MATH 381 Section 4.1

Prof. Olivia Dumitrescu

8 March 2024

Divisibility

Definition $a, b \in \mathbb{Z} \quad a \neq 0$. We say a divides b if $\exists c \in \mathbb{Z} \quad b = ac$ (or $a \mid b$ if $\frac{b}{a} \in \mathbb{Z}$).
If $a \mid b$ we say b is a multiple of a or a is a divisor of b.
$a \mid 0$ since $\frac{0}{a} = 0 \in \mathbb{Z}$.

Remark Notation

$$a \mid b \text{ or } b \,\vdots\, a$$

Remark

$$1 \mid n \wedge n \mid n \quad \forall n \in \mathbb{N}$$

Example Assume n and d are positive integers. How many positive integers not exceeding n are divisible by d?

Fix n and d.

$$\#\{a \in \mathbb{Z} \mid da \leq n\} \quad 0 < da \leq n$$

The positive integers divisible by d are all integers of form $d \cdot k, k \in \mathbb{Z}$.
Therefore, the number of positive integers divisible by d that do not exceed n equals the number of integers k.

$$0 < dk \leq n \quad \text{or} \quad 0 < k \leq \frac{n}{d}$$

$$\#\{k \in \mathbb{Z} \mid 0 < k \leq \frac{n}{d}\} = \lfloor \frac{n}{d} \rfloor$$

Floor function

$$\lfloor \quad \rfloor : \mathbb{R} \to \mathbb{Z}$$
$$\lfloor \quad \rfloor = \{k \in \mathbb{Z} \mid x = k + a \quad a \in [0, 1)\}$$
$$\forall x \in \mathbb{R} \implies \exists! k \in \mathbb{Z}(x = k + a) \quad a \in [0, 1)$$

Returns the largest of all integers k such that $k \leq x$.

Ceiling function

$$\lceil \quad \rceil : \mathbb{R} \to \mathbb{Z}$$
$$\lceil \quad \rceil = \{k \in \mathbb{Z} \mid x = k + a \quad a \in (-1, 0]\}$$
$$\forall x \in \mathbb{R} \implies \exists! k \in \mathbb{Z}(x = k + a) \quad a \in (-1, 0]$$

Returns the smallest of all integers k such that $k \geq x$.

Example Prove that if $x \in \mathbb{R}$

$$\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$$

Proof To prove this statement

$$x = n + \varepsilon \quad n \in \mathbb{Z} \land \varepsilon \in [0, 1)$$

1. $0 \leq \varepsilon \leq \frac{1}{2}$

$$x = n + \varepsilon \implies \lfloor x \rfloor = n$$
$$x + \frac{1}{2} = n + (\varepsilon + \frac{1}{2}) \implies \lfloor x + \frac{1}{2} \rfloor = n$$
$$2x = 2n + 2\varepsilon \implies \lfloor 2x \rfloor = 2n$$
$$2n = n + n$$

$\therefore \lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$

2. $\frac{1}{2} \leq \varepsilon < 1$

$$x = n + \varepsilon \implies \lfloor x \rfloor = n$$
$$x + \frac{1}{2} = n + (\varepsilon + \frac{1}{2}) \implies \lfloor x + \frac{1}{2} \rfloor = n + 1$$
$$2x = 2n + 2\varepsilon \implies \lfloor 2x \rfloor = 2n + 1$$
$$2n + 1 = n + n + 1$$

$\therefore \lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor \quad \blacksquare$

Example

$$\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$$

Proof Proof by cases

1. $\varepsilon \in [0, \frac{1}{3})$
2. $\varepsilon \in [\frac{1}{3}, \frac{2}{3})$
3. $\varepsilon \in [\frac{2}{3}, 1)$

Theorem 0.1 *Let $a, b, c \in \mathbb{Z}, a \neq 0$. Then*

1. *if $a \mid b$ and $b \mid c$ then $a \mid c$*

$$x \mid x \qquad \textit{Reflexive}$$

Proof

$$\begin{aligned} a \mid b &\implies \exists k \in \mathbb{Z}(b = k \cdot a) \\ b \mid c &\implies \exists n \in \mathbb{Z}(c = n \cdot b) \end{aligned}$$

$$\begin{aligned} \implies c &= n \cdot b \\ &= n(k \cdot a) \implies a \mid c \\ &n, k \in \mathbb{Z} \end{aligned}$$

2. *if $a \mid b$ and $a \mid c$ then $a \mid b + c$*

$$x \mid y \wedge y \mid z \implies x \mid z \qquad \textit{Transitive}$$

3. *if $a \mid b$ then $a \mid bc$ for all integers c*

$$x \mid y \wedge y \mid x \implies x = \pm 1$$

Corollary 0.2 *If $a, b, c \in \mathbb{Z}$, $a \neq 0$*

$$a \mid b \wedge a \mid c \implies a \mid mb + nc \quad m, n \in \mathbb{Z}$$

Definition A number $p \geq 2$ is prime if the only integers that divide p are 1 and p.

