$\mathbb{Z}$, $\mathbb{Z}/m$ and rings (Chaps 6&9)

Important properties of numbers with $+,\times$
like $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_2$
and polynomials like $\mathbb{R}[x]$, $\mathbb{F}_2[x]$
abstract to rings and fields.

DEF'N: A ring $(R,+,\times)$ is a set R with
2 binary operations $+,\times$ satisfying familiar rules:

- $+,\times$ are associative and commutative:
  $(a+b)+c = a+(b+c)$ $\quad$ $a+b=b+a$
  $(ab)c = a(bc)$ $\quad$ $ab=ba$

  Actually R is a "commutative ring with 1"

- $\times$ distributes over $+$:
  $a(b+c)=ab+ac$

- there is an additive identity 0, multiplicative identity 1, and
  $0+a=a$ $\quad$ $1\cdot a=a$ $\quad$ $0\neq 1$

- there are additive inverses:
  $\forall a\in R\ \exists -a\in R$ with $a+(-a)=0$

DEF'N: The ring R is called a field if
additionally there are multiplicative inverses for $a\neq 0$:
$\forall a\in R-\{0\}\ \exists a^{-1}\in R$ with $a\cdot a^{-1}=1$.

EXAMPLES

(1) Everyone above is a ring

$\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_2,$ ← as small as it gets!

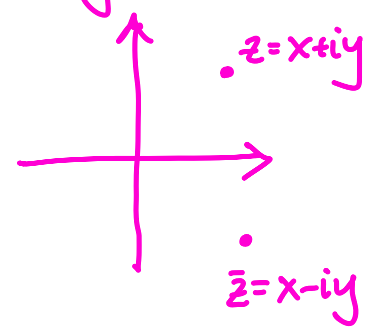
$\mathbb{R}[x], \mathbb{Q}[x], \mathbb{C}[x], \underbrace{\mathbb{F}_2[x]}$

<u>Q</u>: Who is $-f(x)$ here?

(2) Which of them are fields?

$\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_2$

<u>Q</u>: Who is z^{-1} if $z = x+iy \neq 0$ in $\mathbb{C}$?



$$z^{-1} = \frac{1}{z} = \frac{1}{x+iy}$$

$$= \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy}$$

$$= \frac{x-iy}{x^2+y^2} = \frac{x}{x^2+y^2} + \left(-\frac{y}{x^2+y^2}\right) i$$

Why are these denominators not 0?

A new ring $\mathbb{Z}/m$ (§6.7)

DEF'N: $\mathbb{Z}/m = \mathbb{Z}/m\mathbb{Z}$ = integers mod (modulo) m

$= \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$

= residues mod m

in which $+, \times$ are done as usual in $\mathbb{Z}$ followed by taking remainder on division by m

EXAMPLES

(1) $\mathbb{Z}/4$ has $+, \times$ tables

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(2) $\mathbb{F}_2 = \mathbb{Z}/2 = \{\underset{\text{evens}}{\bar{0}}, \underset{\text{odds}}{\bar{1}}\}$

we saw before

(3) We're somewhat familiar with $+$ in

$$\mathbb{Z}/7 = \{ \underset{\substack{\| \\ \text{Sundays}}}{\bar{0}}, \underset{\substack{\| \\ \text{Mondays}}}{\bar{1}}, \underset{\substack{\| \\ \text{Tuesdays}}}{\bar{2}}, \underset{\substack{\| \\ \text{Wednesdays}}}{\bar{3}}, \underset{\substack{\| \\ \text{Thursdays}}}{\bar{4}}, \underset{\substack{\| \\ \text{Fridays}}}{\bar{5}}, \underset{\substack{\| \\ \text{Saturdays}}}{\bar{6}} \}$$

(e.g. if today is Monday, what day is it 40 days from now?)

and $+$ in

$$\mathbb{Z}/24\mathbb{Z} = \{ \underset{\substack{\| \\ \text{midnights}}}{\bar{0}}, \bar{1}, \bar{2}, \ldots, \underset{\substack{\| \\ \text{noons}}}{\overline{12}}, \overline{13}, \ldots, \underset{\substack{\| \\ \text{11 PMs}}}{\overline{23}} \}$$

