The following constitutes the essential text of a complete research article; I have omitted only some comments at the end concerning the history of this type of argument. The author reproves a famous result. He builds his proof into a single sentence as simply a tour-de-force. In fact, he has left many straightforward steps for the reader to verify.

1. As an exercise in critical reading, list all the implicit claims that the reader must verify in order to accept this argument as a proof.

2. As an exercise in logic and algebra, supply all the details necessary to support these claims. Package all this as a long-winded rewrite of Zagier's article written so that any high school algebra student could easily read it with comprehension.

You should expect to expand Zagier's single sentence to a full page or more.

A One-Sentence Proof That Every Prime p congruent to 1 modulo 4 Is a Sum of Two Squares

D. Zagier

Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on a finite set S = {(x,y,z) \in N^3 : x^2 +4yz = p } defined by

```
                      ( x+2z, z, y-x-z )  if   x < y-z
       (x,y,z) ---> { ( 2y-x, y, x-y+z )  if y-z < x < 2y
                      ( x-2y, x-y+z, y )  if   x > 2y
```

has exactly one fixed point, so |S| is odd and the involution defined by

```
       (x,y,z) ---> (x,z,y)
```

also has a fixed point.

Glossary:

Cardinality: We write |S| for the number of elements the set S contains.
This has a clear meaning for a finite set S.

Congruence: We say we have integers a and b congruent modulo n if
n divides a - b. We often abbreviate "modulo" as "mod".