$$\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} = \mathbb{Z}/n\mathbb{Z}$$

↓

It is not just a number, it is a class (infinite set) that consists of all numbers which are divisible by n.

We were discussing polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$.

Given a polynomial, $f(T) = a_0 + a_1 T + \cdots + a_n T^n$

$a_i \in \mathbb{Z}/p\mathbb{Z}$

we defined degree (f) & $|f|$.

For example $p = 7$

$$f(T) = 1 + T + T^2 + \cdots + T^6$$

degree (f) = 6

$|f| = 7^6$

Division of Polynomials

Divide $T^6+T^5+T^4+T^3+T^2+1$ by $T+1 \in \mathbb{Z}/7\mathbb{Z}[T]$.

$$
\begin{array}{r|l}
T+1 & T^6+T^5+T^4+T^3+T^2+1 \\
\hline
 & T^5 \\
 & T^6+T^5 \\
\hline
 & T^4+T^3+T^2+1
\end{array}
$$

$$
\begin{array}{r|l}
T+1 & T^5+T^3+T+6 \\
\hline
 & T^4+T^3+T^2+1 \\
 & T^4+T^3 \\
\hline
 & T^2+1 \\
 & T^2+T \\
\hline
 & -T+1 \\
 & 6T+1 \\
 & 6T+6 \\
\hline
 & -5
\end{array}
$$

$$
\left(T^4+T^3+T^2+1\right)+T^5+T^6 = \underbrace{\left(T^5+T^3+T+6\right)}_{\text{quotient}}(T+1)\underbrace{-5}_{\text{remainder}} \pmod 7
$$

Division in $\mathbb{Z}/p\mathbb{Z}[T]$

Given $f(T), g(T) \in \mathbb{Z}/p\mathbb{Z}[T]$ with $\deg g \leq \deg f$ we can divide & we get a $q(T)$ & $r(T)$ s.t

(quotient) (remainder)

$$f(T) \equiv g(T)\, q(T) + r(T) \pmod{p}$$

where $r(T) = 0$ or $\deg r < \deg g$ $(|r| < |g|)$

Lemma: Under above Conditions, quotient & remainder are unique.

Pf: Suppose $f(T) \equiv g(T)\, q_1(T) + r_1(T) \pmod p$

$f(T) \equiv g(T)\, q_2(T) + r_2(T) \pmod p$

$g(T)\big(q_1(T) - q_2(T)\big) \equiv r_2(T) - r_1(T) \pmod p$

↓

If this is $\neq 0$ $\longrightarrow\leftarrow$

So, $q_1(T) \equiv q_2(T) \pmod p$

$\Rightarrow$ $r_2(T) \equiv r_1(T) \pmod p$

Lemma: If $A(T) \in \mathbb{Z}/p\mathbb{Z}[T]$, then the number of polynomials $B(T) \in \mathbb{Z}/p\mathbb{Z}[T]$ satisfying $|B| < |A|$ is $|A|$.

Pf: If $A = 0$, then lemma holds.

If $|A| = 1$, then $\deg(A) = 0$ & $B = 0$ so lemma holds.

$d = \deg(A) > 0$

$$B = \underbrace{c_0 + c_1 T + \cdots + c_{d-1} T^{d-1}}_{p \text{ possibilities}}$$

No. of possibilities = $\underbrace{p \times p \times \cdots p}_{d \text{ times}}$

$= p^d = |A|$

We have Euclidean algorithm in $\mathbb{Z}/p\mathbb{Z}[T]$

So, we can find GCD of two Polynomials.

" Primes " in $\mathbb{Z}/p\mathbb{Z}[T]$

↓ aka

Irreducible polynomials

What are units in $\mathbb{Z}/p\mathbb{Z}[T]$?

Non-zero constant polynomials

A polynomial $f \in \mathbb{Z}/p\mathbb{Z}[T]$ is $\neq 0$

called <u>irreducible</u> $\iff$

i) f is not a unit

ii) If $f(T) \equiv a(T)\,b(T) \mod p$, then

$a(T)$ or $b(T)$ is a unit in $\mathbb{Z}/p\mathbb{Z}[T]$.

Unique Factorization in $\mathbb{Z}/p\mathbb{Z}[T]$ holds.

$p=2$ — deg 2, 3 polynomials

Which are irreducibles ?

deg 2 —

T^2+T+1 ⟶ Only this is irreducible

T^2+1

T^2+T

T^2

deg 3

$T^3 + T^2 + T + 1$

T^3

$T^3 + T^2 + 1$ ← Irreducible

$T^3 + T^2 + T$

$T^3 + T^2$

$T^3 + T + 1$ ← Irreducible

$T^3 + 1$

$T^3 + T$

Fix a prime p. How many irreducible polynomials are there in $\mathbb{Z}/p\mathbb{Z}[T]$?

Infinitely many because Suppose there are finitely many

Consider $f = g_1 g_2 \cdots g_n + 1$

Either this is a new irreducible or there is an irreducible not equal to g_i that divides f.

