JOURNAL OF NUMBER THEORY 24, 188–196 (1986)

On the mod p^2 Determination of $\binom{(p-1)/2}{(p-1)/4}$

S. CHOWLA

School of Mathematics, Institute of Advanced Study, Princeton, New Jersey 08540

B. DWORK

Department of Mathematics, Princeton University, Princeton, New Jersey 08544

AND

RONALD EVANS

Department of Mathematics, University of California, San Diego, La Jolla, California 92073

Communicated November 28, 1984

The Gross–Koblitz formula and a formula of Diamond are used to prove the congruence

$$A \equiv \left(1 + \frac{2^{p-1}-1}{2}\right)\left(2a - \frac{p}{2a}\right) \pmod{p^2}$$

(p a prime number $\equiv 1 \pmod 4$, $p = a^2 + b^2$ ($a, b \in \mathbb{Z}$, $a \equiv 1 \pmod 4$)), proposed by F. Beukers which refines the well-known congruence $A \equiv 2a \pmod p$ for the binomial coefficient

$$A = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

Let p be a rational prime, $p \equiv 1 \bmod 4$. Then p is a sum of squares of integers

$$p = a^2 + b^2, \tag{1}$$

where a is completely specified by the condition that

$$a \equiv 1 \bmod 4. \tag{2}$$

0022-314X/86 $3.00

It is well known [Ch; H, Sect. 10] that the binomial coefficient

$$A = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}$$

satisfies the congruence

$$A \equiv 2a \bmod p. \tag{3}$$

The main point in the classical proof of (3) is Lemma 2.8 summarizing basic properties of the Jacobi sum, B, defined by (2.7). The proof of (3) may then be completed by a mod p relation between B and A. This can be achieved either by Stickelbergers characterization of gauss sums [H – D] or by an examination of the number, N, of $\mathbb{F}_p$-rational points on the elliptic curve

$$Y^2 + X^4 + 1 = 0. \tag{4}$$

The number N can be computed precisely in terms of B and also can be computed mod p by either the Jacobsthal sum,

$$\sum_{x \in \mathbb{F}_p} (1 + x^4)^{(p-1)/2} \tag{5}$$

or by showing that A is the Hasse invariant of the curve. We shall make no use of (4).

In modern times Stickelberger's characterization has been largely replaced by the Gross–Koblitz formula [Boy, Dw, L]. This method will be used to prove a refinement of (3), proposed by F. Beukers,

$$A \equiv \left(1 + \frac{2^{p-1}-1}{2}\right)\left(2a - \frac{p}{2a}\right) \bmod p^2 \tag{6}$$

and hence

$$A^2 \equiv 2^p c \bmod p^2, \tag{7}$$

where

$$p^2 = c^2 + d^2, \qquad d \neq 0, c \equiv 1(4).$$

Aside from the Gross–Koblitz formula the main ingredient of the present work is Diamond's formula [Di; Dw, p. 285] for the value of Γ_p'/Γ_p at elements of

$$\mathbb{Z}_p \cap \mathbb{Q}.$$

Notation.

$\mathbb{C}_p$ = competion of the algebraic closure of $\mathbb{Q}_p$.

$|\ |$ = valuation on $\mathbb{C}_p$ normalized by $|p| = 1/p$.

$$R = \bigcup_{t=0}^{p-1} D(-t, \rho^{-}).$$

$$D(-t, \rho^{-}) = \{x \in \mathbb{C}_p \mid |x+t| < \rho\}$$

Rep-$x = t$ if $t \in \{0, 1, ..., p-1\}$, $x \in D(-t, \rho)$.

$1/\rho = p^{(1/p + 1/(p-1))} < p$.

Γ_p = p-adic gamma function.

$G = \Gamma_p'/\Gamma_p$.

π = root in $\mathbb{C}_p$ of $x^{p-1} + p = 0$.

ζ_p = pth root of unity, $\zeta_p \equiv 1 + \pi \bmod \pi^2$.

$\bar{x} \to$ Teich $\bar{x}$ is the lifting of $\mathbb{F}_p$ into elements of $\mathbb{Z}_p$ satisfying $x^p = x$.

log denotes the (Iwasawa) p-adic log defined on $\mathbb{C}_p^*$ by $\log p = 0$, $\log x = 0$ if x is root of unity, $\log x + \log y = \log xy$, and

$$-\log(1-x) = \sum_{n=1}^{\infty} x^n/n \qquad \text{if} \quad |x| < 1.$$

μ_m = group of mth roots of unity in $\mathbb{C}_p$.

