Parabola Volume 55, Issue 3 (2019)

Variations on the secret number mind-reading trick

Rishabh Poddar[1]

1 Introduction

You may be familiar with a mathematical magic trick in which the magician starts by instructing a volunteer to secretly pick any number and then perform few basic arithmetic operations on it, after which the magician is able to figure out the resultant number that the volunteer is thinking of. For instance, the magician might ask:

Magician:	"*Think of a secret number.*"
Volunteer:	[You choose some number and call it x.]
Magician:	"*Multiply your number by 5.*"
Volunteer:	[$5x$]
Magician:	"*Add 25.*"
Volunteer:	[$5x + 25$]
Magician:	"*Divide by 5.*"
Volunteer:	[$x + 5$]
Magician:	"*Subtract your secret number.*"
Volunteer:	[5]
Magician:	"*You are now thinking of the number* 5*!*"

Written out like this, you can easily see how the trick works, and you can easily make infinite variations of this secret number mind-reading trick by changing the numbers featuring in its intermediate steps. An interesting paper by Jonathan Hoseana [1] has proposed a few variations to the binary version of the secret number mind-reading trick. This article briefly illustrates how you as the magician can find many more modifications of this trick, by considering mathematical operations other than the four arithmetic operations.

The volunteer might require a calculator as the calculations are sometimes too difficult to do by mental arithmetical. For you however, playing the role as magician, the trick here, so to speak, is to find ways in which to add and delete information that appear to be complex but which are in fact easy to calculate if you know some simple shortcuts.

[1]Rishabh Poddar is a student at the Vellore Institute of Technology (VIT), Vellore, India.

Variation 1: Modular arithmetic

The first simple variation to the above trick is to apply *modulus functions*, defined as follows: "x modulus m", written as $x \mod m$, is the integer remainder when x is divided by m. For instance, $12 \bmod 5 = 2$.

A secret number mind-reading trick could for instance use modulus functions as follows:

You:	"*Think of a number.*"
Volunteer:	[Chooses some number x.]
You:	"*Add 8.*"
Volunteer:	[$x + 8$]
You:	"*Multiply by 12.*"
Volunteer:	[$12x + 96$]
You:	"*Subtract 53.*"
Volunteer:	[$12x + 43$]
You:	"*Reduce modulus 6.*" (or "*Divide by 6 and think of the remainder*")
Volunteer:	[1]
You:	"*You are now thinking of the number 1!*"

Written as one expression, the calculations above are

$$\big(12(x+8) - 53\big) \bmod 6\,.$$

It is clear that, when dividing $12(x + 8) - 53 = 12x + 96 - 53 = 12x + 43$ by 6, the remainder is 1. We could generalise this to the more general form as

$$\big(am(x+b) - (cm-1)\big) \bmod m$$

which will always equal 1 since $am \bmod m$ and $cm \bmod m$ each equal 0.
To change the resulting 1 to and number d less m, just replace 1 by d in the calculations:

$$\big(am(x+b) - (cm-d)\big) \bmod m\,.$$

To make the trick seem more magical, we could use more modular arithmetic, for instance through calculations such as

$$\big((2m+a)(x+b) - (a-1)x - ab\big) \bmod m\,.$$

With $m = 7$, $a = 3$, and $b = 4$, the trick could sound as follows:

You:	"*Think of a number.*"
Volunteer:	[Chooses some number x.]
You:	"*Add 4.*"
Volunteer:	[$x + 4$]
You:	"*Multiply by 17.*"
Volunteer:	[$17x + 68$]
You:	"*Subtract twice the number that you chose.*"
Volunteer:	[$15x + 68$]
You:	"*Subtract 12.*"
Volunteer:	[$15x + 56$]
You:	"*Reduce modulus 7.*"
Volunteer:	[x]
You:	"*You are now thinking of the number that you first thought of!*"

Thinking more creatively, you could also ask the volunteer for values of a, b or m.

The divisibility rules of some natural numbers [2, pp. 160–169] make way for some interesting alterations to this variation of the trick. For instance, we know that the $\mod$ 2, 4, 5, 8, and 10 values of a number can be determined solely by its last 1, 2, 1, 3 and 1 digits, respectively, the $\mod$ 3 and 9 values of any number can be determined by the sum of its digits. There are similarly simple rules for divisibility by 7, 11 and other numbers. Consider, for instance:

You:	"*Think of a number larger between* $1,000$ *and* $1,000,000$."
Volunteer:	[Chooses some number x.]
You:	"*Add 3.*"
Volunteer:	[$x + 3$]
You:	"*Multiply by 22.*"
Volunteer:	[$22x + 66$]
You:	"*Add the 1st, 3rd, 5th, and so on digits together.*"
Volunteer:	[Odd sum]
You:	"*No add the 2nd, 4th, 6th, and so on digits together.*"
Volunteer:	[Even sum]
You:	"*Now subtract the 1st sum from the 2nd.*"
Volunteer:	[Even sum minus the odd sum]
You:	"*Now subtract the 1st sum from the 2nd.*"
Volunteer:	[Even sum minus the odd sum]
You:	"*Reduce modulus 11.*"
Volunteer:	[0]
You:	"*You are now thinking of the number zero.*"

Here, we used the recursive rule that a number is divisible by 11 if the difference between the sum of odd-positioned digits and the sums of even-positioned numbers is divisible by 11.