Addition and Multiplication Modulo m

$m = 8$

$2 \xrightarrow{+2} 4 \xrightarrow{+2} 6 \xrightarrow{+2} 0 \xrightarrow{+2} 2$

Cycle of length 4

$1 \xrightarrow{+2} 3 \xrightarrow{+2} 5 \xrightarrow{+2} 7 \xrightarrow{+2} 1$

Cycle of length 4

Lemma: Let m be a positive integer.

Let a be an integer. Then

Dynamics of addition of a, mod m consists of m/ℓ cycles of length ℓ, where

$$\ell = \frac{m}{GCD(a,m)}$$

Pf: Take $b \in \mathbb{Z}/m\mathbb{Z}$, want to find smallest k such that

$$b + ka \equiv b \pmod{m}$$

$b + Ra \equiv b \pmod{m} \iff Ra \equiv 0 \pmod{m}$

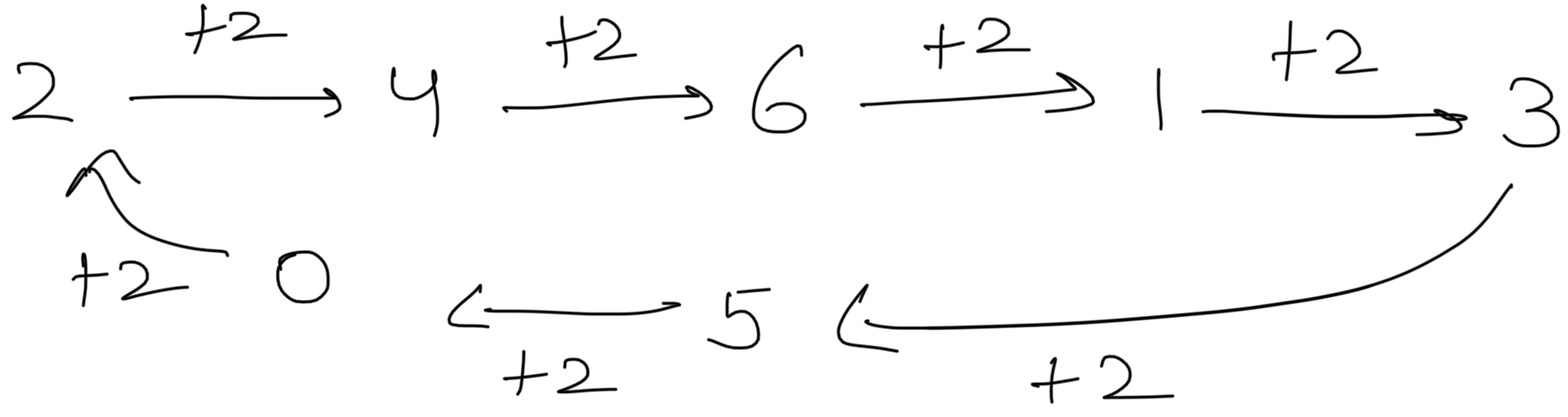
$Ra \equiv lcm(a, m)$

$$R \equiv \frac{lcm(a,m)}{a} = \frac{m}{GCD(a,m)}$$

Qn: When do we get full cycle?

Only when $(a, m) = 1$

$m = 7 \qquad a = 2$



Multiplicative Dynamics

$m = 8$ $\quad a = 2$

$$2 \xrightarrow{\times 2} 4 \xrightarrow{\times 2} \boxed{0}$$

↓

You stay there !

We will assume $(a, m) = 1$

$$S = \{ 1 \leq a < m \mid (a,m) = 1 \}$$

$$\# S = \phi(m)$$

→ Euler Totient function

→ $\phi(p) = p-1 \iff p$ prime

→ $\phi(p^e)$ $(a, p^e) = 1 \iff a$ is not a multiple of p

$\phi(p^e) = p^e - p^{e-1}$

$$\phi(p^e q^f) = p^e q^f - p^{e-1} q^f - p^e q^{f-1} + p^{e-1} q^{f-1}$$

$p \neq q$

p, q primes

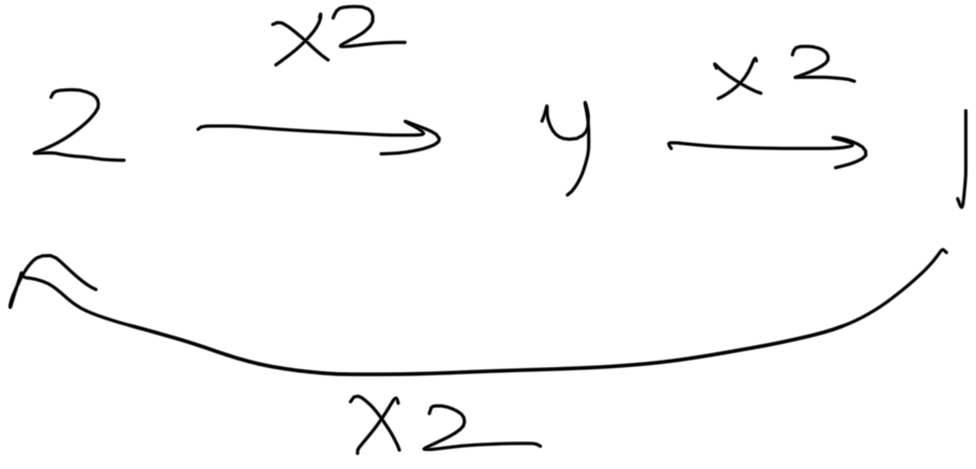
$$= q^f (p^e - p^{e-1}) - q^{f-1} (p^e - p^{e-1})$$

