Notes on Number Theory and Discrete Mathematics
Vol. 18, 2012, No. 4, 1–6

A new proof of Lucas' Theorem

Alexandre Laugier[1] and Manjil P. Saikia[2]

[1] Lycée professionnel hotelier La Closerie
10 rue Pierre Loti - BP 4, 22410 Saint-Quay-Portrieux, France
e-mail: `laugier.alexandre@orange.fr`

[2] Department of Mathematical Sciences, Tezpur University
Napaam, Sonitpur, Assam, Pin-784028, India
e-mail: `manjil@gonitsora.com`

Abstract: We give a new proof of Lucas' Theorem in elementary number theory.
Keywords: Lucas' Theorem.
AMS Classification: 11A07, 11A41, 11A51, 11B50, 11B65, 11B75.

1 Introduction

One of the most useful results in elementary number theory is the following result of E. Lucas.

Theorem 1.1 ([1], E. Lucas (1878))**.** *Let p be a prime and m and n be two integers considered in the following way,*

$$m = a_k p^k + a_{k-1} p^{k-1} + \ldots + a_1 p + a_0,$$
$$n = b_l p^l + b_{l-1} p^{l-1} + \ldots + b_1 p + b_0,$$

where all a_i and b_j are non-negative integers less than p. Then,

$$\binom{m}{n} = \binom{a_k p^k + a_{k-1} p^{k-1} + \ldots + a_1 p + a_0}{b_l p^l + b_{l-1} p^{l-1} + \ldots + b_1 p + b_0} \equiv \prod_{i=0}^{\max(k,l)} \binom{a_i}{b_i} \pmod{p}.$$

Notice that the theorem is true if $a_i \geq b_i$ for $i = 0, 1, 2, \ldots, \max(k, l)$

There has been many different proofs of this result in the years that followed its first publication. We present here an alternate approach using elementary number theoretic techniques.

2 Proof of Theorem 1.1

First of all, we state and prove a few lemmas

Lemma 2.1. *If*

$$a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \equiv b_0 + b_1X + b_2X^2 + \ldots + b_nX^n \pmod p$$

then

$$a_i \equiv b_i \pmod p \ \forall\, i \in [[0, n]].$$

Proof. Indeed, if $a_0+a_1X+a_2X^2+\cdots+a_nX^n \equiv b_0+b_1X+b_2X^2+\cdots+b_nX^n \pmod p$, then there exits a polynomial $k(X) = k_0 + k_1X + k_2X^2 + \cdots + k_nX^n$ at most of degree n such that $a_0+a_1X+a_2X^2+\cdots+a_nX^n = b_0+b_1X+b_2X^2+\cdots+b_nX^n+p(k_0+k_1X+k_2X^2+\cdots+k_nX^n)$. This gives $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = b_0 + pk_0 + (b_1 + pk_1)X + (b_2 + pk_2)X^2 + \cdots + (b_n + pk_n)X^n$. Hence we get $a_0 = b_0 + pk_0$, $a_1 = b_1 + pk_1$, $a_2 = b_2 + pk_2$,..., $a_n = b_n + pk_n$. Or equivalently $a_0 \equiv b_0 \pmod p$, $a_1 = b_1 \pmod p$, $a_2 = b_2 \pmod p$,$\cdots$, $a_n = b_n \pmod p$.

The reciprocal implication is trivial. □

Lemma 2.2. *If the base* p *expansion of a positive integer* n *is* $n = a_0 + a_1p + a_2p^2 + \cdots + a_lp^l$ *then we have* $n! = qa_0!(a_1p)!(a_2p^2)!\cdots(a_lp^l)!$ *with* q *a natural number.*

