Lucas's Theorem

Theorem. *For arbitrary prime p and natural number $n \geq i$, if $n_{(10)} = \overline{n_m n_{m-1} \dots n_1 n_0}_{(p)}$ and $i_{(10)} = \overline{i_m i_{m-1} \dots i_1 i_0}_{(p)}$ with possible leading zeros, then*

$$ {}_nC_i \equiv \prod_{j=0}^{m} {}_{n_j}C_{i_j} \pmod{p} $$

Proof.

Lemma 0.1. $(a+b)^p \equiv a^p + b^p \pmod{p}$ $\forall$ *prime p and $a, b \in \mathbb{Z}$.*

Proof. In modular arithmetic, the Freshman's Dream, which states that $(a+b)^2 = a^2 + b^2$ is not necessarily false. To generalize, the statement $(a+b)^n = a^n + b^n$ may be true in clock arithmetic.

Using binomial expansion, it is evident that

$$ (a+b)^p = {}_pC_0 a^p b^0 + {}_pC_1 a^{p-1} b^1 + \dots + {}_pC_{p-1} a^1 b^{p-1} + {}_pC_p a^0 b^p $$

Lemma 0.1. $p | {}_pC_n$ $\forall$ $0 < n < p$.

Proof. Let a natural number $N = {}_pC_n$. N is also equal to $\frac{p!}{(p-n)!n!}$. However, because $(p-n)!$ and $n!$ are both less than prime p, the factor p remains in the denominator when simplified. Thereby, p is a factor in N, or ${}_pC_n$. □

$$ \begin{aligned} \therefore (a+b)^p &\equiv {}_pC_0 a^p b^0 + {}_pC_1 a^{p-1} b^1 + \dots + {}_pC_{p-1} a^1 b^{p-1} + {}_pC_p a^0 b^p \pmod{p} \\ &\equiv {}_pC_0 a^p b^0 + {}_pC_p a^0 b^p \pmod{p} \\ &\equiv a^p + b^p \pmod{p} \end{aligned} $$

□

Corollary 0.1.1. $(1+x)^{p^r} \equiv 1 + x^{p^r} \pmod{p}$ $\forall$ *prime p and $x, r \in \mathbb{N}$.*

Proof. Let $a = 1$ and $b = x$.

$$ \begin{aligned} (1+x)^p &\equiv 1^p + x^p \pmod{p} \\ &\equiv 1 + x^p \pmod{p} \end{aligned} $$

By exploiting the properties of expansions of the terms, the following conclusion may be driven. Except the first and the last terms, all the terms in between will include ${}_pC_n$ for $0 < n < p$.

$$ \begin{aligned} (1+x)^{p^{k+1}} &\equiv ((1+x)^p)^{p^k} \pmod{p} \\ &\equiv 1 + x^{p^{k+1}} \pmod{p} \end{aligned} $$

Let $r = k + 1$ for clarity.

$$ \therefore (1+x)^{p^r} \equiv 1 + x^{p^r} \pmod{p} $$

□

Let $n = n_m p^m + n'$ and $i = i_m p^m + i'$ by manipulating the base system for n and i.

$$ \begin{aligned} (1+x)^{p^m} &\equiv 1 + x^{p^m} \pmod{p} \text{ (By Corollary 0.0.1.1)} \\ \left((1+x)^{p^m}\right)^{n_m} &\equiv (1 + x^{p^m})^{n_m} \pmod{p} \text{ (By property of Modular Arithmetic)} \\ (1+x)^{n'} \cdot \left((1+x)^{p^m}\right)^{n_m} &\equiv (1+x)^{n'} \cdot (1 + x^{p^m})^{n_m} \pmod{p} \\ (1+x)^n &\equiv (1+x)^{n'} \cdot (1 + x^{p^m})^{n_m} \pmod{p} \end{aligned} $$

Using binomial expansion, it is evident that the following equations are true.

$$\begin{aligned}(1+x^{p^m})^{n_m} &= \sum_{j=0}^{n_m} \binom{n_m}{j} 1^{n_m-j}(x^{p^m})^j \\ &= \sum_{j=0}^{n_m} \binom{n_m}{j} x^{jp^m} \\ (1+x)^{n'} &= \sum_{k=0}^{n'} \binom{n'}{k} 1^{n'-k} x^k \\ &= \sum_{k=0}^{n'} \binom{n'}{k} x^k\end{aligned}$$

Using property of Modular Arithmetic,

$$(1+x)^n \equiv \left(\sum_{k=0}^{n'} \binom{n'}{k} x^k\right) \cdot \left(\sum_{j=0}^{n_m} \binom{n_m}{j} x^{jp^m}\right) \pmod{p}$$

Each term is in the form of $\binom{n'}{k}x^k\binom{n_m}{j}x^{jp^m}$, or $\binom{n'}{k}\binom{n_m}{j}x^{k+jp^m}$.
The following expression provides the sum of the coefficient of x^i.

$$\sum_{k+jp^m=i'+i_mp^m} \binom{n'}{k}\binom{n_m}{j}$$

The reason is because $\binom{n'}{k}\binom{n_m}{j}x^{k+jp^m}$ provides every possible terms with x^{k+jp^m}. Thus, replacing $x^{k+jp^m} = x^i$ leads to selected term(s) with x^i. The term(s) simply does not exist if $x^{k+jp^m} = x^i$ cannot be true. Recall $i = i' + i_mp^m$. Thereby, the expression above provides the coefficient of x^i.

