

RENDICONTI  
*del*  
SEMINARIO MATEMATICO  
*della*  
UNIVERSITÀ DI PADOVA

ALAIN ROBERT

MAXIME ZUBER

**The Kazandzidis supercongruences. A simple  
proof and an application**

*Rendiconti del Seminario Matematico della Università di Padova,*  
tome 94 (1995), p. 235-243

[http://www.numdam.org/item?id=RSMUP\\_1995\\_\\_94\\_\\_235\\_0](http://www.numdam.org/item?id=RSMUP_1995__94__235_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1995, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques*

<http://www.numdam.org/>

## The Kazandzidis Supercongruences. A Simple Proof and an Application.

ALAIN ROBERT - MAXIME ZUBER (\*)

ABSTRACT - Let  $p$  be an odd prime and  $n, k$ , non-negative integers. The following supercongruences

$$\binom{np}{kp} \equiv \binom{n}{k} \pmod{p^3 \cdot n \cdot k \cdot (n-k) \cdot \binom{n}{k} \mathbb{Z}_p} \quad (p \geq 5),$$
$$\binom{3n}{3k} \equiv \binom{n}{k} \pmod{3^2 \cdot n \cdot k \cdot (n-k) \cdot \binom{n}{k} \mathbb{Z}_3} \quad (p = 3),$$

involving binomial coefficients, are due to G. S. Kazandzidis [1, 2, 3]. We propose here a simple proof based on well-known properties of the  $p$ -adic Morita gamma function  $\Gamma_p$ . At the same time, we present an application leading to a new supercongruence concerning the Legendre polynomials. We would like to thank D. Barsky for reading carefully a first draft of this proof and for pointing out an inaccuracy in the argument and the referee for some improvements in the presentation.

### 1. Proof of the supercongruences.

Let us start with the following observation by L. van Hamme [4, p. 116, Ex. 39.D]

$$(1) \quad \binom{np}{kp} \Big/ \binom{n}{k} = \frac{\Gamma_p(np)}{\Gamma_p(kp) \cdot \Gamma_p((n-k)p)}.$$

(\*) Indirizzo degli AA.: Department of Mathematics, University of Neuchâtel, Emile-Argand 11, CH-2007 Neuchâtel (Switzerland).

Research partially supported by the Swiss National Fund for Scientific Research (FNRS), grant number 21-37348.93.

The right member of (1) expresses  $\binom{np}{kp} / \binom{n}{k}$  as a quotient of  $p$ -adic units. Furthermore, the fonction  $\Gamma_p$  satisfies the inequality

$$|\Gamma_p(x) - \Gamma_p(y)| \leq |x - y| \quad (x, y \in \mathbb{Z}_p).$$

Since  $\Gamma_p(0) = 1$ , it follows that

$$|\Gamma_p(x) - 1| \leq |x| \quad (x \in \mathbb{Z}_p).$$

This implies that the  $p$ -adic logarithm of  $\Gamma_p$  is well-defined on  $p\mathbb{Z}_p$ . Thus, in order to compute the quotient

$$\frac{\Gamma_p(np)}{\Gamma_p(kp) \cdot \Gamma_p((n-k)p)},$$

we shall study the function

$$f(x) := \log \Gamma_p(x)$$

on  $p\mathbb{Z}_p$  or more precisely the expression

$$f(x+y) - f(x) - f(y) = \log \left( \frac{\Gamma_p(x+y)}{\Gamma_p(x) \cdot \Gamma_p(y)} \right).$$

Notice that the following equality holds

$$\left| \log \left( \frac{\Gamma_p(x+y)}{\Gamma_p(x) \cdot \Gamma_p(y)} \right) \right| = \left| 1 - \frac{\Gamma_p(x+y)}{\Gamma_p(x) \cdot \Gamma_p(y)} \right|.$$