1. P-adic Gamma Function

We recall [Dw, Chap. 21] the p-adic gamma function is locally analytic on a disjoint union, R, of disks $D(-t, \rho)$ in $\mathbb{C}_p$ which contains $\mathbb{Z}_p$ as a proper subset. In particular

$$\Gamma_p(0) = 1, \tag{1.1}$$

$$\Gamma_p(1+x)/\Gamma_p(x) = \begin{cases} -x & \text{if } |x| = 1, \\ -1 & \text{if } |x| < 1, \end{cases} \tag{1.2}$$

$$|\Gamma_p(x)| = 1, \tag{1.3}$$

$$\Gamma_p(x)\,\Gamma_p(1-x) = -(-1)^t \qquad \text{if} \quad x \in D(-t, \rho^{-}),\ t = 0, 1, ..., p-1. \tag{1.4}$$

$$\Gamma_p^{(s)}(x) \in \mathbb{Q}_p \qquad \text{for all} \quad x \in \mathbb{Z}_p,\ s \in \mathbb{N}. \tag{1.5}$$

Property (1.5), known to Morita [M], may also be deduced from Eq. (21.4.5) [Dw].

For $a \in \mathbb{Q} \cap \mathbb{Z}_p$, $t = \text{Rep} - a$, we define a',

$$pa' - a = t.$$

Then $G = \Gamma_p'/\Gamma_p$ may be evaluated at a by

$$G(a) - G(1) = \sum_{\substack{z^d = 1 \\ z \neq 1}} ((z^{da} - 1) - p^{-1}(z^{da'} - 1)) \log(1 - z), \tag{1.6}$$

where log denotes the Iwasawa extension of log to $\mathbb{C}_p^*$ and d is the denominator of a.

2. Gauss Sums in $\mathbb{F}_p$

For $\pi^{p-1} = -p$, ζ_p a primitive pth root of unity in $\mathbb{C}_p$ such that $\zeta_p \equiv 1 + \pi \bmod \pi^2$ we define a nontrivial additive character, θ, on $\mathbb{F}_p$ by

$$\theta(\bar{t}) = \zeta_p^t, \tag{2.1}$$

where t is any lifting, say Teich $\bar{t}$, to $\mathbb{Z}_p$. For $j \in \mathbb{Z}/(p-1)$ we define the gauss sum

$$g(j) = -\sum_{t \in \mu_{p-1}} \zeta_p^t t^{-j} (\in \mathbb{Q}(\zeta_p, \zeta_{p-1})). \tag{2.2}$$

We define

$$\text{Conj } g(j) = -\sum \zeta_p^{-t} t^j = g(-j)(-1)^j. \tag{2.3}$$

As is well known

$$\text{Conj } g(j) \cdot g(j) = p. \tag{2.4}$$

We recall the Gross–Koblitz formula for such gauss sums. For $0 \leqslant j \leqslant p-2$,

$$g(j) = \pi^j \Gamma_p\left(\frac{j}{p-1}\right). \tag{2.5}$$

Our object is to study

$$B_0 = -\Gamma_p(\tfrac{1}{4})^2 \, \Gamma_p(\tfrac{1}{2}). \tag{2.6}$$

By Eq. (2.5) we may identify B_0 with B, the Jacobi sum,

$$B = p^{-1} g\left(\frac{p-1}{4}\right)^2 g\left(\frac{p-1}{2}\right). \tag{2.7}$$

(2.8) LEMMA ([H, Sect. 10.6, also [*D–H*]). *B lies in* $\mathbb{Z}[i]$ *and has a representation*

$$B = a + ib, \qquad a, b \in \mathbb{Z}, \tag{2.8.1}$$

where

$$p = a^2 + b^2, \tag{2.8.2}$$

$$a \equiv 1 \bmod 4. \tag{2.8.3}$$

Proof. The number B is a product of biquadratic and quadratic gauss sums and hence lies in $\mathbb{Q}(\zeta_p, \sqrt{-1})$. For $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, the automorphism σ_α of $\mathbb{Q}(\zeta_p, \sqrt{-1})/\mathbb{Q}(\sqrt{-1})$ defined by $\zeta_p \mapsto \zeta_p^\alpha$ maps $g(l(p-1)/4)$ into

$$\sigma_\alpha g\left(l\frac{p-1}{4}\right) = (\text{Teich } \alpha)^{l(p-1)/4} g\left(l\frac{p-1}{4}\right) \tag{2.8.4}$$

and hence B lies in $\mathbb{Q}(i)$. Gauss sums are algebraic integers and hance B is certainly integral at all primes other than those extending p. If we view B as an abstract algebraic number then the two imbeddings of B into $\mathbb{C}_p$ are B_0 and the corresponding imbedding of Conj B. By (2.4), (2.7) we have

$$\text{Conj } B = p/B, \tag{2.8.5}$$

i.e., the two embeddings of B into $\mathbb{C}_p$ are B_0 and p/B_0. Since B_0 is a unit, B is indeed integral at all primes. This estabishes (2.8.1), and (2.8.2) follows from (2.8.5). It only remains to establish (2.8.3).