(e.g. if it's 4:30 pm, what time is it 30 hours from now?)

along with both $\times, +$ in

$$\mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{9}\}$$

(e.g. what is the last digit of 797×1024?)

$$\overline{797} \times \overline{1024} = \overline{797 \times 1024} = \bar{7} \times \bar{4} = \overline{28} = \bar{8} = \overline{-2} = \overline{-12} = \ldots$$

$$= \overline{-3} \times \bar{4}$$

We can safely be sloppy about doing the $+, \times$ operations before or after taking remainders.

Why??

DEF'N: Fix the modulus $m = 2, 3, \ldots$ in $\mathbb{Z}$.

Say $n \equiv n' \bmod m$ if $m \mid n' - n$

This is an equivalence relation: $n \equiv n$

$n \equiv n' \Leftrightarrow n' \equiv n$

$n \equiv n', n' \equiv n'' \Rightarrow n \equiv n''$

Call the equivalence class of n by $\bar{n}$, and let $\mathbb{Z}/m := \{\text{the equivalence classes } \bar{n} : n \in \mathbb{Z}\}$

KEY PROPOSITION:

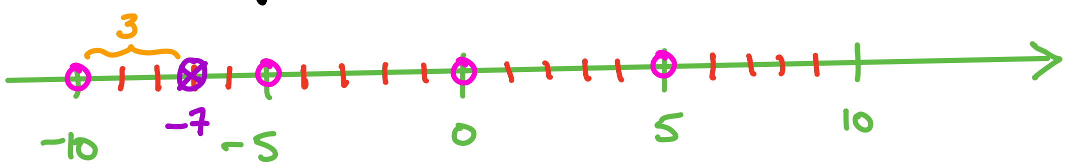
(a) For $n \in \mathbb{Z}$, the quotient q, remainder r in $n = q \cdot m + r$ become unique if we insist $0 \le r < m$

So $\bar{n} = \bar{r}$, and $\bar{n} = \bar{n'} \Leftrightarrow$ they have same remainder r on division by m,

and $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$ has exactly m elements.

(b) Given $\bar{a}, \bar{b} \in \mathbb{Z}/m$, one can pick any representatives $a, b \in \mathbb{Z}$ to compute $a+b$, $a \cdot b$, and the answers will be the same.

proof: (a) We could write down some inequalities, but hopefully this picture of an $m=5$ example makes the uniqueness clear enough:



$$\overset{n}{-7} = \underbrace{(-2)}_{q}\cdot \overset{m}{5} + \underbrace{3}_{r}$$

We have $\bar{n} = \bar{r}$ since $n-r=q\cdot m$ is divisible by m.
The last two assertions in (a) follow from these.

(b) Suppose $\bar{a} = \bar{a}'$, $\bar{b} = \bar{b}'$, that is, $m \mid a'-a,\ b'-b$.
Then $\overline{a+b} = \overline{a'+b'}$ follows because

$$(a'+b')-(a+b) = \underbrace{\underbrace{(a'-a)}_{\substack{\text{divisible}\\ \text{by } m}} + \underbrace{(b'-b)}_{\substack{\text{divisible}\\ \text{by } m}}}_{\Rightarrow\ \text{divisible by } m}$$

Similarly $\overline{a\cdot b} = \overline{a'\cdot b'}$ because

$$\begin{aligned} a'b'-ab &= a'b' - a'b + a'b - ab \\ &= \underbrace{a'\underbrace{(b'-b)}_{\substack{\text{divisible}\\ \text{by } m}} + \underbrace{(a'-a)}_{\substack{\text{divisible}\\ \text{by } m}}b}_{\Rightarrow\ \text{divisible by } m} \end{aligned}$$

$\blacksquare$

Q: For which moduli m is $\mathbb{Z}/m$ a field,

that is $\bar{a} \neq \bar{0}$ in $\mathbb{Z}/m$ always has a multiplicative inverse $\bar{b} = \bar{a}^{-1}$ with $\bar{a} \cdot \bar{b} = \bar{1}$?

