An Euler φ-For-All

by Lola Thompson

Content supported in part by a grant from MathWorks.

Reprinted from the *Girls' Angle Bulletin*, volume 6, number 5, pp 8-11.

The Girls' Angle Bulletin is a bimonthly publication of Girls' Angle.
Electronic Version: ISSN 2151-5743
Print Version: ISSN 2151-5700

Girls' Angle
A Math Club for Girls

An Euler φ-For-All[1]

by Lola Thompson

What is φ?

Primes are the atoms of the number universe: every whole number greater than 1 can be factored uniquely into a product of primes. When two numbers share no common prime factors, we say that they are **relatively prime**. Don't let the terminology fool you. Being "relatively prime" is not like being "relatively smart" or "relatively popular," wherein the subject is "smart" or "popular" compared with her peers. Relatively prime numbers are not necessarily any closer to being prime than other numbers. For example, 4 and 15 are relatively prime and they are both composite. As a silly example, we see that 1 is relatively prime to all other positive whole numbers, since 1 doesn't have any prime factors to share!

Rather than looking at individual pairs of numbers and asking whether they are relatively prime to one another, one could instead take a specific number like 8 and ask, "How many numbers between 1 and 8 are relatively prime to 8?" This question can be generalized by using n to represent *any* positive integer greater than 1, and asking, "How many numbers between 1 and n are relatively prime to n?" In fact, we have a special name for this counting function: we define $\varphi(n)$ to be the number of integers between 1 and n that are relatively prime to n. We call $\varphi(n)$ the **Euler totient function** (the symbol φ is the Greek letter "phi" and the word "totient" rhymes with "quotient"). To answer the question posed above, we observe that 1, 3, 5, and 7 are all relatively prime to 8. However, 2, 4, 6, and 8 all share a common factor with 8 because they're all divisible by 2. As a result, we can conclude that $\varphi(8) = 4$. On the other hand, if p is *any* prime number then $\varphi(p) = p - 1$, since $1, 2, 3, \ldots, p - 1$ are all relatively prime to p (remember, primes are only divisible by 1 and themselves, and 1 is relatively prime to everything).

> The Euler totient function $\varphi(n)$ is defined as the number of integers between 1 and n that are relatively prime to n.

The Arithmetic of φ

The Euler totient function has a number of neat properties. For example, we can show that if n and m are any two relatively prime numbers then $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$. However, this property does not hold when n and m share common factors. For example, $\varphi(6) = 2$ and $\varphi(4) = 2$, so $\varphi(6) \cdot \varphi(4) = 2 \cdot 2 = 4$. Contrast this with the fact that $6 \cdot 4 = 24$ and $\varphi(24) = 8$. In short, while 6 and 4 may be lucky to have something in common, they don't play so nicely with φ.

We will illustrate a general method for proving that $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$ holds for any relatively prime numbers n and m by looking at the case $n = 7$ and $m = 6$. If $n = 7$ and $m = 6$, we write the numbers between 1 and 42 (= $n \cdot m$) in the chart at right.

1	7	13	19	25	31	37
2	8	14	20	26	32	38
3	9	15	21	27	33	39
4	10	16	22	28	34	40
5	11	17	23	29	35	41
6	12	18	24	30	36	42

[1] This content was supported in part by a grant from MathWorks.

To compute $\varphi(42)$, we need to determine how many entries in the chart are relatively prime to 42. This is not so difficult because 42 is a fairly small number; in theory, we could just go through the numbers one by one and cross off any number that is not a multiple of 2, 3, or 7. However, if we had chosen larger numbers for n and m, this would not be a fun task. Imagine trying to compute $\varphi(n \cdot m)$ in this way when n and m are both in the thousands — it would probably take an entire afternoon! Fortunately, we have organized our chart in a way that makes it easier to get rid of the entries that are not relatively prime to 42. Namely, the entries in a given row all have the same remainder when divided by 6. As a result, if an entry in the first column is not relatively prime to 6, then all of the other entries in the same row will also fail to be relatively prime to 6. So, we can immediately eliminate all of the entries in several of the rows.

1	7	13	19	25	31	37
~~2~~	~~8~~	~~14~~	~~20~~	~~26~~	~~32~~	~~38~~
~~3~~	~~9~~	~~15~~	~~21~~	~~27~~	~~33~~	~~39~~
~~4~~	~~10~~	~~16~~	~~22~~	~~28~~	~~34~~	~~40~~
5	11	17	23	29	35	41
~~6~~	~~12~~	~~18~~	~~24~~	~~30~~	~~36~~	~~42~~

Next, we examine the remaining rows. The entries of each row are of the form i, $i + 6$, $i + 2 \cdot 6$, $i + 3 \cdot 6$, $i + 4 \cdot 6$, $i + 5 \cdot 6$, and $i + 6 \cdot 6$ (where $i = 1$ or 5). Since i and 6 are necessarily relatively prime (because we eliminated the rows where i and 6 share a common factor!) then all 7 entries in each row are relatively prime to 6. Moreover, if we divide each of the entries in a given row by 7, we will get all of the numbers between 0 and 6 as remainders. So, exactly $\varphi(7) = 6$ of these entries will be relatively prime to 7. Since these 6 entries are relatively prime to both 6 and 7, they will be relatively prime to 42.

