MAU23101
Introduction to number theory
2 - Congruences and $\mathbb{Z}/n\mathbb{Z}$

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2020–2021
Version: October 15, 2020

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Congruences

Congruences

Definition

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n, and we write*

$$a \equiv b \bmod n,$$

if $n \mid (a - b)$.

Example

$36 \equiv 16 \equiv -4 \bmod 10.$

$a \equiv b \bmod 1$ for all $a, b \in \mathbb{Z}$.

The set $\mathbb{Z}/n\mathbb{Z}$

If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$, because $a - c = (a - b) + (b - c)$.
So if we fix $n \in \mathbb{N}$, we can sort the integers into "bags" of congruence.

Example

For $n = 2$, we have 2 bags:
$\{\cdots, -4, -2, 0, 2, 4, \cdots\}$ and $\{\cdots, -3, -1, 1, 3, 5, \cdots\}$.

For $n = 3$, we have 3 bags:
$\{\cdots, -6, -3, 0, 3, 6, \cdots\}$, $\{\cdots, -5, -2, 1, 4, 7, \cdots\}$, and $\{\cdots, -4, -1, 2, 5, 8, \cdots\}$.

Definition

The set of these "bags" is called $\mathbb{Z}/n\mathbb{Z}$.

The set $\mathbb{Z}/n\mathbb{Z}$

Let $x \in \mathbb{Z}$, and let $x = nq + r$ be its division by n. Then $x \equiv r \bmod n$.

Conversely, if $0 \leqslant x, y < n$, then $x \not\equiv y \bmod n$ unless $x = y$.

Theorem

Let $n \in \mathbb{N}$. The set $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements:

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z} \mid x \equiv 0 \bmod n\} &&= \{nq, \ q \in \mathbb{Z}\}, \\
\overline{1} &= \{x \in \mathbb{Z} \mid x \equiv 1 \bmod n\} &&= \{nq+1, \ q \in \mathbb{Z}\}, \\
\overline{2} &= \{x \in \mathbb{Z} \mid x \equiv 2 \bmod n\} &&= \{nq+2, \ q \in \mathbb{Z}\}, \\
&\vdots \\
\overline{n-1} &= \{x \in \mathbb{Z} \mid x \equiv n-1 \bmod n\} &&= \{nq+n-1, \ q \in \mathbb{Z}\}.
\end{aligned}$$

The ring $\mathbb{Z}/n\mathbb{Z}$

Operations in $\mathbb{Z}/n\mathbb{Z}$

Fix $n \in \mathbb{N}$, and let $X, Y \in \mathbb{Z}/n\mathbb{Z}$. In order to define $X + Y$, we take $x \in X$, $y \in Y$, and we say that $X + Y$ is the bag containing $x + y$. Similarly, XY is the bag containing xy.

Example

Take $n = 5$, $X = \overline{2} = \{\cdots, -3, \mathbf{2}, 7, \cdots\}$, and $Y = \overline{3} = \{\cdots, -2, \mathbf{3}, 8, \cdots\}$. Then

$$X + Y = \text{ bag containing } 2 + 3 = \{\cdots, -5, 0, 5, \cdots\} = \overline{0},$$

$$XY = \text{ bag containing } 2 \times 3 = \{\cdots, -4, 1, 6, \cdots\} = \overline{1}.$$

Lemma

Let $n \in \mathbb{N}$, and let $a, a', b, b' \in \mathbb{Z}$ be such that $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$. Then $a + b \equiv a' + b' \bmod n$, $a - b \equiv a' - b' \bmod n$, and $ab \equiv a'b' \bmod n$.

Operations in $\mathbb{Z}/n\mathbb{Z}$

Lemma

Let $n \in \mathbb{N}$*, and let* $a, a', b, b' \in \mathbb{Z}$ *be such that* $a \equiv a' \bmod n$ *and* $b \equiv b' \bmod n$*. Then* $a + b \equiv a' + b' \bmod n$*,* $a - b \equiv a' - b' \bmod n$*, and* $ab \equiv a'b' \bmod n$*.*

Proof.

$a \equiv a' \bmod n$ means $a' - a = kn$ for some $k \in \mathbb{Z}$; similarly $b' - b = ln$ for some $l \in \mathbb{Z}$. Then

$$(a' + b') - (a + b) = (a' - a) + (b' - b) = kn + ln = (k + l)n,$$

$$(a' - b') - (a - b) = (a' - a) - (b' - b) = kn - ln = (k - l)n,$$

$$\begin{aligned}(a'b') - (ab) &= a'b' - ab' + ab' - ab \\ &= (a' - a)b' + a(b' - b) \\ &= knb' + aln \\ &= (kb' + al)n.\end{aligned}$$

□

The ring $\mathbb{Z}/n\mathbb{Z}$

Computing in $\mathbb{Z}/n\mathbb{Z}$ means that we treat multiples of n as 0. So we can replace any integer with its remainder by n. And $\bar{x} = \bar{y}$ iff. $x \equiv y \bmod n$.

Example

In $\mathbb{Z}/12\mathbb{Z}$, we have $\overline{7} \times \overline{8} - \overline{9} = \overline{56} - \overline{9} = \overline{8} - \overline{9} = \overline{-1} = \overline{11}$.

In $\mathbb{Z}/13\mathbb{Z}$, we have $\overline{7} \times \overline{8} - \overline{9} = \overline{56} - \overline{9} = \overline{4} - \overline{9} = \overline{-5} = \overline{8}$.