Section 4.1.3: The Division algorithm

Theorem 0.3 *The Division Algorithm*
Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exists unique integers q (quotient) and r (remainder), $0 \leq r < d$ and $a = q \cdot d + r$.

$$\begin{aligned} d &= divisor \\ a &= dividend \end{aligned} \qquad \begin{cases} q := a \div d \\ r := a \bmod d \end{cases}$$

$$\begin{gathered} a, d \in \mathbb{Z} \\ q, r \in \mathbb{Z} \textit{ such that } 0 \leq r < d \textit{ and } a = q \cdot d + r \\ a - r = qd \\ q \mid a - r \\ r = 0 \iff \frac{a}{d} \in \mathbb{Z} \iff d \mid a \qquad \begin{cases} q = \lfloor \frac{a}{d} \rfloor \\ r = a - q \cdot d \end{cases} \end{gathered}$$

Definition Modular Arithmetic
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we say a is **congruent** to $b \mod m$ if $m \mid a - b$. $\bmod m$ is an **equivalence relation**.

$$a \equiv b \pmod{m} \iff m \mid a - b$$

Relations

1. Reflexivity
$$a \equiv a \pmod{m} \iff m \mid a - a = 0$$

2. Symmetry
$$a \equiv b \pmod{m} \rightarrow b \equiv a \pmod{m}$$

3. Transitivity
$$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \rightarrow a \equiv c \pmod{m}$$

Theorem 0.4 *Let $m, a, b \in \mathbb{Z}$. If $m \mid a$ and $m \mid b$, then $k, \ell \in \mathbb{Z}$ we have $m \mid ak + b\ell$.*

Theorem 0.5 *Let a and b be two integers and $m \in \mathbb{Z}^+$. Then $a \equiv b \mod m$ if and only if $a \bmod m = b \bmod m$.*

Example Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

- $17 \equiv 5 \pmod 6 \iff 6 \mid 17 - 5$
- $24 \not\equiv 14 \pmod 6 \iff 6 \nmid 24 - 14$

Theorem 0.6 *Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod m \iff \exists k \in \mathbb{Z}(a = b + k \cdot m)$.*

Proof

$$\begin{gathered} a \equiv b \pmod m \iff m \mid a - b \\ \text{i.e. } \exists k \in \mathbb{Z} \text{ so that} \\ a - b = k \cdot m \\ a = b + k \cdot m \end{gathered}$$

Definition The set of all integers congruent to an integer m is called the **congruence class** of m.

Theorem 0.7 *Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$ and $a \cdot c \equiv b \cdot d \pmod m$.*

Proof

$$\begin{gathered} s, t \in \mathbb{Z} \\ b = a + s \cdot m \\ d = c + t \cdot m \\ b \cdot d = (a + sm)(c + tm) = ac + m(sc + at + stm) \\ \implies b \cdot d \equiv ac \pmod m \end{gathered}$$

Corollary 0.8 *$m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$. Then*

$$a + b \pmod m = (a \bmod m + b \bmod m) \mod m$$

$$a \cdot b \pmod m = (a \bmod m) \cdot (b \bmod m) \mod m$$

Proof

$$\exists! q, 0 \leq r < m$$
$$a = qm + r$$
$$m \mid a - r$$
$$a \equiv r \mod m$$
$$a \equiv (a \bmod m) \mod m$$
$$b \equiv (b \bmod m) \mod m$$
$$r = a \bmod m \implies a + b \equiv (a \bmod m + b \bmod m) \mod m$$
$$a \cdot b \equiv (a \bmod m) \cdot (b \bmod m) \mod m$$

Section 4.1.4 Modular Arithmetic

Let m be a positive integer.

$$\frac{\begin{array}{c} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}}{\begin{array}{c} a + c \equiv b + d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{array}}$$

Example

$$(19^3 \bmod 31)^4 \mod 23$$
$$19^3 = 6859 = 31 \cdot 221 + 8$$
$$8^4 = 4096 = 178 \cdot 23 + 2$$

