A CHARACTERIZATION OF A PRIME p FROM THE BINOMIAL COEFFICIENT $\binom{n}{p}$

ALEXANDRE LAUGIER AND MANJIL P. SAIKIA

ABSTRACT. We complete a proof of a theorem that was inspired by an Indian Olympiad problem, which gives an interesting characterization of a prime number p with respect to the binomial coefficients $\binom{n}{p}$. We also derive a related result which generalizes the theorem in one direction.

Key Words: prime moduli, binomial coefficients, floor function.

2010 Mathematical Reviews Classification Numbers: 11A07, 11A41, 11A51, 11B50, 11B65, 11B75.

1. INTRODUCTION AND MOTIVATION

Problem 1.1. 7 *divides* $\binom{n}{7} - \lfloor \frac{n}{7} \rfloor$, $\forall n \in \mathbb{N}$.

The above appeared as a problem in the Regional Mathematical Olympiad, India in 2003. Later in 2007, a similar type of problem was set in the undergraduate admission test of Chennai Mathematical Institute, a premier research institute of India where 7 was replaced by 3.

This became the basis of the following

Theorem 1.2 ([3], Saikia-Vogrinc). *A natural number $p > 1$ is a prime if and only if $\binom{n}{p} - \lfloor \frac{n}{p} \rfloor$ is divisible by p for every non-negative n, where $n > p + 1$ and the symbols have their usual meanings.*

2. PROOF OF THEOREM 1.2

In [3], the above theorem is proved. The authors give three different proofs, however the third proof is incomplete. We present below a completed version of that proof.

Proof. First we assume that p is prime. Now we consider n as $n = ap + b$ where a is a non-negative integer and b an integer $0 \le b < p$. Obviously,

$$(2.1) \qquad \left\lfloor \frac{n}{p} \right\rfloor = \lfloor \frac{ap + b}{p} \rfloor \equiv a \ (mod \ p).$$

Now let us calculate $\binom{n}{p} \ (mod \ p)$.

$$
\begin{aligned}
\binom{n}{p} &= \binom{ap + b}{p} \\
&= \frac{(ap + b) \cdot (ap + b - 1) \cdots (ap + 1) \cdot ap \cdot (ap - 1) \cdots (ap + b - p + 1)}{p \cdot (p - 1) \cdots 2 \cdot 1} \\
&= \frac{a \cdot (ap + b) \cdot (ap + b - 1) \cdots (ap + 1) \cdot (ap - 1) \cdots (ap + b - p + 1)}{(p - 1) \cdot (p - 2) \cdots 2 \cdot 1} \\
&= \frac{aX}{(p - 1)!}
\end{aligned}
$$

where $X = (ap + b) \cdot (ap + b - 1) \cdots (ap + 1) \cdot (ap - 1) \cdots (ap + b - p + 1)$.

We observe that there are $(p-1)$ terms in X and each of them has one of the following forms,
(a) $ap + r_1$, or
(b) $ap - r_2$
where $1 \leq r_1 \leq b$ and $1 \leq r_2 \leq (p-1-b)$.
Thus any two terms from either (a) or (b) differs by a number strictly less than p and hence not congruent modulo p. Similarly, if we take two numbers - one from (a) and the other from (b), it is easily seen that the difference between the two would be $r_1 + r_2$ which is at most $(p-1)$ (by the bounds for r_1 and r_2); thus in this case too we find that the two numbers are not congruent modulo p. Thus the terms in X forms a reduced residue system modulo p and so, we have,

$$(2.2) \qquad\qquad X \equiv (p-1)! \ (mod \ p)$$

Thus using (2.2) we obtain,

$$(2.3) \qquad\qquad \binom{n}{p} = a \frac{X}{(p-1)!} \equiv a \ (mod \ p)$$

So, (2.1) and (2.3) combined gives

$$(2.4) \qquad\qquad \left\lfloor \frac{n}{p} \right\rfloor \equiv \binom{n}{p} \ (mod \ p).$$

So, forward implication is proved.