Remark

Although $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$, computations are easier with a more symmetric choice of representatives. For instance, in $\mathbb{Z}/12\mathbb{Z} = \{\overline{-5}, \overline{-4}, \cdots, \overline{5}, \overline{6}\}$, we have

$$\overline{7} \times \overline{8} - \overline{9} = \overline{-5} \times \overline{-4} + \overline{3} = \overline{20} + \overline{3} = \overline{-4} + \overline{3} = \overline{-1}.$$

$\mathbb{Z}/n\mathbb{Z}$ is a ring: a set in which we can $+, -, \times$.
For division, we will see later!

Application to Diophantine equations

Idea

Suppose we have a Diophantine equation

$$F(x, y, \cdots) = C$$

where F is a polynomial with coefficients in $\mathbb{Z}$, and $C \in \mathbb{Z}$.
If $x = a, y = b, \cdots$ is a solution, then for all $n \in \mathbb{N}$, in $\mathbb{Z}/n\mathbb{Z}$ we have

$$F(\overline{a}, \overline{b}, \cdots) = \overline{C}.$$

So conversely, if for some $n \in \mathbb{N}$ the equation has no solution in $\mathbb{Z}/n\mathbb{Z}$, then it has no solution in $\mathbb{Z}$.

The point is that $\mathbb{Z}/n\mathbb{Z}$ is finite, so we only need to check finitely many possibilities for $x, y, \cdots$ to disprove the existence of solutions in $\mathbb{Z}$!

Example 1: sum of two squares

Does $x^2 + y^2 = 2019$ have integral solutions?
Take $n = 4$: In $\mathbb{Z}/4\mathbb{Z}$, we have

x	$\overline{-1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
x^2	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{0}$

so $\overline{x^2 + y^2} = \overline{x}^2 + \overline{y}^2$ can be either

$$\overline{0} + \overline{0} = \overline{0}, \text{ or } \overline{0} + \overline{1} = \overline{1}, \text{ or } \overline{1} + \overline{1} = \overline{2}.$$

But $\overline{2019} = \overline{19} = \overline{-1} \notin \{\overline{0}, \overline{1}, \overline{2}\}$, so no solutions in $\mathbb{Z}/4\mathbb{Z}$, so no solutions in $\mathbb{Z}$ either!

Similarly, no solutions to $x^2 + y^2 = 4k - 1$ for any $k \in \mathbb{Z}$.

$5x^2 - 7y^2 = 4k - 1$ either.

Example 2: sum of three cubes

In $\mathbb{Z}/9\mathbb{Z}$, we have

x	$-\overline{4}$	$-\overline{3}$	$-\overline{2}$	$-\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
x^3	$-\overline{1}$	$\overline{0}$	$\overline{1}$	$-\overline{1}$	$\overline{0}$	$\overline{1}$	$-\overline{1}$	$\overline{0}$	$\overline{1}$.

So necessarily $\overline{x^3+y^3+z^3} \in \{-\overline{3}, -\overline{2}, -\overline{1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Therefore, for all $C \in \mathbb{Z}$, if $C \equiv \pm 4 \bmod 9$, then the Diophantine equation $x^3 + y^3 + z^3 = C$ has no solutions.

Example: $C = 31$, $C = 32$.

Invertible elements in $\mathbb{Z}/n\mathbb{Z}$

Invertible elements in $\mathbb{Z}/n\mathbb{Z}$

Definition

An element $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible if there exists $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = \overline{1}$. Such an y is then unique, and is denoted by x^{-1}.

Indeed, if $xy = xy' = \overline{1}$, then $y = yxy' = y'$.

Example

In $\mathbb{Z}/11\mathbb{Z}$, $\overline{2}$ is invertible, with inverse $\overline{6}$, since $\overline{2} \times \overline{6} = \overline{12} = \overline{1}$. Thus $\overline{2}^{-1} = \overline{6} = -\overline{5}$.

Counter-example

In $\mathbb{Z}/4\mathbb{Z}$, we have $\overline{2}y \in \{\overline{0}, \overline{2}\}$ for all $y \in \mathbb{Z}/4\mathbb{Z}$, so $\overline{2}$ is not invertible.

Invertible elements in $\mathbb{Z}/n\mathbb{Z}$

Definition

An element $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible if there exists $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = \overline{1}$. Such an y is then unique, and is denoted by x^{-1}.

Definition (Division in $\mathbb{Z}/n\mathbb{Z}$)

Let $x, y \in \mathbb{Z}/n\mathbb{Z}$. If y is invertible, then we define

$$x/y = x \times y^{-1}.$$

Else, the division x/y is forbidden.

Example

In $\mathbb{Z}/11\mathbb{Z}$, we have $\overline{3}/\overline{2} = \overline{3} \times \overline{2}^{-1} = \overline{3} \times \overline{6} = \overline{18} = \overline{7} = -\overline{4}$.

In $\mathbb{Z}/4\mathbb{Z}$, $\overline{3}/\overline{2}$ makes no sense.

