Classroom

In this section of* Resonance, *we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

On Fermat's Two-Square Theorem

Shailesh A Shirali
Rishi Valley School, A. P, India.

Introduction

The purpose of this note is to present a proof of the two-square theorem: *every prime of the form* 1 (mod 4) *can be written as a sum of two squares.* The theorem was first stated by Fermat (as usual, with no proof!) and later proved by Euler. The proof given here is an elaboration of the one presented by Don Zagier in a crisp note that appeared in *The American Mathematical Monthly*, Vol. 97, # 2 (Feb 1990). As Zagier himself remarks in his paper, his proof is not constructive. In the final section we make an interesting conjecture which, if correct, will provide a constructive version of Zagier's proof.

Throughout, p refers to a fixed prime of the form 1 (mod 4), while $\mathbf{N}$ refers to the set of positive integers. For a finite set X, $|X|$ denotes the cardinality of X.

Proof of the Two-Square Theorem

The proof hinges on a study of the solutions in positive integers of the equation $x^2+4yz = p$. Let S_p denote the solution set:

$$S_p = \{(x,y,z) \in \mathbf{N}^3 : x^2+4yz = p\}. \qquad (1)$$

It is easy to verify that S_p is non-empty (for $(1, 1, \frac{p-1}{4}) \in S_p$) and finite. We shall show that $|S_p|$ is odd.

Consider the following relations:

$$x^2+4yz = (x+2z)^2 + 4z(y-x-z) = (2y-x)^2+4y(x-y+z). \quad (2)$$

From this we see that α, β, γ as defined by

$$\alpha(x, y, z) = (x + 2z, z, y-x-z), \quad (3)$$
$$\beta(x, y, z) = (2y-x, y, x-y+z), \quad (4)$$
$$\gamma(x, y, z) = (x-2y, x-y+z, y), \quad (5)$$

are maps of the solution set in real numbers of $x^2 + 4yz = p$ into itself; still better, they are *unimodular* maps – they permute the integer solutions amongst themselves. (This can be checked by observing that the matrices corresponding to the three maps are all unimodular, that is, they have determinant ± 1.) Since our interest lies chiefly in the positive integral solutions, we define subsets A_p, B_p, C_p of S_p as follows:

$$A_p = \{(x,y,z) \in S_p, x < y-z\}, \quad (6)$$
$$B_p = \{(x,y,z) \in S_p, y-z < x < 2y\}, \quad (7)$$
$$C_p = \{(x,y,z) \in S_p, 2y < x\}. \quad (8)$$

We now make the following observations which are easy to verify.

- $S_p = A_p \cup B_p \cup C_p$, that is, A_p, B_p, C_p constitute a *partition* of S_p. Equality cannot hold in any of the defining inequalities because p is prime. Moreover, $(1, 1, \frac{p-1}{4}) \in B_p$.

- α maps A_p into C_p and γ maps C_p into A_p; moreover, α and γ are inverses of one another. Since A_p and C_p are finite sets, it follows that $|A_p| = |C_p|$

- β maps B_p into itself, and β is its own inverse (it is an *involution*), so it pairs up elements of B_p with one another, except possibly for the fixed points–the triples (x, y, z) which get mapped to themselves; these have no mates and stand alone.

- β has just one fixed point. For if (x,y,z) is a fixed point, then $(2y-x, y, x-y+z) = (x,y,z)$, so $x = y$. This gives $p = x(x + 4z)$, implying that $x=1$ and $x + 4z = p$ since p is prime. It follows that $(1,1, \frac{p-1}{4})$ is the sole fixed point of β.

- B_p is odd, for β is an involution on B_p with just one fixed point. In turn this implies that $|S_p|$ is odd (because $|A_p| = |C_p|$).

Observe that for each element $(x,y,z) \in S_p$, its 'mate' (x,z,y) also lies in S_p. Since S_p has an odd number of elements, it follows that S_p must contain an 'odd man out' which is its own 'mate'. If (r, s, s) is such an element of S_p, then $p = r^2+(2s)^2$, and we are through.

