February 28, 2000

Exponential exercises

Alice breaks out

Remember the jail house scenario? When we left Alice and Bob, they had discovered a method of communicating quite securely in spite of Eve's observations of all of their messages.

Of course, Alice and Bob started having a (long distance) relationship. But then, as with many relationships, at least one out of two messes up. Nobody really knows why Alice and Bob broke up, but there are rumors that Bob multiplied numbers instead of taking powers. Alice had enough of men in jail. She decided to break free.

Her other (in-)mates, let's call them Kia, Jeff, and Aaron, are real experts. And because she is a nice person, and even more because they don't like Bob – which has nothing to do with his encrypting abilities but might have something to do with the fact that he was yelling numbers day and night – Kia, Jeff, and Aaron decided to help her. Each of them has some kind of advice to give her about escaping.

The jail hasn't changed much in the meantime, so it's still impossible to talk to each other without everybody else hearing it. Eve is everywhere, and Eve hears everything.

One way Alice could receive messages from Kia, Jeff, and Aaron is by establishing a secret as we saw last week. But this would require Alice to keep track of 3 different secrets which is very irritating to her. (Her cell is an incredible mess!)

What Alice needs is an encryption system known as RSA . This will allow her to shout out some numbers <u>once</u> so that everyone can hear. Then, using these numbers, everyone will be able to create a message only Alice can understand.

In order to be able to understand how and why RSA works, Jeff, Kia, and Aaron had to solve some problems first. You, too, should solve and try to understand the problems.

Some help first

Remember Euler's equation: if p and q are two different primes, then

$$\boxed{m^{(p-1)(q-1)} = 1 \bmod pq}$$

Example Suppose $n = 3 \cdot 5$ and $m = 2$.

A What power of m will be equal to 1 mod n?

B What power of m will be equal to 2 mod n?

Answer Look at Euler's equation above. 3 and 5 are primes. Plug in 3 for p and 5 for q:

$$2^{(3-1)\cdot(5-1)} = 1 \bmod 3 \cdot 5$$

$(3-1)\cdot(5-1) = 8$, so 8 is an answer to **A**.

Now we know $2^8 = 1 \bmod 3 \cdot 5$. Multiply both sides by 2:

$$\underbrace{2 \cdot 2^8}_{=2^9} = 2^9 = 2 \cdot 1 \quad \bmod 3 \cdot 5$$

so 9 is an answer to **B**.

You can also check this computation with `Maple`. The results will look like this:

```
[> n:=3*5;
                              n:=15
[> 2^8 mod n;
                                1
[> 2^9 mod n;
                                2
```

How much is 2^{17} mod n? And how much is 2^{25} mod n? Can you find more such exponents? Notice that $9 = 8 + 1$, $17 = 8 + 8 + 1$, and $25 = 8 + 8 + 8 + 1$.

Some problems

Please do these problems before the next class.

You can use `Maple` to verify your answers but just a small calculator should be enough to handle any of the computations below. In fact, Euler's equation combined with simple arithmetic is really enough to do these problems.

1. Suppose $n = 3 \cdot 11$ and $m = 4$.

A What power of m will be equal to 1 mod n?
B What power of m will be equal to 4 mod n? Can you find more exponents that give 4 mod n?

2. $n = 91$ is a product of two primes. If $m = 5$, what power of m will equal 5 mod n? Can you find more exponents that give 5 mod n?

3. Suppose $n = 17 \cdot 13$ and $m = 6$. An oracle told me that $5 \cdot 77 = 1$ mod $16 \cdot 12$.*

A What power of m will be equal to 6 mod n? Do more exponents give 6 mod n?
B How much is $(m^5)^{77}$ mod n?
C How much is $(m^{77})^5$ mod n?
D How much is $m^{(5\cdot 77)}$ mod n?
E $16 \cdot 12 = 192$, right? How much is $5 \cdot 77$? And how much is $192 + 192 + 1$?

Do your answers to **B**, **C**, and **D** make sense now? If not, please read the **Example** again.

F What power of (m^5) will be equal to m?
G What power of (m^{77}) will be equal to m?**

Algebraic facts that may be useful

$$\left(A^B\right)^C = A^{B\cdot C} = \left(A^C\right)^B \text{ and } A^{B+C} = A^B \cdot A^C$$

Note S. Radomirović wrote a first draft of what's here. It was then lightly edited by S. Greenfield.

* $17 - 1 = 16$ and $13 - 1 = 12$. Compare this to Euler's equation!
** If you solved **B** and **C**, then **F** and **G** are easy. You don't even need a calculator.