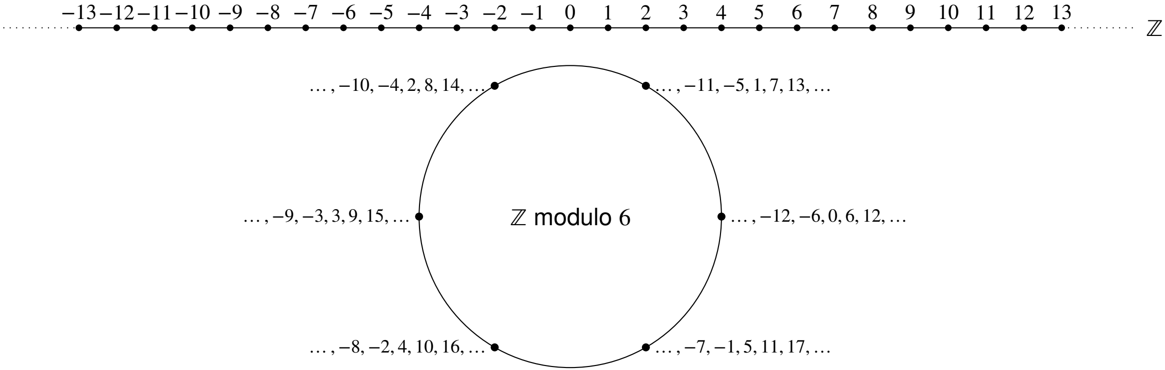
MODULAR ARITHMETIC

UNIVERSITY OF TORONTO

February 11th, 2021

Modular arithmetic: introduction

- Introduced by Gauss during the beginning of the 19th century.
- Working modulo $n \in \mathbb{N} \setminus \{0\}$ means that we identify a with its remainder for the Euclidean division by n.
- If $a = nq + r$ where $0 \leq r < n$ then we set $a \equiv r \pmod{n}$: *a and r are equal modulo n*.
- This new layer of abstraction allowed to simplify previous proofs and to prove new theorems.
- Informally, we wind $\mathbb{Z}$ on itself as below:



Congruences – 1

Definition: equivalence relation

We say that a binary relation $\mathcal{R}$ on a set E is an *equivalence relation* if

1. $\forall x \in E,\ x\mathcal{R}x$ *(reflexivity)*
2. $\forall x, y \in E,\ x\mathcal{R}y \implies y\mathcal{R}x$ *(symmetry)*
3. $\forall x, y, z \in E,\ \left(x\mathcal{R}y \text{ and } y\mathcal{R}z\right) \implies x\mathcal{R}z$ *(transitivity)*

Congruences – 2

Definition: congruence

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
We say that a and b are *congruent modulo* n, denoted by $a \equiv b \pmod{n}$, if $n | a - b$.

Congruences – 2

Definition: congruence

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
We say that a and b are *congruent modulo* n, denoted by $a \equiv b \pmod{n}$, if $n|a - b$.

Proposition

Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Congruences – 2

Definition: congruence

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
We say that a and b are *congruent modulo* n, denoted by $a \equiv b \pmod{n}$, if $n | a - b$.

Proposition

Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof.

- *Reflexivity.* Let $a \in \mathbb{Z}$ then $n|0 = a - a$. Hence $a \equiv a \pmod{n}$.
- *Symmetry.* Let $a, b \in \mathbb{Z}$ be such that $a \equiv b \pmod{n}$.
  Then $n|b - a = -(a - b)$ hence $b \equiv a \pmod{n}$.
- *Transitivity.* Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.
  Then $n|a - b$ and $n|b - c$. Hence $n|a - c = (a - b) + (b - c)$.
  Thus $a \equiv c \pmod{n}$. ∎

Congruences – 3

Proposition

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
Then $a \equiv b \pmod{n}$ if and only if a and b have same remainder for the Euclidean division by n.

Proposition

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
Then $a \equiv b \pmod{n}$ if and only if a and b have same remainder for the Euclidean division by n.

Proof.
$\Rightarrow$. Assume that $a \equiv b \pmod{n}$, then $b - a = kn$ for some $k \in \mathbb{Z}$.
By Euclidean division, $a = nq + r$ for $q, r \in \mathbb{Z}$ satisfying $0 \leq r < n$.
Hence $b = a + kn = nq + r + kn = (q + k)n + r$.
$\Leftarrow$. Assume that a and b have same remainder for the Euclidean division by n.
Then $a = nq_1 + r$ and $b = nq_2 + r$ where $q_1, q_2, r \in \mathbb{Z}$ with $0 \leq r < n$.
Hence $a - b = nq_1 + r - (nq_2 + r) = n(q_1 - q_2)$.
Thus $n | a - b$, i.e. $a \equiv b \pmod{n}$. ∎

Congruences – 3

Proposition

Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$.
Then $a \equiv b \pmod{n}$ if and only if a and b have same remainder for the Euclidean division by n.

