Legendre's and Kummer's Theorems Again

Dorel Miheţ

Some results related to Legendre's Theorem and Kummer's Theorem are discussed.

Dorel Mihet teaches courses on algebra and elementary number theory. His interests are in elementary mathematics, mathematical education and mathematical contests.

"*En général, si on a* $N = \theta^n$, *le nombre des facteurs* θ *compris dans le produit* $1 \cdot 2 \cdot 3 \cdot \ldots \cdot N$ *sera*

$$x = \frac{N-1}{\theta - 1}.$$

Et si on fait, comme on peut toujours le supposer, $N = A\theta^m + B\theta^n + C\theta^p + etc.$, *les coefficiens* $A, B, C, etc.$ *étant plus petits que* θ, *il en résultera*

$$x = \frac{N - A - B - etc.}{\theta - 1}."$$

This is the beautiful observation expressing the p-adic valuation of $n!$ by means of the base-p expansion of n, made by the legendary mathematician Legendre in 1808 in his '*Essai sur la théorie des nombres*' [1].

Some interesting facts about Legendre's theorem and a related one, belonging to Kummer, are nicely discussed by B Sury in the article 'Revisiting Kummer's and Legendre's Formulae' [2].

Here, we discuss some theoretical aspects in the first part of the article; but our main aim is to apply the above mentioned theorems in problem solving. We will see that many olympiad-type problems as: 'If $f(m)$ denotes the greatest k such that 2^k divides m, prove that there are infinite many numbers m such that $m - f(m) = 1989$', or 'The number of odd entries in any given row of Pascal's Triangle is a power of 2' can quite simply be solved with the help of these classical results.

Keywords
Legendre's theorem, Kummer's theorem, binomial coefficient, p-adic valuation, base-p expansion.

1. Legendre's Theorem and Kummer's Theorem

Let p be a prime number and $n > 1$ be an integer. Recall that the *p-adic valuation of* n, denoted by $v_p(n)$, is the

exponent of p in the canonical decomposition in prime factors of n (if p does not divide n, then $v_p(n) = 0$).

Legendre's theorem states as follows:

Theorem 1.1 [Legendre, 1808] *Let p be a prime and let*

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

be the base-p expansion of n. The exact power m of a prime p dividing $n!$ is given by

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

The common proof of this theorem is with the help of Legendre's formula[1]:

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right],$$

where $[x]$ denotes the greatest integer less than or equal to x.

We note here that an inductive proof of (1) can be obtained from the relation

$$v_p((n+1)!) = v_p(n!) + v_p(n+1)$$

(see also [2]), which can easily be derived from (1): if $n+1 = p^r \cdot m$, $(m,p) = 1$, then

$$\begin{aligned} v_p(n!) &= \frac{n - s_p(n)}{p-1} = \frac{n+1-s_p(n+1)}{p-1} - r \\ &= v_p((n+1)!) - r. \end{aligned}$$

An important result deriving from Legendre's theorem, belonging to Kummer, asserts that if $m \leq n$ then the p-adic valuation of the binomial coefficient $\binom{n}{m}$ is simply the number of 'carry-overs' when one adds m and $n-m$ in base p (or, equivalently, the number of 'borrows' required when subtracting the base-p representations of m from n).

Theorem 1.2 [Kummer, 1852] *The p-adic valuation of the binomial coefficient $\binom{n}{m}$ is equal to the number of*

[1] The formula

$$n! = \prod_{p \leq n} p^{[\frac{n}{p}]+[\frac{n}{p^2}]+\cdots}$$

commonly called Legendre's formula, appears in the second edition of '*Essai sur la la théorie des nombres*' [1]. However, it may have been discovered independently by various persons. For example, in [3] this formula is named *De Polignac's Formula*.

'carry-overs' when performing the addition of $n-m$ and m, written in base p.

Here we would like to reveal a heuristic argument leading to Kummer's theorem.

It is well known that if a, b are two positive integers written in decimal scale, then $s(a+b)$ and $s(a)+s(b)$ are congruent modulo 9. Here, s denotes the sum-of-digits function. If a 'carry-over' appears when the sum $a+b$ is performed, then $s(a)+s(b)$ is greater than $s(a+b)$, hence $s(a)+s(b)$ and $s(a+b)$ differ by 9. Generally, the difference between $s(a)+s(b)$ and $s(a+b)$ is nine times the number of 'carry-overs'.