For $j \in \{1, -1, i, -i\} = \mu_4$, let

$$\alpha_j = \sum \zeta_p^k \in \mathbb{Q}(\zeta_p), \tag{2.8.6}$$

the sum being over all $k \in \mathbb{F}_p^*$ such that $(\text{Teich } k)^{(p-1)/4} = j$. We observe that each α_j is an algebraic integer in $\mathbb{Q}(\zeta_p)$, that

$$\alpha_1 + \alpha_{-1} + \alpha_i + \alpha_{-i} = -1, \tag{2.8.7}$$

while

$$-g\left(\frac{p-1}{4}\right) = \alpha_1 - \alpha_{-1} + i(\alpha_i - \alpha_{-i}), \tag{2.8.8}$$

$$-g\left(\frac{p-1}{2}\right) = \alpha_1 + \alpha_{-1} - (\alpha_i + \alpha_{-i}). \tag{2.8.9}$$

Letting

$$\delta = \alpha_1 \alpha_{-1} - \alpha_i \alpha_{-i},$$
$$\gamma = \alpha_1 + \alpha_{-1},$$

then by (2.8.7), (2.8.9),

$$-g\left(\frac{p-1}{2}\right) = 1 + 2\gamma,$$

while for some $v \in \mathbb{Q}(\zeta_p)$ we have

$$\begin{aligned} g\left(\frac{p-1}{4}\right)^2 &= (\alpha_1 - \alpha_{-1})^2 - (\alpha_i - \alpha_{-i})^2 + iv \\ &= (\alpha_1 + \alpha_{-1})^2 - (\alpha_i + \alpha_{-i})^2 - 4\delta + iv \\ &= -(1 + 2\gamma + 4\delta) + iv. \end{aligned}$$

Since 1, i are linearly independent over $\mathbb{Q}(\zeta_p)$ we now obtain from (2.8.1),

$$pa = (1 + 2\gamma)(1 + 2\gamma + 4\delta), \tag{2.8.10}$$

which shows that in the ring of integers of $\mathbb{Q}(\rho_p)$ we have

$$pa \equiv 1 \bmod 4.$$

Equation (2.8.3) is thus verified.

2.9. *Note.* An alternate proof of (2.8.3) may be based on the fact that the number N' of solutions of (4) in $\mathbb{F}_p^* \times \mathbb{F}_p^*$ is divisible by 8. Explicitly with the notation of (2.8.1),

$$N' = 2 - 2a + \begin{cases} p - 9 & \text{if} \quad p \equiv 1\ (8), \\ p - 5 & \text{if} \quad p \equiv 5\ (8). \end{cases}$$

We shall not pursue this point of view.

3. Calculation of A

We write A in terms of Γ_p. It follows from Eqs. (1.1), (1.2) that for $0 \leqslant n \leqslant p - 1$,

$$n! = (-1)^{n+1} \Gamma_p(1 + n). \tag{3.1}$$

Under this condition Rep-$(1 + n) = p - 1 - n$ and hence by (1.4),

$$n! = 1/\Gamma_p(-n), \qquad 0 \leqslant n \leqslant p - 1. \tag{3.2}$$

Thus

$$A = \left(\frac{p-1}{2}\right)! \Big/ \left(\frac{p-1}{4}\right)!^2 = \Gamma_p\left(\frac{1-p}{4}\right)^2 \Big/ \Gamma_p\left(\frac{1-p}{2}\right). \tag{3.3}$$

For $x_0 \in R$, $|z| < \rho$, we have by Taylor's theorem

$$\Gamma_p(x_0 + z) = \sum_{n=0}^{\infty} a_n z^n \tag{3.4}$$

and by (1.3) and Cauchy's inequality we have

$$|a_n|\, \rho^n \leqslant 1, \qquad \forall n \in \mathbb{N}, \tag{3.5}$$

$$|a_0| = |\Gamma_p(x_0)| = 1.$$

In particular if $|z| \leqslant |p|$ then

$$|a_n z^n| \leqslant (|p|/\rho)^n = |p|^{n(1-(1/p)-(1/(p-1))}. \tag{3.6}$$

Furthermore if x_0 lies in $\mathbb{Z}_p$ then $a_n \in \mathbb{Q}_p$, i.e.,

$$\operatorname{ord} a_n \in \mathbb{Z}. \tag{3.7}$$

and so

$$a_n z^n \equiv 0 \bmod p^{\alpha_n}, \tag{3.8}$$

where α_n is the smallest integer such that

$$\alpha_n \geqslant n\left(1 - \frac{1}{p} - \frac{1}{p-1}\right). \tag{3.9}$$

For $n \geqslant 2$ we have

$$\alpha_n \geqslant \alpha_2 \geqslant 2\left(1 - \frac{1}{p} - \frac{1}{p-1}\right).$$

