_0)$$

$$= a_0(p^{k-1} + p^{k-2} + \cdots + 1) + a_1(p^{k-2} + p^{k-3} + \cdots + 1) + \cdots + a_{k-2}(p+1) + a_{k-1}$$

$$= a_0 \cdot \frac{p^k - 1}{p-1} + a_1 \cdot \frac{p^{k-1} - 1}{p-1} + \cdots + a_{k-1} \cdot \frac{p-1}{p-1}$$

$$= \frac{(a_0 p^k + a_1 p^{k-1} + \cdots a_k) - (a_0 + a_1 + \cdots + a_k)}{p-1}$$

$= \frac{n-(a_0+a_1+\cdots+a_k)}{p-1}$ (McCleary 65−67) (4)

This is known as **Legendre's Theorem**. Adrien-Marie Legendre (1752-1833) writes this in his book called *"Essai sur la theorie des nombres"* in 1808 (Miheţ).

Note that the k + 1 digit number $(a_0a_1a_2 \dots a_k)$ equals to n in base p. So, we proved that the highest power of a prime p which divides an integer n is related to the sum of the digits of n in base p.

For the sake of a clearer notation, let's denote the sum of the digits of an integer x as $S(x)$ function. Now the equation becomes:

$$v_p(n!) = \frac{n-(a_0+a_1+\cdots+a_k)}{p-1} = \frac{n-S((n)_p)}{p-1}$$

However, this only investigates the p-adic valuation of a factorial and yet my main aim was about the binomial coefficients. Equation (1) tells us the relationship between the p-adic valuation of the factorials and the binomial coefficients, so we will just plug this in equation (1).

Let us denote the integers $n, m, n+m$ in base p. Assume that n has $\alpha_1 + 1$ digits, m has $\alpha_2 + 1$ digits and $m+n$ has $\alpha_3 + 1$ digits in base p. In other words (where $0 \leq a_0, a_1, \dots a_{\alpha_1}, b_0, b_1, \dots b_{\alpha_2}, c_0, c_1 \dots c_{\alpha_3} \leq p-1$):

$$n = (a_0a_1 \dots a_{\alpha_1})_p$$

$$m = (b_0b_1 \dots b_{\alpha_2})_p$$

$$n+m = (c_0c_1 \dots c_{\alpha_3})_p$$

The first time I wrote this proof, I decided to take different variables as $\alpha_1, \alpha_2, \alpha_3$. After examining other proofs, I saw that taking $\alpha_1 = \alpha_2 = \alpha_3 = \alpha = \max\{\alpha_1, \alpha_2, \alpha_3\}$ is more

convenient for the next calculations. It is clear why we are able to do this. We can take the a_i, b_i or c_i values ($i \in \{1,2,\dots,\alpha\}$) 0 for sufficient amount. In other words, since $(a_0 a_1 \dots a_{\alpha_1})_p$, $(b_0 b_1 \dots b_{\alpha_2})_p$, $(c_0 c_1 \dots c_{\alpha_3})_p$ each are integers with (possibly) different number of digits, we can add 0 for as many times we want to the left hand side of the numbers, to make the number of digits (and hence $\alpha_1, \alpha_2, \alpha_3$) equal.

If we convert these numbers in base p to base 10, we obtain:

$$n = a_0 p^{\alpha} + a_1 p^{\alpha-1} + \cdots + a_{\alpha-1} p + a_{\alpha}$$

$$m = b_0 p^{\alpha} + b_1 p^{\alpha-1} + \cdots + b_{\alpha-1} p + b_{\alpha}$$

$$n + m = c_0 p^{\alpha} + c_1 p^{\alpha-1} + \cdots + c_{\alpha-1} p + c_{\alpha}$$