Now, from the identity [4, p. 109]

$$\Gamma_p(x) \cdot \Gamma_p(1-x) = (-1)^{R(x)}, \quad (x \in \mathbb{Z}_p, 1 \leq R(x) \leq p, R(x) \equiv x \pmod{p}),$$

it follows that, for  $x \in p\mathbb{Z}_p$

$$\Gamma_p(x) \cdot \Gamma_p(1-x) = -1$$

and therefore

$$\Gamma_p(x) \cdot \Gamma_p(-x) = 1.$$

In other words, *the function  $f = \log \Gamma_p$  is odd on  $p\mathbb{Z}_p$* . Moreover it is analytic on  $p\mathbb{Z}_p$  [4, Lemma 58.1, p. 177] and admits the expansion

$$\log \Gamma_p(x) = \lambda_0 x - \sum_{n \geq 1} \frac{\lambda_n}{2n(2n+1)} \cdot x^{2n+1}$$

with coefficients  $\lambda_n$  defined by

$$\lambda_n = \int_{\mathbb{Z}_p^\times} x^{-2n} dx \quad (n \geq 1).$$

Observe that this expansion defines the function  $f(x)$  on  $\{x \in \mathbb{C}_p : |x| \leq |p|\}$ . From this we deduce that

$$(2) \quad f(x+y) - f(x) - f(y) = \sum_{n \geq 1} \frac{-\lambda_n}{2n(2n+1)} \{(x+y)^{2n+1} - x^{2n+1} - y^{2n+1}\}$$

(the linear term vanishes!). The first term of the sum is

$$-\frac{\lambda_1}{2 \cdot 3} (3x^2y + 3xy^2) = -xy(x+y) \frac{\lambda_1}{2}.$$

An estimate of  $\lambda_1$  (depending on the prime  $p$ ) will be given below. The second term of the sum in (2) is

$$-\frac{\lambda_2}{4 \cdot 5} \cdot xy(x+y) \cdot 5(x^2 + xy + y^2) = -\frac{\lambda_2}{4} \cdot xy(x+y) \cdot (x^2 + xy + y^2).$$

It belongs to  $p^2 \lambda_2 xy(x+y)\mathbb{Z}_p$  provided  $x, y \in p\mathbb{Z}_p$  and  $p \neq 2$ . For the next terms, we use the factorization

$$(x+y)^j - x^j - y^j = x \cdot y \cdot (x+y) \cdot a_j(x, y) \quad (j \text{ odd } \geq 3),$$

in which  $a_j(x, y) \in \mathbb{Z}[x, y]$  denotes a homogenous polynomial of degree  $j-3$ . This follows from the fact that  $x^j + y^j$  is divisible by  $x+y$  when  $j$  is odd

$$\frac{x^j + y^j}{x+y} = x^{j-1} - x^{j-2}y + \dots + y^{j-1}.$$

Hence, if  $x$  and  $y$  are both in  $p\mathbb{Z}_p$ , then the following inequality holds

$$|x^j + y^j - (x+y)^j| \leq |x \cdot y \cdot (x+y)| \cdot |p|^{j-3}.$$

LEMMA 1. For any prime  $p$  the number  $p \cdot \lambda_n$  belongs to  $\mathbb{Z}_p$ . More precisely, for  $n \geq 2$  we have

$$\lambda_n - b_{2n} \in \mathbb{Z}_p,$$

(here  $b_{2n} \in (1/p)\mathbb{Z}_p$  denotes the  $2n$ -th Bernoulli number), whereas

$$\lambda_1 = \begin{cases} \lambda_1(p) \in \mathbb{Z}_p & \text{for } p > 3, \\ \lambda_1(3) \in \frac{1}{3}\mathbb{Z}_3 & \text{for } p = 3. \end{cases}$$

PROOF. Recall the definition

$$\lambda_n = \int_{\mathbb{Z}_p^\times} x^{-2n} dx := \lim_{j \rightarrow \infty} \frac{1}{p^j} \sum_{1 \leq i < p^j, p \nmid i} i^{-2n}.$$