Proof. Since the factorial of a natural number is a natural number, there exists a rational number q such that

$$q = \frac{n!}{a_0!(a_1p)!(a_2p^2)!\ldots(a_lp^l)!}.$$

Let S be the set $S = \{x_1, x_2, \ldots, x_l\}$. We consider lists of elements of S where x_0 is repeated a_0 times, x_1 is repeated a_1p times,. . ., x_l is repeated a_lp^l times such that, $0 \le a_i \le p-1$ with $i \in [[0, l]]$. In such a list, there are $l + 1$ unlike groups of identical elements. For instance the selection

$$\left(\underbrace{x_0, x_0, \ldots, x_0}_{a_0}, \underbrace{x_1, x_1, \ldots, x_1}_{a_1p}, \ldots\ldots, \underbrace{x_l, x_l, \ldots, x_l}_{a_lp^l}\right)$$

is such a list of n elements which contains $l + 1$ unlike groups of identical elements.

The number of these lists is given by

$$\frac{n!}{a_0!(a_1p)!(a_2p^2)!\ldots(a_lp^l)!}.$$

It proves that the rational number q is a natural number. And, since the factorial of a natural number is non-zero (even if this number is 0 because $0! = 1$), we deduce that q is a non-zero natural number. □

Theorem 2.3. *Let* $n = ap + b = a_0 + a_1p + a_2p^2 + \ldots + a_lp^l$ *such that* $0 \le b \le p - 1$ *and* $0 \le a_i \le p - 1$ *with* $i \in [[0, l]]$. *Then* $q \equiv 1 \pmod p$.

Before we prove Theorem 2.3 we shall state and prove the following non-trivial lemmas.

Lemma 2.4. *The integers q and p are relatively prime.*

Proof. If $0 < q < p$, since p is prime, q and p are relatively prime.

If $q \geq p$, let us assume that p and q are not relatively prime. It would imply that there exist an integer $x > 0$ and a non-zero natural number q' such that $q = q'p^x$ with $\gcd(q', p) = 1$. Since $n! = qa_0!(a_1p)!\ldots(a_{l-1}p^{l-1})!(a_lp^l)!$ we get $n! = q'p^xa_0!(a_1p)!\ldots(a_lp^l)!$. It follows that $n!$ would contain a factor $a_{l+x}p^{l+x}$ such that $q' = a_{l+x}q''$ with $a_{l+x} \in [[1, p-1]]$. But, $a_{l+x}p^{l+x} > n$.

Indeed we know that $1 + p + \ldots + p^l = \frac{p^{l+1}-1}{p-1}$. So $p^{l+1} = 1 + (p-1)(1 + p + \ldots + p^l)$. Then $p^{l+1} > (p-1) + (p-1)p + \ldots + (p-1)p^l$. Since $0 \leq a_i \leq p-1$ with $i \in [[0, l]]$, we have $0 \leq a_ip^i \leq (p-1)p^i$ with $i \in [[0, l]]$. Therefore, $p^{l+1} > a_0 + a_1p + \ldots + a_lp^l$ so $p^{l+1} > n \Rightarrow a_{l+x}p^{l+x} > n$.

Since $n!$ doesn't include terms like $a_{l+x}p^{l+x} > n$ with $a_{l+x} \in [[1, p-1]]$, we obtain a contradiction. It means that the assumption $q = q'p^x$ with $x \in \mathbb{N}^\star$ and $gcd(q', p) = 1$ is not correct. So, q is not divisible by a power of p. It results that q and p are relatively prime. □

We know that $n! = (ap + b)! = qa_0!(a_1p)!\ldots(a_lp^l)!$ with $a = \lfloor \frac{n}{p} \rfloor$, $0 \leq a_i \leq p-1$ with $i = 0, 1, 2, \ldots, p-1$ and $b = a_0$. Let $q_{a,l,1,i}$ with $0 \leq i \leq a_1 \leq a$ be the natural number

$$q_{a,l,1,i} = \frac{(ap + b - ip)!}{a_0!((a_1 - i)p)!(a_2p^2)!\ldots(a_lp^l)!}.$$

In particular, we have $q = q_{a,l,1,0}$.

Lemma 2.5. $q_{a,l,1,i+1} \equiv q_{a,l,1,i} \pmod{p}$.

