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

In EWD1154 we dealt with D. Zagier's proof that a prime of the form $4k+1$ is the sum of 2 squares. For such a prime, this "square decomposition" is, in fact, unique. Here we show this by proving that an odd number is not prime if it is the sum of 2 different pairs of squares. Proving that a number is not prime will be done by rewriting that number as the product of 2 plurals. (A "plural" is a natural number ≥ 2.)

Remark The definition of primality that we use -and which I often found to be the nicest one- is

$$\text{prime.}n \equiv \langle \forall x,y: x\geq 2 \wedge y\geq 2: x\cdot y \neq n \rangle \ ;$$

the existential quantification expressing non-primality is demonstrated by constructing a witness. (End of Remark.)

* * *

There are two distinct aspects to this problem. There is the algebraic aspect of expressing the sum of 2 squares as the product of 2 plurals, and there is the notational question of how to express that a number admits 2 different square decompositions.

Let us look at the algebraic aspect first. The simplest formula I know that equates the sum of 2 squares to a product

(0) $(a+b)^2 + (a-b)^2 = 2\cdot(a^2+b^2)$.

Remark This formula is of independent interest in the context of square decompositions: regardless of primality it establishes for any n a one-to-one correspondence between the square decompositions of n and those of $2n$. (End of Remark.)

We cannot use (0) "as is", for we have to write odd numbers as the sum of 2 squares. So we generalize the left-hand side to $(a+b)^2 + (c-d)^2$, but restrict ourselves to the situations with

(1) $a\cdot b = c\cdot d$,

so that we inherit from (0) that the 2 cross-products cancel:

(2) $a\cdot b = c\cdot d \Rightarrow$
$(a+b)^2 + (c-d)^2 = a^2+b^2+c^2+d^2$.

Note that the right-hand side of the consequent is an even function of the variables. So much for the algebraic aspect.

We now turn to the question of how to express that an odd n admits 2

different square decompositions. Here the problem is that x^2+y^2 and y^2+x^2 count as the same square decompositions. We can, however, exploit that n is odd; hence, when n is written as sum of 2 squares, the one square is odd and the other square is even. Consequently, if odd n admits 2 different square decompositions, we can choose positive a, b, c, d such that

$$(3) \quad (a+b)^2 + (c-d)^2 = n \quad \wedge \quad (a-b)^2 + (c+d)^2 = n \quad .$$

Here a is the average of the numbers of the one parity, and c the average of those of the other parity; because we are considering different square decompositions of n, also b and d can be chosen positive.

Eliminating after this choice n from (3) by equating the left-hand sides, we deduce after simplification $a \cdot b = c \cdot d$, i.e. (1), and then, combining (1), (2), and (3)

$$(4) \quad n = a^2+b^2+c^2+d^2 \quad ,$$

thus reducing our proof obligation to showing that, thanks to (1), the right-hand side of (4) can be factorized as the product of

two plurals.

We meet this last proof obligation in a totally classic manner: we exploit (1), i.e. $a \cdot b = c \cdot d$, by solving the equation

(5) $\quad a,b,c,d \;:\; a \cdot b = c \cdot d \quad ,$

then substitute the general solution into the right-hand side of (4) and look what we can do with the resulting expression.

Multiplication being symmetric and associative, we have for any q, r, s, t

$$(q \cdot r) \cdot (s \cdot t) \;=\; (q \cdot s) \cdot (r \cdot t)$$

and hence, (5) is solved by

(6)
$$\begin{array}{lll} a = q \cdot r & & \text{(i)} \\ b = s \cdot t & & \text{(ii)} \\ c = q \cdot s & & \text{(iii)} \\ d = r \cdot t & & \text{(iv)} \end{array} ,$$

but this observation only tells us that (6) is a particular solution of equation (5), and we need the latter's general solution. We shall now show that (6) is also the general solution of (5) by showing that for <u>any</u> solution of (5), there exist natural q, r, s, t satisfying (6). We show the existence by constructing a witness:

```
   q:= a gcd c   {
;  r:= a/q       {(6) i)
;  s:= c/q       {(6) iii}
;  t:= b/s   (or t:= d/r )   {(6) ii and (6) iv}
```

Because q is a divisor of a and c, q, r, and s are integer; moreover, since q is the greatest common divisor of a and c,

(7) $\qquad r \text{ gcd } s = 1$.

With (i) and (iii) satisfied, we deduce from (1) -and $q \neq 0$-

$$r \cdot b = s \cdot d$$

from which we conclude, in view of (7), that r divides d and that s divides b, and in general - $r \neq 0$ and $s \neq 0$- $b/s = d/r$. So either assignment to t does the job.

And now we are essentially done, for

$$\begin{aligned} & a^2 + b^2 + c^2 + d^2 \\ = & \quad \{(6)\} \\ & (q \cdot r)^2 + (s \cdot t)^2 + (q \cdot s)^2 + (r \cdot t)^2 \\ = & \quad \{\text{algebra}\} \\ & (q^2 + t^2) \cdot (r^2 + s^2) \end{aligned}$$

and the parameters q, r, s, t differing from 0, the factors are plurals.

For devastating comments on an earlier version — gross omissions and major rabbits — I am indebted to the ETAC, to Wim H. Hesselink and Rutger M. Dijkstra. Lex Bijlsma was so kind to retrieve that — apart from less fortunate notation — my proof, originally conceived between Amarillo and Abilene, had also been designed by Euler.

The above argument is reported because it 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, 19 August 1993

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