For $p \geqslant 5$ (as we may assume here)

$$\alpha_2 \geqslant 2. \tag{3.10}$$

We have thus verified for $p \geqslant 5$,

3.11. PROPOSITION. *For $x_0 \in \mathbb{Z}_p$, $|z| \leqslant |p|$ we have*

$$\Gamma_p(x_0 + z) \equiv \Gamma_p(x_o) + z\Gamma_p'(x_0) \bmod p^2.$$

3.11.1. *Note.* This result is based on considerations of ramification and hence may be false for x_0 outside of $\mathbb{Z}_p$.

Applying this proposition to (3.3) and letting

$$A_0 = \Gamma_p(\tfrac{1}{4})^2/\Gamma_p(\tfrac{1}{2}), \tag{3.12}$$

we deduce

$$A \equiv A_0\left(1 + \frac{p}{2}\left(G\left(\frac{1}{2}\right) - G\left(\frac{1}{4}\right)\right)\right) \quad \bmod p^2. \tag{3.13}$$

Since rep $-\frac{1}{2} = (p-1)/2$, Eq. (1.4) shows

$$\Gamma_p\left(\frac{1}{2}\right)^2 = -(-1)^{(p-1)/2} = -1$$

and so

$$A_0 = B_0. \tag{3.14}$$

We deduce from (1.6) that

$$G\left(\frac{1}{4}\right) - G\left(\frac{1}{2}\right) = \left(1 - \frac{1}{p}\right) \sum (z-1)\log(1-z) \tag{3.15}$$

the sum being over $z \in \mu_4$, $z \notin \mu_2$, i.e., $z = i, -i$. The sum then is the same as

$$-\log(1-i) - \log(1+i) + \mathrm{i}(\log(1-i) - \log(1+i)) = -\log 2$$

since $(1-i)/(1+i)$ is a root of unity. We conclude that

$$A/B_0 \equiv 1 + \frac{p}{2}\left(1 - \frac{1}{p}\right)\log 2 \equiv 1 + \frac{1}{2}\log 2^{p-1} \bmod p^2. \tag{3.16}$$

Since $|2^{p-1} - 1| \leqslant |p|$, the series representation gives

$$\log 2^{p-1} \equiv 2^{p-1} - 1 \bmod p^2. \tag{3.17}$$

LEMMA.

$$A \equiv \left(2a - \frac{p}{2a}\right)\left(1 + \frac{2^{p-1}-1}{2}\right) \bmod p^2.$$

Proof. It only remains to compute B_0 in terms of a. It follows from (2.8.5), that

$$B_0 + \frac{p}{B_0} = 2a,$$

i.e., B_0 is determined as the unit fixed point of

$$x \mapsto 2a - \frac{p}{x}.$$

This shows that

$$B_0 \equiv 2a - \frac{p}{2a} \bmod p^2.$$

This completes the calculation.

REFERENCES

[Boy] M. BOYARSKY, *p*-Adic gamma functions and Dwork cohomology, *Trans. Amer. Math. Soc.* **257** (1980), 359–369.

[Ch] S. CHOWLA, "The Riemann hypothesis and Hilbert's Tenth Problem," Gordon & Breach, New York, 1965.

[D-H] H. DAVENPORT AND H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen fallen, *J. Reine Angew. Math.* **172** (1935), 151–182.

[Di] J. DIAMOND, The *p*-adic log gamma and *p*-adic Euler constants, *Trans. Amer. Math. Soc.* **233** (1977), 321–337.

[Dw] B. DWORK, Lectures on *p*-adic differential equations, Springer-Verlag, New York, 1982; GMW 253.

[L] S. LANG, "Cyclotomic Fields II," Springer-Verlag, New York, 1980; GTM 69.

[H] H. HASSE, "Vorlesungen über Zahlentheorie," Springer-Verlag, Berlin, 1950.

[M] Y. MORITA, A *p*-adic analogue on the Γ-function, *J. Fac. Sci. Univ. Tokyo Sect.* 1*A Math.* **22** (1975), 255–266.