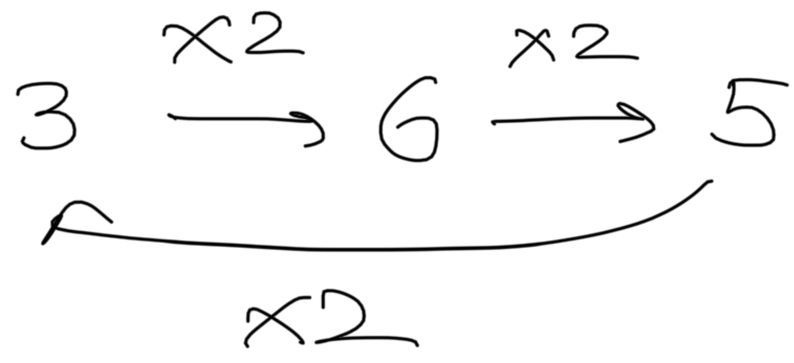
$$= (p^e - p^{e-1})(q^f - q^{f-1})$$

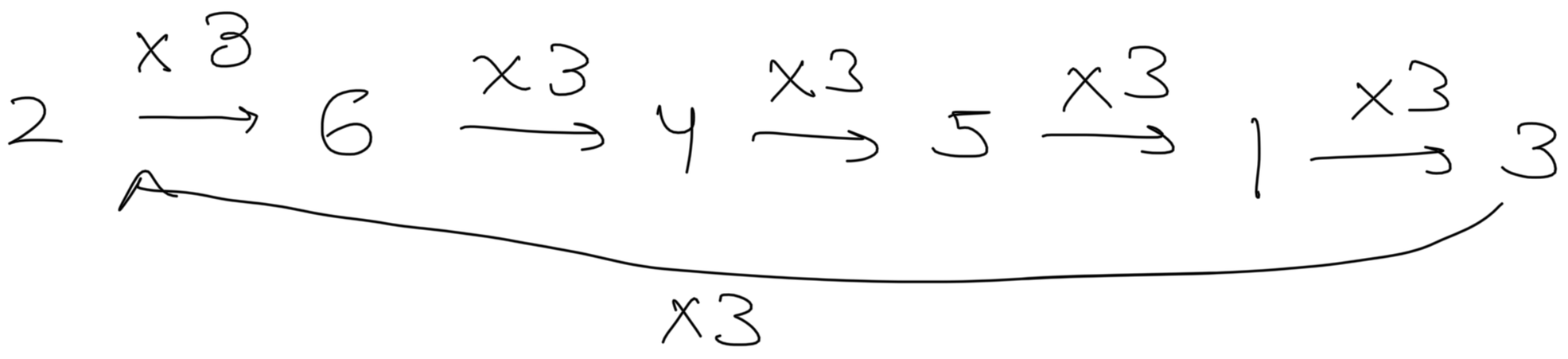
$$= \phi(p^e)\, \phi(q^f)$$

$$\phi(p_1^{q_1} \cdots p_n^{q_n}) = \phi(p_1^{q_1}) \cdots \phi(p_n^{q_n})$$

P- 7







Lemma: Let m be a positive integer & suppose $(a, m) = 1$. Then dynamics of multiplication by a consists of cycles of same length.

Pf: Let $b \in \mathbb{Z}/m\mathbb{Z}$. $(b, m) = 1$

$$b, b \cdot a, b \cdot a^2, \ldots$$

Let l be the smallest power s.t

$$a^l \equiv 1 \pmod{m}$$

$$b \cdot \underbrace{a^{l}}_{\text{cycle of length } l} \equiv b \pmod{m}$$

(Fermat - Euler Theorem) Let m be a positive integer and let $(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

If $m = p$, then $a^{p-1} \equiv 1 \pmod{p}$

Let l be the smallest power s.t

$$a^l \equiv 1 \pmod{m}$$

Let c be the number of cycles.

$$cl = \phi(m)$$

$$a^{\phi(m)} = a^{cl} \equiv 1 \pmod{m}$$

Simplify $2^{1001} \bmod 15$

$$\phi(15) = \phi(3)\,\phi(5) = 8$$

Show that $x^6 + y^{12} = 700003$ has no integer solutions.

Mod 7

$x^6 \equiv 1$ or 0

$y^{12} \equiv 1$ or 0

$700003 \equiv 3$

So, no solutions.