1.3 The Carmichael Function

We assume $n \geq 2$.

The Carmichael function is defined as the exponent of the multiplicative group $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$:

$$\lambda(n) := \exp(\mathbb{M}_n) = \min\{s \geq 1 \mid a^s \equiv 1 \pmod{n} \quad \text{for all } a \in \mathbb{M}_n\};$$

in other words, $\lambda(n)$ is the maximum of the orders of the elements of $\mathbb{M}_n$.

Remarks

1. Euler's theorem may be expressed as $\lambda(n)|\varphi(n)$ ("exponent divides order"). A common way of expressing it is

   $$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{for all } a \in \mathbb{Z} \text{ with } \gcd(a,n) = 1.$$

   Both versions follow immediately from the definition.

2. If p is prime, then $\mathbb{M}_p$ is cyclic—see Proposition 2 below—, hence

   $$\lambda(p) = \varphi(p) = p - 1.$$

By the chinese remainder theorem we have $\mathbb{M}_{mn} \cong \mathbb{M}_m \times \mathbb{M}_n$, hence by Lemma 22 of Appendix A.10:

Corollary 1 *For coprime $m, n \in \mathbb{N}_2$*

$$\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n)).$$

Corollary 2 *If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime decomposition of $n \in \mathbb{N}_2$, then*

$$\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r})).$$

Remarks

3. The Carmichael function for powers of 2 (proof as **exercise** or in Appendix A.1):

   $$\lambda(2) = 1, \quad \lambda(4) = 2, \quad \lambda(2^e) = 2^{e-2} \quad \text{for } e \geq 3.$$

4. The Carmichael function for powers of odd primes (proof as **exercise** or in Appendix A.3):

   $$\lambda(p^e) = \varphi(p^e) = p^{e-1} \cdot (p-1) \quad \text{for } p \text{ prime} \geq 3.$$

To prove the statement in Remark 2 we have to show that the multiplicative group $\bmod p$ is indeed cyclic. We prove a somewhat more general standard result from algebra:

Proposition 2 *Let K be a field and $G \leq K^\times$ be a finite subgroup of order $\#G = n$. Then G is cyclic and consists exactly of the n-th roots of unity in K.*

Proof. For $a \in G$ we have $a^n = 1$, hence G is contained in the set of zeroes of the polynomial $T^n - 1 \in K[T]$. Thus K has exactly n different n-th roots of unity, and G contains all of them.

Now let m be the exponent of G, in particular $m \leq n$. Lemma 24 of Appendix A.10 yields that all $a \in G$ are even m-th roots of unity. Hence $n \leq m$, so $n = m$, and G has an element of order n. $\diamond$