TAIWANESE JOURNAL OF MATHEMATICS
Vol. 16, No. 6, pp. 2197-2202, December 2012
This paper is available online at http://journal.taiwanmathsoc.org.tw

AN ELEMENTARY APPROACH TO $\binom{(p-1)/2}{(p-1)/4}$ modulo p^2

Hao Pan

Abstract. We give an elementary proof of the well-known congruence

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \frac{2^{p-1}+1}{2}\left(2a - \frac{p}{2a}\right) \pmod{p^2},$$

where $p \equiv 1 \pmod 4$ is prime and $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$.

Let p be a prime with $p \equiv 1 \pmod 4$. Then we know that p can be uniquely written as $p = a^2 + b^2$ where $a \equiv 1 \pmod 4$ and $b > 0$. A classical result of Gauss says that the binomial coefficient

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p. \tag{1}$$

In fact, using the facts

$$\sum_{x=1}^{p-1} x^k \equiv \begin{cases} -1 \pmod p, & \text{if } p-1 \mid k \\ 0 \pmod p, & \text{if } p-1 \nmid k, \end{cases} \tag{2}$$

and

$$x^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \pmod p \tag{3}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol, we have

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv -\sum_{x=1}^{p-1} x^{\frac{p-1}{2}}(x^2+1)^{\frac{p-1}{2}} \equiv -\sum_{x=1}^{p-1} \left(\frac{x(x^2+1)}{p}\right) \pmod p.$$

Thus (1) immediately follows from the formula (cf. [1, Theorem 6.2.9])

Received February 15, 2012, accepted March 20, 2012.
Communicated by Wen-Ching Li.
2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B65.
Key words and phrases: Binomial coefficient, Legendre symbol.
The author is supported by National Natural Science Foundation of China (Grant No. 10901078).

$$\sum_{x=1}^{p-1}\left(\frac{x(x^2+1)}{p}\right)=-2a. \tag{4}$$

Furthermore, Beukers conjectured a stronger version of (1):

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}\equiv\frac{2^{p-1}+1}{2}\left(2a-\frac{p}{2a}\right) \pmod{p^2}. \tag{5}$$

This conjecture was confirmed by Chowla, Dwork and Evans [2] (or see [1, Theorem 9.4.3]). Chowla, Dwork and Evans' proof doesn't follow the way we did above. In fact, they used the Gross-Koblitz formula, and considered

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}=-\frac{\Gamma_p(\frac{p+1}{2})}{\Gamma_p(\frac{p+3}{4})^2}$$

where Γ_p is the p-adic gamma function.

The Gross-Koblitz formula establishes a natural connection between the p-adic gamma functions and the Gauss sums. However, the Gross-Koblitz formula is a very deep result in the p-adic theory. We may ask whether there exists an elementary proof of (5), which only uses (4). The main purpose of this note is to give such a proof. That is, here we view $\binom{(p-1)/2}{(p-1)/4}$ as the coefficient of x^{p-1} of $x^{\frac{p-1}{2}}(x^2+1)^{\frac{p-1}{2}}$, rather than the product of gamma functions.

Now suppose that $p\equiv 1 \pmod 4$ and $p=a^2+b^2$ with $a\equiv 1 \pmod 4$. We need the following extension of (2):

$$\sum_{x=1}^{p-1}x^{kp}\equiv\begin{cases}p-1 \pmod{p^2}, & \text{if } p-1\mid k\\ 0 \pmod{p^2}, & \text{if } p-1\nmid k.\end{cases} \tag{6}$$

In fact, letting g be a primitive root of p^2, for every $1\le x\le p-1$, there exists $1\le j\le p-1$ such that $g^j\equiv x \pmod p$, i.e., $g^j+pu_j\equiv x \pmod{p^2}$ for some $u_j\in\mathbb{Z}$. Since

$$(g^j+pu_j)^p=g^{jp}+\sum_{l=1}^{p}\binom{p}{l}g^{jl}(pu_j)^{p-l}\equiv g^{jp} \pmod{p^2},$$

(6) easily follows. Thus we get that

$$(p-1)\binom{\frac{p-1}{2}}{\frac{p-1}{4}}\equiv\sum_{x=1}^{p-1}x^{\frac{p(p-1)}{2}}(x^{2p}+1)^{\frac{p-1}{2}}=\sum_{x=1}^{p-1}x^{\frac{p(p-1)}{2}}(x^p+i)^{\frac{p-1}{2}}(x^p-i)^{\frac{p-1}{2}} \pmod{p^2},$$

where $i=\sqrt{-1}$. With help of the fact

$$\binom{p-1}{k}=\prod_{j=1}^{k}\frac{p-k}{k}\equiv(-1)^k \pmod p,$$

we have

$$x^p \pm i = (x \pm i)^p - \sum_{k=1}^{p-1} \binom{p}{k} (\pm i)^k x^{p-k} \equiv (x \pm i)^p + p \sum_{k=1}^{p-1} \frac{(\mp i)^k}{k} x^{p-k} \pmod{p^2}.$$

