Karen E smith

May 9, 1965-

Karen was born May 9, 1965, in Red Bank, New Jersey. She had a normal suburban childhood. Only one thing kept her from being the normal child, she loved math. Her biggest influence to came while she was in college. It was there that Karen decided to be a mathematician.

During Karen's math career she has ran into some gender problems. She met many sexist people that put her and her work down. These were not all males either. Women also believed that she was not able to do math. The psychological effect is strong because one needs a lot of confidence in his/her self to prove new theorems. Karen obviously did not let this stop her.

Karen's math deals with characteristic p. This is also known as modular arithmetic or clock arithmetic. For example, we do not say that it is 14 o'clock; we say that it is two o'clock. This is because time is in Mod 12.

People have set standard names for the numbers on a clock. They start with 0 not 1. So let 0 through 11 be the standard names on the twelve-hour clock.

<u>Find the standard names for these numbers on a twelve-hour clock</u>

1. 13
2. 24
3. -5
4. -11

<u>Figure out what these expressions are on a clock.</u>

(While doing this, remember that adding and subtracting work the same as on a number line. For example 4 + 2 =6 is the same in both clock arithmetic, and number line arithmetic, but 6 + 9 = 15 on a number line and 3 in clock arithmetic.)

1. 7 + 5
2. 11 + 11
3. 1 - 9
4. -11 + 7

There is another notation for clock notation. In order to write this as an equation people came up with this emodular arithmetic notation. An example of this can be written as

13 = 1(mod 12)

This means that 13 and 1 are the same numbers on a twelve-hour clock.

True/False

1. The definition of characteristic p is, r * r * _ _ _ * r = 0.
2. Sometimes the answers in ZZp tell you about the original problem.
3. Characteristic p is useful in Fermat’s last theorem, x^n + y^n = z^n because even though we know there are no solutions in positive whole numbers, characteristic p can reduce the number of no solutions that we try out.

Question and Answer

Does the elliptic curve y^2 = x^3 - 2 have any solutions? If so, what are they?

Does the elliptic curve y^2 = x^3 - 3x - 5 have any solutions? If so, what are they?

If you graph y^2 = x^3 - 3x - 5 in the real and complex numbers, what shape does it form?

References:

Cryptography. Internet. Microsoft.com. April 23, 2001.

Karen E. Smith. Internet. April 5, 2001
http://www. agnesscott.edu/lriddle/women/smithk.html

Modular Arithmetic. Internet. April 23, 2001
http://www.math.csusb.edu/faculty/susan/number_bracelets/mod_arith.html