EXAMPLES

$\mathbb{Z}/4$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

not a field:

$\bar{1}^{-1} = \bar{1}$

$\bar{3}^{-1} = \bar{3}$

but $\bar{2}^{-1}$ does not exist

$\mathbb{Z}/5$

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a field:

$\bar{1}^{-1} = \bar{1}$

$\bar{2}^{-1} = \bar{3}$

$\bar{3}^{-1} = \bar{2}$

$\bar{4}^{-1} = \bar{4}$

$\mathbb{Z}/6$

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

not a field:

$\bar{1}^{-1} = \bar{1}$

$\bar{5}^{-1} = \bar{5}$

but $\bar{2}^{-1}, \bar{3}^{-1}, \bar{4}^{-1}$ do not exist

The key is that 5 is prime, but 4, 6 are not.

To understand this it helps to see a common feature of the rings $\mathbb{Z}$ and $\mathbb{R}[x]$, $\mathbb{F}_2[x]$.

Division and Euclidean Algorithm (§6.5)

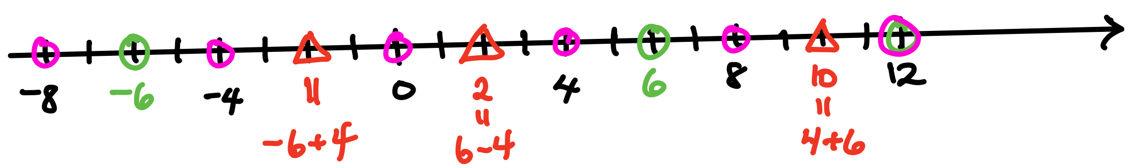
DEF'N: Let $m\mathbb{Z} :=$ multiples of m in $\mathbb{Z}$

$\left(\text{e.g. } 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\} \right)$

and let $m\mathbb{Z} + n\mathbb{Z} :=$ $\mathbb{Z}$-linear combinations of m, n

$= \{am + bn : a, b \in \mathbb{Z}\}$

EXAMPLE $4\mathbb{Z} + 6\mathbb{Z}$



In fact, $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. This always happens...

PROP: For any $m, n \in \mathbb{Z}$, there is a unique $d \in \{0, 1, 2, \ldots\}$ called $d = GCD(m,n)$ with $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

It has these properties:

greatest common divisor $\begin{cases} \text{(i) } d \mid m, n \\ \text{(ii) any } e \text{ with } e \mid m, n \text{ has } e \mid d \end{cases}$

(iii) $\exists\, a, b \in \mathbb{Z}$ with $d = am + bn$

proof: If we're in the degenerate case $m=n=0$ then $m\mathbb{Z}+n\mathbb{Z} = \{0\} = 0\cdot\mathbb{Z}$, so $d=0$.

Otherwise, $m\mathbb{Z}+n\mathbb{Z}$ contains some non-zero elements, and let d be the smallest positive one.

Why are there any positive ones?

We claim $d\mathbb{Z} = m\mathbb{Z}+n\mathbb{Z}$:

To see $d\mathbb{Z} \subseteq m\mathbb{Z}+n\mathbb{Z}$, note $d \in m\mathbb{Z}+n\mathbb{Z}$ so $d\mathbb{Z} \subseteq m\mathbb{Z}+n\mathbb{Z}$.

To see $d\mathbb{Z} \supseteq m\mathbb{Z}+n\mathbb{Z}$, given any $a \in m\mathbb{Z}+n\mathbb{Z}$ one can divide it by d to get

$$a = q\cdot d + r \quad \text{with } q, r \in \mathbb{Z},\ 0 \le r < d$$

and note that

$$r = \underbrace{\underbrace{a}_{\substack{\text{in}\\ m\mathbb{Z}+n\mathbb{Z}}} - \underbrace{q\cdot \underbrace{d}_{\text{in } m\mathbb{Z}+n\mathbb{Z}}}_{\text{in } m\mathbb{Z}+n\mathbb{Z}}}_{\text{in } m\mathbb{Z}+n\mathbb{Z}}$$

Hence $0 \le r < d$ and $r \in m\mathbb{Z}+n\mathbb{Z}$ forces $r=0$ because d was smallest in $m\mathbb{Z}+n\mathbb{Z}-\{0\}$.

