Math Diversion 561

P. Reany

May 5, 2025

> Talent is cheaper than table salt. What separates the
> talented individual from the successful one
> is a lot of hard work.
> — Stephen King

1 The Problem

Let $\varphi(n)$ be the number of positive integers less than n that are relatively prime to n.[1] Let p be a prime and k a positive integer. Show that

$$\varphi(p^k) = p^k - p^{k-1}\,. \tag{1}$$

2 The Preparation

Definition: Let a, b be two positive integers. The **greatest common divisor** of a, b, written as $\mathrm{GCD}(a, b)$, is the largest integer that divides both a and b evenly.

Definition: If the greatest integer that divides both a and b evenly is unity, that is, if

$$\mathrm{GCD}(a, b) = 1\,, \tag{2}$$

then a and b are said to be **relatively prime** or **coprime**.

Definition: Let G be a finite set. The **number of elements** of G, or the **cardinality** of G, is represented by the symbol $|\,G\,|$.

Heuristic: In counting problems, it's often effective to start with a 'count' that you know is an overcount, that is, it contains more elements than fit the set being described. One reason to proceed this way is because that may be an easy place to get started.

Anyway, if we know we've performed an overcount, the logical next step is to remove all the elements in the overcount set. The trick to this method is to find an efficient way to characterize this overcount set.

[1] This function $\varphi(n)$ is referred to as the Euler Totient Function.

By the way, I leave it to the reader to prove the following:

$$\varphi(p) = p - 1\,. \tag{3}$$

3 The Solution

My plan is to adopt this method of overcount to see where it takes us. So, to a first approximation let's include in our 'set of all positive integers relatively prime to p^k' all the integers from 1 to p^k. Then

$$\varphi(p^k) \approx' p^k\,. \tag{4}$$

Okay, so how do we characterize the subset of this set that defines the overcount set? Well, there are two properties that apply to each element in the overcount set:

1) The element has a factor of p in it. (This characteristic guarantees that the product element won't be relatively prime to p^k.)

2) The element must be less than or equal to p^k. Okay, I know that it seems silly to state such an obvious condition, but it will come in handy.

Now all we have to do is to find an implementation of this scheme we've devised. To that end, let S be the set of all integers defined by[2]

$$S \equiv [1..p^k]\,. \tag{5}$$

To discover the overcount set, may I suggest that we begin with the subset of S, which I'll call $\overline{S}$, defined as such

$$\overline{S} \equiv [1..p^{k-1}]\,. \tag{6}$$

In the hope of catching the overcount elements, let's define the derivative set on $\overline{S}$:

$$p\overline{S} \equiv \{px \,|\, x \in [1..p^{k-1}]\}\,. \tag{7}$$

Clearly, every element in this set satisfies the two defining characteristics of the elements in the overcount set. But are there any we've missed. Well, what's left in the set S that we haven't included in the set $\overline{S}$? Answer: Elements larger than p^{k-1} but smaller than p^k. But if we multiply any one of these elements by p, in order to satisfy Condition 1), we end up with a number that's out of range (i.e., $> p^k$), violating Condition 2). Therefore, $p\overline{S}$ is exactly the overcount set. But how big is it?

Well, there is a 1-to-1 mapping from the set $\overline{S}$ to the set $p\overline{S}$, provided by multiplying the elements of $\overline{S}$ by the number p. And since a 1-to-1 map between these sets is also a bijection,[3] then

$$\left|\, p\overline{S} \,\right| = \left|\, \overline{S} \,\right| = p^{k-1}\,. \tag{8}$$

[2] I use the square brackets at times to represent a set containing a sequence.

[3] This mapping is onto precisely because the codomain elements are themselves created by the mapping, therefore it must be onto. In other words, for every $px \in p\overline{S}$, there exists $x \in \overline{S}$.

All we have to do now is to update our 'approximation' given in (4) by subtracting off the overcount value, resulting in

$$\varphi(p^k) = p^k - p^{k-1}\,. \tag{9}$$

4 Afterthoughts

So, how do we know that the mapping f from $\overline{S}$ to $p\overline{S}$ is 1-to-1? Well, when in general is a mapping (function) f from one set to another 1-to-1? The mapping f is 1-to-1 if, whenever

$$f(a) = f(b), \tag{10}$$

then

$$a = b\,. \tag{11}$$

So, if f is the map that sends element x to px, then when does

$$pa = pb? \tag{12}$$

If we were in the real numbers, or even in the rational numbers, we could multiply through by p^{-1}, but I think that that's rather cavalier, don't you? Perhaps better is to consider all the sets we've talked about so far as subsets of the full set of integers. But the ring of integers in an **integral domain**, and as such, it has no zero-divisors.

Definition: Let R be an arbitrary ring with elements x, w, neither of which is zero. Now, if

$$xw = 0\,, \tag{13}$$

then x is called a **zero-divisor** in R. By the way, the same is true of w.

So, if we accept the equality in (12), then, on the basis of a little arithmetic, we can write

$$p(a - b) = 0\,. \tag{14}$$

But, on the claim that the ring of integers is an integral domain, there are no zero divisors, so we are forced to conclude that at least one factor appearing on the LHS of (14) must be zero. But this forces us to conclude that $a - b = 0$, which then forces us to conclude that $a = b$. Hence, we've shown that the mapping is 1-to-1.