PRIME NUMBERS & SECRET MESSAGES

I. "RSA CODEBREAKER" GAME

This is a game with two players or teams. The players take turns selecting either prime or composite numbers as outlined on the board below. The key is that the product of the numbers chosen have to be equal. Here is a sample game:

After Move 1

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

After Move 2

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×		=	2	×	
Composite Number		Prime Number		Prime Number		Composite Number

After Move 3

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×	7	=	2	×	
Composite Number		Prime Number		Prime Number		Composite Number

Team B can now win the game if he can find a composite number to make the equation true. If Team B can not make the equation equal, then Team A wins.

After Move 4

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×	7	=	2	×	28
Composite Number		Prime Number		Prime Number		Composite Number

Keep the initial composite number 12 or less for the initial games. Then, move this to 50 or higher if you like.

Problem 1. (For when you've played enough games.) Which team is most likely to win? Is there a winning strategy? For which team?

RSA GAMEBOARDS

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

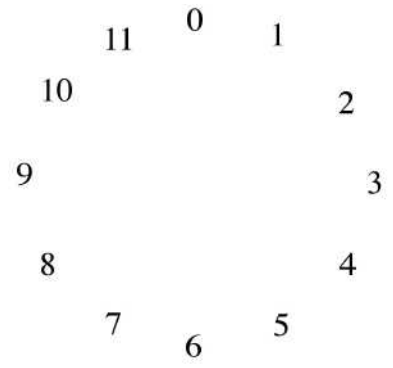
Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

II. CLOCK ARITHMETIC

On your (12-hour) clock, the 13^{th} hour is 1 o'clock, the 14^{th} is 2, 15 is 3, and so on. We'll call 12 "0".



Problem 2. (a) Add $9 + 10$ on the clock. Subtract $3 - 7$.

(b) Multiply $5 \cdot 7$ on the clock. Then try $4 \cdot 9$.

(c) What are 5^2 and 7^2 on the clock? How about 5^3? 5^4? 5^5?

(d) Is there anything you can multpliy by 5 (on the clock) to get 0?

We don't have to do this with a 12-hour clock. Let N be any integer bigger than 1, and imagine a clock with N evenly spaced "hours": 0, 1, 2, ..., $N-1$. Arithmetic on this clock is called "arithmetic mod N".

To do it without the clock, notice that every integer m can be "reduced" to one of 0, 1, 2, ..., $N-1$ by adding or subtracting N enough times. Call the result $\overline{m}$.

For example, if $N = 7$, $\overline{25} = 4$.

Another way of writing this is "$25 \equiv 4 \pmod 7$" or "$25 \underset{(7)}{\equiv} 4$". The "$\underset{(7)}{\equiv}$" means "equals mod 7"; it's there so you don't have to write "$25 = 4$" – which, after all, isn't true.

To add, multiply, or subtract two "integers mod N", just do it as you would normally to get some number m, and then find $\overline{m}$. For example, with $N = 7$, $4 \cdot 4 = 16 \underset{(7)}{\equiv} 2$.

III. POWERS MOD N

Try some modular arithmetic:

Problem 3. (a) Find all the powers of 3 (mod 7).

(b) Now that you've found them all, what is 3^7 (mod 7)?

(c) How about 3^5 (mod 5)? 2^5 (mod 5)? 4^5 (mod 5)?

(d) What do you think 10^{17} (mod 17) should be?

Just as you are getting a good feeling about this . . .

Problem 4. What about 2^6 (mod 6)? 3^{10} (mod 10)? [Hint: think of 9 as -1 mod 10.]

So perhaps there is just something about N being a prime number?

Problem 5. Try to guess a general statement that is true! Write it in the box:

What if $N = 2 \cdot p$, with p a prime number (other than 2). Then it turns out that for any number m between 0 and N,

$$m^p \equiv m \text{ (mod } N).$$

Try it: let's "fix" Problem 4.

Problem 6. What is 2^3 (mod 6)? 3^5 (mod 10)?

IV. SECRETS IN BROAD DAYLIGHT

The first public key cryptosystem was invented by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman in 1978. Prior to its introduction, encryption research in the US was the exclusive business of the National Security Agency, and all information was classified. Here is the idea:

- Alice broadcasts an encryption (i.e. encoding) algorithm;
- Bob uses it to encode his message and broadcasts this;
- Alice "reverses" the algorithm to decode the message.

If all the information is publically broadcast, then how can this be secure? The answer is that the encryption algorithm needs to be very difficult (for anyone but Alice) to reverse.

The **RSA** cryptosystem gives a way for Alice to make such an algorithm. Here is the recipe:

- Take two large prime numbers P, Q (as much as 300 digits each!);
- Let $N = P \cdot Q$, and $n = (P-1) \cdot (Q-1)$;
- Pick some number[1] a between 0 and n;
- Find b (between 0 and n) so that $a \cdot b \equiv 1$ mod n.

Let's say your message is a number M (for "Message"!) between 0 and N.

Encoding Algorithm: $M \rightsquigarrow \overline{M^a} = E$ (for "Encoded message").

Decryption Algorithm: $E \rightsquigarrow \overline{E^b} = D$ (for "Decoded message").

RSA Theorem: $D = M$ (i.e. $\overline{M^{ab}} = M$).

Here, of course, the $\overline{\text{bar}}$ means to "go mod N".

To encode a message, all Bob needs is N and a, and these are what Alice broadcasts, keeping P, Q, n, and b secret.

Bob then sends E to Alice, and Alice decodes it.

If Clive wants to break the code (without cheating), he'll have to find b, which is too hard without also knowing n. To find n, you need P and Q, which means he'll have to factor N – again, probably too hard if Alice used large enough numbers.

Two questions are: (1) How does Alice find b solving $a \cdot b \equiv 1$ mod n? (This is not hard: perhaps something for the next math circle.)

(2) How does Alice find large prime numbers P and Q? (Much harder, for many years a central problem in algorithmic number theory.)

Problem 7. How does any of this relate to the game we played earlier?

[1] It should be "relatively prime" to n – something for the next Math Circle.

V. RSA WITH $p = 13$, $q = 2$

Let's give it a try!

Each of you think of a number from 0 to 25.

Write it here: $M =$ $\boxed{}$.

I make public $N = 26$ and some number a between 0 and $n = (13-1)\cdot(2-1) = 12$, say $a = 5$.

You compute $E = \overline{M^5} =$ $\boxed{}$.

Problem 8. Once you tell me E, what do I have to do to figure out your M? What is b?

If $a \cdot b \underset{(12)}{\equiv} 1$, then $a \cdot b = 12 \cdot c + 1$ for some number c.

Problem 9. Bearing in mind that $M^{13} \underset{(N)}{\equiv} M$ since $N = 2p$, why is the RSA theorem true in this case – i.e. why is $M^{ab} \underset{(N)}{\equiv} M$?

VI. ALPHABET DECRYPTION (HOMEWORK)

Let's reverse roles, but keep the same a and b.

I have encoded a secret message below, by converting each letter to a number with the table

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

and then raising the number to the 5^{th} power (mod 26). Here is the encoded message:

$$8/6/0/13/1/10/6/23/0/6/4/10/9,\ 8/6/0/13/1/10/12/0/9/10,$$
$$8/6/0/13/1/10/15/14/7/9,\ 8/6/0/13/1/10/19/7/0/20/10/9;$$
$$16/11/0/15/0/12/8?$$

You'll probably want a calculator to decode it. Write the decoded message here:

Indeed, it's a riddle. What is the answer?