Towards a Constructive Proof

Note that the proof presented is not constructive–it provides no clue as to how the desired (r, s) can be computed for a given p. (Curiously, this is true for most known proofs of the theorem.) However the argument used does suggest the possibility of an algorithmic proof. I have empirically found that the following algorithm 'works', in the sense that it always seems to terminate. However I have not been able to devise a proof of termination; if found, then a constructive proof of the two-square theorem is at hand.[1] Perhaps some reader would like to take up the challenge and settle the matter.

Consider the set I_p of integer triples (x,y,z) for which $x^2 + 4yz = p$. The set is non–empty, for $(1,1, \frac{p-1}{4}) \in I_p$. Our objective is to find a triple in I_p of the form (r, s, s); this would immediately

[1] This conjecture has been settled in the affirmative by B Bagchi.

provide the desired representation of p as a sum of two squares ($p=r^2+(2s)^2$). Towards this end we define a function $f: I_p \to I_p$ as follows:

$$f(x,y,z) = \begin{cases} (x+2z, y-z-x, z) & \text{if } z+x<y, \\ (2y-x, z+x-y, y) & \text{if } z+x>y. \end{cases}$$

Example: Let $p=17$; then $f(1,1,4) = (1.4,1)$ and $f(1,4,1) = (3,2,1)$.

We now compute the orbit of the triple $(1,1,\frac{p-1}{4})$ under action by f. If at some stage we reach a triple of the form (r, s, s) we terminate the computation. The curious thing is that we always seem to reach such a triple. Listed below are the initial segments of the orbits for a few p's. In each case we stop when the desired triple is reached.

- $p=17$
  (1, 1, 4) (1, 4, 1), (3, 2, 1), (1, 2, 2); result: $17=1^2+4^2$.
- $p=29$
  (1, 1, 7), (1,7,1), (3,5,1), (5,1,1); result: $29=5^2+2^2$.
- $p=41$
  (1, 1,10), (1, 10, 1), (3, 8, 1), (5, 4, 1), (3, 2, 4), (1, 5,2), (5, 2, 2); result: $41=5^2+4^2$.
- $p=53$
  (1, 1, 13), (1, 13, 1), (3, 11, 1), (5, 7, 1), (7, 1, 1); result: $53=7^2+2^2$.
- $p=109$
  (1, 1, 27), (1, 27, 1), (3, 25, 1), (5, 21, 1), (7, 15, 1), (9, 7, 1), (5, 3, 7), (1, 9, 3), (7, 5, 3), (3, 5, 5); result: $109=3^2+10^2$.

Any takers?

Further Remarks

- Weil writes, in his book (see Suggested Reading) that "all known proofs begin by showing that –1 is a quadratic

residue of $p = 4n + 1$". This being so, Zagier's proof is rather atypical.

- The theorem was stated by Fermat in 1640; he never published any proof but in all likelihood did possess one, probably based on the principle of infinite descent (which itself is one of Fermat's inventions). The first published proof, by Euler, appeared in the 1740's; it too uses the principle of infinite descent.

Suggested Reading

- **Andre Weil.** ***Number Theory: An approach through history*****, 1984.**

Substituent Effect of the Methoxy Group: A Matter of Give and Take

Gurumayum S D Sharma and
S V Eswaran
St. Stephen's College
New Delhi 110 007, India.

Oxygen containing functional groups such as hydroxy (HO^-) and alkoxy (RO^-) groups are present in numerous aromatic compounds. The way these groups affect equilibria and kinetic parameters in different reactions depends on a variety of factors. In some cases the groups act as electron donors but in others as acceptors. The differing behaviour can be understood by considering the nature of the electronic interactions in detail. It is important to distinguish between electronic effects in the σ and π frameworks. Two different case histories are given below which illustrate these points.

Case I: Effect on Equilibria

One of the simplest aromatic carboxylic acids, benzoic acid, can be made stronger or weaker by placing an electron withdrawing or a donating group on the aromatic ring, respectively. A methoxy group with its lone pair of electrons which can be used in conjugation is a good donor. Hence, 4-methoxybenzoic