A.2 Primitive Elements for Prime Modules

More difficult (and mathematically more interesting) is the search for primitive elements for a prime module. Since the multiplicative group is cyclic it suffices to find *one* primitive element—all the other ones are powers of it with exponents coprime with $p-1$. In particular there are exactly $\varphi(p-1)$ primitive elements $\bmod p$. Usually the primitive elements for any module n where $\mathbb{M}_n$ is cyclic are also called **primitive roots** $\bmod n$.

The simplest, but not best, method is trying $x = 2, 3, 4, \ldots$, and testing if $x^d \neq 1$ for each proper divisor d of $p-1$. We need not to test all divisors:

Lemma 12 *Let p be a prime ≥ 5. An integer x is primitive $\bmod p$, if and only if $x^{(p-1)/q} \neq 1$ in $\mathbb{F}_p$ for each prime factor q of $p-1$.*

Proof. The order of x divides $p-1$, and each proper divisor of $p-1$ divides at least one of the quotients $\frac{p-1}{q}$. $\diamond$

To apply this criterion we need the prime decomposition of $p-1$. Then the test is efficient: The number of prime factors is $\leq \log_2(p-1)$, and for each of them we apply the binary power algorithm.

Example For $p = 41$ we have $p-1 = 40 = 2^3 \cdot 5$. Hence x is primitive if and only if $x^{20} \neq 1$ and $x^8 \neq 1$. The test runs through the following steps in $\mathbb{F}_{41}$:

$$\begin{array}{llll}
x = 2: & x^2 = 4, & x^4 = 16, & \begin{cases} x^8 = 10, \\ x^{20} = x^8x^8x^4 = 1. \end{cases} \\
x = 3: & x^2 = 9, & x^4 = 81, & x^4 = -1,\ x^8 = 1. \\
x = 4: & x = 2^2, & \text{hence} & x^{20} = 1. \\
x = 5: & x^2 = 25, & x^4 = 10 & \begin{cases} x^8 = 18, \\ x^{20} = x^8x^8x^4 = 1. \end{cases} \\
x = 6: & x^2 = 36, & x^4 = 25 & \begin{cases} x^8 = 10, \\ x^{20} = x^8x^8x^4 = -1. \end{cases}
\end{array}$$

Hence 6 *is a primitive root for* $p = 41$.

The obvious question is how many integers must we try to find a primitive root? The quantity

$$\alpha(p) := \min\{x \in \mathbb{N} \mid x \text{ is primitive for } p\}$$

measures the complexity of complete search (but neglects the complexity of the proof of primitivity). It is known that the the function α is not bounded. In 1962 Burgess proved

$$\alpha(p) = \mathrm{O}(\sqrt[6]{p}).$$

Assuming ERH this exponential bound may be lessened to a polynomial one. The best known result is by SHOUP 1990:

$$\alpha(p) = \mathrm{O}(\log(p)^6(1 + \log\log(p))^4).$$

Even completely simple questions are yet unanswered:

- Is 2 primitive for infinitely many primes?
- Is 10 primitive for infinitely many primes? (GAUSS' conjecture)

ARTIN more generally conjectured: If $a \in \mathbb{N}$, and a is not an integer square (i. e. $a \neq 0, 1, 4, 9, \ldots$), then a is primitive for infinitely many primes.

Some relevant references:

- D. R. HEATH-BROWN: Artin's conjecture for primitive roots. Quart. J. Math. Oxford 37 (1986), 27–38.
- M. RAM MURTY: Artin's conjecture for primitive roots. Math. Intelligencer 10 (1988), 59–67.
- V. SHOUP: Searching for primitive roots in finite fields. Proc. 22nd STOC 1990, 546–554.
- MURATA: On the magnitude of the least prime primitive root. J. Number Theory 37 (1991), 47–66.