Using Legendre, we can say:

$$v_p(n!) = \frac{n - S((n)_p)}{p-1}$$

$$v_p(m!) = \frac{m - S((m)_p)}{p-1}$$

$$v_p((n+m)!) = \frac{(m+n) - S((n+m)_p)}{p-1}$$

Substituting these in the LHS of the equality (1), we obtain:

$$v_p\left(\binom{n+m}{n}\right) = v_p\big((n+m)!\big) - v_p(n!) - v_p(m!)$$

$$= \frac{(m+n) - S((n+m)_p)}{p-1} - \frac{n - S((n)_p)}{p-1} - \frac{m - S((m)_p)}{p-1}$$

$$= \frac{S\big((a_0 a_1 a_2 \dots a_{\alpha})_p\big) + S\big((b_0 b_1 b_2 \dots b_{\alpha})_p\big) - S((c_0 c_1 c_2 \dots c_{\alpha})_p)}{p-1} \quad (5)$$

The fact that the sums, $(a_0{+}a_1 + \cdots + a_\alpha), (b_0{+}b_1 + \cdots + a_\alpha), (c_0{+}c_1 + \cdots + c_\alpha)$, are the sums of digits of the integers $n, m, n+m$ in base p leads us to define this equation using base arithmetic.

It is clear:

$$(c_0c_1c_2 \dots c_\alpha)_p = n + m = (a_0a_1a_2 \dots a_\alpha)_p + (b_0b_1b_2 \dots b_\alpha)_p$$

This leads to a summation in base p. But how can we relate this to these numbers' sums of digits?

We start by realizing that if there is no "carries" in this sum in base p, $(a_0{+}a_1 + \cdots + a_\alpha) + (b_0{+}b_1 + \cdots + a_\alpha) - (c_0{+}c_1 + \cdots + c_\alpha) = 0$. In this case from (5), $v_p\left(\binom{n+m}{n}\right)$ also equals to zero. This means that we could potentially simplify equation (5), by observing the "carries" in the sum $(a_0a_1a_2 \dots a_\alpha)_p + (b_0b_1b_2 \dots b_\alpha)_p$.

In order to find out about the nature of the carries and the sum of the digits, I decided to start with base 10, independent from my exploration, since it refers to the decimal system that we use every day. (Although acknowledging that 10 is not a prime and we wouldn't be able to plug it in equation (5).) For example, let's take the sum of $365 + 326 = 691$. In this case there is only one carry and $-(6 + 9 + 1) + (3 + 6 + 5) + (3 + 2 + 6) = 9$. Taking another example, in the sum $7456 + 1395 = 8851$ there are two carries and $-(8 + 8 + 5 + 1) + (7 + 4 + 5 + 6) + (1 + 3 + 9 + 5) = 18$. Carrying on like this, we can guess that $S((n)_{10}) + S((m)_{10}) - S((n+m)_{10}) = (10 - 1) \times (the\ number\ of\ carries\ in\ the\ sum\ of\ n + m)$. This gives a good understanding for the calculations we are to do, but it is not a proof and we need that which proves for all bases.

Let's organize (5) so that we can work with the digits of the n and m at the same place values:

$$v_p\left(\binom{n+m}{n}\right) = \frac{(a_0 + b_0) + (a_1 + b_1) + \cdots + (a_\alpha + b_\alpha) - (c_0 + c_1 + \cdots + c_\alpha)}{p-1}$$

Let us imagine that we sum the numbers $(a_0 a_1 a_2 \dots a_\alpha)_p$ and $(b_0 b_1 b_2 \dots b_\alpha)_p$ like this:

$$\begin{array}{r} a_0 a_1 a_2 \dots a_\alpha \\ +\ b_0 b_1 b_2 \dots b_\alpha \\ \hline c_0 c_1 c_2 \dots c_\alpha \end{array}$$

Let's define λ_i $(i \in \{0, 1, 2, \dots \alpha\})$

$$\lambda_i = \begin{cases} 0, if\ there\ is\ no\ carries\ while\ adding\ up\ numbers\ a_i\ and\ b_i\ in\ base\ p \\ 1, if\ there\ is\ a\ carry\ while\ adding\ up\ numbers\ a_i\ and\ b_i\ in\ base\ p \end{cases}$$

It is obvious that for j $\in \{1, 2, \dots \alpha - 1\}$

$a_j + b_j + \lambda_{j+1} = p\lambda_j + c_j$ because λ_{i+1} refers to the carry that is carried to this place from the previous column of the sum and λ_i refers to the carry that is going to be carried to the next column.