Proof. We have $(0 \leq i < a_1)$

$$\binom{ap + b - ip}{p} = \frac{q_{a,l,1,i}}{q_{a,l,1,i+1}} \binom{(a_1 - i)p}{p}$$

Or equivalently

$$q_{a,l,1,i+1} \binom{ap + b - ip}{p} = q_{a,l,1,i} \binom{(a_1 - i)p}{p}.$$

Now

$$\binom{ap + b - ip}{p} = \binom{(a - i)p + b}{p} \equiv a - i \equiv a_1 - i \pmod{p},$$

and

$$\binom{(a_1 - i)p}{p} \equiv a_1 - i \pmod{p}.$$

Therefore $q_{a,l,1,i+1}(a_1 - i) \equiv q_{a,l,1,i}(a_1 - i) \pmod{p}$. Since $a_1 - i$ with $i = 0, 1, 2, \ldots, a_1 - 1$ and p are relatively prime, so $q_{a,l,1,i+1} \equiv q_{a,l,1,i} \pmod{p}$. □

Notice that $q_{a,l,1,a_1}$ corresponds to the case where $a_1 = 0$, $(a_0 + a_2p^2 + \ldots + a_lp^l)! = q_{a,l,1,a_1}a_0!(a_2p^2)!\ldots(a_lp^l)!$.

Lemma 2.6. *For $n = ap + b = a_{(k)}p^k + b_{(k)}$ with $0 \leq b_{(k)} \leq p^k - 1$ and defining ($1 \leq k \leq l$ and $0 \leq i \leq a_k$)*

$$q_{a,l,k,i} = \frac{(a_{(k)}p^k + b_{(k)} - ip^k)!}{a_0!(a_1p)!\ldots((a_k - i)p^k)!\ldots(a_lp^l)!}$$

with $a_k \geq 1$, (where it is understood that when a and l appears together as the two first labels of one $q_{....}$, it implies that a is given by $a = a_{(1)} = (a_1 a_2 \dots a_l)_p = a_1 + a_2 p + \dots + a_l p^{l-1}$) we have ($0 \leq i < a_k$)

$$\binom{a_{(k)}p^k + b_{(k)} - ip^k}{p^k} = \frac{q_{a,l,k,i}}{q_{a,l,k,i+1}} \binom{(a_k - i)p^k}{p^k}$$

Additionally, $q_{a,l,k,i} \equiv q_{a,l,k,i+1} \pmod{p}$.

In particular for $k = 0$, we have ($0 \leq i < a_0$),

$$ap + b = \frac{q_{a,l,0,i}}{q_{a,l,0,i+1}}(a_0 - i)$$

with $a_0 \geq 1$.

We can prove this lemma by the following a similar reasoning as earlier and hence we omit it here.

Notice that $q = q_{a,l,k,0}$. And q_{a,l,k,a_k} corresponds to the case where $a_k = 0$. Also

$$q_{a-i,l,k,0} = q_{a,l,1,i} \equiv q_{a,l,1,i+1} \pmod{p},$$

with $0 \leq i < a_1$ and $a_1 \geq 1$. So, since $q_{a,l,k,j} \equiv q_{a,l,k,j+1} \pmod{p}$ with $0 \leq j < a_k$, we have $q_{a-i,l,k,j} \equiv q_{a-i,l,k,0} \equiv q_{a,l,1,i} \equiv q_{a,l,1,0} \pmod{p}$ and $q_{a-i,l,k,0} = q_{a-i,l,l,0} \equiv q_{a-i,l,l,j} \equiv q_{a-i,l,l,a_l} \equiv q_{a-i,l-1,k,0} \pmod{p}$.

So $q_{a-i,l,k,0} \equiv q_{a-i,l-1,k,0} \equiv \dots \equiv q_{a-i,l,k,0} \equiv q_{a-i,1,1,0} \equiv q_{a,1,1,i} \equiv q_{a,1,1,0} \pmod{p}$. Or $q_{a-i,l,k,0} = q_{a,l,1,i} \equiv q_{a,l,1,0} \equiv q_{a,l,k,0} \pmod{p}$.

