**Def.** In a unitary commutative ring $(R, +, \cdot)$ a non-zero element $x \in R$ is called a zero divisor if $x \cdot y = 0$ for some non-zero $y \in R$.

**Proposition 1** In a unitary commutative ring, zero divisors are not invertible.

**Proof:** Let $x \in R \setminus \{0\}$ be a zero divisor, which means $x \cdot y = 0$ for some $y \in R \setminus \{0\}$.

If $x^{-1}$ existed, then we had

$$\underbrace{x^{-1} \cdot x \cdot y}_{= y} = \underbrace{x^{-1} \cdot 0}_{= 0} \Rightarrow y = 0, \text{ contradiction to } y \neq 0.$$

$\Rightarrow x^{-1}$ does not exist. $\square$

## Example $\mathbb{Z}_{15}$.

Invert one, if you can.

$[1] \cdot [1] = [1]$

$[2] \cdot [8] = [1]$

$[3] \cdot [5] = [0]$

$[4] \cdot [4] = [1]$

$[6] \cdot [5] = [0]$

$[13] \cdot [7] = [1]$

$[9] \cdot [5] = [0]$

$[10] \cdot [3] = [0]$

$[11] \cdot [11] = [1]$

$[12] \cdot [5] = [0]$

$[14] \cdot [14] = [1]$

| | invertible? |
|---|---|
| [1] | ✓ |
| [2] | ✓ |
| [3] | × |
| [4] | ✓ |
| [5] | × |
| [6] | × |
| [7] | ✓ |
| [8] | ✓ |
| [9] | × |
| [10] | × |
| [11] | ✓ |
| [12] | × |
| [13] | ✓ |
| [14] | ✓ |

Hack.

$(-x) \cdot (-y) = xy$

Every non-zero element in this example is either invertible or a zero divisor. There is a general result.

**Proposition 2.** In a finite unitary commutative ring $(R, +, \cdot)$, every non-zero element is either invertible or a zero divisor.

**Proof:** By Proposition 1, we know that zero divisors are not invertible. It remains to show that every $a \in R \setminus \{0\}$, which is not a zero divisor is invertible. We have:

$x \in R \setminus \{0\} \Rightarrow a \cdot x \neq 0$. So, we can define a function $f: R \setminus \{0\} \to R \setminus \{0\}$ by $f(x) = a \cdot x$.

We know that $f$ is injective (different inputs go to different outputs)

Consider arbitrary $x', x'' \in R \setminus \{0\}$, with $x' \neq x''$.

We need to show that $f(x') \neq f(x'')$, meaning $a \cdot x' \neq a \cdot x''$. Assume, we had $a \cdot x' = a \cdot x''$. Then, we'd have

$$a \cdot \underbrace{(x' - x'')}_{\neq 0} = 0 \Rightarrow$$

$a$ is a zero divisor, a contradiction to the assumption on $a$. $\Rightarrow$ $f$ is injective.

Let $s := |R|$ be the (finite) size of the ring $R$.

Then $f$ sends $s-1$ elements of $R\setminus\{0\}$ to the $s-1$ different elements of the set $R\setminus\{0\}$ of size $s-1$. So, every $y \in R\setminus\{0\}$ is an output $y = f(x)$ for some $x \in R\setminus\{0\}$.

$\Rightarrow$ $f$ is surjective. $\Rightarrow$ $f$ is both surjective and injective $\Leftrightarrow$ $f$ is bijective.

By picking $y = 1$, we know that there exists $x \in R\setminus\{0\}$ with $f(x) = 1$, which means $a \cdot x = 1$. This means $x = a^{-1}$. $\Rightarrow$ $a$ is invertible. □

**Example.** $\mathbb{Z}_{15}$ $\quad a = [2]$.

$f(x) = ax$ $\qquad f : \mathbb{Z}_{15}\setminus\{0\} \to \mathbb{Z}_{15}\setminus\{0\}$

| $x$ | $ax$ |
|---|---|
| $[1]$ | $[2]$ |
| $[2]$ | $[4]$ |
| $[3]$ | $[6]$ |
| $[4]$ | $[8]$ |
| $[5]$ | $[10]$ |
| $[6]$ | $[12]$ |
| $[7]$ | $[14]$ |
| $[8]$ | $[1]$ |
| $[9]$ | $[3]$ |
| $[10]$ | $[5]$ |
| $[11]$ | $[7]$ |
| $[12]$ | $[9]$ |
| $[13]$ | $[11]$ |
| $[14]$ | $[13]$ |

$\leftarrow$ the inverse of $a$ is $[8]$.