Now, both terms of the congruence

$$\sum_{1 \leq i < p^j, p \nmid i} i^{-2n} \equiv \sum_{1 \leq i < p^j, p \nmid i} i^{2n} \pmod{p^j \mathbb{Z}_p}$$

represent the same element in the group  $(\mathbb{Z}/p^j\mathbb{Z})^\times$  of units of  $\mathbb{Z}/p^j\mathbb{Z}$ . In the field  $\mathbb{Q}_p$ , this leads to the congruence

$$\frac{1}{p^j} \sum_{1 \leq i < p^j, p \nmid i} i^{-2n} \equiv \frac{1}{p^j} \sum_{1 \leq i < p^j, p \nmid i} i^{2n} \pmod{\mathbb{Z}_p}.$$

Taking the limit  $j \rightarrow \infty$  we obtain

$$\lambda_n \equiv \lambda'_n := \int_{\mathbb{Z}_p^\times} x^{2n} dx \pmod{\mathbb{Z}_p}.$$

But it is possible to compute  $\lambda'_n$  explicitly

$$\lambda'_n = \int_{\mathbb{Z}_p} x^{2n} dx - \int_{p\mathbb{Z}_p} x^{2n} dx = b_{2n} - \int_{p\mathbb{Z}_p} (py)^{2n} d(py).$$

Since  $d(py) = |p| dy = \frac{1}{p} dy$

$$\lambda'_n = (1 - p^{2n-1}) \cdot b_{2n} \equiv b_{2n} \in \frac{1}{p} \mathbb{Z}_p \pmod{\mathbb{Z}_p}$$

[4, p. 177]. In particular  $p\lambda_n \in \mathbb{Z}_p$  which implies that  $|p\lambda_n| \leq 1$ . ■

The preceding estimates let appear that the first term

$$-xy(x+y) \frac{\lambda_1}{2} \in \begin{cases} xy(x+y) \cdot \mathbb{Z}_p & \text{for } p > 3, \\ xy(x+y) \cdot \frac{1}{3} \mathbb{Z}_3 & \text{for } p = 3, \end{cases}$$

in the sum of (2), prevails over all other terms. In fact, the second one

$$-\frac{\lambda_2}{4} xy(x+y) \cdot (x^2 + xy + y^2)$$

already belongs to  $p^2 \lambda_2 xy(x+y) \cdot \mathbb{Z}_p$  ( $p \geq 3$ ) and since  $p\lambda_2 \in \mathbb{Z}_p$  it is always an element of  $p \cdot xy(x+y) \cdot \mathbb{Z}_p$ . Notice that the denominator of  $\lambda_2$  and  $b_4$  is equal to 30. Hence for  $p > 5$  the second term even belongs to  $p^2 \cdot xy(x+y) \cdot \mathbb{Z}_p$ .

In order to say something relevant about the next terms

$$-\frac{\lambda_n}{2n(2n+1)} \cdot p^{2n-2} a_{2n-2}(x/p, y/p) \cdot xy(x+y)$$

appearing in the sum, let us state the following lemma.

LEMMA 2. For  $n \geq 2$  we have

$$\left| \frac{\lambda_n}{2n(2n+1)} \cdot p^{2n-2} \right| < 1.$$

PROOF. The case  $n = 2$  has been treated before. Let us write

$$\left| \frac{\lambda_n}{2n(2n+1)} \cdot p^{2n-2} \right| = \left| \frac{p\lambda_n}{2n(2n+1)} \cdot p^{2n-3} \right| \leq \left| \frac{1}{2n(2n+1)} \cdot p^{2n-3} \right|$$

and discuss the exponent of  $|p|$  in this last expression. Recall that  $\text{ord}_p(n!) = (n - S_p(n))/(p - 1) \leq (n - 1)/(p - 1)$  (where  $S_p(n)$  is the sum of the digits in the base  $p$  representation of  $n$ ). Thus

$$\text{ord}_p \left( \frac{p^{2n-3}}{2n(2n+1)} \right) \geq \text{ord}_p \left( \frac{p^{2n-3}}{(2n+1)!} \right) \geq 2n - 3 - \frac{2n}{p-1} \geq n - 3$$

if  $p \geq 3$ . This proves the assertion for  $n \geq 3$  while for  $n = 2$  we need only examine  $|p/(4 \cdot 5)| \leq 1$  for  $p \geq 3$ . ■

Finally, taking

$$x = kp, \quad y = (n - k)p, \quad x + y = np,$$

(all in  $p\mathbb{Z}_p$  if  $n$  and  $k$  are integers) we obtain the supercongruences of Kazandzidis.