We also know that $a_\alpha + b_\alpha = p\lambda_\alpha + c_\alpha$ and $a_0 + b_0 + \lambda_1 = c_0$.

So, we get the following equations:

$$a_\alpha + b_\alpha = p\lambda_\alpha + c_\alpha$$

$$a_{\alpha-1} + b_{\alpha-1} = p\lambda_{\alpha-1} - \lambda_\alpha + c_{\alpha-1}$$

$$a_{\alpha-2} + b_{\alpha-2} = p\lambda_{\alpha-2} - \lambda_{\alpha-1} + c_{\alpha-2}$$

$$\vdots$$

$$a_1 + b_1 = p\lambda_1 - \lambda_2 + c_1$$

$$a_0 + b_0 = c_0 - \lambda_1$$

If we sum them up:

$$(a_0 + b_0) + (a_1 + b_1) + \cdots (a_\alpha + b_\alpha) = (p-1)(\lambda_1 + \lambda_2 + \cdots \lambda_\alpha) + (c_0 + c_1 + \cdots + c_\alpha)$$

$$\sum_{i=0}^{\alpha}(a_i + b_i - c_i) = (p-1)\sum_{j=1}^{\alpha}\lambda_j$$

We obtained the intended equation, a relationship between the value of $S\big((a_0a_1a_2 \dots a_\alpha)_p\big) + S\big((b_0b_1b_2 \dots b_\alpha)_p\big) - S((c_0c_1c_2 \dots c_\alpha)_p)$ and the "carries".

Plugging in this in (5) we get

$$v_p\left(\binom{n+m}{n}\right) = \frac{S\big((a_0a_1a_2 \dots a_\alpha)_p\big) + S\big((b_0b_1b_2 \dots b_\alpha)_p\big) - S((c_0c_1c_2 \dots c_\alpha)_p)}{p-1}$$

$$= \frac{(p-1)\sum_{j=1}^{\alpha}\lambda_j}{(p-1)} = \sum_{j=1}^{\alpha}\lambda_j$$

This means, that the number of p factors in $\binom{n+m}{n}$ is equal to the number of carries in the addition of n and m in base p.

This is also known as the **Kummer's theorem**. Ernst Kummer (1810-1893) first proved this on a paper in 1852 (McCleary 66–67; Miheț).

Now we have the ultimate theorem for finding $v_p\left(\binom{n+m}{n}\right)$. We can try my stimulus binomial coefficient $\binom{2020}{1071}$ to see if 13 divides it. $1071 = (645)_{13}$ and $2020 - 1071 = 949 = (580)_{13}$. If we sum them up in base 13, $(645)_{13} + (580)_{13} = (ABC)_{13}$ where $A = 10$ $B = 12$ and $C = 5$, we get no carries. So, we can say $v_p\left(\binom{2020}{1071}\right) = 0$.

With these calculations, we found out that the binomial coefficient is not congruent to 0 modulus p, if it were, we would be done here and I would reach my aim. However, I saw that other operations are needed to answer my stimulus question, *"What is* $\binom{2020}{1071}$ *congruent to in modulo 13?"*. Trying to find ways to find the remainder of this binomial coefficient, I came across Lucas' theorem.

Lucas' theorem (1878): If $k = k_0p^t + k_1p^{t-1} + \cdots + k_tp^0$ and $l = l_0p^t + l_1p^{t-1} + \cdots + l_tp^0$ are the p-ary notation of integers k and l such that $0 \leq k_i, l_i \leq p-1$ for $i \in \{0,1,2,\ldots t\}$

$$\binom{k}{l} \equiv \prod_{i=0}^{t} \binom{k_i}{l_i} \ (mod\ p)$$

(Meštrović)

Proof: We will get to the binomial coefficients from the binomial expansion, and later on compare the coefficients of the polynomial that we find.

$$\sum_{l=0}^{k} \binom{k}{l} \times x^l = (1+x)^k = (x+1)^{k_0p^t + k_1p^{t-1} + \cdots + k_tp^0} = \prod_{i=0}^{t} (x+1)^{k_ip^{t-i}}$$

$$= \prod_{i=0}^{t} (x+1)^{k_ip^{t-i}} = \prod_{i=0}^{t} ((x+1)^{p^{t-i}})^{k_i}$$

Lemma: $(x+1)^{p^i} \equiv x^{p^i} + 1\ (mod\ p)$ where p is a prime and i is a non-negative integer.