To prove the reverse implication, we adopt a contrapositive argument meaning that if p were not prime (that is composite) then we must construct an n such that (4) does not hold. So, let q be a prime factor of p. We write p as $p = q^x k$, where $(q, k) = 1$. In other words, x is the largest power of q such that $q^x | p$ but $q^{x+1} \nmid p$ (in notation, $q^x || p$). By taking, $n = p + q = q^x k + q$, we have

$$\binom{p+q}{p} = \binom{p+q}{q} = \frac{(q^x k + q)(q^x k + q - 1) \ldots (q^x k + 1)}{q!}$$

which after simplifying the fraction equals $(q^{x-1}k+1)\frac{(q^x k+q-1)\ldots(q^x k+1)}{(q-1)!}$. Clearly, $(q^x k+q-1)\ldots(q^x k+1) \equiv (q-1)! \not\equiv 0 \ (mod \ q^x)$. Therefore,

$$\frac{(q^x k + q - 1) \ldots (q^x k + 1)}{(q-1)!} \equiv 1 \ (mod \ q^x)$$

and

$$\binom{p+q}{p} \equiv q^{x-1}k + 1 \ (mod \ q^x).$$

On the other hand obviously,

$$\left\lfloor \frac{p+q}{p} \right\rfloor = \left\lfloor \frac{q^x k + q}{q^x k} \right\rfloor \equiv 1 \ (mod \ q^x).$$

Now, since $(q, k) = 1$, it follows that $q^{x-1}k + 1 \not\equiv 1 \ (mod \ q^x)$. So we conclude,

$$(2.5) \qquad\qquad \binom{p+q}{p} \not\equiv \left\lfloor \frac{p+q}{p} \right\rfloor \ (mod \ q^x).$$

So, $p \nmid (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, for if $p | (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, then since $q^x | p$, we would have $q^x | (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, a contradiction to (5). Thus, $\binom{p+q}{p} \not\equiv \lfloor \frac{p+q}{p} \rfloor \ (mod \ p)$. Hence we are through with the reverse implication too.

This completes the proof of Theorem 1.2. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

3. ANOTHER SIMPLE RESULT

We state and prove the following simple result which generalizes one part of Theorem 1.2

Theorem 3.1. *For* $n = ap + b = a_{(k)}p^k + b_{(k)}$, *we have*

$$\binom{a_{(k)}p^k + b_{(k)}}{p^k} - \left\lfloor \frac{a_{(k)}p^k + b_{(k)}}{p^k} \right\rfloor \equiv 0 \pmod{p}$$

with p *a prime,* $0 \le b_{(k)} \le p^k - 1$ *and* k *a positive integer such that* $1 \le k \le l$, *where*

$$n = a_0 + a_1 p + \ldots + a_k p^k + a_{k+1} p^{k+1} + \ldots + a_l p^l$$

and for $k \ge 1$

$$a_{(k)} = a_k + a_{k+1}p + \ldots + a_l p^{l-k}$$

and

$$b_{(k)} = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1}.$$

.

The proof of this follows from the reasoning of the proof of Theorem 1.2 although there are some subtleties.

In particular, we have

$$a = a_{(1)} = a_1 + a_2 p + \ldots + a_l p^{l-1}$$

and

$$b = b_{(0)} = a_0.$$

For $k = 0$, we set the convention that $a_{(0)} = n = a_0 + a_1 p + \ldots + a_l p^l$ and $b_{(0)} = 0$. Notice that Theorem 3.1 is obviously true for $k = 0$. But the case $k = 0$ doesn't correspond really to a power of p where p is a prime.

