A.1 Primitive Elements for Powers of 2

The cases $n = 2$ or 4 are trivial: $\mathbb{M}_2$ is the one-element group. $\mathbb{M}_4$ is cyclic of order 2, thus $3 \equiv -1 \pmod 4$ is primitive.

From now on we assume $n = 2^e$ with $e \geq 3$. Note that $\mathbb{M}_n$ consists of the residue classes of the odd integers, hence $\varphi(n) = 2^{e-1}$.

Lemma 10 *Let $n = 2^e$ with $e \geq 2$.*

(i) *If a is odd, then*

$$a^{2^s} \equiv 1 \pmod{2^{s+2}} \quad \textit{for all } s \geq 1.$$

(ii) *If $a \equiv 3 \pmod 4$, then $n \mid 1 + a + \cdots + a^{n/2-1}$.*

Proof. (i) First we prove the statement for $s = 1$. In the case $a = 4q + 1$ we have $a^2 = 16q^2 + 8q + 1$. In the case $a = 4q + 3$ we have $a^2 = 16q^2 + 24q + 9$, hence $a^2 \equiv 1 \pmod 8$.

The assertion for general s follows by induction:

$$a^{2^{s-1}} = 1 + t2^{s+1} \Longrightarrow a^{2^s} = (a^{2^{s-1}})^2 = 1 + 2t2^{s+1} + t^2 2^{2s+2}.$$

(ii) By (i) we have $2n = 2^{e+1} \mid a^{n/2} - 1$. Since only the first power of 2 divides $a - 1$ we conclude

$$n = 2^e \mid \frac{a^{n/2} - 1}{a - 1}$$

as claimed. $\diamond$

Lemma 11 *Let p a prime and e an integer with $p^e \geq 3$. Let p^e be the largest power of p that divides $x - 1$. Then p^{e+1} is the largest power of p that divides $x^p - 1$.*

Proof. We have $x = 1 + tp^e$ with an integer t that is not a multiple of p. The binomial theorem yields

$$x^p = 1 + \sum_{k=1}^{p} \binom{p}{k} t^k p^{ke}.$$

Since p divides all binomial coefficients $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $k = 1, \ldots, p-1$ we can factor out p^{e+1} from the sum:

$$x^p = 1 + tp^{e+1}s$$

with some integer s. Hence p^{e+1} divides $x^p - 1$. It remains to show that s is not a multiple of p. We take a closer look at s:

$$\begin{aligned} s &= \sum_{k=1}^{p} \frac{1}{p}\binom{p}{k} \cdot t^{k-1} p^{e(k-1)} \\ &= 1 + \frac{1}{p}\binom{p}{2} \cdot tp^e + \cdots + \frac{1}{p} \cdot t^{p-1} p^{e(p-1)}. \end{aligned}$$

Since $p^e \geq 3$ we have $e(p-1) \geq 2$, hence $s \equiv 1 \pmod{p}$. $\diamond$

Lemma 10 implies

$$a^{2^{e-2}} \equiv 1 \pmod{n} \quad \text{for all odd } a.$$

Hence the exponent $\lambda(n) \leq 2^{e-2}$, and $\mathbb{M}_n$ is not cyclic. More exactly:

Proposition 17 *Let $n = 2^e$ with $e \geq 3$. Then:*

(i) *The order of -1 in $G = \mathbb{M}_n$ is 2, the order of 5 is 2^{e-2}, and G is the direct product of the cyclic groups generated by -1 and 5.*

(ii) *If $e \geq 4$, then the primitive elements $\bmod n$ are the integers $a \equiv 3,\ 5 \pmod{8}$. Their number is $n/4$.*

Proof. (i) Since $\operatorname{ord} 5 \mid 2^e$ and $\operatorname{ord} 5 \leq 2^{e-2}$, we conclude that $\operatorname{ord} 5$ is a power of 2 and $\leq 2^{e-2}$.

Now 2^2 is the largest power of 2 in $5-1$, thus 2^3 is the largest power of 2 in $5^2 - 1$ (by Lemma 11). Successively we conclude that 2^{e-1} is the largest power of 2 in $5^{2^{e-3}} - 1$. Hence the 2^{e-2}-th power of 5 is the smallest one $\equiv 1 \pmod{2^e}$.

The product of the two subgroups is direct since -1 is not a power of 5—otherwise $5^k \equiv -1 \pmod{n}$, and, because of $e \geq 2$, also $5^k \equiv -1 \pmod{4}$, contradicting $5 \equiv 1 \pmod{4}$.

The direct product is all of G since its order is $2 \cdot 2^{e-2}$.

(ii) By (i) each element $a \in G$ has a unique expression of the form $a = (-1)^r 5^s$ with $r = 0$ or 1, and $0 \leq s < 2^{e-2}$. Hence a^k equals 1 in $\mathbb{Z}/n\mathbb{Z}$ if and only if kr is even and ks is a multiple of 2^{e-2}. In particular then k is even. If s is even, then the condition is satisfied for some $k < 2^{e-2}$. Thus a is primitive if and only if s is odd, or equivalently $a \equiv \pm 5 \pmod{8}$. $\diamond$

As a corollary we have $\lambda(2^e) = 2^{e-2}$ for $e \geq 4$, and $\lambda(8) = 2$.