Relation between additive and multiplicative dynamics

Relation between additive and multiplicative dynamics

Corollary 4.6.1 (Of Euler-Fermat, 4.4.7)

Let m be a modulus and $a \in \Phi(m)$. Then for any integers b, c such that $b \equiv c \pmod{\varphi(m)}$, we have

$$a^b \equiv a^c \pmod{m}.$$

Relation between additive and multiplicative dynamics

Corollary 4.6.1 (Of Euler-Fermat, 4.4.7)

Let m be a modulus and $a \in \Phi(m)$. Then for any integers b, c such that $b \equiv c \pmod{\varphi(m)}$, we have

$$a^b \equiv a^c \pmod{m}.$$

N.B. It is NOT TRUE that $b \equiv c \pmod{m} \Rightarrow a^b \equiv a^c \pmod{m}$ even given $a \in \Phi(m)$. E.g. $2 \in \Phi(7)$. $10 \equiv 3 \pmod{7}$ but $2^{10} \not\equiv 2^3 \pmod{7}$.

1024 8

2 ≠ 1

Relation between additive and multiplicative dynamics

The corollary 4.6.1 relates the additive dynamics on $\mathbb{Z}/\varphi(m)$ and the multiplicative dynamics on $\Phi(m)$:

$$\begin{aligned} \exp_{a \pmod m} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \overline{x} &\longmapsto a^x \pmod m. \end{aligned}$$

Moreover, this map is a *homomorphism* from the abelian group $(\mathbb{Z}/\varphi(m), +, \mathbf{0})$ to the abelian group $(\Phi(m), \cdot, 1)$.

Relation between additive and multiplicative dynamics

The corollary 4.6.1 relates the additive dynamics on $\mathbb{Z}/\varphi(m)$ and the multiplicative dynamics on $\Phi(m)$:

$$\begin{aligned} \exp_{a \pmod m} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \overline{x} &\longmapsto a^x \pmod m. \end{aligned}$$

Moreover, this map is a *homomorphism* from the abelian group $(\mathbb{Z}/\varphi(m), +, \mathbf{0})$ to the abelian group $(\Phi(m), \cdot, 1)$.

But it may not be bijective! E.g. Let 14 be the modulus and consider the base 9. Then $\Phi(14) = \{1, 3, 5, 9, 11, 13\}$ and hence, $\varphi(14) = 6$. However, although $[1]_6$ and $[4]_6$ are different classes in $\mathbb{Z}/\varphi(14)$, 9^1 and 9^4 have the same natural representative in $\Phi(14)$.

Relation between additive and multiplicative dynamics

Definition 4.6.2

Let m be a modulus. Then a *primitive root modulo* m is an element a in $\Phi(m)$ such that the dynamic of $\boxed{\cdot a \pmod{m}}$ consists of only one circle. Namely, any element of $\Phi(m)$ can be expressed as a power of a modulo m.

Definition 4.6.2

Let m be a modulus. Then a *primitive root modulo* m is an element a in $\Phi(m)$ such that the dynamic of $\boxed{\cdot a \pmod m}$ consists of only one circle. Namely, any element of $\Phi(m)$ can be expressed as a power of a modulo m.

Example 4.6.3

3 is a primitive root modulo 14.

$$1 \to 3 \to 9 \to 27 \equiv 13 \to 39 \equiv 11 \to 33 \equiv 5 \to 15 \equiv 1$$

$$\{1, 3, 9, 13, 11, 5\} = \Phi(14)$$

Relation between additive and multiplicative dynamics

However, primitive roots do not always exist.

Example 4.6.4

There is no primitive root modulo 12.

However, primitive roots do not always exist.

Example 4.6.4

There is no primitive root modulo 12.

First, $\Phi(12) = \{1, 5, 7, 11\}$. For each of them, we investigate the multiplicative dynamic.

- $\ell_{12}(1) = 1$. $a \mapsto a$

However, primitive roots do not always exist.

Example 4.6.4

There is no primitive root modulo 12.

First, $\Phi(12) = \{1, 5, 7, 11\}$. For each of them, we investigate the multiplicative dynamic.

- $\ell_{12}(1) = 1$. $a \mapsto a$
- $\ell_{12}(5) = 2$. $1 \mapsto 5 \mapsto 1, 7 \mapsto 11 \mapsto 7$

However, primitive roots do not always exist.

Example 4.6.4

There is no primitive root modulo 12.

First, $\Phi(12) = \{1, 5, 7, 11\}$. For each of them, we investigate the multiplicative dynamic.

- $\ell_{12}(1) = 1$. $a \mapsto a$
- $\ell_{12}(5) = 2$. $1 \mapsto 5 \mapsto 1, 7 \mapsto 11 \mapsto 7$
- $\ell_{12}(7) = 2$. $1 \mapsto 7 \mapsto 1, 5 \mapsto 11 \mapsto 5$

However, primitive roots do not always exist.

Example 4.6.4

There is no primitive root modulo 12.

First, $\Phi(12) = \{1, 5, 7, 11\}$. For each of them, we investigate the multiplicative dynamic.

- $\ell_{12}(1) = 1$. $a \mapsto a$
- $\ell_{12}(5) = 2$. $1 \mapsto 5 \mapsto 1, 7 \mapsto 11 \mapsto 7$
- $\ell_{12}(7) = 2$. $1 \mapsto 7 \mapsto 1, 5 \mapsto 11 \mapsto 5$
- $\ell_{12}(11) = 2$. $1 \mapsto 11 \mapsto 1, 5 \mapsto 7 \mapsto 5$

Relation between additive and multiplicative dynamics

When a primitive root g modulo m exists, we have an *isomorphism* between abelian groups:

$$\begin{aligned} \exp_{g \pmod m} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \overline{x} &\longmapsto g^x \pmod m. \end{aligned}$$

Relation between additive and multiplicative dynamics

When a primitive root g modulo m exists, we have an *isomorphism* between abelian groups:

$$\begin{aligned} \exp_{g \pmod m} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \overline{x} &\longmapsto g^x \pmod m. \end{aligned}$$

In particular, any element a of $\Phi(m)$ can be expressed as a power of g modulo m. Then exponent, which is a congruence class modulo $\varphi(m)$, is called the *discrete logarithm of a to the base g modulo $\varphi(m)$*. Notation: $\log_{g \pmod m}(a)$.