Proof.
$\Rightarrow$. Assume that $a \equiv b \pmod{n}$, then $b - a = kn$ for some $k \in \mathbb{Z}$.
By Euclidean division, $a = nq + r$ for $q, r \in \mathbb{Z}$ satisfying $0 \leq r < n$.
Hence $b = a + kn = nq + r + kn = (q + k)n + r$.
$\Leftarrow$. Assume that a and b have same remainder for the Euclidean division by n.
Then $a = nq_1 + r$ and $b = nq_2 + r$ where $q_1, q_2, r \in \mathbb{Z}$ with $0 \leq r < n$.
Hence $a - b = nq_1 + r - (nq_2 + r) = n(q_1 - q_2)$.
Thus $n|a - b$, i.e. $a \equiv b \pmod{n}$. ∎

Corollary

Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$. Then a is congruent modulo n to exactly one element of $\{0, 1, \dots, n - 1\}$.

Modular arithmetic

Proposition: addition and multiplication are well-defined modulo n

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$ then

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

Modular arithmetic

Proposition: addition and multiplication are well-defined modulo n

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$ then

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$.
Hence $a - b = nk$ and $c - d = nl$ for some $k, l \in \mathbb{Z}$. Then

- $(a + c) - (b + d) = (a - b) + (c - d) = nk + nl = n(k + l)$, hence $a + c \equiv b + d \pmod{n}$.
- $ac - bd = (b + nk)(d + nl) - bd = bnl + dnk + n^2kl = n(bl + dk + nkl)$, hence $ac \equiv bd \pmod{n}$. ∎

Modular arithmetic

Proposition: addition and multiplication are well-defined modulo n

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$ then

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$.
Hence $a - b = nk$ and $c - d = nl$ for some $k, l \in \mathbb{Z}$. Then

- $(a + c) - (b + d) = (a - b) + (c - d) = nk + nl = n(k + l)$, hence $a + c \equiv b + d \pmod{n}$.
- $ac - bd = (b + nk)(d + nl) - bd = bnl + dnk + n^2kl = n(bl + dk + nkl)$, hence $ac \equiv bd \pmod{n}$. ∎

Corollary

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then $\forall k \in \mathbb{N}$, $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$.

Modular arithmetic

Proposition: addition and multiplication are well-defined modulo n

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$ then

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$.
Hence $a - b = nk$ and $c - d = nl$ for some $k, l \in \mathbb{Z}$. Then

- $(a + c) - (b + d) = (a - b) + (c - d) = nk + nl = n(k + l)$, hence $a + c \equiv b + d \pmod{n}$.
- $ac - bd = (b + nk)(d + nl) - bd = bnl + dnk + n^2kl = n(bl + dk + nkl)$, hence $ac \equiv bd \pmod{n}$. ■

Corollary

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then $\forall k \in \mathbb{N}$, $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$.

Proof. We prove the statement by induction on k.
Base case at $k = 0$: $a^0 = b^0 = 1$ hence $a^0 \equiv b^0 \pmod{n}$.
Induction step: assume that $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$ for some $k \in \mathbb{N}$.
If $a \equiv b \pmod{n}$ then by the IH we also have $a^k \equiv b^k \pmod{n}$. Hence $a^k a \equiv b^k b \pmod{n}$. ■

Modular multiplicative inverse

Proposition

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
Otherwise stated,

$$\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1$$

Modular multiplicative inverse

Proposition

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
Otherwise stated,

$$\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod n \Leftrightarrow \gcd(a, n) = 1$$

Proof. $\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod n \Leftrightarrow \exists b, c \in \mathbb{Z},\ ab + nc = 1 \Leftrightarrow \gcd(a, n) = 1$ ∎

Modular multiplicative inverse

Proposition

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
Otherwise stated,

$$\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1$$

Proof. $\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \exists b, c \in \mathbb{Z},\ ab + nc = 1 \Leftrightarrow \gcd(a, n) = 1$ ∎

Remark

When it exists, the multiplicative inverse is unique modulo n.
Indeed, assume that $ab \equiv 1 \pmod{n}$ and $ab' \equiv 1 \pmod{n}$ then $ab \equiv ab' \pmod{n}$ so $n | a(b - b')$.
Since $\gcd(a, n) = 1$, by Gauss' lemma we get $n | b - b'$.
Therefore $b' \equiv b \pmod{n}$.

Modular multiplicative inverse

Proposition

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
Otherwise stated,

$$\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1$$

Proof. $\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \exists b, c \in \mathbb{Z},\ ab + nc = 1 \Leftrightarrow \gcd(a, n) = 1$ ∎

Remark

When it exists, the multiplicative inverse is unique modulo n.
Indeed, assume that $ab \equiv 1 \pmod{n}$ and $ab' \equiv 1 \pmod{n}$ then $ab \equiv ab' \pmod{n}$ so $n | a(b - b')$.
Since $\gcd(a, n) = 1$, by Gauss' lemma we get $n | b - b'$.
Therefore $b' \equiv b \pmod{n}$.

Note that $\gcd(4, 25) = 1$ so 4 has a multiplicative inverse modulo 25.
We may find one representative of the inverse from a Bézout's identity: $4 \times (-6) + 25 \times 1 = 1$.
So $4 \times (-6) \equiv 1 \pmod{25}$.

