

A prime is in at most 1 way the sum of 2 squares

EWD1154 dealt with D. Zagier's proof that a prime of the form  $4k+1$  is the sum of 2 squares. In fact, such a prime is in only 1 way the sum of 2 squares. In this note we show this by proving that if an odd  $n$  is the sum of 2 different pairs of squares, then that  $n$  is not prime.

Let an odd  $n$  be the sum of 2 squares; then the one square is odd, the other is even: the squares are of different parity. Let  $n$  be the sum of 2 squares in 2 ways; then there exist positive  $a, b, c, d$  such that

$$\begin{aligned} (0) \quad (a+b)^2 + (c-d)^2 &= n \\ (a-b)^2 + (c+d)^2 &= n \end{aligned}$$

(Here  $a$  is the average of the numbers of the one parity,  $c$  the average of those of the other parity. Because we are considering distinct square decompositions, also  $b$  and  $c$  can be chosen positive.)

Eliminating  $n$  from (0) by equating the left-hand sides, we deduce after simplification

$$(1) \quad ab = cd \quad ,$$

from which we deduce the existence of posi-

tive  $r, s, t, v$  such that

$$\begin{aligned} (2) \quad a &= sv \\ b &= rt \\ c &= st \\ d &= rv \end{aligned}$$

(Consider " $s := a \text{ gcd } c$ ;  $v := a/s$ ;  $t := c/s$ ;  
 $r := b/t$ ".)

Now we observe

$$\begin{aligned} &n \\ = &\{ (0) \} \\ &(a+b)^2 + (c-d)^2 \\ = &\{ (1) \} \\ &a^2 + b^2 + c^2 + d^2 \\ = &\{ (2) \} \\ &s^2v^2 + r^2t^2 + s^2t^2 + r^2v^2 \\ = &\{ \text{algebra} \} \\ &(s^2 + r^2) \cdot (t^2 + v^2) \end{aligned}$$

and because the 4 variables are positive,  
the two factors are each at least 2,  
and hence  $n$  is not a prime number.

\* \* \*

The above was written down in Abilene State Park. In contrast to the proof discussed in EWD1154, I designed this proof myself, but the title of this note does not mention "derivation" of the proof, since I did not

"derive" it in any technical sense.

I have considered investigation of the situation  $x^2+y^2=n \wedge u^2+v^2=n \wedge \text{prime}.n$  with the aim of showing  $(x,y)=(u,v) \vee (x,y)=(v,u)$ , but rejected that approach for the disjunction, and for the fact that I saw no way of using  $n$ 's primality. So I did some shunting and set myself to show that  $n$  was composite by writing it as a product of 2 plurals. I knew my complex numbers, in particular, that the modulus of a product is the product of the moduli, and then discovered that there was no point in looking at  $(x+yi) \cdot (u+vi)$ . Hence

$$(3) (sv-rt)^2 + (st+rv)^2 = (s^2+r^2) \cdot (t^2+v^2)$$

- the 2 expressions for the modulus of  $(s+ri) \cdot (t+vi)$ , which do equate a sum of squares to a product - has to be used differently. The right-hand side being even in  $r$ , it also equals  $(sv+rt)^2 + (st-rv)^2$ , and now we see the  $a, b, c, d$  entering the picture. The introduction of  $a \pm b$  and  $c \pm d$  circumvented the disjunctive complication of comparing unordered pairs.

I think I knew (3) outside the context of complex numbers as well; it is very common to separate in  $(a \pm b)^2$  the squares from the cross product, as in

$$(a+b)^2 = (a-b)^2 + 4ab$$

$$(a+b)^2 + (a-b)^2 = 2(a^2 + b^2)$$

The proof reported provides a striking example of a proof in which the algebra is totally trivial while all subtlety has been invested in the decision what to name.

Austin, 7 June 1993

prof. dr. Edsger W. Dijkstra  
Department of Computer Sciences  
The University of Texas at Austin  
Austin, TX 78712-1188  
USA