Recall that if D is relatively prime to N, then the remainders of the numbers

$$M, M + D, M + 2D, \ldots, M + (N - 1)D$$

upon division by N produce a complete set of remainders (where M is any integer). To see this, pick two of the numbers in the list: $M + KD$ and $M + JD$, where $0 \leq K < J < N$. Suppose they both leave the same remainder upon division by N. Then N divides their difference, i.e., N divides $(M + JD) - (M + KD)$ or, simplifying, $N \mid (J - K)D$. Since D and N are relatively prime, N must divide evenly into $J - K$. But $0 < J - K < N$, a contradiction. Therefore, the remainders of the numbers are all distinct. Since there are N numbers in the list and N total possible remainders, we must get them all.

We can summarize what we have done in more general terms. We start by writing the numbers 1 through $n \cdot m$ in a rectangular array that has n columns and m rows. We place the 1 in the upper left and then place the numbers sequentially top to bottom then left to right. We have argued that exactly $\varphi(m)$ rows in the chart contain numbers that are relatively prime to $n \cdot m$. Each of these $\varphi(m)$ rows contains exactly $\varphi(n)$ numbers that are relatively prime to n. So, there are $\varphi(n) \cdot \varphi(m)$ numbers in the chart that are relatively prime to $n \cdot m$. But, by the very definition of Euler's totient function, there are $\varphi(n \cdot m)$ integers relatively prime to $n \cdot m$ that are between 1 and $n \cdot m$ (which is exactly what this chart was designed to count in the first place!). So, we have shown that $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

The Arithmetic of φ, Part II

We know how to multiply together totients of different numbers (provided that they are relatively prime to one another), but what if we want to add them instead? It turns out that, if we add the totients of just the right numbers, we will discover another neat property of Euler's totient function. First, we will need some new notation. We write $d \mid n$ as shorthand for "d divides n." In other words, $d \mid n$ means that, if we compute n/d, we will get a whole number answer (without a remainder).

One more piece of notation[2] that will be useful to us is

$$\sum_{d \mid n} \varphi(d),$$

which tells us that we are summing $\varphi(d)$ for each value of d that divides n. For example,

$$\sum_{d \mid 4} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4),$$

since the divisors of 4 are precisely 1, 2, and 4. Our "neat" property about summing totients can now be stated in the following manner:

$$\sum_{d \mid n} \varphi(d) = n.$$

In order to show why this is true, we will give an argument in the case where $n = 12$. However, the same argument will work when 12 is replaced with any whole number n.

If $n = 12$, we observe that the (positive) divisors of n are 1, 2, 3, 4, 6, and 12. So, using the notation from above, our goal is to show that

$$\sum_{d \mid 12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12.$$

Of course, we could just compute $\varphi(1)$, $\varphi(2)$, $\varphi(3)$, $\varphi(4)$, $\varphi(6)$, and $\varphi(12)$ and add them together. That said, since we want to write a proof that generalizes to any value of n, we will give a different argument (one that doesn't rely on knowing the specific φ-values!). The first step is to write down all of the fractions with denominator 12 and numerator between 1 and 12:

$$\frac{1}{12} \quad \frac{2}{12} \quad \frac{3}{12} \quad \frac{4}{12} \quad \frac{5}{12} \quad \frac{6}{12} \quad \frac{7}{12} \quad \frac{8}{12} \quad \frac{9}{12} \quad \frac{10}{12} \quad \frac{11}{12} \quad \frac{12}{12}$$

Next, we will go through the list of fractions and rewrite each of them in "lowest terms":

$$\frac{1}{12} \quad \frac{1}{6} \quad \frac{1}{4} \quad \frac{1}{3} \quad \frac{5}{12} \quad \frac{1}{2} \quad \frac{7}{12} \quad \frac{2}{3} \quad \frac{3}{4} \quad \frac{5}{6} \quad \frac{11}{12} \quad \frac{1}{1}$$

[2] See Notation Station on page **Error! Bookmark not defined.** for more information on sigma notation.

Now, we will go through and count the number of fractions with a given denominator, compiling our data into the following list:

d	**# of fractions with denominator *d***
1	1
2	1
3	2
4	2
6	2
12	4

Notice that there are always $\varphi(d)$ fractions with denominator d (for d = 1, 2, 3, 4, 6, and 12) and that the total number of fractions in our list is (still) equal to 12. This pattern will always hold, regardless of the number that we choose for n. As an exercise, try to think about why this argument works for *any* choice of n. (Hint: It has to do with the fact that we are making the numerator and denominator relatively prime when we rewrite each of the fractions in lowest terms.)

The History (and Future) of φ

The Euler totient function dates all the way back to 1760, when Leonhard Euler unveiled it to the world. However, it wasn't until forty years later when Gauss wrote his famous *Disquisitiones Arithmeticae* that the modern-day "φ" notation started to be used. In spite of the fact that mathematicians have studied Euler's totient function for over 250 years, there is still a lot that we do not know about this (somewhat mysterious) function. For example, D. H. Lehmer posed the question, "Are there any composite numbers n such that $\varphi(n) \mid (n-1)$?" This question has not yet been answered, in spite of the best efforts of many experts in the field.

Another unsolved problem about Euler's totient function is called Carmichael's conjecture, which says that if there is a number n for which $\varphi(n) = m$ then there is at least one other number (call it n') with $\varphi(n') = m$. In other words, if we were to list the totients of all the positive numbers, every totient would appear on our list at least twice. Carmichael's conjecture has been checked for all "small" values of n. Here, "small" is a relative term — with the help of computers, mathematicians have shown that any counterexample to Carmichael's conjecture must be at least $10^{10^{10}}$! However, since there are infinitely many positive whole numbers, we are still infinitely far away from finding a solution. The good news is that there are still plenty of interesting questions about the φ-function that are waiting to be answered. Perhaps some of you will answer them one day!

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Table of the first 30 φ values.