Characterisation of invertibles in $\mathbb{Z}/n\mathbb{Z}$

Theorem (Invertibility test)

Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $\bar{x}$ is invertible in $\mathbb{Z}/n\mathbb{Z}$ iff.

$$\gcd(x, n) = 1.$$

Proof.

$$\begin{aligned}
\bar{x} \text{ invertible} &\iff \overline{xy} = \bar{1} \text{ for some } y \in \mathbb{Z} \\
&\iff xy \equiv 1 \bmod n \text{ for some } y \in \mathbb{Z} \\
&\iff xy = 1 + nk \text{ for some } y, k \in \mathbb{Z} \\
&\iff xy - nk = 1 \text{ for some } y, k \in \mathbb{Z} \\
&\underset{\text{Bézout}}{\iff} \gcd(x, n) = 1.
\end{aligned}$$

□

Characterisation of invertibles in $\mathbb{Z}/n\mathbb{Z}$

Proof.

$$\begin{aligned} \bar{x} \text{ invertible } &\iff \overline{xy} = \bar{1} \text{ for some } y \in \mathbb{Z} \\ &\iff xy \equiv 1 \bmod n \text{ for some } y \in \mathbb{Z} \\ &\iff xy = 1 + nk \text{ for some } y, k \in \mathbb{Z} \\ &\iff xy - nk = 1 \text{ for some } y, k \in \mathbb{Z} \\ &\underset{\text{Bézout}}{\iff} \gcd(x, n) = 1. \end{aligned}$$

□

Example

By Euclid's algorithm, we see that $\gcd(8, 27) = 1$, so 8 is invertible mod 27. Working backwards, we find that $8u + 27v = 1$ for $u = -10$, $v = 3$; so $\bar{8}^{-1} = -\overline{10} = \overline{17}$.

Characterisation of invertibles in $\mathbb{Z}/n\mathbb{Z}$

Theorem (Invertibility test)

Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $\bar{x}$ is invertible in $\mathbb{Z}/n\mathbb{Z}$ iff.

$$\gcd(x, n) = 1.$$

Theorem (Simplifiability)

$x \in \mathbb{Z}/n\mathbb{Z}$ is invertible iff. for all $L, R \in \mathbb{Z}/n\mathbb{Z}$,

$$xL = xR \text{ implies } L = R.$$

Proof.

If x is invertible, then $xL = xR$ implies $x^{-1}xL = x^{-1}xR$.
Conversely, if $xL = xR$ always implies $L = R$, then the map $\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ y & \longmapsto & xy \end{array}$ is injective, hence bijective because $\mathbb{Z}/n\mathbb{Z}$ is finite, hence surjective, so there exists y such that $xy = \bar{1}$. □

Characterisation of invertibles in $\mathbb{Z}/n\mathbb{Z}$

Theorem (Invertibility test)

Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $\bar{x}$ is invertible in $\mathbb{Z}/n\mathbb{Z}$ iff.

$$\gcd(x, n) = 1.$$

Theorem (Simplifiability)

$x \in \mathbb{Z}/n\mathbb{Z}$ is invertible iff. for all $L, R \in \mathbb{Z}/n\mathbb{Z}$,

$$xL = xR \text{ implies } L = R.$$

Example

In $\mathbb{Z}/27\mathbb{Z}$, $8x = 5 \iff x = 8^{-1} \times 5 = -10 \times 5 = 4$.

Counter-example

In $\mathbb{Z}/4\mathbb{Z}$, the solutions to $2x = 0$ are $x = 0$ and $x = 2$; whereas $2x = 1$ has no solutions.

Primes are a nice case

Theorem

Let $n \in \mathbb{N}$. TFAE:

1. *Every nonzero $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible,*
2. *For all $x, y \in \mathbb{Z}/n\mathbb{Z}$, $xy = \overline{0}$ only if $x = \overline{0}$ or $y = \overline{0}$,*
3. *n is prime.*

Counter-example

In $\mathbb{Z}/6\mathbb{Z}$, $\overline{2} \neq \overline{0}$ is not invertible, and $\overline{2} \times \overline{3} = \overline{0}$.

Primes are a nice case

Theorem

Let $n \in \mathbb{N}$. TFAE:

1. *Every nonzero $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible,*
2. *For all $x, y \in \mathbb{Z}/n\mathbb{Z}$, $xy = \overline{0}$ only if $x = \overline{0}$ or $y = \overline{0}$,*
3. *n is prime.*

Proof.

(1) $\Rightarrow$ (2): If $xy = \overline{0}$ and $x \neq \overline{0}$, then $y = x^{-1}xy = x^{-1}\overline{0} = \overline{0}$.
(2) $\Rightarrow$ (3): If $n = ab$, then $\overline{a}\overline{b} = \overline{n} = \overline{0}$, so $\overline{a}$ or $\overline{b}$ is $\overline{0}$, so $n \mid a$ or $n \mid b$, so $a = n$ or $b = n$.
(3) $\Rightarrow$ (1): If $\overline{a} \neq 0$, then $n \nmid a$, so $\gcd(a, n) = 1$ as n is prime. □

The group of invertibles and Euler's totient

Proposition

Invertible elements in $\mathbb{Z}/n\mathbb{Z}$ for a group under multiplication, denoted by

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{x \in \mathbb{Z}/n\mathbb{Z} \mid x \text{ invertible}\}.$$

In other words, $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times \implies xy \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Definition

Euler's totient function is

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{0 \leqslant x < n \mid \gcd(x, n) = 1\}.$$

Example

$(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, -\overline{1}\}$, so $\phi(6) = 2$.

We will see a formula for $\phi(n)$ very soon.

Chinese remainders

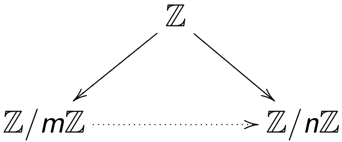
Reduction maps

Let $n \in \mathbb{N}$. Given $x \in \mathbb{Z}$, we can consider its image in $\mathbb{Z}/n\mathbb{Z}$
$\rightsquigarrow$ reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

Reduction maps

Let $n \in \mathbb{N}$. Given $x \in \mathbb{Z}$, we can consider its image in $\mathbb{Z}/n\mathbb{Z}$
$\rightsquigarrow$ reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

If now $m, n \in \mathbb{N}$, do we have a map such that



commutes?

