SRQR: Euler's ϕ function (April 12, 2021)

> The justification for theorem 7.1 still confuses me a bit.

It might be useful to work out an example. Let's consider $\phi(81)$. Notice that $81 = 3^4$ is the prime factorization of 81, so a number is relatively prime with 81 if and only if it is not divisible by 3. In other words, to calculate $\phi(81)$, we have to calculate how many integers between 1 and 81 are *not* divisible by 3. Equivalently, we can count how many *are* divisible by 3 and then subtract that number for 81. The ones that are divisible by 3 are:

$$3, 6, 9, 12, 15, \ldots, 78, 81.$$

How many multiples of 81 are there here? Well, it's 3 times 1, 3 times 2, 3 times 3, and so forth, all the way up to 3 times 27 (which is 81). In other words, we have $81/3$ numbers between 1 and 81 that are multiples of 3. Thus

$$\phi(81) = 81 - \frac{81}{3} = 81 \cdot \left(1 - \frac{1}{3}\right).$$

> Why (on bottom of page 133) is k congruent j mod n a contradiction?

It's because $0 \leqslant k < j < n$. This inequality means that $0 < j - k < n$, but there are no multiples of n strictly between 0 and n, so n cannot divide $j - k$. In other words, j cannot be congruent to k mod n.

> I'm not totally understanding the application of theorem 7.3 to example 7.1. Specifically, I'm confused how the fraction $(1 - \frac{1}{p_k})$ accounts for the exponents of the prime factors?

The fraction doesn't account for the power! That's one of the interesting things about this formula for Euler's ϕ function. The only reason $\phi(n)$ remembers that power is because of the "n'' that shows up in the very beginning:

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

> In the proof of theorem 7.4, how do we know p^k and m must be relatively prime? This seems to be important, since if I understood the previous proofs correctly, the two numbers being relative primes is a necessary condition for the multiplicative property of the ϕ function to hold.

The claim is that if $n \geqslant 2$ and p is one of its prime divisors, then there exists an integer k such that $n = p^k m$ for some integer m such that $\gcd(p^k, m) = 1$. There are various ways to prove this.

Here's one possibility. Let $p_1, \ldots, p_s$ be all of its prime divisors besides p (I allow the possibility that $s = 0$ here). Then the fundamental theorem of arithmetic implies that I can write $n = p^k p_1^{k_1} \cdots p_s^{k_s}$ for positive integers $k, k_1, \ldots, k_s$. Then let $m = p_1^{k_1} \cdots p_s^{k_s}$, so that $n = p^k m$. Notice that p is the only prime divisor of p^k, while $p_1, \ldots, p_k$ are the prime divisors of m, so p^k and m share no prime divisors. Thus $\gcd(p^k, m) = 1$.

Here's another possibility. Let k be the largest integer such that $p^k \mid n$ and let $m = n/p^k$. We want to show that $d = \gcd(p^k, m) = 1$, so suppose for a contradiction that $d \neq 1$. Since d divides p^k, its only prime factor is p, so $p \mid d$. But d also divides m, so $p \mid m$. But then $p \mid m$ and $p^k \mid p^k$ implies that $p^{k+1} \mid mp^k = n$ (cf. theorem 2.2(c)), which contradicts our choice of k as the largest power of p which divides n.

> I remember learning about Euler's method during calculus. Does this topic have anything to do with that besides their sharing of the name?

The Euler's method that I know from calculus is the one that's used to solve differential equations. At least to me, it doesn't seem like Euler's ϕ function has anything to do with that Euler's method beyond the fact that they're both named after the same person. But Euler was quite a prolific mathematician and there's a lot of stuff named after him.

> My question may seem unrelated to the reading. While I was writing my answers, I wanted to say that "according to the theorem we have . . . ", but in some cases, though I know where the theorem is in the textbook, I am still unsure of the name of the theorem (or if the theorem has a name). So, I was wondering if there is a formal way to quote these theorems when writing my response to the problem.

Yes, most theorems do not have names! If you know where it is in the book, one possibility is to cite the theorem by its number ("according to theorem 7.4, . . . "). Another possibility is to just make sure that you phrase things in a way that makes clear what theorem you're talking about. This takes some practice, but ultimately I think it's easier than having to look through the book to find theorem numbers.

The one thing I would caution you about if you use the second strategy is that you should be pretty confident that the theorem is in fact a theorem in the book.

For example, let's say I have some number n and I've just shown that 2 and 7 both divide n. I want to conclude that 14 divides n. Here's what the two options I've suggested above would look like:

- Since $\gcd(2, 7) = 1$, corollary 2 after theorem 2.4 implies that $14 \mid n$.

- Since $2 \mid n$, $7 \mid n$, and $\gcd(2, 7) = 1$, we can conclude that $14 = 2 \cdot 7 \mid n$ as well.