A.3 Primitive Elements for Prime Powers

For prime powers we need one more lemma.

Lemma 13 *Let p be prime ≥ 3, k, an integer, and $d \geq 0$. Then*

$$(1+kp)^{p^d} \equiv 1 + kp^{d+1} \pmod{p^{d+2}}.$$

Proof. For $d = 0$ the statement is trivial. For $d \geq 1$ we reason by induction: Assume

$$(1+kp)^{p^{d-1}} = 1 + kp^d + rp^{d+1} = 1 + (k+rp)p^d.$$

Then

$$(1+kp)^{p^d} = (1+(k+rp)p^d)^p \equiv 1 + p \cdot (k+rp) \cdot p^d \equiv 1 + kp^{d+1} \pmod{p^{d+2}},$$

since $d + 2 \leq 2d + 1$ and $p \geq 3$. $\diamond$

Proposition 18 *Let p be prime ≥ 3, e, an exponent ≥ 2, and a be primitive* $\bmod\, p$. *Then:*

(i) *a generates the group $\mathbb{M}_{p^e}$ if and only if $a^{p-1} \bmod p^2 \neq 1$.*

(ii) *a or $a + p$ generates $\mathbb{M}_{p^e}$.*

(iii) *$\mathbb{M}_{p^e}$ is cyclic, and $\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$.*

Proof. (i) Let t be the multiplicative order of $a \bmod p^e$, necessarily a multiple of the order of $a \bmod p$, hence of $p - 1$. On the other hand t divides $\varphi(p^e) = p^{e-1}(p-1)$. Hence $t = p^d(p-1)$ with $0 \leq d \leq e - 1$.

Choose k such that $a^{p-1} = 1 + kp$. Then by Lemma 13

$$(a^{p-1})^{p^{e-2}} \equiv 1 + kp^{e-1} \equiv 1 \pmod{p^e} \iff p|k \iff a^{p-1} \equiv 1 \pmod{p^2}.$$

This is *not* the case if and only if $d = e - 1$.

(ii) Assume a doesn't generate $\mathbb{M}_{p^e}$. Then $a^{p-1} \equiv 1 \pmod{p^2}$, hence

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 - a^{p-2} \pmod{p^2},$$

and this is not $\equiv 1 \pmod{p^2}$.

(iii) follows immediately from (ii). $\diamond$

We immediately get an analogous result for modules that are twice a prime power:

Corollary 1 *Let $q = p^e$ be a power of a prime $p \geq 3$. Then:*

(i) *The multiplicative group* $\mathbb{M}_{2q}$ *is canonically isomorphic with* $\mathbb{M}_q$*, hence cyclic.*

(ii) *If* a *is a primitive element* $\bmod q$*, then* a *is primitive* $\bmod 2q$ *for odd* a*, and* $a + q$ *is primitive* $\bmod 2q$ *for even* a*.*

(iii) $\lambda(2p^e) = p^{e-1}(p-1)$.

Proof. (i) Since q and 2 are coprime, and $\mathbb{M}_2$ is the trivial group, by the chinese remainder theorem $\mathbb{M}_{2q} \cong \mathbb{M}_2 \times \mathbb{M}_q \cong \mathbb{M}_q$. This map is explicitely given by $a \bmod 2q \mapsto a \bmod q$.

(ii) Exactly one of a and $a + q$ is odd, hence coprime with $2q$. Thus the inverse isomorphism is

$$a \mapsto \begin{cases} a, & \text{if } a \text{ is odd,} \\ a + q, & \text{if } a \text{ is even.} \end{cases}$$

(iii) obvious. $\diamond$