Reduction maps

Let $n \in \mathbb{N}$. Given $x \in \mathbb{Z}$, we can consider its image in $\mathbb{Z}/n\mathbb{Z}$
$\rightsquigarrow$ reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

If now $m, n \in \mathbb{N}$, do we have a map such that

$$\begin{array}{ccc} & \mathbb{Z} & \\ \swarrow & & \searrow \\ \mathbb{Z}/m\mathbb{Z} & \dashrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

commutes?

Yes iff. for all $x, x' \in \mathbb{Z}$, $x \equiv x' \mod m \Longrightarrow x \equiv x' \mod n$.

Reduction maps

Let $n \in \mathbb{N}$. Given $x \in \mathbb{Z}$, we can consider its image in $\mathbb{Z}/n\mathbb{Z}$
$\rightsquigarrow$ reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

If now $m, n \in \mathbb{N}$, do we have a map such that

$$\begin{array}{ccc} & \mathbb{Z} & \\ \swarrow & & \searrow \\ \mathbb{Z}/m\mathbb{Z} & \dashrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

commutes?

Yes iff. for all $x, x' \in \mathbb{Z}$, $x \equiv x' \bmod m \Longrightarrow x \equiv x' \bmod n$.

In particular, we must have $m \equiv 0 \bmod n$, i.e. $n \mid m$.
Conversely, if $n \mid m$, then

$$x \equiv x' \bmod m \Longleftrightarrow m \mid (x - x') \Longrightarrow n \mid (x - x') \Longleftrightarrow x \equiv x' \bmod n.$$

Reduction maps

If now $m, n \in \mathbb{N}$, do we have a map such that

$$\begin{array}{ccc} & \mathbb{Z} & \\ \swarrow & & \searrow \\ \mathbb{Z}/m\mathbb{Z} & \dashrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

commutes?

Theorem

We have a reduction map $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ iff. $n \mid m$.

Example

We have a reduction map from $\mathbb{Z}/6\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$, e.g.

$$5 \bmod 6 \mapsto 1 \bmod 2.$$

But we do not have a reduction map from $\mathbb{Z}/6\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$. Indeed, $5 \bmod 6$ could be $1 \bmod 4$, but also $3 \bmod 4$.

The Chinese remainders problem

Let now $m, n \in \mathbb{N}$. Given $y, z \in \mathbb{Z}$, can we find $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv y \bmod m, \\ x \equiv z \bmod n \; ? \end{cases}$$

Example

Find $x \in \mathbb{Z}$ such that $x \equiv 1 \bmod 7$ and $x \equiv 2 \bmod 9$.

The Chinese remainders problem

Let now $m, n \in \mathbb{N}$. Given $y, z \in \mathbb{Z}$, can we find $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv y \bmod m, \\ x \equiv z \bmod n \ ? \end{cases}$$

Not always! Let $g = \gcd(m, n)$. Then we have reduction maps

$$\begin{array}{ccccc} & & \mathbb{Z} & & \\ & \swarrow & & \searrow & \\ \mathbb{Z}/m\mathbb{Z} & & & & \mathbb{Z}/n\mathbb{Z} \\ & \searrow & & \swarrow & \\ & & \mathbb{Z}/g\mathbb{Z}, & & \end{array}$$

so no solution if y and z do not have the same image in $\mathbb{Z}/g\mathbb{Z}$.

Example

There is no $x \in \mathbb{Z}$ such that $x \equiv 5 \bmod 6$ and $x \equiv 2 \bmod 4$.

$\rightsquigarrow$ we will suppose that $\gcd(m, n) = 1$ from now on.

The Chinese remainders theorem

Theorem (CRT)

Let $m, n \in \mathbb{N}$ be coprime. Then the map

$$中 : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ (x \bmod mn) & \longmapsto & (x \bmod m, x \bmod n) \end{array}$$

is bijective.

Proof.

We construct its inverse. Since m and n are coprime, there exist $u, v \in \mathbb{Z}$ such that $mu + nv = 1$. Then $中(mu) = (0, 1)$ and $中(nv) = (1, 0)$. Thus for all $y, z \in \mathbb{Z}$, we have $中(ynv + zmu) = (y, z)$, so

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (y \bmod m, z \bmod n) & \longmapsto & ynv + zmu \bmod mn \end{array}$$

is an inverse of 中. □

The Chinese remainders theorem

Theorem (CRT)

Let $m, n \in \mathbb{N}$ be coprime. Then the map

$$中 : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ (x \bmod mn) & \longmapsto & (x \bmod m, x \bmod n) \end{array}$$

is bijective.

Example

To find $x \in \mathbb{Z}$ such that $x \equiv 1 \bmod 7$ and $x \equiv 2 \bmod 9$:
We use Euclid to find $7u + 9v = 1$ with $u = 4$, $v = -3$.
We have $7u = 28$, which is $0 \bmod 7$ and $1 \bmod 9$;
and $9v = -27$, which is $1 \bmod 7$ and $0 \bmod 9$.
Then $x = 1 \times 9v + 2 \times 7u = 29$ is $1 \bmod 7$ and $2 \bmod 9$.
The general solution is $x \equiv 29 \bmod 63$.

Application to Euler's ϕ

For m, n coprime, CRT reduces the study of $\mathbb{Z}/mn\mathbb{Z}$ to that of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

Example

中 induces $(\mathbb{Z}/mn\mathbb{Z})^\times \longleftrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Thus x invertible mod $mn \iff x$ invertible mod m and mod n.

Application to Euler's ϕ

For m, n coprime, CRT reduces the study of $\mathbb{Z}/mn\mathbb{Z}$ to that of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

Example

中 induces $(\mathbb{Z}/mn\mathbb{Z})^\times \longleftrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Thus x invertible mod $mn \iff x$ invertible mod m and mod n.