Proof by induction:

I) For $\forall j \in \{1,2,\ldots p-1\}$ $p \mid \binom{p}{j}$. This is obvious because $\binom{p}{j} = \frac{p!}{(p-j)!j!}$ and p divides the numerator and not the denominator. Hence, $(x+1)^p = \binom{p}{0}x^0 + \binom{p}{1}x^1 + \cdots + \binom{p}{p}x^p \equiv \binom{p}{0}x^0 + \binom{p}{p}x^p = x^p + 1\ (mod\ p)$.

II) Let's assume the lemma holds for $i = k$ where k is a non-negative integer. $(x+1)^{p^k} \equiv x^{p^k} + 1\ (mod\ p)$ satisfies.

III) $(x+1)^{p^{k+1}} \equiv ((x+1)^{p^k})^p \equiv \left(x^{p^k} + 1\right)^p \equiv \cdots (from\ I) \ldots \equiv \left(x^{p^k}\right)^p + 1 \equiv x^{p^{k+1}} + 1$. Induction is complete as the lemma also holds for $i = k+1$.

Using this lemma, we continue our calculations using binomial expansion once again:

$$\prod_{i=0}^{t}((x+1)^{p^{t-i}})^{k_i} \equiv \prod_{i=0}^{t}\left(x^{p^{t-i}}+1\right)^{k_i} = \prod_{i=0}^{t}\sum_{j=0}^{k_i}\binom{k_i}{j}x^{p^{t-i}j}$$

$$= \prod_{i=0}^{t}\binom{k_i}{0}x^{p^{t-i}\times 0} + \binom{k_i}{1}x^{p^{t-i}\times 1} + \cdots + \binom{k_i}{k_i}x^{p^{t-i}k_i}$$

Now we want to change the upper bound of the summation (which is now k_i) to $p-1$, we will see its benefits later on (*). We can easily do this. Since $k_i \leq p-1$, there will be new terms that will be added to the summation if we change the upper bound, and those terms are $\binom{k_i}{k_i+1}x^{p^{t-i}(k_i+1)}, \binom{k_i}{k_i+2}x^{p^{t-i}(k_i+2)}, \ldots, \binom{k_i}{p-1}x^{p^{t-i}(p-1)}$. But we can see that these are equal to 0. The reason for this is that for values $k_i < j\ (\leq p-1)$, $\binom{k_i}{j} = 0$. Hence, the newly added terms $\binom{k_i}{j}x^{p^{t-i}j} = 0$ so they won't affect the sum. Now let's eliminate the product symbol:

$$\prod_{i=0}^{t}\left(\sum_{j_i=0}^{p-1}\binom{k_i}{j}x^{p^{t-i}j}\right) = \sum_{j_0=0}^{p-1}\binom{k_0}{j_0}x^{p^t j_0} \times \sum_{j_1=0}^{p-1}\binom{k_1}{j_1}x^{p^{t-1}j_1} \times \ldots \times \sum_{j_t=0}^{p-1}\binom{k_t}{j_t}x^{p^0 j_t}$$

All the j are named as different indexes in order not to lose some permutations and for a clearer notation. Let's convert this product of sums to sums of products. Define a set $P = \{1,2,\ldots p-1\}$ and we can see that:

$$= \sum_{j_0,j_1,\ldots,j_t \in P}\binom{k_0}{j_0}x^{p^t j_0} \times \binom{k_1}{j_1}x^{p^{t-1}j_1} \ldots \times \binom{k_t}{j_t}x^{p^0 j_t}$$

Although this is clear, I would like to elaborate further why this is true.