Definition The **equivalence class** is defined as

$$\mathbb{Z}_m = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{m-1}\}$$
$$0 \le k < m$$
$$\hat{k} = \{z \in \mathbb{Z} \mid z \bmod m = k\}$$
$$\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$$
$$\begin{aligned} S_0 = \hat{0} &= \{z \in \mathbb{Z} \mid z \bmod 4 = 0 \iff 4 \mid z\} \\ &= \{\dots, -8, -4, 0, 4, 8, 12, 16, 20, 24, \dots\} = \{4k \mid k \in \mathbb{Z}\} \\ S_1 = \hat{1} &= \{z \in \mathbb{Z} \mid z \bmod 4 = 1 \iff 4 \mid z-1\} \\ &= \{\dots, -7, -3, 1, 5, 9, 13, \dots\} = \{4k+1 \mid k \in \mathbb{Z}\} \\ S_2 = \hat{2} &= \{z \in \mathbb{Z} \mid z \bmod 4 = 2 \iff 4 \mid z-2\} \\ &= \{\dots, -6, -2, 2, 6, 10, 14, \dots\} = \{4k+2 \mid k \in \mathbb{Z}\} \\ S_3 = \hat{3} &= \{z \in \mathbb{Z} \mid z \bmod 4 = 3 \iff 4 \mid z-3\} \\ &= \{\dots, -5, -1, 3, 7, 11, 15, \dots\} = \{4k+3 \mid k \in \mathbb{Z}\} \end{aligned}$$
$$\mathbb{Z}_4 = S_0 \sqcup S_1 \sqcup S_2 \sqcup S_3$$

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

0. $\forall z, w, v \in \mathbb{Z}((z+w)+v = z+(w+v))$
1. $\exists z = 0$ so that $\forall z \in \mathbb{Z}(z+0 = 0+z = z)$
2. $\forall z \in \mathbb{Z}\ \exists! w \in \mathbb{Z}$ so that $z + w = 0$
3. $z + w = w + z$ for any $z, w \in \mathbb{Z}$ (abelian)

- $(\mathbb{N}, +)$ is not an abelian group
- $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups

Theorem 0.9

1. $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$ *are examples of abelian groups. Yes*
2. $(R \setminus \{0\}, \cdot), (\mathbb{Q}^*, \cdot), (\mathbb{C}^*, \cdot)$ *are abelian groups. Yes*
3. $(\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}, \cdot)$ *is an abelian group. NO*

Proof

1. $\exists 1 \in \mathbb{Q} \quad ab \neq 0 \quad z = \dfrac{a}{b} \implies w = \dfrac{b}{a}$
2. $\forall z \in \mathbb{Q}^* \implies \exists w$ so that $z \cdot w = w \cdot = 1$

Definition $(k, +, \cdot)$ is a **field** if

1. $(k, +)$
2. $(k \setminus \{0\}, \cdot)$ is an abelian group
3. $(a + b) \cdot z = az + bz$ and/or $a(z + w) = az + aw$ (distribution law of multiplication over addition)

$(k, +, \cdot)$ is a **ring** if it satisfies 1, 2, 3 besides $\exists$ an inverse with respect to multiplication

Corollary 0.10

1. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ *are fields*
2. $(\mathbb{Z}, +, \cdot)$ *is a ring*

Theorem 0.11
$(\mathbb{Z}_m, +, \cdot)$ *is a commutative (abelian) ring.*
If m is prime, $(\mathbb{Z}_p, +, \cdot)$ is a field.

$$\mathbb{Z}_m = \{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}\}$$

1. $\hat{a} + \hat{b} \equiv \widehat{a+b} \pmod{m}$
2. $\hat{a} \cdot \hat{b} \equiv \widehat{a \cdot b} \pmod{m}$

While working with equivalence relations, we always need to check that the operations are well-defined i.e. they don't depend on the representative of claim.

1. Closure
   For any $\hat{a}, \hat{b} \in \mathbb{Z}_m$ then $\hat{a} + \hat{b} \in \mathbb{Z}_m$ and $\hat{a} \cdot \hat{b} \in \mathbb{Z}_m$.

