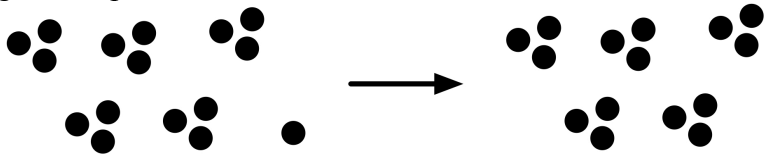
The Hidden Role of Modular Arithmetic

We have seen the mathematical concept of *modular arithmetic* in a number of problems. We saw patterns using remainders in the Take Away Game, and in the pattern game during the first few classes of the quarter.

In the "1,2-take-away game," in which each player must take 1 or 2 counters, and the player taking the last counter wins, we learned that there is a winning strategy based on multiples of 3. This strategy says that the winning move if a player is left with 16 counters is to remove one counter, leaving a multiple of 3.



Or if the player is left with 100 counters, the winning move is again to take one counter, since that also leaves a multiple of 3. In general, the winning move - if possible - always leaves the opponent with a number of counters that is a multiple of 3; if on a player's move the number is already a multiple of 3, then the opponent could win if the opponent is aware of this strategy, since on that turn the player must leave a number of counters that is either 1 or 2 more than the next lower multiple of 3.

We say that $16 \equiv 100 \pmod 3$, which is read "*16 is congruent to 100, mod 3*," because 16 and 100 both leave remainder 1 when divided by the *modulus* 3:

$$16 = 3 \bullet 5 + 1$$
$$100 = 3 \bullet 33 + 1$$

In general, $a \equiv b$ (mod m) means that when you divide *a* by *m* you get the same remainder that you get when you divide *b* by *m*.
The "≡" symbol is not an equal sign, but is read "is congruent to" (since after all 16 is not equal to 100!)

(1) If there are 23 counters left in the 1,2-take-away game, then the winning move at this point is to remove _____ counters.

Note that, for example, $0 \equiv 6 \pmod 3$, because both 0 and 6 both leave a remainder of 0 when divided by 3.

(2) Why is 0 considered to be a "multiple of 3?" _____

Another way to see that 100 and 16 leave the same remainder when divided by 3 is to notice that their difference 100 – 16 = 84 is a multiple of 3.

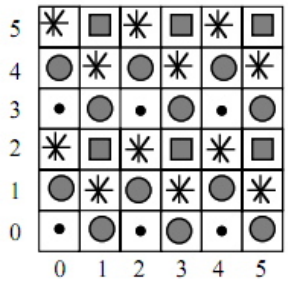
To test whether $a \equiv b$ (mod m) check that $a - b$ is divisible by m.

A way to see that this rule is true in the case of 16 and 100, with respect to modulus 3, is that

$$100 - 16 = (3 \cdot 33 + 1) - (3 \cdot 5 + 1) = 3 \cdot 33 - 3 \cdot 5 + 1 - 1 = 3(33 - 5) = 3 \cdot 28$$

We also examined the 1,2,3 take-away game, in which each player may remove 1, 2, or 3 counters on each turn. In that game we found that the winning strategy is always to leave the opponent with a number of counters that is a multiple of 4. In this case we look at the remainder when a number of counters is divided by 4 and that tells us how many to remove on that turn. Of course, if the remainder is 0, then the number is a multiple of 4 already, and we have to hope that our opponent is not aware of the strategy!

In the pattern game we saw the pattern at the right that repeats every second column and every third row.



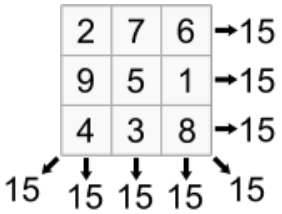
Assume the same pattern continues throughout the plane.
(3) Which symbol would be found in box (0,28)? _____