Thus $a = q\cdot d \in d\mathbb{Z}$.

For the remaining properties of d, note

(iii): $d\mathbb{Z} = m\mathbb{Z}+n\mathbb{Z} \Rightarrow d = d\cdot 1 \in m\mathbb{Z}+n\mathbb{Z}$

$\Rightarrow d = am+bn$ for some $a,b\in\mathbb{Z}$

(i): $\left.\begin{array}{l} m = m\cdot 1 + n\cdot 0 \\ n = m\cdot 0 + n\cdot 1 \end{array}\right\} \Rightarrow m,n \in m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$

$\Rightarrow d$ divides m,n

(ii): if e divides m,n then

$$m,n \in e\mathbb{Z} \Rightarrow \underset{\substack{\parallel \\ d\mathbb{Z}}}{m\mathbb{Z}+n\mathbb{Z}} \subseteq e\mathbb{Z}$$

$$\Rightarrow d \in e\mathbb{Z} \Rightarrow e \mid d. \qquad \blacksquare$$

COROLLARY:

$\bar{n} \in \mathbb{Z}/m$ has a multiplicative inverse

$\iff \mathrm{GCD}(n,m) = 1$

and hence $\mathbb{Z}/m$ is a field

(i.e. every $\bar{n} \in \mathbb{Z}/m - \{0\}$ has a mult. inverse)

$\iff m$ is a prime

One calls $\{\bar{n} \in \mathbb{Z}/m : \gcd(n,m) = 1\} =: (\mathbb{Z}/m)^\times$

and its size $\varphi(m) := \#(\mathbb{Z}/m)^\times$ the Euler phi function

EXAMPLES

$$(\mathbb{Z}/4)^\times = \{\cancel{\bar 0}, \underset{\bar 1^{-1}}{\underset{\|}{\bar 1}}, \cancel{\bar 2}, \underset{\bar 3^{-1}}{\underset{\|}{\bar 3}}\} \quad \text{so} \quad \varphi(4)=2$$

$$(\mathbb{Z}/5)^\times = \{\cancel{\bar 0}, \underset{\bar 1^{-1}}{\underset{\|}{\bar 1}}, \underset{\bar 3^{-1}}{\underset{\|}{\bar 2}}, \underset{\bar 2^{-1}}{\underset{\|}{\bar 3}}, \underset{\bar 4^{-1}}{\underset{\|}{\bar 4}}\} \quad \varphi(5)=4$$

$$(\mathbb{Z}/6)^\times = \{\cancel{\bar 0}, \underset{\bar 1^{-1}}{\underset{\|}{\bar 1}}, \cancel{\bar 2}, \cancel{\bar 3}, \cancel{\bar 4}, \underset{\bar 5^{-1}}{\underset{\|}{\bar 5}}\} \quad \varphi(6)=2$$

---

proof of COROLLARY:

$\bar n \in \mathbb{Z}/m$ has a mult. inverse $\bar b$

$\iff \exists\, b \in \mathbb{Z}$ with $\bar b \cdot \bar n = \bar 1$ in $\mathbb{Z}/m$

i.e. $bn \equiv 1 \mod m$

i.e. $bn = 1 + am$ for some $a \in \mathbb{Z}$

$\iff \exists\, a,b \in \mathbb{Z}$ with $1 = -am + bn$

$\iff 1 \in m\mathbb{Z} + n\mathbb{Z}$

$\iff 1 \cdot \mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$

i.e. $GCD(m,n) = 1$.

For m a prime, note any $\bar{r} \in \{\bar{1}, \bar{2}, \dots, \overline{m-1}\}$ will have $d = GCD(r,m) = 1$

since $d \mid r \Rightarrow d \le r \le m-1$

$d \mid m \Rightarrow d = 1$ or $\cancel{m}$ too big .

