Skeleton key to non-existence of primitive roots

Suppose $p$ is an odd prime. An integer $a$, $1 \leq a < p$, is called a primitive root modulo $p$ if $\{a^r \mid 0 \leq r < p\}$ generates the group $(\mathbb{Z}/p\mathbb{Z})^*$, which turns out to be cyclic of order $p-1$. We already know that if $1 \leq a < p$, then the order of $a^k$ is $\frac{p-1}{\gcd(p-1, k)}$, from general facts about cyclic groups.

The main point is that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, which is not obvious and we do this by showing the existence of such a generator. If $a$ is a generator, then so is $a^k$, where $\gcd(k, p-1) = 1$, but first we have to find one.

Building Blocks:

(i) The Principle of Inclusion and Exclusion for Finite Sets

Let $S$ be a set, $S_1, S_2, \ldots, S_n$ subsets of $S$, and let $|X|$ denote the number of elements in $X$. We are interested in $|A_1 \cup A_2 \cup \cdots \cup A_n|$, the number of elements in the complement of $A_1, A_2, \ldots, A_n$; that is, the number of elements which are in none of $A_k$.

Familiar Example:

For $n = 3$:

$|A_1 \cup A_2 \cup A_3| = 15 - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|

The general formula is the same:

$|A_1 \cup \cdots \cup A_n| = 15 - \sum |A_i| + \sum |A_i \cap A_j| - \sum |A_i \cap A_j \cap A_k| + \cdots$, etc.
My guess is that many of you have seen this before. Proofs are easy to find in textbooks and even Wikipedia!

2. The Euler-Phi function

Suppose \( n = p_1^{a_1} \cdots p_r^{a_r} \) is written in its usual prime factorization. Let \( \phi(n) \) denote the number of \( \alpha, 1 \leq \alpha \leq n \) so that \( \gcd(\alpha, n) = 1 \). Notice that \( \gcd(\alpha, n) = 1 \) if and only if \( p_1, a_1, p_2, a_2, \ldots, p_r, a_r \). For any \( p_i \), let

\[
\alpha_i = \{ \alpha : 1 \leq \alpha \leq n \mid p_i \nmid \alpha \}
\]

So \( \phi(n) \) is precisely \( |\alpha_1 \times \alpha_2 \times \cdots \times \alpha_r| \). (If \( \gcd(\alpha, n) = 1 \) then \( \alpha \in \alpha_1 \times \alpha_2 \times \cdots \times \alpha_r \) and vice versa.)

How big are \( \alpha_i \)? \( |\alpha_i| = \frac{n}{p_i} \)

How big is \( \alpha_1 \times \alpha_2 \times \cdots \times \alpha_r \)? \( |\alpha_1 \times \alpha_2 \times \cdots \times \alpha_r| = \prod_{i=1}^{r} \frac{n}{p_i} \)

If we apply (1) to this, we see that

\[
\phi(n) = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \cdots
\]

and this factors onto \( n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) \), which is \((p_1^{a_1 - 1} \cdots p_r^{a_r - 1})(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})\). Since

\[
p_i^{a_i}(1 - \frac{1}{p_i}) = p_i^{a_i - 1} - p_i^{a_i - 2}
\]

This is our old formula!

3. We saw in class a sequence of theorems

a. Corollary 23.5. A non-zero polynomial \( f \in F[x] \) can have at most \( n \) zeros in a field \( F \).
I proved in class that if $f(x)g(x) = h(x)$, $d \equiv g \equiv n \equiv$ and $d \equiv f \equiv n$, and $f$ has $n$ zeros, then $g$ has $n$ zeros and $h$ has $n - s$ zeros. The proof is basically that if $g$ has $s$ zeros ($s \leq n$) and $h$ has $t_1$ zeros ($t_1 \leq n - s$) by 23.5, but any zero of $f$ must be a zero of $g$ or a zero of $h$. So, $n = s + t_1 \leq s + (n - s) = n$, so there is equality.