(4) Which symbol would be found in box (0,100)? _____

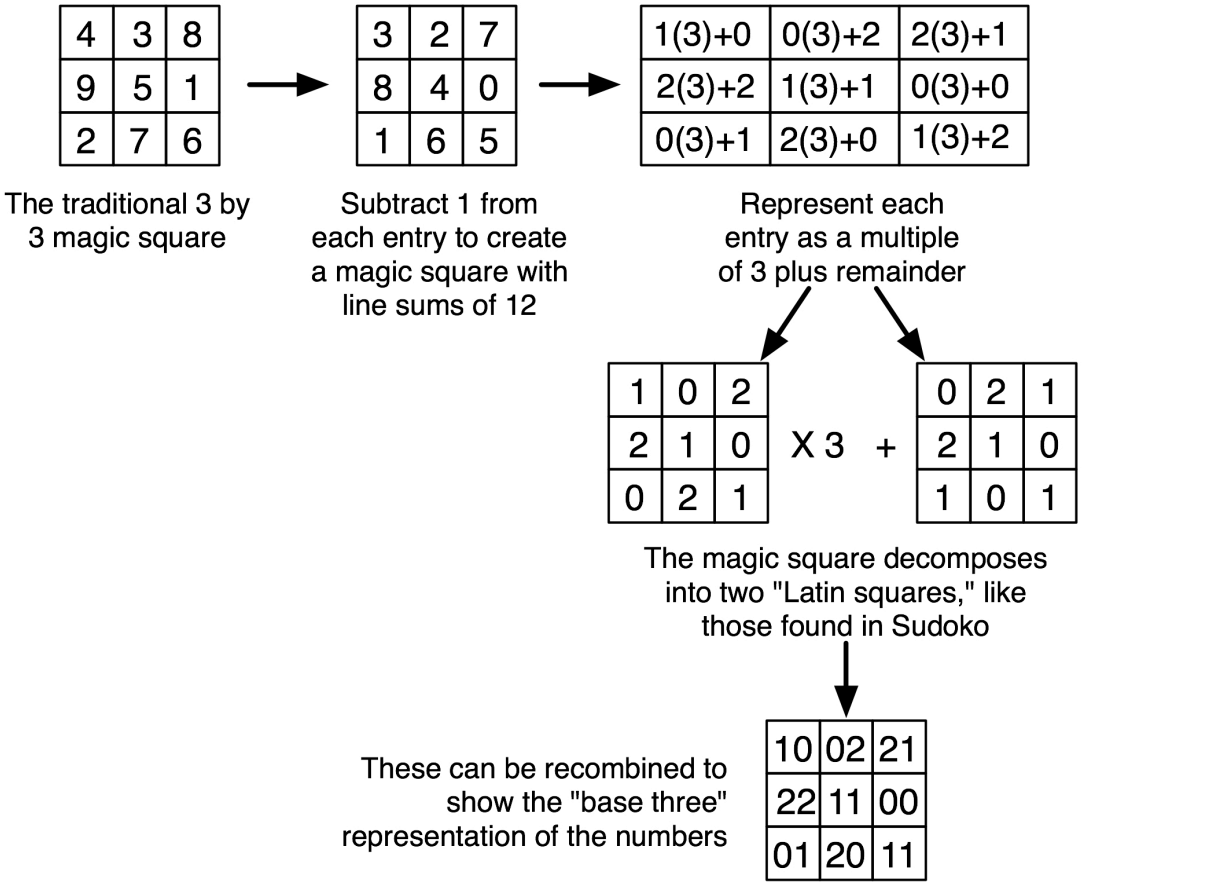
(5) Which symbol would be found in box (1,100)? _____

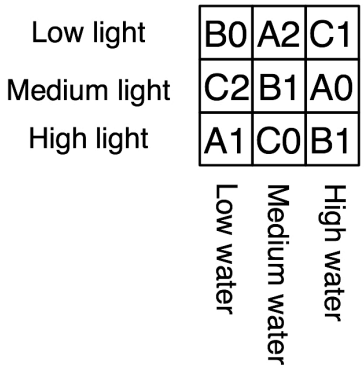
(6) Which symbol would be found in box (199,100)? _____
(Hint: is column 199 the same as column 0 or 1?)