Application: divisibility criterion for 3

Proposition

$3 | \overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $3 | \sum_{k=0}^{r} a_k$

Application: divisibility criterion for 3

Proposition

$3|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $3|\sum_{k=0}^{r} a_k$

Proof. Note that $10 \equiv 1 \pmod 3$, hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{r} a_k 1^k \pmod 3 \equiv \sum_{k=0}^{r} a_k \pmod 3$$

Thus, $$3|\overline{a_r a_{r-1} \dots a_0}^{10} \Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 3 \Leftrightarrow \sum_{k=0}^{r} a_k \equiv 0 \pmod 3 \Leftrightarrow 3|\sum_{k=0}^{r} a_k$$ ∎

Application: divisibility criterion for 3

Proposition

$3 | \overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $3 | \sum_{k=0}^{r} a_k$

Proof. Note that $10 \equiv 1 \pmod 3$, hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{r} a_k 1^k \pmod 3 \equiv \sum_{k=0}^{r} a_k \pmod 3$$

Thus,

$$3 | \overline{a_r a_{r-1} \dots a_0}^{10} \Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 3 \Leftrightarrow \sum_{k=0}^{r} a_k \equiv 0 \pmod 3 \Leftrightarrow 3 | \sum_{k=0}^{r} a_k$$

∎

Examples

- 91524 is divisible by 3 since $9 + 1 + 5 + 2 + 4 = 21 = 7 \times 3$ is.

Application: divisibility criterion for 3

Proposition

$3|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $3| \sum_{k=0}^{r} a_k$

Proof. Note that $10 \equiv 1 \pmod 3$, hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{r} a_k 1^k \pmod 3 \equiv \sum_{k=0}^{r} a_k \pmod 3$$

Thus, $$3|\overline{a_r a_{r-1} \dots a_0}^{10} \Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 3 \Leftrightarrow \sum_{k=0}^{r} a_k \equiv 0 \pmod 3 \Leftrightarrow 3| \sum_{k=0}^{r} a_k$$ ∎

Examples

- 91524 is divisible by 3 since $9+1+5+2+4=21=7\times 3$ is.
- Let's study whether 8546921469 is a multiple of 3 or not:

Application: divisibility criterion for 3

Proposition

$3|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $3| \sum_{k=0}^{r} a_k$

Proof. Note that $10 \equiv 1 \pmod 3$, hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{r} a_k 1^k \pmod 3 \equiv \sum_{k=0}^{r} a_k \pmod 3$$

Thus, $$3|\overline{a_r a_{r-1} \dots a_0}^{10} \Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 3 \Leftrightarrow \sum_{k=0}^{r} a_k \equiv 0 \pmod 3 \Leftrightarrow 3| \sum_{k=0}^{r} a_k$$ ∎

Examples

- 91524 is divisible by 3 since $9+1+5+2+4=21=7\times 3$ is.
- Let's study whether 8546921469 is a multiple of 3 or not:
  $3|8546921469 \Leftrightarrow 3|8+5+4+6+9+2+1+4+6+9=54 \Leftrightarrow 3|5+4=9$.
  But $9=3\times 3$, hence $3|8546921469$.

Application: divisibility criterion for 9

Note that $10 \equiv 1 \pmod 9$, hence we have a similar result:

Proposition

$9 | \overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $9 | \sum_{k=0}^{r} a_k$

Application: divisibility criterion for 4

Proposition

$4|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $4|\overline{a_1 a_0}^{10}$.

Application: divisibility criterion for 4

Proposition

$4|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $4|\overline{a_1 a_0}^{10}$.

Proof. Note that $10^2 = 4 \times 25$ hence $10^k \equiv 0 \pmod 4$ for $k \geq 2$. Hence

$$\begin{aligned} 4|\overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 4 \\ &\Leftrightarrow \sum_{k=0}^{r} a_k 10^k \equiv 0 \pmod 4 \\ &\Leftrightarrow a_1 \times 10 + a_0 \equiv 0 \pmod 4 \\ &\Leftrightarrow \overline{a_1 a_0}^{10} \equiv 0 \pmod 4 \\ &\Leftrightarrow 4|\overline{a_1 a_0}^{10} \end{aligned}$$

∎

Application: divisibility criterion for 4

Proposition

$4|\overline{a_r a_{r-1} \dots a_0}^{10}$ if and only if $4|\overline{a_1 a_0}^{10}$.

Proof. Note that $10^2 = 4 \times 25$ hence $10^k \equiv 0 \pmod 4$ for $k \geq 2$. Hence

$$\begin{aligned}
4|\overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod 4 \\
&\Leftrightarrow \sum_{k=0}^{r} a_k 10^k \equiv 0 \pmod 4 \\
&\Leftrightarrow a_1 \times 10 + a_0 \equiv 0 \pmod 4 \\
&\Leftrightarrow \overline{a_1 a_0}^{10} \equiv 0 \pmod 4 \\
&\Leftrightarrow 4|\overline{a_1 a_0}^{10}
\end{aligned}$$

∎

Example

- $4 \nmid 856987454251100125$ since $4 \nmid 25$.
- $4|98854558715580$ since $4|80 = 4 \times 20$.