A simple proof of Jacobi's two-square theorem

1. In a recent note, John A. Ewell [**1**] derives Fermat's two-square theorem:

A prime $p = 4n + 1$ *is the sum of two squares*

from the triple-product identity.

I have observed that from the triple-product identity one can obtain the stronger result due to Jacobi, namely:

THEOREM 1. *The number* $r_2(n)$ *of representations of the positive integer* n *as a sum of two squares is given by*

$$r_2(n) = 4(d_1(n) - d_3(n)),$$

where

$$d_i(n) = \sum_{d|n,\ d\equiv i \pmod 4} 1.$$

2. The triple-product identity is

(1)

$$\prod_{n\geq 1}(1+ax^{2n-1})(1+a^{-1}x^{2n-1})(1-x^{2n}) = \sum_{-\infty}^{\infty} a^n x^{n^2},$$

and this holds for each pair of complex numbera $a,\ x$ with $a \neq 0$ and $|x| < 1$.

Put $-a^2x$ for a, then x for x^2, multiply by a and we obtain the identity, invariant

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX under $a \to -a^{-1}$,

(2)

$$\begin{aligned}(a-a^{-1})\prod_{n\geq 1}&(1-a^2x^n)(1-a^{-2}x^n)(1-x^n)\\ &=\sum_{-\infty}^{\infty}(-1)^n a^{2n+1}x^{(n^2+n)/2}\\ &=\sum_{-\infty}^{\infty}a^{4n+1}x^{2n^2+n}-\sum_{-\infty}^{\infty}a^{4n-1}x^{2n^2-n}\\ &=a\prod_{n\geq 1}(1+a^4x^{4n-1})(1+a^{-4}x^{4n-3})(1-x^{4n})\\ &\quad -a^{-1}\prod_{n\geq 1}(1+a^4x^{4n-3})(1+a^{-4}x^{4n-1})(1-x^{4n}).\end{aligned}$$

Differentiate (2) with respect to a, put $a=1$, divide by 2, and we find

(3)

$$\begin{aligned}\prod_{n\geq 1}(1-x^n)^3=\prod_{n\geq 1}&(1+x^{4n-3})(1+x^{4n-1})(1-x^{4n})\\ &\times\left\{1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right)\right\}.\end{aligned}$$

[The derivative of the infinite product of the left of (2) is unimportant, since it vanishes on substituting $a=1$, while the derivatives of the infinite products on the right of (2) are found from

$$\left(\prod_{n\geq 1}u_n\right)'=\left(\prod_{n\geq 1}u_n\right)\sum_{n\geq 1}\frac{u_n'}{u_n}.]$$

Divide (3) by

$$\prod_{n\geq 1}(1+x^n)^2(1-x^n)=\prod_{n\geq 1}(1+x^n)(1-x^{2n})$$

$$= \prod_{n\geq 1}(1+x^{2n-1})(1+x^{2n})(1-x^{2n})$$

$$= \prod_{n\geq 1}(1+x^{2n-1})(1-x^{4n})$$

$$= \prod_{n\geq 1}(1+x^{4n-3})(1+x^{4n-1})(1-x^{4n}),$$

and we have

(4)

$$\prod_{n\geq 1}\left(\frac{1-x^n}{1+x^n}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Now,

$$\prod_{n\geq 1}\left(\frac{1-x^n}{1+x^n}\right) = \prod_{n\geq 1}\frac{(1-x^{2n-1})(1-x^{2n})}{(1+x^n)}$$

$$= \prod_{n\geq 1}(1-x^{2n-1})(1-x^n)$$

$$= \prod_{n\geq 1}(1-x^{2n-1})(1-x^{2n-1})(1-x^{2n})$$

$$= \sum_{-\infty}^{\infty}(-1)^n x^{n^2},$$

so (4) is

(5)

$$\left(\sum_{-\infty}^{\infty}(-1)^n x^{n^2}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Put $-x$ for x, and we obtain

(6)

$$\left(\sum_{-\infty}^{\infty}x^{n^2}\right)^2 = 1+4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1-x^{4n-3}}-\frac{x^{4n-1}}{1-x^{4n-1}}\right),$$

from which Theorem 1 follows immediately [**2**].

References

1. John A. Ewell, A simple proof of Fermat's two-square theorem, this MONTHLY, 90 (1983) 635-637.

2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Clarendon Press, Oxford, 1960, p. 258.