SRQR: Order, Primitive Roots for Primes (April 14, 2021)

> In the proof for theorem 8.1, where do we choose k as the smallest positive integer such that $a^k \equiv 1 \bmod n$?

That's how k is defined in the theorem statement. Remember that the order of a mod n is defined to be the smallest positive integer such that $a^k \equiv 1 \bmod n$.

The first part of the proof doesn't use the fact that k is the order, but the second part really does make use of this. The rough idea is that, if you had some h not divisible by k such that $a^h \equiv 1 \bmod n$, then you could divide h by k and get a remainder r that's nonzero and smaller than k and that also has the property that $a^r \equiv 1 \bmod n$.

> I'm not sure if I understood example 8.2 correctly. My understanding is that because $2(n+1) < 2(2^n)$ for $n > 1$, then $2(n+1) < \phi(n)$. Therefore, by definition 8.2, 2 is not of order $\phi(n)$ modulo n, then it cannot be the primitive root of n?

Yes, you've got it I think! In order for 2 to be a primitive root of F_n, it would need to have order $\phi(F_n)$, and if F_n is prime, then $\phi(F_n) = F_n - 1 = 2^{2^n}$. But we can show that 2 has order at most 2^{n+1}, so 2 cannot be a primitive root for F_n.

> Could you explain a little more how theorem 8.4 suggests the corollary that follows? The theorem proves something about the integers but I can't seem to understand why that allows us to find how many there are.

The corollary to theorem 8.4 uses not just theorem 8.4, but also the corollary to theorem 8.3. Let me re-write the proof of the corollary to theorem 8.4 in slightly different words to explain this.

If a is a primitive root of n, then theorem 8.4 tells us that every positive integer less than n and relatively prime to n is congruent to exactly one of the integers $a, a^2, \ldots, a^{\phi(n)}$. That means that any primitive root b must be of the form a^h for some $1 \leqslant h \leqslant \phi(n)$. But then a and $b = a^h$ have the same order, which, by the corollary to theorem 8.3, happens if and only if $\gcd(h, \phi(n)) = 1$. The number of integers h between 1 and $\phi(n)$ such that $\gcd(h, \phi(n))$ is precisely $\phi(\phi(n))$, which proves what we wanted to show.

> At the end of chap 8.1, I wondered why the two primitive roots of 9 are 2 and 5. I thought by the definition, n has a as a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$. Here, n is 9 and $\phi(9)$ is 6. Shouldn't the primitive root be 6?

By definition, a is a primitive root of n if it is relatively prime with n and it has order $\phi(n)$ mod n. (Note that any integer that's relatively prime with n will satisfy $a^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's theorem, so that is not sufficient for checking that something is a primitive root! You really need to know that $\phi(n)$ is the *smallest* exponent that gets you to something that's congruent to 1 mod n.)

6 is not relatively prime with 9, so it can't be a primitive root. The fact that $\phi(9) = 6$ means that we're looking for integers that are relatively prime to 9 and for which 6 is the smallest exponent that gets me to something congruent to 1. This is the case for 2:

$$\begin{aligned} 2^2 &= 4 \\ 2^3 &= 2 \cdot 4 = 8 \\ 2^4 &= 2 \cdot 8 = 16 \equiv 7 \\ 2^5 &\equiv 2 \cdot 7 = 14 \equiv 5 \\ 2^6 &\equiv 2 \cdot 5 = 10 \equiv 1 \end{aligned}$$

Since 6 is the smallest power of 2 which is congruent to 1 mod 9, we see that 2 has order 6, so 2 is a primitive root. You can go through the same kind of calculation with 5 to check that it's also a primitive root.

On the other hand, 4 is relatively prime with 9 but it's *not* a primitive root:

$$\begin{aligned} 4^2 &= 16 \equiv 7 \\ 4^3 &= 4 \cdot 7 = 28 \equiv 1 \end{aligned}$$

Since 3 is the smallest power of 4 which is congruent to 1 mod 9, that tells us that 4 only has order 3 mod 9. It is therefore not a primitive root.

> On page 153, in the proof of Theorem 8.5, what does it mean by "integral coefficients"? Does it just mean the coefficients must be integers, and if so, what is the difference in usage between "integral" and "integer"?

It does just mean that the coefficients should be integers. I think the difference is just that "integer" is a noun and "integral" is an adjective.

Of course, in English, we frequently use nouns as attributives in front of other nouns, so it would be grammatically just fine to say something like "integer coefficients" instead of "integral coefficients."

Not all languages are like this. My understanding is that French, for example, does not like stacking nouns immediately next to other nouns in this way. A lot of research in math was (and, in some areas, continues to be) done in French. In other words, French was sort of a prestige language in math up until very recently. Perhaps as a result of this, some grammatical restrictions of French show in mathematical English prose as well.

I am a bit confused on concepts from 8.2. Could you do problem 8.2.1(a)?

If $x \equiv 1 \pmod{p}$, then $x^2 \equiv 1^2 = 1 \pmod{p}$ as well by theorem 4.2(f). If $x \equiv p-1 \pmod{p}$, then

$$x \equiv p - 1 \equiv -1 \pmod{p}$$

so $x^2 \equiv (-1)^2 = 1 \pmod{p}$ again by theorem 4.2(f). Also, 1 and $p-1$ are incongruent mod p, so $x \equiv 1$ and $x \equiv p-1$ are two (mutually) incongruent solutions mod p.

The final step is to say why these are the only two solutions. Notice that $x^2 \equiv 1 \pmod{p}$ if and only if $x^2 - 1 \equiv 0 \pmod{p}$. By the corollary to theorem 8.5, we know that this congruence has exactly 2 solutions. But we've already found 2 solutions (namely, 1 and $p-1$), so these must be the only two solutions.