Variation 2: Fermat's Little Theorem

Fermat's Little Theorem states that if p is a prime number, then $a^p \bmod p = a$ as long as a is not divisible by p (in which case, $a^p \bmod p = 0$). This allows us to add an additional step to our trick. We could for instance use this theorem in a variation of our trick, as follows:

You:	"*Think of a number strictly less than 40.*"
Volunteer:	[Chooses a number x.]
You:	"*Raise this number to the 5*th *power.*"
Volunteer:	[x^5]
You:	"*Reduce modulus 5.*"
Volunteer:	[0] or [x]
You:	"*You are now thinking of either zero or the number that you chose!*"

Here, the volunteer was asked to choose a number x strictly less than 40 because $39^5 = 90,224,199$ is the largest 5*th* power that can fit on older calculators with only eight visible digits.

You can make the trick seem more magical by using *Euler's Theorem* which is a stronger version of *Fermat's Little Theorem*, stating that $a^{\varphi(n)} \bmod n = a$ as long as a is coprime with n. Here, $\varphi(n)$ is a beautiful and fascinating function called *Euler's totient* function. A few values of this function are given here:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Choosing for instance the value $n = 14$, we could use *Euler's Theorem* in a variation of our trick, as follows:

You:	"*Think of an odd number between 10 and 20.*"
Volunteer:	[Chooses a number x.]
You:	"*Raise this number to the 6*th *power.*"
Volunteer:	[x^6]
You:	"*Reduce modulus 14.*"
Volunteer:	[x]
You:	"*You are now thinking of the number that you first thought of!*"

Here, the trick worked because the chosen x was coprime with $n = 14$ since it was odd and not divisible by 7.

Variation 3: The Chinese Remainder Theorem

To actually find the number that the volunteer is thinking of, we can use the *Chinese Remainder Theorem*, though it might require a pen and paper. The theorem states that, given two coprime numbers n_1 and n_2 and any two numbers a_1 and a_2, there is exactly one number x less than $n_1 n_2$ that satisfies both equations

$$x \bmod n_1 = a_1$$
$$x \bmod n_2 = a_2$$

The trick could be enacted as follows:

You:	"*Think of a number less than 1000.*"
Volunteer:	[Chooses a number x.]
You:	"*What is* x mod 35*?*"
Volunteer:	[Calculates and states x mod 35.]
You:	"*What is* x mod 36*?*"
Volunteer:	[Calculates and states x mod 36.]
You:	[Calling these two numbers a_1 and a_2, calculates $x = 36a_1 - 35a_2$.]
You:	"*The number that you thought of is* x*!*"

Here, 1000 was chosen to be iconic and to limit large calculations. The numbers $n_1 = 35$ and $n_2 = 36$ were chosen for three reasons: the product $n_1 n_2 = 35 \times 36 = 1,260$ is bigger than 1000; they are coprime; and they yield the simple formula $x = 36a_1 - 35a_2$.

In theory, *The Chinese Remainder Theorem* ensures that this trick variant will always work whenever we choose any two coprime numbers n_1 and n_2 with product bigger than the number thought of by the volunteer. The trick will also work in practise since we can always calculate x with relative ease from a general formula for x. To find that formula, we must first find integers m_1 and m_2 that satisfy

$$m_1 n_1 + m_2 n_2 = 1 \, .$$

Such numbers exist whenever n_1 and n_2 are coprime, as here, according to another theorem, called *Bezout's Identity*, and we can find those numbers quickly by using what is called *The Extended Euclidean Algorithm*.[2] The formula for x is then

$$x = a_1 m_2 n_2 + a_2 m_1 n_1 \, .$$

(Can you show that $x \bmod n_1 = a_1$ and $x \bmod n_2 = a_2$?)

Sometimes, it is not necessary to use the Algorithm; we can often just guess. For instance for $n_1 = 35$ and $n_2 = 36$, or any two adjacent (and therefore coprime) numbers, we can choose $m_1 = -1$ and $m_2 = 1$ since

$$m_1 n_1 + m_2 n_2 = n_2 - n_1 = 1 \, ,$$

[2]Bezout's Identity and the Extended Euclidean Algorithm form the basis for a large part of elementary number theory. This is beautiful and fascinating maths and we hope that you, dear Reader, might feel inspired to explore the details of this maths for your yourself.

and so

$$x = n_2 a_1 - n_2 a_2 \,.$$

For instance, if $n_1 = 50$ and $n_2 = 51$, say, then

$$x = 51a_1 - 50a_2 \,.$$

Concluding comments

The variations of the secret number mind-reading trick given above illustrate just a few ways in which this trick can be modified, and they could also be used to help teach students about modular arithmetic, *Fermat's Little Theorem*, *Euler's Theorem*, *The Chinese Remainder Theorem*, *Bezout's Identity*, *The Extended Euclidean Algorithm* and others aspects of number theory.

There are however infinitely many other ways in which this trick can be modified, also in mathematical areas beyond number theory. Can you find more ways yourself?

References

[1] J. Hoseana, Variations on the Binary Mind-Reading Trick, *The College Mathematics Journal* **49** (2018), 262–268.

[2] M. Gardner, *The Unexpected Hanging and Other Mathematical Diversions*, revised ed., Simon and Schuster, New York, 1991.