More formally, let $a = a_0 + 10a_1 + ... + 10^d a_d$, $b = b_0 + 10b_1 + ... + 10^d b_d$, the decimal expansion of a and b ($a_d + b_d > 0$) and let $\varepsilon_j = 1$ if there is a 'carry-over' in the jth digit when adding a and b and $\varepsilon_j = 0$ otherwise (hence the total number of carry-overs is $\sum_{j=0}^{d} \varepsilon_j$).

If s denotes the sum $a+b$, then

$$s = s_0 + 10s_1 + ... + 10^d s_d + 10^{d+1}\varepsilon_d,$$

where $s_0 = a_0 + b_0 - 10\varepsilon_0$ and $s_j = a_j + b_j + \varepsilon_{j-1} - 10\varepsilon_j$ for each $1 \leq j \leq d$. Therefore, we have

$$\begin{aligned} \frac{s(a)+s(b)-s(a+b)}{9} &= \frac{\sum_{j=0}^{d}(a_j+b_j-s_j)-\varepsilon_d}{9} \\ &= \frac{10(\varepsilon_0+\varepsilon_1+...+\varepsilon_d)-(\varepsilon_0+\varepsilon_1+...+\varepsilon_{d-1})-\varepsilon_d}{9} \\ &= \sum_{j=0}^{d}\varepsilon_j. \end{aligned}$$

Kummer's theorem follows in a similar way from Legendre's formula (simply replace 10 by p and 9 by $p-1$), since if $n = m + r$ and n, m, r are written in base p as

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_s p^s,$$

$$m = m_0 + m_1 p + \cdots + m_s p^s,$$

$$r = r_0 + r_1 p + r_2 p^2 + \cdots + r_s p^s,$$

then

$$v_p\left(\binom{n}{m}\right) = v_p((m+r)!) - v_p(m!) - v_p(r!)$$
$$= \frac{s_p(m) + s_p(r) - s_p(m+r)}{p-1},$$

where $s_p(n)$ denotes the sum $n_0 + n_1 + ... + n_s$ in base p.

To exemplify how Kummer's theorem works, let us show that the number $\binom{1000}{500}$ is not divisible by 7 (USSR Math. Olympiad).

Indeed, the representation of 500 in base 7 is 1313. As no carry-over appears when the addition (in base 7) $1313 + 1313$ is performed, the exponent of 7 in $\binom{1000}{500}$ is 0.

2. Some Applications

In what follows some specific applications of Legendre's theorem and Kummer's theorem are presented.

The 2-adic Valuation of n!

From Legendre's formula (1) with $p = 2$, one obtains the following remarkable particular case, concerning the 2-adic valuation of $n!$:

PROPOSITION 2.1

The greatest power of 2 *dividing* $n!$ *is* 2^{n-r}, *where* r *is the number of* $1s$ *when we write* n *in base* 2.

This is a result from Legendre's book [1]. Let us read it in Legendre's words:

"Dans le cas particulier oú $\theta = 2$, *si l'on a* $N = 2^m$, *il en résultera* $x = N - 1$, *et si l'on fait généralement*

$$N = 2^m + 2^n + 2^p + etc.,$$

on aura

$$x = N - k,$$

k *étant le nombre des termes* $2^m, 2^n, 2^p, etc.$ *dont se compose la valeur* N."

Below the reader can find three immediate consequences of the above result. The problems in the form of corollaries are taken from the Mathematical Olympiads of USSR, Canada and Australia.

COROLLARY 2.2

a) 2^n *does not divide* $n!$ $(n > 1)$.

b) *If* $2^{n-1}|n!$, *then* n *is a power of* 2.

(It suffices to see that $v_2(n) = n - s_2(n) < n$ and $v_2(n) = n - 1 \Longrightarrow s(n) = 1 \Longrightarrow n = 2^k$.)

We note here that 2 is the only prime p such that p^{n-1} divides $n!$. This is because $\frac{n-s_p(n)}{p-1} \leq n-1$, and $\frac{n-s_p(n)}{p-1} = n-1$ iff $s_p(n) = 1$ and $p = 2$.

COROLLARY 2.3

There is no integer m *such that the number* $\frac{n!}{2^{n-m}}$ *is an integer for every positive integer* n.