So

$$\begin{aligned}
&\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x^p + i)^{\frac{p-1}{2}} (x^p - i)^{\frac{p-1}{2}} \\
\equiv &\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} \left((x+i)^p + p \sum_{k=1}^{p-1} \frac{(-i)^k x^{p-k}}{k} \right)^{\frac{p-1}{2}} \cdot \left((x-i)^p + p \sum_{k=1}^{p-1} \frac{i^k x^{p-k}}{k} \right)^{\frac{p-1}{2}} \\
\equiv &\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} \left((x+i)^{\frac{p(p-1)}{2}} + \frac{p(p-1)}{2} (x+i)^{\frac{p(p-3)}{2}} \sum_{k=1}^{p-1} \frac{(-i)^k x^{p-k}}{k} \right) \\
&\cdot \left((x-i)^{\frac{p(p-1)}{2}} + \frac{p(p-1)}{2} (x-i)^{\frac{p(p-3)}{2}} \sum_{k=1}^{p-1} \frac{i^k x^{p-k}}{k} \right) \\
\equiv &\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x^2+1)^{\frac{p(p-1)}{2}} - \frac{p}{2} \sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x-i)^p (x^2+1)^{\frac{p(p-3)}{2}} \sum_{k=1}^{p-1} \frac{(-i)^k x^{p-k}}{k} \\
&- \frac{p}{2} \sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x+i)^p (x^2+1)^{\frac{p(p-3)}{2}} \sum_{k=1}^{p-1} \frac{i^k x^{p-k}}{k} \pmod{p^2}.
\end{aligned}$$

On the other hand, since

$$x^{\frac{p(p-1)}{2}} = \left(x^{\frac{p-1}{2}} - \left(\frac{x}{p}\right) + \left(\frac{x}{p}\right) \right)^p \equiv \left(\frac{x}{p}\right)^p = \left(\frac{x}{p}\right) \pmod{p^2},$$

we have

$$\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x^2+1)^{\frac{p(p-1)}{2}} \equiv \sum_{x=1}^{p-1} \left(\frac{x(x^2+1)}{p} \right) = -2a \pmod{p^2}.$$

And

$$\begin{aligned}
&\sum_{x=1}^{p-1} x^{\frac{p(p-1)}{2}} (x \pm i)^p (x^2+1)^{\frac{p(p-3)}{2}} \sum_{k=1}^{p-1} \frac{(\pm i)^k x^{p-k}}{k} \\
\equiv &\sum_{x=1}^{p-1} x^{\frac{p-1}{2}} (x \pm i) \sum_{j=0}^{\frac{p-3}{2}} \binom{\frac{p-3}{2}}{j} x^{2j} \sum_{k=1}^{p-1} \frac{(\pm i)^k x^{p-k}}{k} \\
\equiv &- i \sum_{j=0}^{\frac{p-5}{4}} \binom{\frac{p-3}{2}}{j} \frac{i^{2j+\frac{p+1}{2}}}{2j+\frac{p+1}{2}} - \sum_{j=0}^{\frac{p-5}{4}} \binom{\frac{p-3}{2}}{j} \frac{i^{2j+\frac{p+3}{2}}}{2j+\frac{p+3}{2}}
\end{aligned}$$

$$-i\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j-\frac{p-3}{2}}}{2j-\frac{p-3}{2}}-\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j-\frac{p-5}{2}}}{2j-\frac{p-5}{2}}\pmod p,$$

where we used (2) in the last step. Clearly,

$$\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j-\frac{p-3}{2}}}{2j-\frac{p-3}{2}}=\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{i^{\frac{p-3}{2}-2j}}{\frac{p-3}{2}-2j}\equiv\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j+\frac{p+1}{2}}}{2j+\frac{p+3}{2}}\pmod p,$$

and similarly

$$\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j-\frac{p-5}{2}}}{2j-\frac{p-5}{2}}\equiv\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{i^{2j+\frac{p+3}{2}}}{2j+\frac{p+1}{2}}\pmod p.$$

Hence we get that

$$(p-1)\binom{\frac{p-1}{2}}{\frac{p-1}{4}}\equiv-2a-4p(-1)^{\frac{p-1}{4}}\sum_{j=0}^{\frac{p-5}{4}}(-1)^j\binom{\frac{p-3}{2}}{j}\left(\frac{1}{4j+1}+\frac{1}{4j+3}\right)\pmod{p^2}.$$

