HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 2

Mehmet Taha USTA – 21527472

Subject: What is the primitive root? Show an example

Primitive roots

A primitive root b modulo m is a generator for the group $(\mathbb{Z}/m)^\times$. Existence of a primitive root modulo m is equivalent to the cyclic-ness of the multiplicative group $(\mathbb{Z}/m)^\times$. For p prime, $(\mathbb{Z}/p)^\times$ is cyclic, because $\mathbb{Z}/p$ is a field. Relatively elementary arguments then show that there are primitive roots modulo p^ℓ and $2p^\ell$ for $p > 2$ prime, and modulo 4. Non-existence of primitive roots for all other moduli is easier. This was understood by Fermat and Euler.

Because of the cyclic-ness of $(\mathbb{Z}/p)^\times$ for $p > 2$ prime, we have **Euler's criterion**: $b \in (\mathbb{Z}/p)^\times$ is a square modulo p if and only if

$$b^{(p-1)/2} = 1 \bmod p$$

An analogous result holds for q^{th} powers when p is a prime with $p = 1 \bmod q$.

Modulo a prime p, for a fixed primitive root b, for $x \in (\mathbb{Z}/p)^\times$ the **discrete logarithm** or **index** of x modulo p base g is the integer ℓ (uniquely determined modulo $p-1$) such that

$$x = b^\ell \bmod p$$

$$\begin{array}{lclclclclcl}
3^1 & = & 3 & = & 3^0 \times 3 & \equiv & 1 \times 3 & = & 3 & \equiv & 3 \pmod 7 \\
3^2 & = & 9 & = & 3^1 \times 3 & \equiv & 3 \times 3 & = & 9 & \equiv & 2 \pmod 7 \\
3^3 & = & 27 & = & 3^2 \times 3 & \equiv & 2 \times 3 & = & 6 & \equiv & 6 \pmod 7 \\
3^4 & = & 81 & = & 3^3 \times 3 & \equiv & 6 \times 3 & = & 18 & \equiv & 4 \pmod 7 \\
3^5 & = & 243 & = & 3^4 \times 3 & \equiv & 4 \times 3 & = & 12 & \equiv & 5 \pmod 7 \\
3^6 & = & 729 & = & 3^5 \times 3 & \equiv & 5 \times 3 & = & 15 & \equiv & 1 \pmod 7 \\
3^7 & = & 2187 & = & 3^6 \times 3 & \equiv & 1 \times 3 & = & 3 & \equiv & 3 \pmod 7
\end{array}$$

On Cryptographic Primitive Roots

We call primitive roots which are small powers of small primes *cryptographic primitive roots*. Without small primitive roots which are a prime power, a prime may have little cryptographic value for stream ciphers. Thus the distribution of primitive roots has cryptographic importance. This distribution has been investigated by many scholars.