## 2. Application to Legendre polynomials.

The Legendre polynomials  $P_n(\xi)$  can be defined as coefficients of the generating function

$$\frac{1}{\sqrt{1 - 2\xi x + x^2}} = \sum_{n \geq 0} P_n(\xi) x^n.$$

Carrying out the substitution  $\xi = 1 + 2t$ , we obtain [5] the following explicit formula for the polynomial  $P_n(1 + 2t)$

$$P_n(1 + 2t) = \sum_{k=0}^n \binom{n}{k} \binom{n+k}{k} t^k.$$

These polynomials verify remarkable congruences: the so-called *congruences of Honda* [6, 7] which can be stated as follows

$$1) \quad P_{np-1}(1 + 2t) \equiv P_{n-1}(1 + 2t^p) \pmod{np\mathbb{Z}_p[t]} \quad (n \geq 1),$$

$$2) \quad P_{np}(1 + 2t) \equiv P_n(1 + 2t^p) \pmod{np\mathbb{Z}_p[t]} \quad (n \geq 0).$$

Now let  $Q_n(t) \in \mathbb{Z}[t]$  be the polynomials defined by

$$Q_n(t) := P_n(1 + 2t) + P_{n-1}(1 + 2t) \quad (n \geq 1),$$

so that, by the Honda congruences, we have

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{np\mathbb{Z}_p[t]}.$$

Using the results of Kazandzidis, we shall establish that the last expression is actually a supercongruence. More precisely, one can state:

**THEOREM.** *For  $p$  odd and for all integers  $n \geq 1$  the following polynomial supercongruence holds*

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{n^2 p^2 \mathbb{Z}_p[t]}.$$

PROOF. Using the explicit formula for  $P_n(1+2t)$ , we find

$$Q_{np}(t) - Q_n(t^p) = \sum_{k=0}^{np} \binom{np}{k} \binom{np+k}{k} t^k + \sum_{k=0}^{np-1} \binom{np-1}{k} \binom{np+k-1}{k} t^k - \sum_{k=0}^n \binom{n}{k} \binom{n+k}{k} t^{pk} - \sum_{k=0}^{n-1} \binom{n-1}{k} \binom{n+k-1}{k} t^{pk}.$$

Now put

$$Q_{np}(t) - Q_n(t^p) = \sum_{k=0}^{np} q_k t^k,$$

then, for the coefficient  $q_k$ , we get

a)  $q_0 = 0.$

b) If  $k \geq 1$  is prime to  $p$ , then

$$\begin{aligned} q_k &= \binom{np}{k} \binom{np+k}{k} + \binom{np-1}{k} \binom{np+k-1}{k} = \\ &= \frac{np}{k} \binom{np-1}{k-1} \cdot \left\{ \binom{np+k-1}{k-1} + \binom{np+k-1}{k} \right\} + \\ &+ \left\{ \binom{np}{k} - \binom{np-1}{k-1} \right\} \frac{np}{k} \binom{np+k-1}{k-1} = \\ &= \frac{np}{k} \binom{np-1}{k-1} \binom{np+k}{k} + \frac{np}{k} \binom{np-1}{k} \binom{np+k-1}{k-1} = \\ &= 2 \frac{n^2 p^2}{k^2} \binom{np-1}{k-1} \binom{np+k-1}{k-1}, \end{aligned}$$

and therefore

$$q_k \equiv 0 \pmod{n^2 p^2 \mathbb{Z}_p}.$$

c) Now the coefficient  $q_{pk}$ , with  $k < n$ , is

$$\begin{aligned} q_{pk} &= \binom{np}{kp} \binom{np+kp}{kp} - \binom{n}{k} \binom{n+k}{k} + \binom{np-1}{kp} \binom{np+kp-1}{kp} - \\ &- \binom{n-1}{k} \binom{n+k-1}{k} = \frac{2n}{n+k} \cdot \left\{ \binom{np}{kp} \binom{np+kp}{kp} - \binom{n}{k} \binom{n+k}{k} \right\}. \end{aligned}$$

