LUCIEN VAN HAMME

The p-adic gamma function and the congruences of Atkin and Swinnerton-Dyer

Groupe de travail d'analyse ultramétrique, tome 9, nº 3 (1981-1982), exp. nº J17, p. J1-J6
<http://www.numdam.org/item?id=GAU_1981-1982__9_3_A18_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE G. CHRISTOL, P. ROBBA)
9e année, 1981/82, fasc. 3, n° J17, 6 p.
Journée d'Analyse p-adique
[1982. Marseille-Luminy]

THE p-ADIC GAMMA FUNCTION AND THE CONGRUENCES OF ATKIN AND SWINNERTON-DYER

by Lucien VAN HAMME (*)

[Vrije Universiteit Brussel]

1. Introduction.

The p-adic gamma function is defined as follows.

Whrite

$$\Gamma_p(n) = (-1)^n \prod_{\substack{i=1 \\ (i,p)=1}}^{n-1} i \quad \text{for } n \in \underset{\sim}{N} , \quad n \geqslant 2 .$$

The sequence $n \longrightarrow \Gamma_p(n)$ is the restriction of a continuous function $\Gamma_p : \underset{\sim}{Z} \longrightarrow \underset{\sim}{Z}_p^*$ which is, by definition, the p-adic gamma function.

We will need the following properties of this function [5] :

If $x \equiv y \pmod{p^r}$, then $\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^r}$.

If $p \neq 2$, then $\Gamma_p(x)\,\Gamma_p(1-x) = (-1)^{R(x)}$ where $R(x)$ is the representative of x mod p in the set $\{1 , 2 , \ldots , p\}$.

We will discuss the following two formulas.

FORMULA 1. - If p is a prime number of the form $p = 1 + 3m$, $m \in \underset{\sim}{N}$, then

$$\Gamma_p(\tfrac{1}{3})^3 = \frac{a + \sqrt{-3}\, b}{2} \tag{F.1}$$

where a and b are integers defined by the conditions $4p = a^2 + 3b^2$, $b \equiv 0 \pmod 3$, $a \equiv +1 \pmod 3$ and $a \equiv \sqrt{-3}\, b \pmod p$.

FORMULA 2. - If p is a prime number of the form $p = 1 + 4m$, $m \in \underset{\sim}{N}$, then

$$\Gamma_p(\tfrac{1}{4})^2 = -\,i(a + ib) \tag{F.2}$$

where $i^2 = -1$, $i \equiv (\frac{p-1}{2})! \pmod p$, and a and b are integers defined by the conditions $p = a^2 + b^2$, $a \equiv 1 \pmod 4$ and $a \equiv ib \pmod p$.

The formulas (F.1) and (F.2) can be proved in several ways. They are both special

---

(*) Lucien VAN HAMME, Faculty of applied Sciences, Vrije Universiteit Brussel, 2 Pleinlaan, B-1050 BRUSSEL (Belgique).

cases of the formula of Gross-Koblitz ([3], [5]), and they can also be deduced from the p-adic version of the formula of Chowla-Selberg (formula (4.12) of [3] and (3.10) of [4]).

The purpose of this note is to prove the formulas by means of the congruences of Atkin and Swinnerton-Dyer.

The fact that the values of the p-adic gamma function are related to certain elliptic curves is hardly suprising since the (complex) formula of Chowla-Selberg shows that there is a relation between the (complex) gamma function and elliptic functions.

We will only give the detailed proof of (F.1). The proof of (F.2) is similar.

2. The congruences of Atkin and Swinnnerton-Dyer.

THEOREM [1]. - *Let* $p \neq 2$ *or* 3 *and let* $y^2 = x^3 - Bx - C$ *be an elliptic curve over* $\mathbb{F}_p$, *the field of* p *elements. Let* $x = t^{-2} + \sum_{n=-1}^{\infty} c(n)\, t^n$ *be any expansion, with* $y = t^{-3} + \dots$, *and write*

$$-\frac{1}{2y}\frac{dx}{dt} = 1 + \sum_{n=1}^{\infty} a(n)\, t^{n-1} \quad B, C, c(n), a(n) \in \mathbb{Z}_p .$$

Then $a(np) - A\, a(n) + p\, a(\frac{n}{p}) \equiv 0 \pmod{p^{r+1}}$, *if* $n \equiv 0 \pmod{p^r}$, *where*

$$a(\tfrac{n}{p}) = \begin{cases} 0 & \text{if } p \nmid n \\ a(\frac{n}{p}) & \text{if } p \mid n \end{cases}$$

and $p - A = N_p =$ *the number of points on the affine curve.*

3. Proof of (F.1).

We now apply the theorem of Atkin and Swinnerton-Dyer to the curve

(1) $$y^2 = x^3 + \frac{1}{4} .$$

In order to simplify the calculations, we replace y by $y + \frac{1}{2}$, and write the equation in the form