Since $(p-1)^{-1}\equiv-1-p\pmod{p^2}$, it suffices to show that

$$4(-1)^{\frac{p-1}{4}}\sum_{j=0}^{\frac{p-5}{4}}(-1)^j\binom{\frac{p-3}{2}}{j}\frac{1}{4j+1}\equiv\left(\frac{2^{p-1}-1}{p}-2\right)a\pmod p \tag{7}$$

and

$$\sum_{j=0}^{\frac{p-5}{4}}(-1)^j\binom{\frac{p-3}{2}}{j}\frac{1}{4j+3}\equiv-\frac{(-1)^{\frac{p-1}{4}}}{8a}\pmod p. \tag{8}$$

Note that

$$\sum_{j=0}^{n}\binom{n}{j}\frac{(-1)^j}{uj+v}=\int_0^1 t^{v-1}(1-t^u)^n dt=\frac{\Gamma(n+1)\Gamma(\frac{v}{u})}{u\Gamma(\frac{v}{u}+n+1)},$$

and

$$\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{4j+3}=\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^{\frac{p-3}{2}-j}}{4(\frac{p-3}{2}-j)+3}\equiv\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{4j+3}\pmod p.$$

We have

$$2\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{4j+3}\equiv\sum_{j=0}^{\frac{p-3}{2}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{4j+3}=\frac{1}{3\binom{\frac{2p-3}{4}}{\frac{p-3}{2}}}$$

$$\equiv\frac{1}{3\binom{\frac{3p-3}{4}}{\frac{p-3}{2}}}=\frac{\frac{p+3}{4}}{\frac{p-1}{2}}\cdot\frac{\binom{p-1}{\frac{p-1}{4}}}{3\binom{p-1}{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{\frac{p-1}{4}}}\equiv-\frac{(-1)^{\frac{p-1}{4}}}{4a}\pmod p.$$

So (8) is done. Also, by the Chu-Vandermonde identity,

$$\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{4j+1}\equiv-\frac{1}{4}\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\frac{(-1)^j}{\frac{p-1}{4}-j}$$

$$\equiv\frac{(-1)^{\frac{p-1}{4}}}{4p}\sum_{j=0}^{\frac{p-5}{4}}\binom{\frac{p-3}{2}}{j}\binom{p}{\frac{p-1}{4}-j}=\frac{(-1)^{\frac{p-1}{4}}}{4p}\left(\binom{p+\frac{p-3}{2}}{\frac{p-1}{4}}-\binom{\frac{p-3}{2}}{\frac{p-1}{4}}\right)$$

$$=\frac{(-1)^{\frac{p-1}{4}}}{4p}\binom{\frac{p-3}{2}}{\frac{p-1}{4}}\left(\prod_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\frac{p+j}{j}-1\right)\equiv\frac{(-1)^{\frac{p-1}{4}}}{8}\binom{\frac{p-1}{2}}{\frac{p-1}{4}}\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\frac{1}{j}\pmod p.$$

Clearly,

$$2+\sum_{j=\frac{p-1}{4}}^{\frac{p-3}{2}}\frac{1}{j}\equiv 4\sum_{j=\frac{p+3}{4}}^{\frac{p-1}{2}}\frac{1}{4j}\equiv-\frac{4}{p}\sum_{\substack{1\le k\le p-1\\ k\equiv 3\ (\mathrm{mod}\ 4)}}\binom{p}{k}(-1)^k\pmod p.$$

And

$$\frac{4}{p}\sum_{\substack{1\le k\le p-1\\ k\equiv 3\ (\mathrm{mod}\ 4)}}\binom{p}{k}(-1)^k=\frac{i(1-i)^p-2^p-i(1+i)^p}{p}$$

$$=-\frac{2^{\frac{p+1}{2}}(2^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{4}})}{p}=-2\left(2^{\frac{p-1}{2}}-\left(\frac{2}{p}\right)+\left(\frac{2}{p}\right)\right)\cdot\frac{2^{\frac{p-1}{2}}-\left(\frac{2}{p}\right)}{p}$$

$$\equiv-\left(2^{\frac{p-1}{2}}-\left(\frac{2}{p}\right)+2\left(\frac{2}{p}\right)\right)\cdot\frac{2^{\frac{p-1}{2}}-\left(\frac{2}{p}\right)}{p}=-\frac{2^{p-1}-1}{p}\pmod p.$$

Thus we get (7). ■

ACKNOWLEDGMENTS

I am grateful to the anonymous referee for his/her very useful comments on this paper. I also thank Professor Zhi-Wei Sun for his helpful discussions.

REFERENCES

1. B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Wiley, New York, 1998.
2. S. Chowla, B. Dwork and R. Evans, On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$, *J. Number Theory*, **24** (1986), 188-196.

Hao Pan
Department of Mathematics
Nanjing University
Nanjing 210093
P. R. China
E-mail: haopan79@yahoo.com.cn