If the previous product of sums is expanded and observed, the proof is obvious. However, this expansion would take a lot of space on the paper and it might be complicated to work with so many variables. So, in order to see this conversion in a better way, I will change the variable and show that this equation is true in a simpler way.

Let's define a function $K(a,b) = \binom{k_a}{b} x^{p^{t-a}b}$. So:

$$\sum_{j_0=0}^{p-1} \binom{k_0}{j_0} x^{p^t j_0} \times \sum_{j_1=0}^{p-1} \binom{k_1}{j_1} x^{p^{t-1} j_1} \times \dots \times \sum_{j_t=0}^{p-1} \binom{k_t}{j_t} x^{p^0 j_t}$$

$$= \big(K(0,0) + K(0,1) + \cdots + K(0,p-1)\big) \times \big(K(1,0) + K(1,1) + \cdots + K(1,p-1)\big) \times \dots$$

$$\times \big(K(1,0) + K(1,1) + \cdots + K(1,p-1)\big)$$

Doing this product, we obtain:

$$= \sum_{j_0, j_1, \dots, j_t \in P} K(0,j_1) K(1,j_2) \dots K(t,j_t)$$

$$= \sum_{j_0, j_1, \dots, j_t \in P} \binom{k_0}{j_0} x^{p^t j_0} \times \binom{k_1}{j_1} x^{p^{t-1} j_1} \dots \times \binom{k_t}{j_t} x^{p^0 j_t}$$

Moving on with the rest of the proof, let us condense this to:

$$= \sum_{j_0, j_1, \dots, j_t \in P} \left(\prod_{i=0}^{t} \binom{k_i}{j_i} x^{p^{t-i} j_i} \right) = \sum_{j_0, j_1, \dots, j_t \in P} \left(\prod_{i=0}^{t} \binom{k_i}{j_i} \prod_{i=0}^{t} x^{p^{t-i} j_i} \right)$$

Since $\prod_{i=0}^{x} x^{p^{t-i} j_i} = x^{x^t j_0 + x^{t-1} j_1 + \cdots + x^0 j_t}$, the power of x refers to an integer (let us denote that with A) for each set $(j_0, j_1, \dots, j_t)$, which can be written in base p as $(j_0 j_1 j_2 \dots j_t)_p$. So now we have:

$$\sum_{j_0, j_1, \dots, j_t \in P} \left(\prod_{i=0}^{t} \binom{k_i}{j_i} x^A \right)$$

where $A = (j_0 j_1 j_2 \dots j_t)_p$

*Let us not forget that this is equal to our initial summation which is $\sum_{l=0}^{k} \binom{k}{l} \times x^l$. So, our motivation here while approaching the last summation that we found, is to bound the summation (and hence the value of A) between 0 and k (Recall that our initial aim was to compare the coefficients of the polynomial that we find).

It is clear that $A \geq 0$. Let us investigate what happens if $A > k$. Since both A and k have $t + 1$ digits in base p, and j_i refer to the digits of A and k_i refer to the digits of k ($i \in \{0,1,2, \dots t\}$) , we can say $j_i > k_i$ at least for one value of i. This makes $\binom{k_i}{j_i} = 0$ and the product inside 0 as well. So, these sets of $(j_0, j_1, \dots, j_t)$ (and hence these values of A) can be ignored.

As a result, we can only consider the values $0 \leq A \leq k$ and naturally the sets of $(j_0, j_1, \dots, j_t)$ correspond to these A values. And this new summation is congruent to our initial summation:

$$\sum_{l=0}^{k} \binom{k}{l} \times x^l \equiv \sum_{A=0}^{k} \left(\prod_{i=0}^{t} \binom{k_i}{j_i} x^A \right)$$

Since both sides are polynomials, we can use the congruence of the coefficients, taking $l = A$:

$$\binom{k}{l} \equiv \prod_{i=0}^{t} \binom{k_i}{j_i} = \prod_{i=0}^{t} \binom{k_i}{l_i} \ (mod\ p)$$