(Consider n of the form $2^k - 1$ (many 1's in base 2). Then the exact power of 2 in $n!$ is $n - k$, which is $< n - m$ if $k > m$.)

COROLLARY 2.4 (Proposed by Columbia for IMO 1989)

Let m *be a positive integer and* $f(m)$ *be the greatest* k *such that* 2^k *divides* m. *Prove that there exist infinitely many numbers* m *such that* $m - f(m) = 1989$.

(The proof immediately follows by noting that $m - f(m)$ represents the number of ones in the binary expansion of m.)

2.2 *Central Binomial Coefficients*

PROPOSITION 2.5

$\binom{2n}{n}$ *is a multiple of* $n + 1$.

Proof. We apply Kummer's theorem: If p is an arbitrary prime divisor of $n+1$ and $v_p(n+1) = l$, then the base-p representation of $n+1$ is of the form $\overline{a_k...a_1a_0\underbrace{0...0}_{l}}$ with $a_0 \neq 0$, and n is written in base p as

$$\overline{a_k...a_1(a_0-1)\underbrace{(p-1)...(p-1)}_{l}}\ .$$

Hence the base-p addition $n+n$ has at least l carry-overs, that is,

$$v_p(n+1) \leq v_p(\binom{2n}{n}).$$

□

(The common proof makes use of the combinatorial formula $\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$).

The number $C_n := \frac{1}{n+1}\binom{2n}{n}$, called 'the n-th Catalan number', appears in various problems of enumerative combinatorics. For example, C_n is the number of ways $n+1$ factors can be completely parenthesized as well as the number of ways to triangulate a regular polygon with $n+2$ sides.

The following is another interesting property of the 'central coefficient' $\binom{2n}{n}$.

PROPOSITION 2.6 (Laurenţiu Panaitopol, [4])

Let $n > 1$. Then $\binom{2n}{n}$ is even and 4 does not divide $\binom{2n}{n}$ if and only if n is a power of 2.

Indeed, the exponent of 2 in $\binom{2n}{n}$ is $v_2(\binom{2n}{n}) = v_2(2n) - 2v_2(n) = 2n - s_2(n) - 2(n - s_2(n)) = s_2(n) \geq 1$. If n has more than one nonzero digit in the binary scale (that is, it is not a power of 2), then $v_2(\binom{2n}{n}) = s_2(n) \geq 2$.

2.3 *A Useful Inequality*

From $v_p(n!) = \frac{n-s_p(n)}{p-1}$ the following useful inequality immediately follows:

$$v_p(n!) \leq \left[\frac{n-1}{p-1}\right].$$

We exemplify its usefulness by the following problem (originated from the journal *American Mathematical Monthly*), from 2010 Romanian IMO and BMO selection tests:

Let n, q be positive integers such that all prime divisors of q are greater than n. Show that

$$(q-1)\cdot(q^2-1)\cdot\ldots\cdot(q^{n-1}-1) \equiv 0 \ (mod n!). \tag{2}$$

Indeed, let p be an arbitrary prime $\leq n$. Since p is not a divisor of q^k, by Fermat's Little Theorem we deduce that $q^{k(p-1)} \equiv 1 \ mod(p)$ for all k, hence at least $\left[\frac{n-1}{p-1}\right]$ factors from the left-hand side of (2) are divisible by p.

This means that the exponent $e(p)$ of p in $(q-1)\cdot(q^2-1)\cdot\ldots\cdot(q^{n-1}-1)$ is at least $\left[\frac{n-1}{p-1}\right]$.

On the other hand, $v_p(n!) \leq \left[\frac{n-1}{p-1}\right]$, that is, $e(p) \geq v_p(n!)$, concluding the proof.

(The upper bound $\left[\frac{n-1}{p-1}\right]$ for $v_p(n!)$ is attained when $s_p(n) = 1$, that is, when n is a power of p. We also note that if $p^k \leq n < p^{k+1}$, then $v_p(n)$ is not less than $\left[\frac{n-1}{p-1}\right] - k$, with equality when $n = p^{k+1} - 1$.)

2.4 *Binomial Coefficients Modulo p*

The results of this section are mainly related to an Olympiad problem by I Tomescu in Romanian mathematical journal *Gazeta Matematică*[2] (*Mathematical Gazette*, in English) Vol. XCIV, 1983, expressing the number of binomial coefficients divisible by a prime p.