Corollary

ϕ is (weakly) multiplicative.

Application to Euler's ϕ

For m, n coprime, CRT reduces the study of $\mathbb{Z}/mn\mathbb{Z}$ to that of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

Example

中 induces $(\mathbb{Z}/mn\mathbb{Z})^\times \longleftrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Thus x invertible mod $mn \iff x$ invertible mod m and mod n.

Corollary

ϕ is (weakly) multiplicative.

Theorem

Let $n = \prod_i p_i^{v_i}$, with the p_i pairwise distinct primes and the $v_i \geqslant 1$. Then

$$\phi(n) = \prod_i (p_i - 1)p_i^{v_i - 1} = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Application to Euler's ϕ

Theorem

Let $n = \prod_i p_i^{v_i}$, with the p_i pairwise distinct primes and the $v_i \geqslant 1$. Then

$$\phi(n) = \prod_i (p_i - 1) p_i^{v_i - 1} = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Proof.

By multiplicativity, $\phi(\prod_i p_i^{v_i}) = \prod_i \phi(p_i^{v_i})$.
And in $\mathbb{Z}/p^v\mathbb{Z}$, an element is invertible iff. it is coprime to p^v, iff. it is coprime to p.
So exactly 1 out of p element is non-invertible.
$\rightsquigarrow p^{v-1}$ non-invertibles, and $p^v - p^{v-1}$ invertibles. □

Additive and multiplicative order

Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

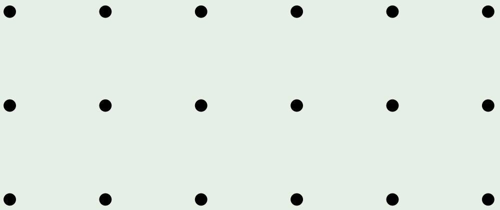
Sequences in finite sets

Let S be a finite set, and $f : S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



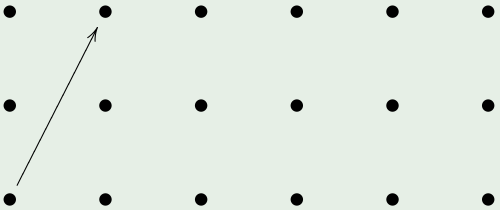
Sequences in finite sets

Let S be a finite set, and $f: S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



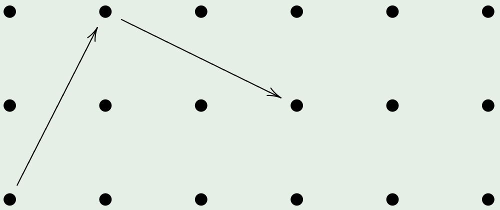
Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



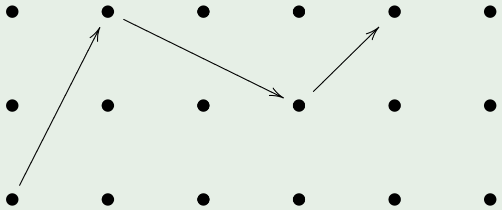
Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



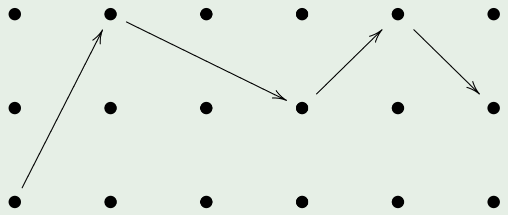
Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



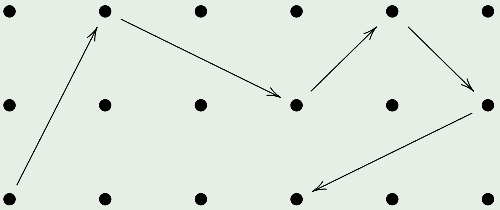
Sequences in finite sets

Let S be a finite set, and $f: S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



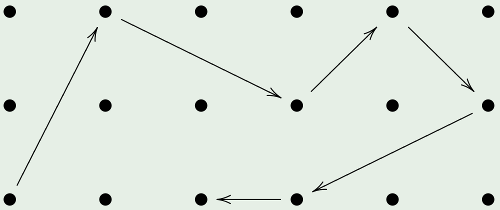
Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



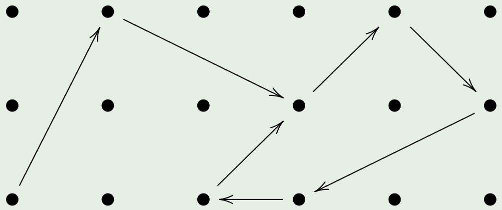
Sequences in finite sets

Let S be a finite set, and $f\colon S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



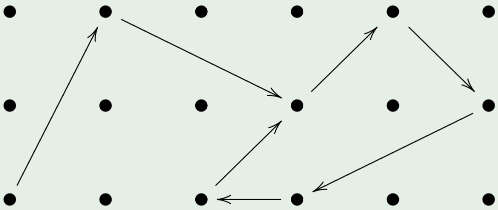
Sequences in finite sets

Let S be a finite set, and $f: S \longrightarrow S$ a function. Define a sequence in S by picking $s_0 \in S$ and defining inductively $s_{m+1} = f(s_m)$.

Theorem

Such a sequence is always ultimately periodic.

Example



Tail of length 2, period of length 5.

Additive order

Let $x \in \mathbb{Z}/n\mathbb{Z}$. Define a sequence in $\mathbb{Z}/n\mathbb{Z}$ by $s_0 = 0$ and $s_{m+1} = s_m + x$; thus $s_m = mx \in \mathbb{Z}/n\mathbb{Z}$ for all m.

