EULER PHI AND MODULAR EXPONENTS

MATH CIRCLE (BEGINNERS) 03/11/2012

Two numbers are *relatively prime* if they share no prime factors with each other. This means they can't have any common divisors other than 1, so their gcd must be 1. On the other hand, if their gcd is 1, they don't have any common divisors other than 1, so they don't share any prime factors, so they are relatively prime:

Fact: x and y have no prime factors in common if and only if $\gcd(x, y) = 1$.

The Greek letter ϕ is written "phi" and pronounced "fee." The mathematician Euler used it to describe how many numbers less than a certain number, were relatively prime to that number. Nowadays we call this number the *Euler phi function*.

$\phi(n) =$**the number of numbers between 1 and $n - 1$, that are relatively prime to n.**

For example, $\phi(10) = 4$, because there are 4 numbers less than 10 that are relatively prime to 10 (1, 3, 7, and 9). The other numbers less than 10 (2, 4, 5, 6, and 8) all share a prime factor with 10.

Here is the table you filled out last time with values of $\phi(n)$ for n from 1 to 21.

n	2	3	4	5	6	7	8	9	10	11
$\phi(n)$	1	2	2	4	2	6	4	6	4	10

n	12	13	14	15	16	17	18	19	20	21
$\phi(n)$	4	12	6	8	8	16	6	18	8	12

(1) What is the value of $\phi(p)$ when p is a prime number?

(2) What is the value of $\phi(1024)$? (Hint 1: $1024 = 2^{10}$.) (Hint 2: Look for a pattern with $\phi(2)$, $\phi(4)$, $\phi(8)$, $\phi(16)$, ...)

(3) Sometimes $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$–for example, $\phi(3 \cdot 5) = \phi(15) = 8$, and also $\phi(3) = 2$, $\phi(5) = 4$, and $8 = 2 \cdot 4$.

Other times this doesn't work: $\phi(2 \cdot 4) = \phi(8) = 4$, but $\phi(2) = 1$ and $\phi(4) = 2$ and $4 \neq 1 \cdot 2$.

Let's call a pair of numbers a and b a *happy couple* if $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. Find the values $\phi(a \cdot b)$, $\phi(a)$, and $\phi(b)$ for several pairs of numbers a and b (at least 4 different pairs–you don't have to compute them from nothing, since you have the table you made above). Make a list of which ones are happy couples and which ones aren't. Compare lists with your neighbors. Try to find an underlying pattern–when is a pair of numbers a happy couple?

Use your understanding of Euler's ϕ function to solve the following problems:

(4) Find $\phi(77)$.

(5) If k is an odd number and $\phi(k) = 48$, what is $\phi(8k)$?

(6) Find $\phi(3)$, $\phi(9)$, $\phi(27)$, $\phi(81)$.

(7) What is $\phi(3^n)$ in terms of n?

(8) What is $\phi(\phi(100))$?

(9) If p and q are two different prime numbers, what is $\phi(p \cdot q)$? (Your answer will be in terms of p and q, but shouldn't have any ϕ's)

(10) If $p_1, p_2, p_3, \ldots, p_m$ are m different prime numbers, what is $\phi(p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_m)$? (Again, your answer will use p_1, etc. (and probably dots ... to indicate a pattern) but shouldn't involve ϕ.)

(11) Find $\phi(5)$, $\phi(25)$, $\phi(125)$.

(12) What is $\phi(5^n)$ in terms of n?

(13) Find $\phi(4)$, $\phi(9)$, $\phi(25)$, $\phi(49)$, $\phi(121)$.

(14) What is $\phi(p^2)$ for a prime p? (your answer will have one or more p's, but shouldn't have any ϕ)

(15) Is it true that $\phi(x)$ is even for all $x \geq 3$? Why or why not?

(16) Find $\phi(1,000,000)$.

(17) Find $\phi(8!) = \phi(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)$. (You can leave your answer as a product of numbers, you don't have to multiply them out. Hint: It's NOT just $\phi(8) \cdot \phi(7) \cdot \phi(6) \cdot \phi(5) \cdot \phi(4) \cdot \phi(3) \cdot \phi(2)$.)

(18) Find $\phi(x)$, where x is the year you were born.

(Some hints for different years:

- 1001 has 3 prime factors, none of them larger than 15.
- 667 is divisible by 23.
- 2003 is prime!)

Now we're going to shift gears about and go back to modular arithmetic–in particular, modular exponentiation. But we'll come back to the ϕ function...

For each modulus that follows, fill in the table with the powers of all the numbers that are relatively prime to it, and see how long it takes each of the powers to cycle. The example of 4 is done for you:

Modulus 4

#s relatively prime to 4:	1	3
to power 1	$1^1 \equiv 1 \pmod 4$	$3^1 \equiv 3 \pmod 4$
to power 2	$1^2 \equiv 1 \pmod 4$	$3^2 \equiv 1 \pmod 4$
to power 3	$1^3 \equiv 1 \pmod 4$	$3^3 \equiv 3 \pmod 4$
to power 4	$1^4 \equiv 1 \pmod 4$	$3^4 \equiv 1 \pmod 4$
pattern	$1, 1, 1, 1, \ldots$	$3, 1, 3, 1, \ldots$
length of pattern	1	2

Modulus 5

#s relatively prime to 5:	1			
to power 1	$1^1 \equiv 1 \pmod 5$			
to power 2				
to power 3				
to power 4				
to power 5				
to power 6				
pattern				
length of pattern				

Modulus 6

#s relatively prime to 6:	1	
to power 1	$1^1 \equiv 1 \pmod 6$	
to power 2		
to power 3		
to power 4		
to power 5		
to power 6		
to power 7		
pattern		
length of pattern		

Modulus 7

# rel prime to 7:	1					
to power 1	$1^1 \equiv 1 \pmod 7$					
to power 2						
to power 3						
to power 4						
to power 5						
to power 6						
to power 7						
to power 8						
pattern						
pattern length						