$x = [8] \Rightarrow a \cdot x = [2]\cdot[8]$

$= [16] = [1]$

**Remark.** finiteness of $R$ is essential in Proposition 2.

Let's take $R = \mathbb{Z}$ and let's take $a = 2$.

$f : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{Z} \setminus \{0\}$ defined

by $f(x) = ax = 2x$ is still injective,

but not surjective anymore, because

$f(x)$ is always even and never odd,

in particular you cannot have $f(x) = 1$ for

any choice of $x \in \mathbb{Z}$.

# A field or not a field, that is the question.

**Theorem 3.** For $n \geq 2$, $\mathbb{Z}_n$ is a field if and only if $n$ is prime.

**Proof.** If $n$ is not a prime, then

$n = a \cdot b$ for some $a, b \in \mathbb{Z}$ with $a \geq 2$, $b \geq 2$.

$\Rightarrow$ $\underbrace{[a]}_{\neq [0]} \cdot \underbrace{[b]}_{\neq [0]} = [0]$ $\Rightarrow$ $[a]$ and $[b]$ are

zero divisors $\xRightarrow{\text{Prop 1}}$ $[a]$ and $[b]$ are not invertible

a non-zero elements $\Rightarrow$ $\mathbb{Z}_n$ is not a field.

If $n$ is prime, we show that $\mathbb{Z}_n$ is a field using Proposition 2, that is, by showing that $\mathbb{Z}_n$ has no zero divisors. Assume $\mathbb{Z}_n$ had zero divisors, Then we would have

$$[a] \cdot [b] = [0] \quad \text{for some}$$

$[a] \neq [0]$ and $[b] \neq 0$.

The equation $[a] \cdot [b] = [0]$ means

$[a \cdot b] = [0]$, which means that

$a \cdot b$ is divisible by the prime number $n$.

Since $a$ is prime, we have $a$ is divisible by $n$ or $b$ is divisible by $n$. But that means

$[a] = [0]$ or $[b] = [0]$, which is a contradiction to our assumption on $[a]$ and $[b]$.

**Example** How could we use the + and · of $\mathbb{Z}_n$ in cryptography? We have already mentioned the use of +.

Caesar was: $y = x + b$ over $\mathbb{Z}_{26}$

- $y$: cipher for the symbol
- $x$: symbol
- $b$: key

Decryption: $x = y - b$.

Now, we could also do:

$$y = a \cdot x + b \quad \text{over } \mathbb{Z}_{26}$$

The key would be $k = (a, b)$.

To use this one, we need $a$ that can be inverted. Because, we can also

decipher $x = a^{-1} \cdot (y - b)$.

## 1.2. Back to integers and the GCD.

In practice $n$ in $\mathbb{Z}_n$ can be a huge number: many, many, many digits. We need to do algebra in $\mathbb{Z}_n$ efficiently.

### A naive inverse algorithm for $a \in \mathbb{Z}_n \setminus \{0\}$.

For $x \in \mathbb{Z}_n \setminus \{0\}$:
    if $x \cdot a = 0$:
        return "a not invertible".
    else if $x \cdot a = 1$:
        return "the inverse of $a$ is $x$".

Not an option ($n-1$ iterations in the worst case). Exponential running time in the bit size of $n$.

**Def.** For $a, b \in \mathbb{Z}$ the greatest common divisor of $a$ and $b$ is defined as the largest natural number $g \in \mathbb{N}$ such that $a$ and $b$ are both divisible by $g$ if $a$ and $b$ are not both equal to zero. If $a = b = 0$, we define the greatest common divisor of $a$ and $b$ to be zero.

Notation: $\gcd(a, b)$

**Remark:** $\gcd(a, b)$ does not depend on the sign and on the order of $a$ and $b$:

$$\gcd(a, b) = \gcd(\pm a, \pm b), \quad \gcd(a, b) = \gcd(b, a)$$

In particular, one can ensure that $0 \leq a \leq b$.
It is also clear that $\gcd(0, b) = b$ for $b \geq 0$.