Definition

The additive order of x is

$$\mathrm{AO}(x) = \textit{period of } s_m.$$

Example

Take $x = 4 \in \mathbb{Z}/6\mathbb{Z}$. Then
$s_0 = 0$, $s_1 = s_0 + x = 4$, $s_2 = s_1 + x = 2$, $s_3 = s_2 + x = 0$
$\rightsquigarrow \mathrm{AO}(4 \bmod 6) = 3$.

Determination of the additive order

Theorem

For all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, the sequence $s_m = m\bar{x}$ is purely periodic (no tail), and we have $\mathrm{AO}(\bar{x}) = \frac{n}{\gcd(x,n)}$.

Proof.

Let $g = \gcd(x, n)$. For all $i, j \in \mathbb{Z}_{\geqslant 0}$, we have

$$\begin{aligned} i\bar{x} = j\bar{x} &\iff ix \equiv jx \bmod n \\ &\iff n \mid (ix - jx) = (i-j)x \\ &\iff \frac{n}{g} \mid (i-j)\frac{x}{g} \\ &\underset{\gcd(\frac{n}{g},\frac{x}{g})=1}{\overset{\text{Gauss}}{\iff}} \frac{n}{g} \mid (i-j) \\ &\iff i \equiv j \bmod \frac{n}{g}. \end{aligned}$$

□

Multiplicative order

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Define a sequence in $(\mathbb{Z}/n\mathbb{Z})^\times$ by $t_0 = 1$ and $t_{m+1} = t_m \times x$; thus $t_m = x^m \in (\mathbb{Z}/n\mathbb{Z})^\times$ for all m.

Definition

The multiplicative order of x is

$$\mathrm{MO}(x) = \textit{period of } t_m.$$

Example

Take $x = 2 \in \mathbb{Z}/7\mathbb{Z}$. Then
$t_0 = 1,\ t_1 = t_0 \times x = 2,\ t_2 = t_1 \times x = 4,\ t_3 = t_2 \times x = 1$
$\rightsquigarrow \mathrm{MO}(2 \bmod 7) = 3.$

Properties of the multiplicative order

Theorem (Fermat's little theorem)

For all $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $x^{\phi(n)} = 1$.

Proof.

Lagrange. Alternatively, let $(\mathbb{Z}/n\mathbb{Z})^\times = \{y_1, y_2, \cdots, y_{\phi(n)}\}$. As x is invertible, the map $\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ y & \longmapsto & xy \end{array}$ is bijective with inverse $\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ y & \longmapsto & x^{-1}y \end{array}$, so we also have $(\mathbb{Z}/n\mathbb{Z})^\times = \{xy_1, xy_2, \cdots, xy_{\phi(n)}\}$. Multiplying yields

$$y_1 y_2 \cdots y_{\phi(n)} = xy_1 xy_2 \cdots xy_{\phi(n)} = x^{\phi(n)} y_1 y_2 \cdots y_{\phi(n)},$$

and we can simplify by the y_i because they are invertible. $\square$

Properties of the multiplicative order

Theorem (Fermat's little theorem)

For all $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, *we have* $x^{\phi(n)} = 1$.

Corollary

For all $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$, *the sequence* $t_m = \bar{x}^m$ *is* *purely* *periodic (no tail), and we have* $\mathrm{MO}(\bar{x}) \mid \phi(n)$.

Corollary

For all $x \in \mathbb{Z}$ *coprime to* n, *for all* $i, j \in \mathbb{Z}$,

$$i \equiv j \bmod \phi(n) \Longrightarrow x^i \equiv x^j \bmod n.$$

Properties of the multiplicative order

Theorem (Fermat's little theorem)

For all $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $x^{\phi(n)} = 1$.

Corollary

For all $x \in \mathbb{Z}$ coprime to n, for all $i, j \in \mathbb{Z}$,

$$i \equiv j \bmod \phi(n) \implies x^i \equiv x^j \bmod n.$$

Example

What is $353^{2021} \bmod 10$?
First, $353 \equiv 3 \bmod 10$, so $353^{2021} \equiv 3^{2021} \bmod 10$.
Next, $\phi(10) = 10(1 - 1/2)(1 - 1/5) = 4$. As $2021 \equiv 1 \bmod 4$, $3^{2021} \equiv 3^1 = 3 \bmod 10$.

Primitive roots

Primitive roots

Definition

Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that x is a primitive root mod n if $\gcd(x, n) = 1$ and $\mathrm{MO}(x \bmod n) = \phi(n)$.

Example

$\mathrm{MO}(2 \bmod 7) = 3 < \phi(7) = 6$, so 2 is not a primitive root mod 7.

In $\mathbb{Z}/7\mathbb{Z}$, we have $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = -1$, $3^4 = -3$, $3^5 = -2$, $3^6 = 1$. So 3 is a primitive root mod 7.

Counter-example

Primitive roots do not always exist! For instance, every $x \in (\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\}$ satisfies $x^2 = 1$, so $MO(x) \mid 2$, whereas $\phi(8) = 4$.

Discrete logarithm

Definition (Reminder)

Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that x is a primitive root mod n if $\gcd(x, n) = 1$ and $\mathrm{MO}(x \bmod n) = \phi(n)$.

Remark

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathrm{MO}(x) = \#\{x^m, m \in \mathbb{Z}\}$, and every power of x is of the form x^m for some unique $m \in \mathbb{Z}/\mathrm{MO}(x)\mathbb{Z}$. In particular, x is a primitive root iff. $(\mathbb{Z}/n\mathbb{Z})^\times = \{x^m, m \in \mathbb{Z}\}$.