[2] The first issue of *Gazeta Matematica* appeared in September 1895. *Gazeta Matematica* was a true school of mathematics, that contributed to the formation of many generations of young math enthusiasts. Almost all romanian mathematicians were collaborators of *Gazeta*.

PROPOSITION 2.7

Let p be a prime number. The number of binomial coefficients $\binom{n}{0}, \binom{n}{1}, ..., \binom{n}{n}$ that are multiples of p is

$$n + 1 - (n_0 + 1)(n_1 + 1)...(n_r + 1),$$

where $n_0, ..., n_r$ denote the digits in the expansion of n in base p.

Proof. Let $n = n_0 + n_1 p + ... + n_r p^r \quad (n_r \neq 0)$ and $a = a_0 + a_1 p + ... + a_r p^r$ be the expansions of n and a in base p.

From Kummer's theorem it follows that p does not divide $\binom{n}{a}$ iff $n_i \geq a_i \ \forall i = \overline{0, r}$.

Therefore, the number of binomial coefficients which are not multiples of p is $(n_0 + 1)(n_1 + 1)...(n_r + 1)$ (we can choose a_0 in $n_0 + 1$ ways, etc.), hence the number of multiples of p is

$$n + 1 - (n_0 + 1)(n_1 + 1)...(n_r + 1),$$

as desired. □

The following corollaries are immediate consequences of Proposition 2.7.

COROLLARY 2.8 (Glaisher, 1899).

The number of odd entries in any given row of Pascal's Triangle is a power of 2

Indeed, we have just seen that if n is expressed in base 2 as $n = n_0 + 2n_1 + ... + 2^r n_r$, then the number of odd (not divisible by 2) binomial coefficients is $(n_0 + 1)...(n_r + 1)$, which is exactly 2^u, where u is the number of 1s in the binary representation of n.

We take the opportunity to note the following important result: *All the binomial coefficients $\binom{n}{0}, ..., \binom{n}{n}$ are odd iff n is of the form $2^s - 1$.*

(This follows from $n + 1 = 2^u$.)

There is a nice combinatorial argument for Glaisher's result:

$\binom{n}{m}$ is odd if and only if there are no carry-overs when adding m and $n-m$ in base 2; in other words, if $m_i = 1$ for some i, then n_i is 1 as well. Let u be the number of 1s in the binary expansion of n. Then each of the 2^u possible subsets of these 1s, gives a value of m. Hence there are exactly 2^u odd entries in the n-th row of Pascal's Triangle.

COROLLARY 2.9

A prime p divides all the binomial coefficients $\binom{n}{k}$ $(k = 1, ..., n-1)$ iff

$$(n_0+1)(n_1+1)...(n_r+1) = 2 \Longrightarrow n_r = 1, n_0 = n_1 = ... = n_{r-1} = 0,$$

that is, iff $n = p^r$.

COROLLARY 2.10 (Luxembourg Math. Olympiad, 1980)

Let p be a prime and n be a positive integer. Then p does not divide $\prod_{k=0}^{n} \binom{n}{k}$ iff $n = p^s \cdot m - 1$, with $1 \leq m < p$.

If $p = 2$ one obtains the previously mentioned result: all the binomial coefficients $\binom{n}{0}, ..., \binom{n}{n}$ are odd iff n is of the form $2^s - 1$.

(It suffices to note that if $0 < a < p-1, 0 \leq b < p-1$, then $pa + b > (a+1)(b+1)$. This proves that at most one digit of n could be less than $p-1$.)

Remark. The result in Proposition 2.7 can be obtained by using another classical theorem concerning binomial coefficients, due to Lucas.

Theorem 2.11 [Lucas, 1878] *If $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$ and $m = m_0 + m_1 p + \cdots + m_r p^r$ are the*

expansions of n and m in base p, then

$$\binom{n}{m} \equiv \binom{n_0}{m_0} \cdot \binom{n_1}{m_1} \cdot \binom{n_r}{m_r} \pmod{p}.$$

For the proof of this theorem and other interesting facts about binomial coefficients we refer the reader to [5].

2.5 *The GCD of* $\binom{n}{1}, \binom{n}{2}, ..., \binom{n}{n-1}$.