("Lucas Theorem - Proof and Applications")

Now that we have proven the theorem we needed, we can investigate the binomial coefficient $\binom{2020}{1071}$. We have already calculated that $1071 = (645)_{13}$. It is also clear that $2020 = (XYZ)_{13}$ where X= $11, Y = 12, Z = 5$. From Lucas' theorem:

$$\binom{2020}{1071} \equiv \binom{11}{6}\binom{12}{4}\binom{5}{5} \equiv \frac{11 \times 10 \times 9 \ldots \times 6}{6 \times 5 \times \ldots \times 1} \times \frac{12 \times 11 \times 10 \times 9}{4 \times 3 \times 2 \times 1} \times 1 \equiv 462 \times 495$$

$$\equiv 7 \times 1 \equiv 7 \ (mod\ 13)$$

The goal is reached.

Applications

These theorems that were included in this paper, Legendre's, Lucas' and Kummer's theorems, are used by many other mathematicians in their pure mathematics theoretical studies. These theorems are found to be the basis of many corollaries and other theorems. The analysis of binomial coefficients in modular arithmetic also lead mathematicians to observe Pascal Triangle from different perspectives (Meštrović 36).

As a real-life connection, we can say that number theory in general is commonly used in cryptology. Modular arithmetic, number bases and prime numbers are branches of number theory, that are commonly used in privacy of communication and data in the modern world (*Crypto-IT*).

Conclusion

In this paper, I tried to find ways to analyze a binomial coefficient and its connection with a prime number; starting off with my stimulus question. I followed a sequence of logical steps in order to reach my aim. At first, I decided to see how I could understand if a prime divides a binomial coefficient and furthermore found the greatest power of a prime that divides a binomial coefficient through Lucas' and Legendre's theorems. As these did not completely answer my stimulus question, I proceeded to prove Lucas' theorem that gave me the answer. As seen, I tried different methods to reach my aim and found other solutions to the methods which failed to fulfill my aim. This exploration gave me the chance to dig deeper into a topic that I was intrigued by and also expand my knowledge outside of the HL curriculum.

Not only I solved the question but also, I generalized my steps for every binomial coefficient and every prime number. This required rigorous and precise mathematical operations which required me to be careful of any errors that could have been made through the process. I believe this prepared me to write more complicated and academic proofs as a further mathematician in the future.

Bibliography

Crypto-IT. http://www.crypto-it.net/eng/theory/modular-arithmetic.html. Accessed 6 July 2022.

"Lucas Theorem - Proof and Applications." *Forthright48*, 16 Nov. 2018, https://forthright48.com/lucas-theorem-proof-and-applications/.

McCleary, John. "Exercises in (Mathematical) Style: Stories of Binomial Coefficients by John McCleary." *The Mathematical Intelligencer*, vol. 42, no. 4, Dec. 2020, pp. 82–83. *Springer Link*, https://doi.org/10.1007/s00283-020-10002-4.

Meštrović, Romeo. *Lucas' Theorem: Its Generalizations, Extensions and Applications (1878--2014), Cornell University Library, 2014, 51 Pages, Available at ArXiv:1409.3820 [Math.NT], 2014.* Sept. 2014.

Miheţ, Dorel. "Legendre's and Kummer's Theorems Again." *Resonance*, vol. 15, no. 12, Dec. 2010, pp. 1111–21. *Springer Link*, https://doi.org/10.1007/s12045-010-0123-4.

Modular Arithmetic | Britannica. https://www.britannica.com/science/modular-arithmetic. Accessed 14 May 2022.

Özdemir, Mustafa. *Matematik Olimpiyatlarına Hazirlik 1*. 6th ed., Altın Nokta, 2018.

---. *Matematik Olimpiyatlarına Hazırlık 3*. 5th ed., Altın Nokta, 2017.

Virnuls, Andrew. "Number Bases." *Computing and ICT in a Nutshell*, https://www.advanced-ict.info/mathematics/bases.html. Accessed 6 July 2022.