Finally we have $q = q_{a,l,k,0} \equiv q_{a,1,1,0} \pmod{p}$.

Lemma 2.7. *We have also the congruence $(a_i p^i)! \equiv a_i! p^{a_i(1+p+\dots+p^{i-1})} \pmod{p}$.*

Proof. We proceed by induction on i.

Indeed, we have $(a_1 p)! \equiv 1p \cdot 2p \cdots (a_1 - 1)p \cdot a_1 p \pmod{p}$. So $(a_1 p)! \equiv a_1! p^{a_1} \pmod{p}$.

It follows that $(a_2 p^2)! = ((a_2 p)p)! \equiv (a_2 p)! p^{a_2 p} \equiv a_2! p^{a_2} p^{a_2 p} \pmod{p}$. So $(a_2 p^2)! \equiv a_2! p^{a_2(1+p)} \pmod{p}$.

Let us assume that $(a_i p^i)! \equiv a_i! p^{a_i(1+p+\dots+p^{i-1})} \pmod{p}$.

We have $(a_{i+1} p^{i+1})! = ((a_{i+1} p^i)p)! \equiv (a_{i+1} p^i)! p^{a_{i+1} p^i} \equiv a_{i+1}! p^{a_{i+1}(1+p+\dots+p^{i-1})} p^{a_{i+1} p^i} \pmod{p}$. Thus $(a_{i+1} p^{i+1})! \equiv a_{i+1}! p^{a_{i+1}(1+p+\dots+p^{i-1}+p^i)} \pmod{p}$.

Hence the result follows. □

We now prove Theorem 2.3.

Proof. If $a_i = 0$ for $i \in [[1, l]]$, then $n = a_0$ and we have $n! = q a_0!$ with $q = 1$. So, if $a_i = 0$ for $i \in [[1, l]]$, $q \equiv 1 \pmod{p}$.

Let consider the case where $a_i = 0$ for all $i > 1$, then $n = a_0 + a_1 p$ and we have $n! = q a_0! (a_1 p)!$. Then

$$q a_0! = \frac{n!}{(a_1 p)!} = (a_0 + a_1 p)(a_0 + a_1 p - 1) \dots (a_1 p + 1) = \prod_{r=0}^{a_0 - 1} (a_1 p + a_0 - r).$$

Since $0 < a_0 - r \leq a_0$ for $r \in [[0, a_0 - 1]]$, we obtain

$$qa_0! \equiv \prod_{r=0}^{a_0-1} (a_0 - r) \equiv \prod_{r=1}^{a_0} r \equiv a_0! \pmod{p}.$$

Since $a_0!$ and p are relatively prime, we have $q \equiv 1 \pmod{p}$.

Since $q = q_{a,l,k,0} \equiv q_{a,l,1,0} \pmod{p}$, we conclude that $q \equiv 1 \pmod{p}$ whatever n is. □

We come back to the proof of Theorem 1.1.

Proof. Let m, n be two positive integers whose base p expansion with p a prime, are

$$m = a_0 + a_1 p + \ldots + a_k p^k,$$

and

$$n = b_0 + b_1 p + \ldots + b_l p^l,$$

such that $m \geq n$. We assume that $a_i \geq b_i$ with $i = 0, 1, 2, \ldots, \max(k, l)$. We denote $a = \lfloor \frac{m}{p} \rfloor$ and $b = \lfloor \frac{n}{p} \rfloor$. Since $a_i \geq b_i$ with $i = 0, 1, 2, \ldots, \max(k, l)$, we have $a \geq b$. We define

$$a_{\max(k,l)} = \begin{cases} 0 & \text{if} \quad k < l \\ a_k & \text{if} \quad k \geq l \end{cases}$$

and

$$b_{\max(k,l)} = \begin{cases} b_l & \text{if} \quad k \leq l \\ 0 & \text{if} \quad k > l \end{cases}$$

In particular if $\max(k, l) = k$, $b_i = 0$ for $i > l$ and if $\max(k, l) = l$, $a_i = 0$ for $i > k$. Since $m \geq n$, $\max(k, l) = k$. So, we have $a_{\max(k,l)} = a_k$ and $b_{\max(k,l)} = b_k$ with $b_k = 0$ when $l < k$.