Let d denote the GCD of $\binom{n}{1}, \binom{n}{2}, ..., \binom{n}{n-1}$, where $n > 1$ is a given positive integer. Since $\binom{n}{1} = n$, it follows that d is a divisor of n. Let p be any prime dividing n.

We first consider the case when n is a power of p and show that if $1 \leq k \leq p^r - 1$ is an integer of the form $k = p^s \cdot l$, with $(p, l) = 1$, then $v_p(\binom{p^r}{k}) = r - s$. Indeed, let k be written in base p as $\overline{a_k...a_1a_0\underbrace{0...0}_{s}}$, with $a_0 \neq 0$. Then the number of carry-overs in the addition:

$$\overline{\underbrace{(p-1)...(p-1)(p-1-a_k)...(p-1-a_1)(p-a_0)}_{r-s}\underbrace{0...0}_{s}}$$
$$+ \overline{a_k...a_0\underbrace{0...0}_{s}}$$

is exactly $r - s$, as claimed.

(Although an immediate proof can be obtained from the formula $k\binom{p^r}{k} = p^r\binom{p^r-1}{k-1}$, we have just seen that the proof with the help of Kummer's theorem is equally simple.)

In particular, if $k = p^{r-1}$, then $v_p(\binom{p^r}{k})$ is $r-(r-1) = 1$, that is, $p^2\binom{p^r}{k}$. This shows that in this case the greatest common divisor of $\binom{p^r}{1}, ..., \binom{p^r}{p^r-1}$ is p.

If $n = p^r \cdot m$, with $(p, m) = 1$ and $m > 1$, then the base-p expansion of n is of the form

$$\overline{n_r...n_1n_{r-s}\underbrace{0...0}_{s}}$$

with $n_{r-s} \geq 1$ and one of binomial coefficients $\binom{n}{1}, \binom{n}{2}$, ..., $\binom{n}{n-1}$ is $\binom{n}{p^s}$. Because no carry-over appears when the addition:

$$\overline{n_r...n_1(n_{r-s}-1)\underbrace{0...0}_{s}} + \overline{1\underbrace{0...0}_{s}}$$

is performed, this binomial coefficient is not divisible by p. Therefore, no prime factor of n divides d, concluding that $d = 1$.

As a conclusion, the greatest common divisor of $\binom{n}{1}, \binom{n}{2}$, ..., $\binom{n}{n-1}$ is either 1 (if n is not a power of a prime) or a prime.

2.6 *Challenges*

1) Probably most readers know that a number having (in base 10) more than one digit cannot be equal to the product of its digits. Can you quickly answer the following question: What is the set of all positive integers n such that $n+1 = (n_0+1)\cdot...\cdot(n_k+1)$? Here $n_0, ..., n_k$ denote the digits of n in decimal scale.

2) Let $n \geq 2$. How many binomial coefficients $\binom{2^n}{k}$, $k = 1, 2, ..., 2^n - 1$ are not multiples of 4?

3) Prove that $\binom{2n}{n}$ divides LCM$(1, 2, ..., 2n)$.

Address for Correspondence
Dorel Mihet
West University of Timisoara
Faculty of Mathematics and
Computer Science
Bv. V. Parvan 4, 300223
Timisoara, Romania
Email: mihet@math.uvt.ro

Suggested Reading

[1] A M Legendre, *Essai sur la théorie des nombres*, Second Edition, Paris, Chez Courcier, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, *n*° 57, pp.8–10, 1808.
[2] B Sury, Revisiting Kummer's and Legendre's Formulae, *Resonance*, Vol.10, No.2, pp.62–66, 2005.
[3] D A Santos, *Number Theory for Mathematical Contests*, http://www.opencontent.org/openpub/.
[4] L Panaitopol and A Gica, *Problems in Arithmetic and Number Theory*, GIL Zalau, (in Romanian), 2003.
[5] A Granville, *Arithmetical Properties of Binomial Coefficients*, www.dms.umontreal.ca/~andrew/Binomial/.
[6] V Boju and L Funar, *The Math Problems Notebook*, Birkhauser, Boston–Basel–Berlin, 2007.
[7] R Honsberger, *In Polya's Footsteps*, published and distributed by the Mathematical Association of America, pp. 229–233, 1997.
[8] E Lozansky and C Rousseau, *Winning Solutions*, Springer, 1996.