2. Associativity
$$(\hat{a}+\hat{b})+\hat{c}=\hat{a}+(\hat{b}+\hat{c})$$
$$(\hat{a}\cdot\hat{b})\cdot\hat{c}=\hat{a}\cdot(\hat{b}\cdot\hat{c})$$

3. Commutativity
$$\hat{a}\cdot\hat{b}=\hat{b}\cdot\hat{a}$$
$$\hat{a}+\hat{b}=\hat{b}+\hat{a}$$

4. Identity elements
$$\hat{0}=\{m\cdot k\mid k\in\mathbb{Z}\}$$
$$\forall\hat{a}\in\mathbb{Z}_m\implies\begin{cases}\hat{a}+\hat{0}=\hat{0}+\hat{a}=\hat{a}\\ \hat{a}\cdot\hat{1}=\hat{1}\cdot\hat{a}=\hat{a}\end{cases}$$

5. $\mathbb{Z}_m$ has an additive inverse if $\hat{a}\in\mathbb{Z}_m$ $\exists!\hat{b}\in\mathbb{Z}_m$ so that $\hat{b}+\hat{a}=\hat{a}+\hat{b}=\hat{0}$.

6. Distributivity $(+,\cdot)$
$$\hat{a},\hat{b},\hat{c}\in\mathbb{Z}_m$$

Example

$$\forall z\in\mathbb{Z}_5\setminus\{0\}\implies\exists w\in\mathbb{Z}_5(z\cdot w)=\hat{1}$$
$$(\mathbb{Z}_5,+,\cdot)$$
$$\mathbb{Z}_5=\{\hat{0},\hat{1},\hat{2},\hat{3},\hat{4}\}$$
$$(\hat{1})^{-1}=\hat{1}$$
$$(\hat{2})^{-1}=\hat{3}\iff\hat{2}\cdot\hat{3}=\hat{6}=\hat{1}$$
$$(\hat{3})^{-1}=\hat{2}$$
$$(\hat{4})^{-1}=\hat{4}$$

Example

$$a,b,k,m\in\mathbb{Z}$$
$$k\geq 1,m\geq 2$$

Prove that if $a\equiv b \mod m$ then $a^k\equiv b^k \mod m$.

$$m\mid a-b\to m\mid a^k-b^k$$
$$(a-b)(a^{k-1}+a^{k-2}b+\cdots+ab^{k-2}+b^{k-1})$$

Definition Euclidean domain

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Euclidean algorithm exists so that

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z_2}}{z_2 \cdot \bar{z_2}} = \frac{z}{|z_2|^2} \in \mathbb{C} \because z \in \mathbb{C} \wedge |z_2| \in \mathbb{R}$$

Ordering can be done in complex based on absolute value

$$z_1 \leq z_2 \iff |z_1| \leq |z_2|$$

Theorem 0.12 *If p is prime, then $(\mathbb{Z}_p, +, \cdot)$ is a field.*

$$\begin{cases} (\mathbb{Z}_p, +) \text{ is an abelian group} \\ (\mathbb{Z}_p \setminus \{0\}, \cdot) \text{ is an abelian group} \\ +, \cdot \text{ is distributive} \end{cases}$$

- $(\hat{a} + \hat{b}) + \hat{c} = \hat{a} + (\hat{b} + \hat{c})$
- $\exists \hat{0} \in \mathbb{Z}_p (\hat{a} + \hat{0} = \hat{0} + \hat{a} = \hat{a})$
- $\forall \hat{a} \in \mathbb{Z}_n \; \exists \hat{b} (\hat{a} + \hat{b} = \hat{0})$

Lemma 0.13 *If p is prime, then any non-zero element in $\mathbb{Z}_p$ is invertible with respect to multiplication.*

$$\forall \hat{a} \in \mathbb{Z}_p [(a, p) = 1]$$

Theorem 0.14 *If n is not a prime*

$$(\mathbb{Z}_n, +, \cdot) \text{ is a ring}$$

$$U(\mathbb{Z}_n) = \{\hat{a} \mid (a, n) = 1\}$$
$$|U(\mathbb{Z}_n)| = \phi(n)$$

Definition Euler Function
Let $n \in \mathbb{N}$.

$$\phi(n) = \#\{m \in \mathbb{N} \mid 1 \leq m < n \text{ so that } (m, n) = 1\}$$

$$\phi(n) = n \prod_{d|n} \left(1 - \frac{1}{d}\right)$$

Theorem 0.15 *Let* $n = p_1^{k_1} \dots p_r^{k_r}$.

$$\phi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \dots p_r^{k_r-1}(p_r - 1)$$

Theorem 0.16 *Gauss' Divisor Sum Property*

$$\sum_{d|n} \phi(d) = n$$

Theorem 0.17 *Euler's theorem*
If $(a, n) = 1$, *then*

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