Using these

$$m! = q_{a,k,1,0} a_0! (a_1 p)! \ldots (a_k p^k)!,$$

$$n! = q_{b,l,1,0} b_0! (b_1 p)! \ldots (b_l p^l)!,$$

and

$$(m - n)! = q_{a-b,k,1,0} (a_0 - b_0)! ((a_1 - b_1)p)! \ldots ((a_k - b_k)p^k)!.$$

We have

$$\binom{m}{n} = \frac{q_{a,k,1,0}}{q_{b,l,1,0} q_{a-b,k,1,0}} \binom{a_0}{b_0} \binom{a_1 p}{b_1 p} \cdots \binom{a_{\max(k,l)} p^{\max(k,l)}}{b_{\max(k,l)} p^{\max(k,l)}}.$$

Rearranging

$$q_{b,l,1,0} q_{a-b,k,1,0} \binom{m}{n} = q_{a,k,1,0} \binom{a_0}{b_0} \binom{a_1 p}{b_1 p} \cdots \binom{a_{\max(k,l)} p^{\max(k,l)}}{b_{\max(k,l)} p^{\max(k,l)}}.$$

Since $q_{a,k,1,0} \equiv q_{b,l,1,0} \equiv q_{a-b,k,1,0} \equiv 1 \pmod{p}$, we get

$$\binom{m}{n} \equiv \binom{a_0}{b_0}\binom{a_1 p}{b_1 p}\cdots\binom{a_{\max(k,l)}p^{\max(k,l)}}{b_{\max(k,l)}p^{\max(k,l)}} \pmod{p}.$$

Notice that if for some i, $a_i = 0$, then $b_i = 0$ since we assume that $a_i \geq b_i$ and $b_i \geq 0$. In such a case $\binom{a_i p^i}{b_i p^i} = \binom{a_i}{b_i} = 1$.

We assume that $a_i \geq 1$. For $k \in [[1, a_i p^i - 1]]$ and for $i \in [[0, \max(k,l)]]$ with $1 \leq a_i \leq p^i - 1$, $\binom{a_i p^i}{k} \equiv 0 \pmod{p}$.

Therefore for $a_i = 1$ we have

$$(1+x)^{p^i} = \sum_{k=0}^{p^i} \binom{p^i}{k} x^k \equiv 1 + x^{p^i} \pmod{p},$$

and for any $a_i \in [[1, p^i - 1]]$, $(1+x)^{a_i p^i} = ((1+x)^{p^i})^{a_i} \equiv (1 + x^{p^i})^{a_i} \pmod{p}$.

Now comparing

$$(1+x)^{a_i p^i} = \sum_{k=0}^{a_i p^i} \binom{a_i p^i}{k} x^k,$$

and

$$(1 + x^{p^i})^{a_i} = \sum_{l=0}^{a_i} \binom{a_i}{l} x^{l p^i}$$

we get by taking $k = b_i p^i$ and $l = b_i$,

$$\binom{a_i p^i}{b_i p^i} \equiv \binom{a_i}{b_i} \pmod{p}.$$

Finally we have

$$\binom{m}{n} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_{\max(k,l)}}{b_{\max(k,l)}} \pmod{p}.$$

□

Acknowledgements

The second author is supported by DST INSPIRE Scholarship 422/2009 from Department of Science and Technology, Government of India.

References

[1] Lucas, E. Théorie des Fonctions Numériques Simplement Périodiques, *Amer. J. Math.*, Vol. 1, 1878, No. 2, 184–196 (part 1); Vol. 1, 1878, No. 3, 197–240 (part 2); Vol. 1, 1878, No. 4, 289–321 (part 3).