We also found multiples of 3 in the "15 game," which we saw could be better understood by using a 3 by 3 magic square (see problems 14-15 in section 1.1). Recall that in the 15 game, we take turns removing numbers from the list 1,2,3,…,9, and crossing off the removed numbers. The winner the first player who collects 3 numbers with sum 15. We saw that it is easier to strategize about this game by playing it as tic-tac-toe on the 3 by 3 magic square, which uses the numbers 1 through 9 and which has row, column, and diagonal sums of 15:



This square was known as the Lo Shu in ancient China, and was known to mathematicians there as early as 650 BCE. It was also known to ancient Arab and African mathematicians later.

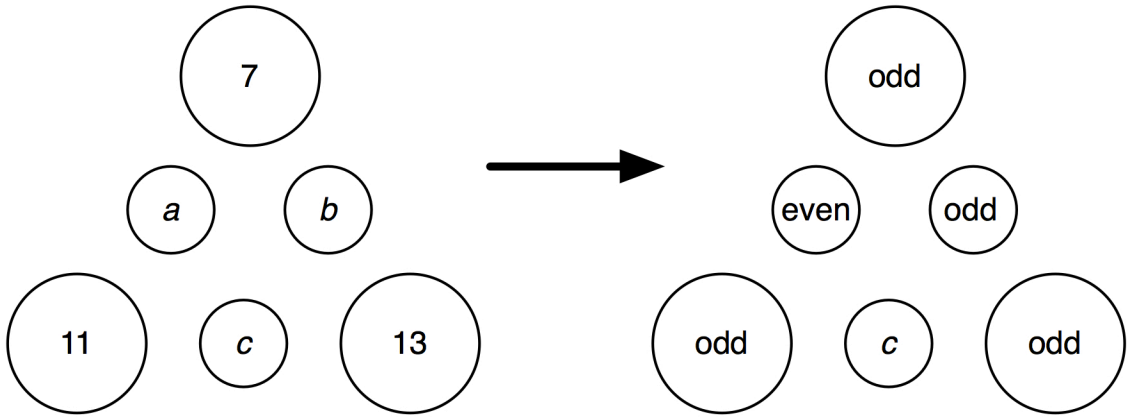




Who cares? Latin squares are used in experimental design. For example, a test is run in which tomato plants of seed types 0, 1, and 2 are placed in three rows and three columns, with each row receiving a different amount of light, each column receiving a different amount of water, and plants receiving fertilizers of either type A, B, or C, as shown. In this magic square array, each fertilizer type is tested with each amount of light, water and seed, etc. Every pairing of experimental characteristics is tested.

Latin squares are also used in "error-correctiing codes," used to make digital communications less susceptible to errors from noise.

Even and odd numbers can also be understood in terms of modular arithmetic. The even numbers are those which leave a remainder of 0 when divided by 2. The odds leave a remainder of 1 when divided by 2. For example, $100 \equiv 28 \pmod 2$ and $101 \equiv 15 \pmod 2$. Problem 6 in section 1.2 asks you to place numbers in the small circles so that each of the numbers in the large circles is the sum of the two numbers in the adjacent smaller circles. Problem 6(c) has no solution, and that can be seen by thinking about evens and odds:



One of *a* and *b* must be even and one odd, in order to have a sum that is odd. But then what would *c* be? If odd then we cannot get sum 11 in the lower left, if odd, we cannot get the sum 13 in the lower right. So there is no solution to this problem.

Here are some further modular arithmetic problems. 15 is a winning position for the first player in the "1,2,3 Take Away Game," who wins by first taking 3, leaving 12, which is a multiple of 4, and thereafter "completing" groups of 4 no matter what the second player does.

(7) Does the first or second player have a winning strategy in the "1,2,3,4 Take Away Game," in which each player takes 1,2,3,or 4 buttons, and the player taking the last button wins, if the game starts with 20 buttons? _____ Describe the strategy:

(8) Who wins if the "1,2,3,4 Take Away Game" starts with 99 buttons, and what is the strategy?

(10) Fill in the blank with one of the numbers 0,1,2,3,4, or 5 to make these statements correct:
$20 \equiv$ ____ (mod 6) $100 \equiv$ ____ (mod 6)

(11) Find three solutions to _____ $\equiv 2 \pmod{12}$

(12) Find three solutions to $17 \equiv 5 \pmod{\_\_\_\_\_}$. (Hint: try numbers starting with 2 and see which work!)