(2) $$y^2 + y = x^3 .$$

If we put $t = \frac{x}{y}$ (the local parameter at 0) and $s = \frac{1}{y}$, the equation (2) gives

(3) $$s + s^2 = t^3 .$$

Hence

$$s = t^3 \sum_{m=0}^{\infty} \frac{(-1)^m}{m+1} \binom{2m}{m} t^{3m} .$$

Since $y = \frac{1+s}{t^3}$ and $x = \frac{1+s}{t^2}$, we know the expansions of x and y.
However, what we really need are the coefficients in the expansion of

$$\omega = -\frac{\frac{dx}{dt}}{2y+1} = -\frac{s\frac{dx}{dt}}{2+s}$$

Now $xs = t$, $\frac{dx}{dt}s + x\frac{ds}{dt} = 1$ and from (3) we have $\frac{ds}{dt} = \frac{3t^2}{1+2s}$. Hence

$$\omega = \frac{x\frac{ds}{dt} - 1}{2+s} = \frac{1}{2+s}\left[\frac{3t^3}{s(1+2s)} - 1\right] = \frac{1}{1+2s} = \pm\frac{1}{\sqrt{1+4t^3}} .$$

Since the constant term of ω is $+1$, we must take the $+$ sign.

Hence

$$\omega = \sum_{m=0}^{\infty} (-1)^m \binom{2m}{m} t^{3m} ,$$

and

$a(n) = 0$ if $n \not\equiv 1 \pmod 3$,

$a(n) = (-1)^m \binom{2m}{m}$ if $n = 1 + 3m$.

Let p be a prime number, $p \equiv 1 \pmod 3$. Put $p^r = 1 + 3m_r$. Hence

(4) $$m_0 = 0 , \quad m_{r+1} = p\, m_r + m_1 .$$

If we apply the theorem of Atkin and Swinnerton-Dyer with $n = p^r$ we get, for $r \geq 1$,

$$a(1 + 3m_{r+1}) - A\, a(1 + 3m_r) + p\, a(1 + 3m_{r-1}) \equiv 0 \pmod{p^{r+1}}$$

$$(-1)^{m_{r+1}}\binom{2m_{r+1}}{m_{r+1}} - A(-1)^{m_r}\binom{2m_r}{m_r} + p(-1)^{m_{r-1}}\binom{2m_{r-1}}{m_{r-1}} \equiv 0 \pmod{p^{r+1}} .$$

Since m_r is even this simplifies to

(5) $$\binom{2m_{r+1}}{m_{r+1}} - A\binom{2m_r}{m_r} + p\binom{2m_{r-1}}{m_{r-1}} \equiv 0 \pmod{p^{r+1}} , \quad r \geq 1$$

For $r = 0$, we simply get

(6) $$\binom{2m_1}{m_1} \equiv A \pmod p$$

We now turn to the calculation of $A = p - N_p$. We will determine N'_p, the number of points, over $\underset{\sim}{F}_p$, on the <u>projective</u> curve $zy^2 = x^3 + \frac{z^3}{4}$.

Since this curve has one point at infinity $N'_p = N_p + 1$. But N'_p is also the number of points on the projective curve $u^3 + v^3 = w^3$. This follows from the birational transformation

$$x = -\frac{1}{u+v}, \quad y = \frac{\sqrt{-3}}{2}\,\frac{u-v}{u+v}$$

which transforms (1) in $u^3 + v^3 = 1$. Note that $\sqrt{-3} \in \mathbb{F}_p$.

A well-known theorem of Gauss ([2], [6]) states that for $p \equiv 1 \pmod 3$, the number of points on the projective curve $u^3 + v^3 = w^3$ is equal to $p + 1 - a$, where the integer a in determined by the decomposition $4p = a^2 + 3b^2$ and the congruences $a \equiv -1 \pmod 3$, $b \equiv 0 \pmod 3$.

Hence $N_p = p - a$ and the number A in (5) and (6) is equal to a.

Observe that (6) is a classical congruence of Jacobi and Stern.

We now use (5) to calculate $\Gamma_p(\frac{1}{3})^3$.