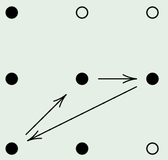
Discrete logarithm

Remark

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathrm{MO}(x) = \#\{x^m, m \in \mathbb{Z}\}$, and every power of x is of the form x^m for some unique $m \in \mathbb{Z}/\mathrm{MO}(x)\mathbb{Z}$. In particular, x is a primitive root iff. $(\mathbb{Z}/n\mathbb{Z})^\times = \{x^m, m \in \mathbb{Z}\}$.

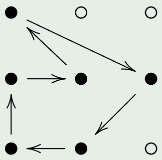
Example

$\bullet$=invertible, $\circ$=non-invertible. $\phi(n) = 6$.



$\mathrm{MO} = 3$

$\rightsquigarrow$ no



$\mathrm{MO} = 6$

$\rightsquigarrow$ yes

Discrete logarithm

Remark

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathrm{MO}(x) = \#\{x^m, m \in \mathbb{Z}\}$, and every power of x is of the form x^m for some unique $m \in \mathbb{Z}/\mathrm{MO}(x)\mathbb{Z}$. In particular, x is a primitive root iff. $(\mathbb{Z}/n\mathbb{Z})^\times = \{x^m, m \in \mathbb{Z}\}$.

Definition (Discrete logarithm)

Suppose $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ is a primitive root. Then every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ is of the form $x = g^m$ for some unique $m \in \mathbb{Z}/\phi(n)\mathbb{Z}$, which is denoted by $m = \log_g x \in \mathbb{Z}/\phi(n)\mathbb{Z}$.

Discrete logarithm

Definition (Discrete logarithm)

Suppose $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ *is a primitive root. Then every* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ *is of the form* $x = g^m$ *for some unique* $m \in \mathbb{Z}/\phi(n)\mathbb{Z}$*, which is denoted by* $m = \log_g x \in \mathbb{Z}/\phi(n)\mathbb{Z}$*.*

Example

Using the primitive root $g = 3 \in (\mathbb{Z}/7\mathbb{Z})^\times$, we have

$$\log_g(-1 \bmod 7) = 3 \bmod 6, \quad \text{because } g^3 = -1 \bmod 7,$$

and indeed

$$g^m = -1 \bmod 7 \iff m \equiv 3 \bmod 6.$$

Calculation of MO

Lemma (MO lemma)

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$*. Then for all* $m \in \mathbb{Z}$*, we have* $(x^m)^{\mathrm{MO}(x)} = 1$ *so* $\mathrm{MO}(x^m) \mid \mathrm{MO}(x)$*, and in fact* $\mathrm{MO}(x^m) = \frac{\mathrm{MO}(x)}{\gcd(m, \mathrm{MO}(x))}$.

Proof.

Recall that for all $k \in \mathbb{Z}$, we have $x^k = 1 \iff \mathrm{MO}(x) \mid k$.
First, $(x^m)^{\mathrm{MO}(x)} = x^{m\,\mathrm{MO}(x)} = (x^{\mathrm{MO}(x)})^m = 1^m = 1$.
Let $m \in \mathbb{Z}$, and let $g = \gcd(m, \mathrm{MO}(x))$; then for all $k \in \mathbb{Z}$,

$$\begin{aligned} (x^m)^k = 1 &\iff x^{mk} = 1 \\ &\iff \mathrm{MO}(x) \mid mk \\ &\iff \frac{\mathrm{MO}(x)}{g} \mid \frac{m}{g} k \\ &\overset{\text{Gauss}}{\iff} \frac{\mathrm{MO}(x)}{g} \mid k. \end{aligned}$$

□

Calculation of MO

Lemma (MO lemma)

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. *Then for all* $m \in \mathbb{Z}$, *we have* $(x^m)^{\mathrm{MO}(x)} = 1$ *so* $\mathrm{MO}(x^m) \mid \mathrm{MO}(x)$, *and in fact* $\mathrm{MO}(x^m) = \frac{\mathrm{MO}(x)}{\gcd(m, \mathrm{MO}(x))}$.

Corollary

Suppose $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ *is a primitive root. Then for all* $x \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\mathrm{MO}(x) = \frac{\phi(n)}{\gcd(\phi(n), \log_g x)}.$$

Corollary

If there exist primitive roots in $\mathbb{Z}/n\mathbb{Z}$, *then there are exactly* $\phi(\phi(n))$ *of them.*

Primitive roots mod p

Lemma

Let $p \in \mathbb{N}$ prime, and $F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ a polynomial of degree d with coefficients in $\mathbb{Z}/p\mathbb{Z}$.
Then $F(x)$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.

Counter-example

The polynomial $x^2 - 1$ has degree 2, but all 4 elements of $(\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\}$ are roots of it.

Primitive roots mod p

Lemma

Let $p \in \mathbb{N}$ prime, and $F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ a polynomial of degree d with coefficients in $\mathbb{Z}/p\mathbb{Z}$.
Then $F(x)$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.

Proof.

We prove by induction on $n \geqslant 1$ that if $z_1, \cdots, z_n$ are distinct roots, then $F(x) = (x - z_1)\cdots(x - z_n)G(x)$.
For $n = 1$, shift variable $x = y + z_1$: $F(x) = F(y + z_1) = yG(y)$.
And if z_{n+1} is another root of $F(x) = (x - z_1)\cdots(x - z_n)G(x)$, then $(z_{n+1} - z_1)\cdots(z_{n+1} - z_n)G(z_{n+1}) = 0$, so $G(z_{n+1}) = 0$ because p is prime. □

Primitive roots mod p

Lemma

Let $p \in \mathbb{N}$ prime, and $F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ a polynomial of degree d with coefficients in $\mathbb{Z}/p\mathbb{Z}$.
Then $F(x)$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.