For m not a prime, any proper factorization $m = m_1 m_2$ with $m_1, m_2 \ge 2$ gives $\bar{m}_1, \bar{m}_2 \ne \bar{0}$ but $GCD(m_i, m) = m_i \ne 1$,

so $\bar{m}_1^{-1}, \bar{m}_2^{-1}$ do not exist ∎

Q: How to compute $\bar{n}^{-1}$ in $\mathbb{Z}/m$ when $GCD(m,n) = 1$?

Euclid gave us an algorithm that both computes $d = GCD(m,n)$ and in its extended version, finds an expression $d = am + bn$.

So if $1 = d = am + bn$, then $\bar{b} = \bar{n}^{-1}$

since $\bar{b} \cdot \bar{n} = \bar{1}$ in $\mathbb{Z}/m$

EUCLID'S ALGORITHM for GCD(m,n)

If $m<n$, compute $\begin{array}{r} q \\ m\overline{)\,n\,} \\ \vdots \\ \hline r \end{array}$ giving $n = q\cdot m + r$, $0 \le r < m$.

When $r=0$, $m \mid n$ and GCD$(m,n) = m$.

Otherwise, we claim one has

$$\mathrm{GCD}(m,n) = \mathrm{GCD}(r,m)$$

proof: This happens $\Longleftrightarrow$ $m\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z} + m\mathbb{Z}$
which occurs because
$n = q\cdot m + r$ shows $\subseteq$
$r = n - q\cdot m$ shows $\supseteq$ ∎

and so you repeat, replacing (m,n) by (r,m).

Working backward step-by-step, one can find an expression $d = am + bn$

using the various $r = n - q\cdot m$ equations from $\begin{array}{r} q \\ m\overline{)\,n\,} \\ \vdots \\ \hline r \end{array}$

EXAMPLE $\mathrm{GCD}(\underset{m}{28}, \underset{n}{92}) = \mathrm{GCD}(8, 28) = \mathrm{GCD}(4, 8) = \underset{d}{4}$

$92 = 3\cdot 28 + 8$
$8 = 92 - 3\cdot 28$

$28 = 3\cdot 8 + 4$
$4 = 28 - 3\cdot 8$

$$\begin{array}{r} 3 \\ 28\overline{)92} \\ \underline{84} \\ 8 \end{array} \qquad \begin{array}{r} 3 \\ 8\overline{)28} \\ \underline{24} \\ 4 \end{array}$$

Try to express $d=4$ as $a\cdot 28 + b\cdot 92$:

$$\begin{aligned} 4 &= 28 - 3\cdot 8 \\ &= (1)(28) + (-3)(8) \\ &= (1)(28) + (-3)(92 - 3\cdot 28) \end{aligned}$$

$$4 = (10)(28) + (-3)(92)$$
$$d = a \quad m \quad + \quad b \quad n$$

EXAMPLE $p = 23$ is prime, so $\mathbb{Z}/23$ is a field.

What is $\bar{7}^{-1}$ in $\mathbb{Z}/23$?

Need $1 = a\cdot 7 + b\cdot 23$ from extended Euclid

$\mathrm{GCD}(7, 23) = \mathrm{GCD}(2, 7) = \mathrm{GCD}(1, 2) = 1$

$23 = 3\cdot 7 + 2$
$2 = 23 - 3\cdot 7$

$7 = 3\cdot 2 + 1$
$1 = 7 - 3\cdot 2$

$$\begin{array}{r} 3 \\ 7\overline{)23} \\ \underline{21} \\ 2 \end{array} \qquad \begin{array}{r} 3 \\ 2\overline{)7} \\ \underline{6} \\ 1 \end{array}$$

$$\begin{aligned} 1 &= 7 - 3\cdot 2 \\ &= (1)(7) + (-3)(2) \\ &= (1)(7) + (-3)(23 - 3\cdot 7) \end{aligned}$$

$$1 = \underbrace{(10)}_{a}\underbrace{(7)}_{n} + \underbrace{(-3)}_{b}\underbrace{(23)}_{m} \Rightarrow \bar{7}^{-1} = \bar{a} = \overline{10}$$

Check: $\overline{7\cdot 10} = \overline{70} = \bar{1}$ ✓ in $\mathbb{Z}/23$