Let g be a positive integer, and put $h = [\frac{g}{p}]$. Suppose that $[\frac{2g}{p}] = 2[\frac{g}{p}]$, then

$$g! = \prod_{i=1}^{g} i = p^h\, h! \prod_{\substack{i=1\\(i,p)=1}}^{g} i = (-1)^{g+1}\,\Gamma_p(1+g)\, p^h\, h!$$

$$\binom{2g}{g} = \frac{(2g)!}{g!\ g!} = \frac{(-1)^{1+2g}\,\Gamma_p(1+2g)\,p^{2h}(2h)!}{(-1)^{2+2g}\,\Gamma_p(1+g)^2\,p^{2h}(h!)^2}$$

so

$$\binom{2g}{g} = -\binom{2h}{h}\frac{\Gamma_p(1+2g)}{\Gamma_p(1+g)^2}.$$

We use this with $g = m_{r+1}$. From (4), we see that $h = m_r$ and $[\frac{2g}{p}] = 2[\frac{g}{p}]$. Hence

$$\binom{2m_{r+1}}{m_{r+1}} = -\binom{2m_r}{m_r}\frac{\Gamma_p(1+2m_{r+1})}{\Gamma_p(1+m_{r+1})^2}. \tag{7}$$

From the definition of m_{r+1}, it is clear that $m_{r+1} \equiv -\frac{1}{3} \pmod{p^{r+1}}$.

Using the properties of the p-adic gamma function stated in the introduction, we deduce from (7)

$$\frac{\binom{2m_{r+1}}{m_{r+1}}}{\binom{2m_r}{m_r}} \equiv -\frac{\Gamma_p(\frac{1}{3})}{\Gamma_p(\frac{2}{3})^2} \equiv -\Gamma_p(\tfrac{1}{3})^3 \pmod{p^{r+1}}$$

Substituting in (5), we obtain

$$-\Gamma_p(\tfrac{1}{3})^3 - a - p\,\Gamma_p(\tfrac{1}{3})^{-3} \equiv 0 \pmod{p^r} .$$

If $r \to \infty$, we conclude that $\Gamma_p(\frac{1}{3})^3$ is a root of the equation

$$X^2 + aX + p = 0 . \tag{8}$$

The discriminant of this equation is $a^2 - 4p = -3b^2$, and hence

$$\Gamma_p(\tfrac{1}{3})^3 = \frac{-a \pm b\sqrt{-3}}{2} .$$

Note that one of the roots of (8) is a p-adic unit while the other root is in $p\,\mathbb{Z}_p$. If we fix the sign of $b\sqrt{-3}$ by the congruence $-a \equiv b\sqrt{-3} \pmod{p}$, the root $\frac{-a + b\sqrt{-3}}{2}$ is a p-adic unit. Hence

$$\Gamma_p(\tfrac{1}{3})^3 = \frac{-a + b\sqrt{-3}}{2} .$$

This proves (F.1), where a has been replaced by $-a$.

4. The formula (F.2).

The proof is similar but uses the curve $y^2 = x^3 - x$. Putting $x = ty$ as before, we find

$$-\frac{1}{2y}\,\frac{dx}{dt} = \sum_{m=0}^{\infty} (-1)^m \binom{2m}{m} t^{4m}$$

and

$a(n) = 0$ if $n \not\equiv 1 \pmod{4}$,

$a(n) = (-1)^m \binom{2m}{m}$ if $n = 1 + 4m$.

Putting $p^r = 1 + 4m_r$ and reasoning in the same way as in section 3, we obtain a congruence which has the same form as (5), but where the meaning of A is different. Formula (F.2) can be deduced from this congruence as before. The congruence (6) is now a classical congruence due to Gauss.

REFERENCES

[1] ATKIN (A.) and SWINNERTON-DYER (H.). - Modular forms on noncongruence subgroups, "Combinatorics", p. 1-25. - Providence, American mathematical Society, 1979 (Proceedings of Symposia in pure Mathematics, 19).

[2] GAUSS (C. F.). - Disquisitiones arithmeticae. - New Haven, London, Yale university Press, 1966.

[3] GROSS (B.) and KOBLITZ (N.). - Gauss sums and the p-adic Γ-function, Annals of Math., Series 2, t. 109, 1979, p. 569-581.

[4] GROSS (B.). - On the factorization of p-adic L-series, Invent. Math., Berlin, t. 57, 1980, p. 83-95.

[5] LANG (S.). - Cyclotomic fields, II. - New York, Heidelberg, Berlin, Springer-Verlag, 1980 (Graduate texts in Mathematics, 69).

[6] TATE (J.). - Rational Points on elliptic curves, Philips Lectures, Haverford College, 1961.