A.4 The Structure of the Multiplicative Group

The previous results allow a complete characterization of the modules n for which the multiplicative group $\mathbb{M}_n$ is cyclic:

Corollary 2 (Gauss 1799) *For $n \geq 2$ the multiplicative group $\mathbb{M}_n$ is cyclic if and only if n is one of the integers 2, 4, p^e, or $2p^e$ with an odd prime p.*

Proof. This follows from Proposition 18, Corollary 1, and the following Lemma 14. $\diamond$

Lemma 14 *If $m, n \geq 3$ are coprime, then $\mathbb{M}_{mn}$ is not cyclic, and $\lambda(mn) < \varphi(mn)$.*

Proof. If $n \geq 3$, then $\varphi(n)$ is even. For a prime power this follows from the explicit formula. In the general case we reason by the multiplicativity of the φ-function. We conclude

$$\mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(m)\,\varphi(n) = \varphi(mn),$$

$$\lambda(mn) = \mathrm{kgV}(\lambda(m), \lambda(n)) \leq \mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(mn).$$

Hence $\mathbb{M}_{mn}$ is not cyclic. $\diamond$

Now the structure of the multiplicative group is completely known also for a general module. Let us denote the cyclic group of order d by $\mathcal{Z}_d$.

Theorem 2 *Let $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of the integer $n \geq 2$ with different odd primes $p_1, \ldots, p_r$, and $e \geq 0$, $r \geq 0$, $e_1, \ldots, e_r \geq 1$. Let $q_i = p_i^{e_i}$ and $q_i' = p_i^{e_i - 1}(p_i - 1)$ for $i = 1, \ldots, r$. Then*

$$\mathbb{M}_n \cong \begin{cases} \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{if } e = 0 \text{ or } 1, \\ \mathcal{Z}_2 \times \mathcal{Z}_{2^{e-2}} \times \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{if } e \geq 2. \end{cases}$$

We find a primitive element $a \bmod n$ by choosing primitive elements $a_0 \bmod 2^e$ (if $e \geq 2$) and $a_i \bmod q_i$ and solving the simultaneous congruences $a \equiv a_i \pmod{q_i}$, and if applicable $a \equiv a_0 \pmod{2^e}$.

Proof. All this follows from the chinese remainder theorem. $\diamond$

Exercise Derive a general formula for $\lambda(n)$.