Proof. We have

$$\binom{n}{p^k} = \binom{a_{(k)}p^k + b_{(k)}}{p^k}$$

$$= \frac{(a_{(k)}p^k + b_{(k)}) \cdot (a_{(k)}p^k + b_{(k)} - 1) \cdots (a_{(k)}p^k + 1) \cdot a_{(k)}p^k \cdot (a_{(k)}p^k - 1) \cdots (a_{(k)}p^k + b_{(k)} - p^k + 1)}{p^k \cdot (p^k - 1) \cdots 2 \cdot 1}$$

$$= \frac{a_{(k)} \cdot (a_{(k)}p^k + b_{(k)}) \cdot (a_{(k)}p^k + b_{(k)} - 1) \cdots (a_{(k)}p^k + 1) \cdot (a_{(k)}p^k - 1) \cdots (a_{(k)}p^k + b_{(k)} - p^k + 1)}{(p^k - 1) \cdot (p^k - 2) \cdots 2 \cdot 1}.$$

Thus we obtain

$$(p^k - 1)! \binom{n}{p^k} = a_{(k)} \left(\prod_{r=1}^{b} (a_{(k)}p^k + r) \right) \left(\prod_{r=1}^{p^k - 1 - b} (a_{(k)}p^k - r) \right).$$

Or $a_{(k)}p^k + r \equiv r \pmod{p^k}$ and $a_{(k)}p^k - r \equiv -r \equiv p^k - r \pmod{p^k}$ with $0 < r < p^k$. It follows

$$\left(\prod_{r=1}^{b} (a_{(k)}p^k + r) \right) \left(\prod_{r=1}^{p^k - 1 - b} (a_{(k)}p^k - r) \right) \equiv \left(\prod_{r=1}^{b} r \right) \left(\prod_{r=1}^{p^k - 1 - b} (p^k - r) \right) \pmod{p^k}.$$

Since

$$\left(\prod_{r=1}^{b} r \right) \left(\prod_{r=1}^{p^k - 1 - b} (p^k - r) \right) = \left(\prod_{r=1}^{b} r \right) \left(\prod_{r=b+1}^{p^k - 1} r \right) = \prod_{r=1}^{p^k - 1} r = (p^k - 1)!$$

we have

$$\left(\prod_{r=1}^{b} (a_{(k)}p^k + r) \right) \left(\prod_{r=1}^{p^k - 1 - b} (a_{(k)}p^k - r) \right) \equiv (p^k - 1)! \pmod{p^k}.$$

We can notice that,
$$(p^k - 1)! = q(p-1)! \, p^{1+p+\ldots+p^{k-1}-k}$$
with $\gcd(p,q) = 1$ and because $\mathrm{ord}_p((p^k - 1)!) = 1 + p + \ldots + p^{k-1} - k$. Therefore we have
$$a_{(k)} c_{(k)} p^{k(p^k - 1)} + (p^k - 1)! \left\{ a_{(k)} - \binom{n}{p^k} \right\} = 0.$$

Equivalently
$$a_{(k)} c_{(k)} p^{k(p-1)(1+p+\ldots+p^{k-1})} + q(p-1)! \, p^{1+p+\ldots+p^{k-1}-k} \left\{ a_{(k)} - \binom{n}{p^k} \right\} = 0$$

Dividing the above equation by $p^{1+p+\ldots+p^{k-1}-k}$ we have
$$q(p-1)! \left\{ a_{(k)} - \binom{n}{p^k} \right\} + a_{(k)} c_{(k)} p^{k+(k(p-1)-1)(1+p+\ldots+p^{k-1})} = 0.$$

Thus
$$q(p-1)! \left\{ a_{(k)} - \binom{n}{p^k} \right\} \equiv 0 \pmod{p^k}$$

Since if $m \equiv n \pmod{p^k}$ implies $m \equiv n \pmod{p}$ (the converse is not always true), we also have
$$q(p-1)! \left\{ a_{(k)} - \binom{n}{p^k} \right\} \equiv 0 \pmod{p}.$$

As $q(p-1)!$ with $\gcd(p,q) = 1$ and p are relatively prime, we get
$$\binom{n}{p^k} - a_{(k)} \equiv 0 \pmod{p}.$$

We finally have
$$\binom{n}{p^k} \equiv \left\lfloor \frac{n}{p^k} \right\rfloor \pmod{p}.$$

$\square$

Theorem 3.2. *Let p be a prime number, let k be a natural number and let x be a positive integer such that*
$$x \equiv r \pmod{p^k}$$
with $0 \le r < p^k$. Denoting $q = \lfloor \frac{x}{p^k} \rfloor$ the quotient of the division of x by p^k, if there exists $s \in \mathbb{N}^\star$ for which
$$\left\lfloor \frac{x}{p^{ks}} \right\rfloor = q^s$$
then we have
$$x \equiv r \pmod{p^{ks}}.$$