By virtue of Kazandzidis supercongruences, there exist two  $p$ -adic integers  $u, v \in \mathbb{Z}_p$  such that

$$\begin{aligned}
 q_{pk} &= \frac{2n}{n+k} \left\{ \binom{n}{k} + up^2 nk(n-k) \binom{n}{k} \right\} \\
 &\cdot \left\{ \binom{n+k}{k} + vp^2 (n+k) kn \binom{n+k}{k} \right\} - \frac{2n}{n+k} \binom{n}{k} \binom{n+k}{k} \equiv \\
 &\equiv 2n^2 p^2 \left\{ u(n-k) \binom{n}{k} \binom{n+k-1}{k-1} + vk \binom{n}{k} \binom{n+k}{k} \right\} \pmod{n^3 p^2 \mathbb{Z}_p} \equiv \\
 &\equiv 2n^3 p^2 \left\{ u \binom{n-1}{n-k-1} \binom{n+k-1}{k-1} + v \binom{n-1}{k-1} \binom{n+k}{k} \right\} \pmod{n^3 p^2 \mathbb{Z}_p} \equiv \\
 &\equiv 0 \pmod{n^3 p^2 \mathbb{Z}_p}.
 \end{aligned}$$

This congruence is even stronger than the one we had to establish.

d) Finally, once again with the help of Kazandzidis, we treat the term  $q_{np}$

$$q_{np} = \binom{2np}{np} - \binom{2n}{n} \equiv 0 \pmod{p^2 2n \cdot n \cdot n} \binom{2n}{n} \mathbb{Z}_p \equiv 0 \pmod{2n^3 p^2 \mathbb{Z}_p}.$$

This concludes the proof of the theorem.  $\blacksquare$

In this proof we have used the identities

$$\begin{aligned}
 \binom{A}{B} \binom{A+B+2}{B+1} + \binom{A}{B+1} \binom{A+B+1}{B} &= 2 \frac{A+1}{B+1} \binom{A}{B} \binom{A+B+1}{B}, \\
 \binom{A}{B} \binom{A+B}{B} + \binom{A-1}{B} \binom{A+B-1}{B} &= 2 \frac{A}{B} \binom{A}{B} \binom{A+B}{B}.
 \end{aligned}$$

## BIBLIOGRAPHY

- [1] G. S. KAZANDZIDIS, *A commentary on Lagrange's congruence*, D. Phil. Thesis, Oxford University 1948, published version: Dept. of Mathematics, University of Ioannina, 1970.
- [2] G. S. KAZANDZIDIS, *Congruences on the binomial coefficients*, Bull. Soc. Math. Grèce, (N.S.) **9**, 1968, pp. 1-12.
- [3] G. S. KAZANDZIDIS, *On congruences in number theory*, Bull. Soc. Math. Grèce, (N.S.) **10**, fasc. 1 (1969), pp. 35-40.
- [4] W. H. SCHIKHOF, *Ultrametric Calculus-An Introduction to  $p$ -Adic Analysis*, Cambridge Studies in Advanced Mathematics, 4, Cambridge University Press (1984).
- [5] A. ROBERT, *Polynômes de Legendre mod 4*, Comptes Rendus Acad. Sci. Paris, **316**, Série I (1993), pp. 1235-1240.
- [6] T. HONDA, *Two congruence properties of Legendre polynomials*, Osaka J. Math., **13** (1976), pp. 131-133.
- [7] M. ZUBER, *Propriétés  $p$ -adiques de polynômes classiques*, Thèse, Université de Neuchâtel (1992).
- [8] E. ARTIN, *Collected Works*, Addison-Wesley (1965).

Manoscritto pervenuto in redazione il 20 giugno 1994  
e, in forma revisionata, il 5 settembre 1994.