Lemma

For all $n \in \mathbb{N}$, we have $\sum_{d \mid n} \phi(d) = n$.

Proof.

Consider the n fractions $\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \cdots, \frac{n-1}{n}$. When we simplify them, we get the $\frac{x}{d}$ with $d \mid n$, $\gcd(x, d) = 1$, and $0 \leqslant x < d$.
For each d, there are $\phi(d)$ such fractions. □

Primitive roots mod p

Lemma

Let $p \in \mathbb{N}$ prime, and $F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ a polynomial of degree d with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Then $F(x)$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.

Lemma

For all $n \in \mathbb{N}$, we have $\sum_{d|n} \phi(d) = n$.

Theorem

For all $p \in \mathbb{N}$ prime, there are $\phi(p-1) > 0$ primitive roots in $\mathbb{Z}/p\mathbb{Z}$.

Primitive roots mod p: proof

Lemma

For all $d \in \mathbb{N}$, let

$$Y_d = \{y \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \mathrm{MO}(y) = d\}, \quad \psi(d) = \# Y_d.$$

Then $\psi(d) \leqslant \phi(d)$ for all d.

Proof.

If $Y_d = \emptyset$, then $\psi(d) = 0 < \phi(d)$ so OK. By Fermat, this always happens if $d \nmid \phi(p)$.

Else, let $y \in Y_d$. Then $\mathrm{MO}(y) = d$, so $\{y^m, m \in \mathbb{Z}\}$ has d elements. By MO lemma, they are all roots of $x^d - 1$; thus $\{y^m, m \in \mathbb{Z}\} = \{\text{roots of } x^d - 1\}$. In particular, every element of Y_d is a power of y. Therefore

$$Y_d = \{y^m \mid m \in \mathbb{Z}/d\mathbb{Z},\ \mathrm{MO}(y^m) = d\} = \{y^m \mid m \in (\mathbb{Z}/d\mathbb{Z})^\times\}$$

by MO lemma, whence $\psi(d) = \phi(d)$. □

Primitive roots mod p: proof

Lemma

For all $d \in \mathbb{N}$, let

$$Y_d = \{y \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \mathrm{MO}(y) = d\}, \quad \psi(d) = \# Y_d.$$

Then $\psi(d) \leqslant \phi(d)$ for all d.

Proof of Theorem.

We have

$$\phi(p) = \#(\mathbb{Z}/p\mathbb{Z})^\times = \sum_{d \mid \phi(p)} \psi(d) \leqslant \sum_{d \mid \phi(p)} \phi(d) = \phi(p).$$

This forces $\psi(d) = \phi(d)$ for all $d \mid \phi(p)$; in particular for $d = \phi(p)$ we have $\psi(\phi(p)) = \phi(\phi(p)) = \phi(p-1)$. □

Finding primitive roots

Lemma

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$*, and let* $k \in \mathbb{N}$ *be such that* $x^k = 1$*. Then* $\mathrm{MO}(x) = k$ *iff. for all primes* $p \mid k$*,* $x^{k/p} \neq 1$*.*

Proof.

We have that $\mathrm{MO}(x) \mid k$, so

$$\begin{aligned}\mathrm{MO}(x) < k &\iff k/\mathrm{MO}(x) \geqslant 2 \\ &\iff \text{there is a prime } p \mid \frac{k}{\mathrm{MO}(x)} \\ &\iff \text{there is a prime } p \text{ s.t. } \mathrm{MO}(x) \mid \frac{k}{p}.\end{aligned}$$

□

Finding primitive roots

Lemma

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, and let $k \in \mathbb{N}$ be such that $x^k = 1$. Then $\mathrm{MO}(x) = k$ iff. for all primes $p \mid k$, $x^{k/p} \neq 1$.

Example

What is $\mathrm{MO}(7 \bmod 19)$?
We have $\phi(19) = 18 = 2 \times 3^2$.
We compute in $\mathbb{Z}/19\mathbb{Z}$ that $7^{18/3} = 7^6 = 1$,
so $\mathrm{MO}(7 \bmod 19) \mid 6 = 2 \times 3$.
Next, $7^{6/3} \neq 1$, so $\mathrm{MO}(7 \bmod 19) \nmid 2$,
but $7^{6/2} = 1$ so $\mathrm{MO}(7 \bmod 19) \mid 3$.
Finally, $7^{3/3} \neq 1$, so $\mathrm{MO}(7 \bmod 19) \nmid 1$; thus

$$\mathrm{MO}(7 \bmod 19) = 3.$$

Finding primitive roots

Lemma

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, and let $k \in \mathbb{N}$ be such that $x^k = 1$. Then $\mathrm{MO}(x) = k$ iff. for all primes $p \mid k$, $x^{k/p} \neq 1$.

Corollary

Let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then x is a primitive root iff. for all primes $p \mid \phi(n)$, we have $x^{\phi(n)/p} \neq 1$.

Example

We want to find a primitive root in $\mathbb{Z}/11\mathbb{Z}$. We have $\phi(11) = 10 = 2 \times 5$, so the proportion of primitive roots in $(\mathbb{Z}/11\mathbb{Z})^\times$ is $\phi(10)/10 = (1 - \frac{1}{2})(1 - \frac{1}{5}) = 40\%$.
We try $x = 2$; as

$$2^2 = 4 \neq 1 \bmod 11 \text{ and } 2^5 = 32 = -1 \neq 1 \bmod 11,$$

2 is a primitive root.