Proof. Given p a prime number, let x be a positive integer such that $x \equiv r \pmod{p^k}$ with $0 \le r < p^k$. Denoting $q = \lfloor \frac{x}{p^k} \rfloor$, we assume that there exists $s \in \mathbb{N}^\star$ for which
$$\left\lfloor \frac{x}{p^{ks}} \right\rfloor = q^s.$$

If $k = 0$, the result is obvious since for all integers x, r, we have $x \equiv r \pmod{1}$. In the following, we assume that $k \in \mathbb{N}^\star$.

Then, we have
$$x = qp^k + r$$
and
$$x = q^s p^{ks} + r'$$
with $0 \le r' < p^{ks}$. It comes that
$$qp^k + r = q^s p^{ks} + r'.$$

So ($s \in \mathbb{N}^\star$)

$$q^s p^{ks} - qp^k = r - r' \geq 0.$$

Since $0 \leq r < p^k$, we have

$$0 \leq r - r' < p^k.$$

Moreover, rewriting the equality $q^s p^{ks} - qp^k = r - r'$ as

$$qp^k(q^{s-1}p^{k(s-1)} - 1) = r - r'$$

we can notice that $p^k | r - r'$. Since $0 \leq r - r' < p^k$, it is only possible if $r - r' = 0$ and so

$$r = r'.$$

From the equality $x = q^s p^{ks} + r'$, we deduce that

$$x \equiv r \pmod{p^{ks}}.$$

$\square$

A consequence of the Theorem 3.2 is that if an integer y is congruent to a positive integer x modulo p^k such that $x \equiv r \pmod{p^k}$, provided the conditions stated in the Theorem 3.2 are fulfilled, we have also $y \equiv r \pmod{p^{ks}}$.

It can be verified easily that the product $\left(\prod_{r=1}^{b}(a_{(k)}p^k + r)\right)\left(\prod_{r=1}^{p^k-1-b}(a_{(k)}p^k - r)\right)$ contains the term $(a_{(k)}p^k)^{p^k-1} = a_{(k)}^{p^k-1}p^{k(p^k-1)}$. The term $(a_{(k)}p^k)^{p^k-1}$ is the only term in $p^{k(p^k-1)}$ which appears in the decomposition of this product into sum of linear combination of powers of p. Notice also that the number $k(p^k - 1)$ is the greatest exponent of p in this product when we decompose this product into sum of linear combination of powers of p (like a polynomial expression in variable p). Afterwards, we write $a_{(k)}^{p^k-1}$ as $c_{(k)}$ in order to simplify the notation. Thus, the quotient of the division of this product by $p^{k(p^k-1)}$ is $c_{(k)} = a_{(k)}^{p^k-1}$.

So, from the Theorem 3.2, we can now write

$$\left(\prod_{r=1}^{b}(a_{(k)}p^k + r)\right)\left(\prod_{r=1}^{p^k-1-b}(a_{(k)}p^k - r)\right) = c_{(k)}p^{k(p^k-1)} + (p^k - 1)!.$$

4. Acknowledgements

References

[1] D. M. Burton, *Elementary Number Theory*, 6 ed., Tata McGraw–Hill, 2010.

[2] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math., **1** (2), 184–196; **1** (3), 197–240; **1** (4), 289–321 (1878).

[3] M. P. Saikia, J. Vogrinc, *A Simple Number Theoretic Result*, J. Assam Acad. Math., **3**, Dec., 91-96, 2010 (`arXiv:1207.6707 [math.NT]`).

[4] M. P. Saikia, J. Vogrinc, *Binomial Symbols and Prime Moduli*, J. Ind. Math. Soc., **79**, (1-4), 137-143, 2011.

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

Department of Mathematical Sciences, Tezpur University, Napaam, Sonitpur, Assam, Pin-784028, India
E-mail address: `manjil@gonitsora.com`