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>

REND. SEM. MAT. UNIV. PADOVA, Vol. 94 (1995)

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

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

$$\binom{3n}{3k} \equiv \binom{n}{k} \quad \bmod 3^2 \cdot n \cdot k \cdot (n-k) \cdot \binom{n}{k} \mathbb{Z}_3 \qquad (p = 3),$$

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 Γ_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]

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

(*) 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 $\binom{np}{kp}\Big/\binom{n}{k}$ as a quotient of p-adic units. Furthermore, the fonction Γ_p satisfies the inequality

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

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

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

This implies that the p-adic logarithm of Γ_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]

$$\Gamma_p(x)\cdot\Gamma_p(1-x) = (-1)^{R(x)}, \qquad (x \in \mathbb{Z}_p,\ 1 \leqslant R(x) \leqslant p,\ R(x) \equiv x \bmod p),$$

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

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

with coefficients λ_n defined by

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

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

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

(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 λ_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

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

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

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

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

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

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

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

PROOF. Recall the definition

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

Now, both terms of the congruence

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

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

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

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

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

But it is possible to compute λ_n' explicitely

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

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

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

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

The preceding estimates let appear that the first term

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

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 $p^2\lambda_2 xy(x+y)\cdot\mathbb{Z}_p$ ($p \geqslant 3$) 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 λ_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 $n \geqslant 2$ 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

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

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

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

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

Finally, taking

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

(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

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

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

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

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

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

so that, by the Honda congruences, we have

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

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 $n \geqslant 1$ the following polynomial supercongruence holds*

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

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 $k \geqslant 1$ is prime to p, then

$$q_k = \binom{np}{k}\binom{np+k}{k} + \binom{np-1}{k}\binom{np+k-1}{k} =$$

$$= \frac{np}{k}\binom{np-1}{k-1} \cdot \left\{\binom{np+k-1}{k-1} + \binom{np+k-1}{k}\right\} +$$

$$+ \left\{\binom{np}{k} - \binom{np-1}{k-1}\right\} \frac{np}{k}\binom{np+k-1}{k-1} =$$

$$= \frac{np}{k}\binom{(np-1}{k-1}\binom{np+k}{k} + \frac{np}{k}\binom{np-1}{k}\binom{np+k-1}{k-1} =$$

$$= 2\,\frac{n^2p^2}{k^2}\binom{np-1}{k-1}\binom{np+k-1}{k-1},$$

and therefore

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

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

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

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

$$q_{pk} = \frac{2n}{n+k}\left\{\binom{n}{k} + up^2 nk(n-k)\binom{n}{k}\right\} \cdot$$

$$\cdot\left\{\binom{n+k}{k} + vp^2(n+k)kn\binom{n+k}{k}\right\} - \frac{2n}{n+k}\binom{n}{k}\binom{n+k}{k} \equiv$$

$$\equiv 2n^2p^2\left\{u(n-k)\binom{n}{k}\binom{n+k-1}{k-1} + vk\binom{n}{k}\binom{n+k}{k}\right\} \bmod n^3p^2\mathbb{Z}_p \equiv$$

$$\equiv 2n^3p^2\left\{u\binom{n-1}{n-k-1}\binom{n+k-1}{k-1} + v\binom{n-1}{k-1}\binom{n+k}{k}\right\} \bmod n^3p^2\mathbb{Z}_p \equiv$$

$$\equiv 0 \bmod n^3p^2\mathbb{Z}_p \,.$$

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}

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

This concludes the proof of the theorem. ∎

In this proof we have used the identities

$$\binom{A}{B}\binom{A+B+2}{B+1} + \binom{A}{B+1}\binom{A+B+1}{B} = 2\,\frac{A+1}{B+1}\binom{A}{B}\binom{A+B+1}{B},$$

$$\binom{A}{B}\binom{A+B}{B} + \binom{A-1}{B}\binom{A+B-1}{B} = 2\,\frac{A}{B}\binom{A}{B}\binom{A+B}{B}.$$

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.