b. Fermat's Theorem says that $a^{p-1} \equiv 1 \pmod{p}$ for all $a$, $\gcd(a, p) = 1$. Thus, the polynomial $x^{p-1} - 1$ has $p-1$ zeros in $(\mathbb{Z}/p\mathbb{Z})[x]$. Since this is a field, if any polynomial $f(x)$ is a factor of $x^{p-1}$ and $f$ has degree $d$, then $f$ has $d$ zeros. In particular, if $p-1 = de$, then

$$x^{p-1} - 1 = (x^d - 1)(x^{de-2} + x^{de-3} + \ldots + x + 1)$$

So, the equation $x^{d-1} = 0$ has $d$ zeros in $(\mathbb{Z}/p\mathbb{Z})[x]$.

c. Suppose $p-1 = p_1^{e_1} \ldots p_r^{e_r}$. Let $\alpha$ be a primitive root. Then the order of $\alpha$ is less than $p-1$, so $\alpha$ is a zero of $x^{d-1}$ for some $d < p-1$, where $d|p-1$.

Let's be specific. Write $p-1 = de$, where $d > 1$. Then $e$ is also a factor of $p-1$, so some $p_i$, $i \leq e$. What this means is that $p^{-1}_i = \frac{d}{p_i}$, where everything here is an integer. Thus, if $d < p-1$, then $d|p_i$, and if $d = 1 \pmod{p}$, then $\alpha^{p_i} = 1 \pmod{p}$ as well. Now: Let $S = (\mathbb{Z}/p\mathbb{Z})^*$, $A = \{a : 1 \leq a \leq p-1, \alpha \equiv 1 \pmod{p}\}$

Yeah, I know it looks funny. But if $a$ is not a primitive root, then $\alpha = \alpha^e$ for some $e$, so $ae \equiv A \pmod{p}$. And if $a$ is a primitive root, then $ae \equiv (A \pmod{p}$.
Let's count. \( S = \phi - 1 \) \( \frac{p-1}{p-1} \) because \( x^{p-1} \) has \( p-1 \) roots. What about \( 1A_1 = 1AA_1 \) ? Thus (key)

\[ A_1A_2 \Rightarrow \frac{p-1}{p-1} = 1 \mod p \text{ and } a \frac{p-1}{p-1} = 1 \mod p \Rightarrow \]

\[ a \frac{p-1}{p-1} = 1 \mod p \Rightarrow a^{\frac{p-1}{p-1}} = 1 \mod p \]

because \( \gcd(p-1, p) = p-1 \). (This is an old lemma and if you didn't believe it, work some examples.)

So how many primitive roots are there? (I'm hoping \( > 0 \)) By inclusion/exclusion, as

\[ 1 \leq \sum (A_1) + \sum (A_1A_2) - \sum (A_1A_2A_3) \leq p-1 \leq \sum \frac{p-1}{p-1} + \sum \frac{p-1}{p-1} - \sum \frac{p-1}{p-1} \]

We've seen this before. It's \( \phi(p-1) \)

and \( \phi(s) \) is positive!

**Example:**

\[ p = 31, \quad p-1 = 30 = 2 \cdot 3 \cdot 5 \]

\[ S = \{ 1, 3, 5, 6, 10, 11, 15, 17, 19, 23, 29, 3 \} \]

\[ A_2 = \{ 30, 1, 3, 5, 6, 10, 11, 15, 17, 19, 23, 29 \} \]

\[ A_1A_2 = \{ 6, 12, 30 \} \]

\[ A_1A_2A_3 = \{ 1, 3, 5, 6, 10, 11, 15, 17, 19, 23, 29, 30 \} \]

\[ \phi(30) = 20 - \frac{20}{2} - \frac{20}{3} - \frac{20}{5} - \frac{20}{6} - \frac{20}{10} - \frac{20}{15} - \frac{20}{30} = 8 \]

\[ \phi(30)|S = 8 \text{ primitive roots mod } 31 \]

\[ 15 a = 2 \text{ one, no!} \]

\[ 2^7 = 32 = 1 \mod 31 \text{ (here } \phi(31) = 30 \text{ really) } 2^7 = 1 \mod 31 \]

It turns out that 3 is a primitive root mod 31, ad thanks to Mathematica. These are

\[ 2^3 \cdot 3^{17} \cdot 3^{11} \cdot 3^{13} \cdot 3^{17} \cdot 3^{19} \cdot 3^{23} \cdot 3^{29} = \{ 3, 17, 13, 22, 12, 11, 21 \} \mod 31 \]