The pair(s) of (k, j) that satisfy the equation $k + jp^m = i' + i_mp^m$ must be found.

$$k - i' + (j - i_m)p^m = 0$$

Due to property of combinations, it is evident that $k \leq n'$ and $j \leq n_m$. For $k \leq n'$, recall that $n' = n_0p^0 + n_1p^1 + \cdots + n_{m-1}p^{m-1}$. The maximum of n' is when $n_0, n_1, \ldots n_{m-1}$ are maximum, or $p - 1$. In another words,

$$\begin{aligned}\max(n') &= (p-1)p^0 + (p-1)p^1 + \cdots + (p-1)p_{m-1} \\ &= (p-1)(p^0 + p^1 + \ldots p^{m-1}) \\ &= (p-1)[p^0 \cdot \frac{1-p^m}{1-p}] \\ &= p^m - 1.\end{aligned}$$

Because $\max(n') < p^m$, $n' < p^m$.

For $j \leq n_m$, Using the properties of base number representation, it is evident that $j < p$ because $n_m < p$. □

Example

Problem Math Virus School has a total of 4 classes, and each class contains a certain number of viruses: 1246, 896, 4050, and 7547 viruses, respectively. Every virus from all the classes leaves its class and selects one hat from 58 distinct hats, each differing in shape and color. After making a selection, the viruses return

to their respective classes. Let the remainder when the total number of possible selections is divided by 7 be r_7, and the remainder when it is divided by 3 be r_3. Find the value $r_7 r_3$.

Key Word Lucas's Theorem, Stars and Bars, Modular Arithmetic Properties

Let stars represent the number of viruses in each class for each case. If 57 bars are used, the number of cases in which each virus choose one hat in each class could be obtained.

$\boxed{1246}$	$\boxed{896}$	$\boxed{4050}$	$\boxed{7547}$
1246 Stars, 57 Bars	896 Stars, 57 Bars	4050 Stars, 57 Bars	7547 Stars, 57 Bars
$\frac{(1246+57)!}{1246!57!}$	$\frac{(896+57)!}{896!57!}$	$\frac{(4050+57)!}{4050!57!}$	$\frac{(7547+57)!}{7547!57!}$
$= {}_{1303}C_{57}$	$= {}_{953}C_{57}$	$= {}_{4107}C_{57}$	$= {}_{7604}C_{57}$

The total probability is ${}_{1303}C_{57} \cdot {}_{953}C_{57} \cdot {}_{4107}C_{57} \cdot {}_{7604}C_{57}$

Finding remainder when a number involving multiplication of combinations is divided by an integer reminds Lucas's Theorem.

Applying Lucas's Theorem for r_7

$$\begin{aligned} 57_{(10)} &= 111_{(7)} \\ 1303_{(10)} &= 3542_{(7)} \\ 953_{(10)} &= 2531_{(7)} \\ 4107_{(10)} &= 14655_{(7)} \\ 7604_{(10)} &= 31111_{(7)} \end{aligned}$$

Lucas's Theorem is applied to find r_7.

$$\begin{aligned} {}_{1303}C_{57} &\equiv {}_3C_0 \cdot {}_5C_1 \cdot {}_4C_1 \cdot {}_2C_1 \pmod 7 \\ &\equiv 1 \cdot 5 \cdot 4 \cdot 2 \pmod 7 \\ &\equiv 40 \pmod 7 \\ &\equiv 5 \pmod 7 \end{aligned}$$

$$\begin{aligned} {}_{953}C_{57} &\equiv {}_2C_0 \cdot {}_5C_1 \cdot {}_3C_1 \cdot {}_1C_1 \pmod 7 \\ &\equiv 1 \cdot 5 \cdot 3 \cdot 1 \pmod 7 \\ &\equiv 15 \pmod 7 \\ &\equiv 1 \pmod 7 \end{aligned}$$

$$\begin{aligned} {}_{4107}C_{57} &\equiv {}_1C_0 \cdot {}_4C_0 \cdot {}_6C_1 \cdot {}_5C_1 \cdot {}_5C_1 \pmod 7 \\ &\equiv 1 \cdot 1 \cdot 6 \cdot 5 \cdot 5 \pmod 7 \\ &\equiv 150 \pmod 7 \\ &\equiv 3 \pmod 7 \end{aligned}$$

$$\begin{aligned} {}_{7604}C_{57} &\equiv {}_3C_0 \cdot {}_1C_0 \cdot {}_1C_1 \cdot {}_1C_1 \cdot {}_1C_1 \pmod 7 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \pmod 7 \\ &\equiv 1 \pmod 7 \end{aligned}$$

$$\begin{aligned} {}_{1303}C_{57} \cdot {}_{953}C_{57} \cdot {}_{4107}C_{57} \cdot {}_{7604}C_{57} &\equiv 5 \cdot 1 \cdot 3 \cdot 1 \pmod 7 \\ &\equiv 15 \pmod 7 \\ &\equiv 1 \pmod 7 \end{aligned}$$

$\therefore r_7 = 1$

Applying Lucas's Theorem for r_3

$$\begin{aligned} 57_{(10)} &= 2010_{(3)} \\ 1303_{(10)} &= 1201021_{(3)} \\ 953_{(10)} &= 1022022_{(3)} \\ 4107_{(10)} &= 111212100_{(3)} \\ 7604_{(10)} &= 101102122_{(3)} \end{aligned}$$

$$\begin{aligned} {}_{1303}C_{57} &\equiv {}_1C_0 \cdot {}_2C_0 \cdot {}_0C_0 \cdot {}_1C_2 \cdot {}_0C_0 \cdot {}_2C_1 \cdot {}_1C_0 \pmod 3 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 0 \cdot 1 \cdot 2 \cdot 1 \pmod 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

$r_3 = 0$ $(\because {}_{1303}C_{57} \equiv 0 \pmod 3)$

$r_7 \cdot r_3 = 1 \cdot 0 = 0$

Conclusion $r_7 \cdot r_3 = \boxed{0}$.