In our previous handout, we learned about Fermat’s Little Theorem which says the following:

Let $p$ be a prime number and let $a$ be any number which is relatively prime to $p$ (i.e., $\gcd(a,p)=1$). Then we know $a^{p-1} \equiv 1 \pmod{p}$.

One of the questions we raised at the end of that handout was whether we could write down any sort of congruence like the one above where the modulus $p$ is replaced by some non-prime number. In preparation for such a result (which we will see in our next handout), we need to consider a function we have not seen before – Euler’s phi function which is denoted $\varphi(n)$.

**Definition:** Let $n$ be a positive number. Then Euler’s phi function, denoted $\varphi(n)$, counts the number of integers between 1 and $n$ which are relatively prime to $n$. (Note also that we define $\varphi(1) = 1$.)

**Examples:**

$\varphi(6) = 2$ because the only numbers between 1 and 6 which are relatively prime to 6 are 1 and 5.

$\varphi(10) = 4$ because the only numbers between 1 and 10 which are relatively prime to 10 are 1, 3, 7, and 9.

**Calculations:**

Compute each of the following:

$\varphi(2) = \underline{}$  \hspace{1cm} $\varphi(3) = \underline{}$  \hspace{1cm} $\varphi(4) = \underline{}$  \hspace{1cm} $\varphi(5) = \underline{}$

$\varphi(6) = \underline{}$  \hspace{1cm} $\varphi(7) = \underline{}$  \hspace{1cm} $\varphi(8) = \underline{}$  \hspace{1cm} $\varphi(9) = \underline{}$

$\varphi(10) = \underline{}$  \hspace{1cm} $\varphi(11) = \underline{}$  \hspace{1cm} $\varphi(12) = \underline{}$  \hspace{1cm} $\varphi(13) = \underline{}$

$\varphi(14) = \underline{}$  \hspace{1cm} $\varphi(15) = \underline{}$  \hspace{1cm} $\varphi(16) = \underline{}$  \hspace{1cm} $\varphi(17) = \underline{}$
Questions:

1. Do you see any patterns in the above?

   (Hint 1: Look at the primes!)

   (Hint 2: Look at the evenness/oddness of the answers!)

2. What if I asked you to calculate something bigger, like $\phi(100)$ or $\phi(1000)$?

   (Multiplicativity to the rescue again!!!)

Closing Comments:

1. Leonhard Euler appears to be the first mathematician who considered this function $\phi(n)$. As best we can tell, his first reference to calculating this function appears in his paper “Theoremata arithmetica nova methodo demonstrata” (reference number E271). However, Euler does not use the “phi” notation in that paper. Later, in E564, “Speculationes circa quasdam insignes proprietates numerorum”, he does use a more function-oriented notation, but he writes the number of integers up to $n$ with are relatively prime to $n$ as $\pi n$ (Euler avoided using parentheses around such functions, which is confusing today). We will stick with our “phi” notation!

2. Related to item 1 above, the first time someone actually used the $\phi(n)$ notation turns out to be our friend Gauss in his Disquisitiones Arithmeticae published in 1801 (less than 30 years after Euler’s death).

3. This phi function is immensely important in RSA public-key cryptography.

4. Next time, we will consider Euler’s beautiful generalization of Fermat’s Little Theorem; this phi function will play a major role!

© 2010, James A. Sellers