Beauty of Mathematics Decal PSET #9 Solutions

Due 11/15

Let's consider the integers mod 7, which consists of the numbers $\{0, 1, 2, 3, 4, 5, 6\}$.

1. Remember we should be able to divide; so which of these numbers is "1/2"? (That is, which number can we multiply by 2 to get 1?)

Let's compute all the multiples of 2.

0 * 2 = 0 1 * 2 = 2 2 * 2 = 4 3 * 2 = 6 4 * 2 = 1 (of course 4*2=8 but 8 reduces to 1 mod 7) 5 * 2 = 3 (etc.) 6 * 2 = 5

Since 4 * 2 = 1, we see that "1/2" is 4.

2. Some of these numbers are squares, and others are not. Show that 3 is a "square root" of 2, but that 5 has no square root.

Let's compute all the squares.

 $0^{2} = 0$ $1^{2} = 1$ $2^{2} = 4$ $3^{2} = 2$ (of course $3^{2} = 9$, but 9 reduces to 2 mod 7) $4^{2} = 2$ (etc.) $5^{2} = 4$ $6^{2} = 1$

Observe that 5 is not the square of anything, so it has no square root; but $3^2 = 2$ so 3 is a "square root" of 2.

Now let's instead consider the integers mod 6, consisting of $\{0, 1, 2, 3, 4, 5\}$.

3. Show that there is no "1/2" here; that is, multiplying something by 2 will never give 1. Let's compute all the multiples of 2.

$$0 * 2 = 0$$

 $1 * 2 = 2$
 $2 * 2 = 4$
 $3 * 2 = 0$ (of course $3 * 2 = 6$ but 6 reduces to 0 mod 6)
 $4 * 2 = 2$ (etc.)
 $5 * 2 = 4$

We see that nothing multiplies 2 to make 1, so there is no "1/2" here.

Observe that we can't necessarily divide mod 6, but we can divide mod 7. This is because 7 is prime and 6 is not.