**Lemma 4.** For $a, b, k \in \mathbb{Z}$, one has

$$\gcd(a, b) = \gcd(a, b + k \cdot a).$$

**Proof:** We need to verify that both pairs $(a, b)$ and $(a, b + ka)$ have the same set of common divisors.

If $g \in \mathbb{N}$ divides $a$ and $b$, then $\frac{a}{g}, \frac{b}{g} \in \mathbb{Z}$

$$\mathbb{Z} \ni \frac{a}{g}, \underbrace{\frac{b}{g}}_{\in \mathbb{Z}} + k \cdot \underbrace{\frac{a}{g}}_{\in \mathbb{Z}} \in \mathbb{Z} \quad \Rightarrow \quad \frac{a}{g}, \frac{b + k \cdot a}{g} \in \mathbb{Z}$$

$\Rightarrow$ $g$ is a common divisor of $a$ and $b + ka$.

Conversely, if $g \in \mathbb{N}$ is a common divisor of $a$ and $b + k \cdot a$, then $\frac{a}{g}, \frac{b+k\cdot a}{g} \in \mathbb{Z}$

$$\Rightarrow \frac{a}{g}, \frac{b}{g} + k \cdot \frac{a}{g} \in \mathbb{Z} \Rightarrow$$

$$\Rightarrow \underbrace{\frac{a}{g}}_{\in \mathbb{Z}}, \frac{b}{g} = \underbrace{\left(\frac{b}{g} + k \cdot \frac{a}{g}\right)}_{\in \mathbb{Z}} - \underbrace{k \cdot \frac{a}{g}}_{\in \mathbb{Z}} \Rightarrow \frac{a}{g}, \frac{b}{g} \in \mathbb{Z} \Rightarrow$$

$g$ is a common divisor of $a$ and $b$. □

**Example** Let's try computing a gcd relying on Lemma 4:

$$\begin{aligned} \gcd(12,70) &= \gcd(12, 70 - 5\cdot 12) = \gcd(12,10) \\ &= \gcd(10,12) = \gcd(10, 12-10) = \gcd(10,2) \\ &= \gcd(2,10) = \gcd(2, 10 - 5\cdot 2) = \gcd(2,0) \\ &= \gcd(0,2) = 2. \end{aligned}$$

When we use $\gcd(a,b) = \gcd(a, b-k\cdot a)$

in the algorithmic

setting with $0 < a \leq b$ we can

stick to the case where $b - k\cdot a = (b \bmod a)$

$k =$ Quotient of the long division of $b$ by $a$.

(b mod a) = remainder of the long division of $b$ by $a$

This gives the so-called Euclidean Algorithm (EA)

recursive_EA(a, b):

Assume: $0 \leq a \leq b$, $a, b \in \mathbb{Z}$

if $a = 0$:

return $b$

return recursive_EA($b \bmod a$, $a$)

The standard iterative version of the EA.

standard_EA(a,b)

Assume: $0 \leq a \leq b$, $a, b \in \mathbb{Z}$

while $a \neq 0$:

$a, b := b \bmod a, a$

return $b$

How could you convince someone that $\gcd(a,b) = g$? By what data?

How could we verify that $\gcd(12,70) = 2$?

$6, -1$ are a certificate!

$$6 \cdot 12 + (-1) \cdot 70 = 2$$

We want to learn how to calculate such certificates.

**Example.** Let's see how we can construct the above certificate.

$$\begin{cases} x = 12 & (1) \\ y = 70 & (2) \end{cases} \qquad (2) := (2) - 5\cdot(1)$$

$$\begin{cases} x = 12 & (1) \\ -5x + y = 10 & (2) \end{cases} \qquad (1) := 2(1) - (2)$$

$$\begin{cases} 6x - y = 2 & (1) \\ -5x + y = 10 & (2) \end{cases} \qquad (2) := (2) - 5\cdot(1)$$

$$\begin{cases} 6x - y = 2 & (1) \\ -35x + 6y = 0 & (2) \end{cases}$$

We know $2 = \gcd(12, 70)$

and when $x = 12, y = 70 \Rightarrow 6x + (-1)\cdot y = 2$

# Extended Euclidean Algorithm

Assume: $0 \leq a \leq b$, $a, b \in \mathbb{Z}$

Start with the system $\begin{cases} x = a \\ y = b \end{cases}$

with the unknowns $x$ and $y$. Apply the same operations $(a\ b) \mapsto (a\ b - ka)$ to the pair of the equations of the system (which you would apply to the pair of the right hand sides in the Euclidean Algorithm.

You terminate with the system

$$\begin{cases} u \cdot x + v \cdot y = 0 \\ s \cdot x + t \cdot y = g \end{cases}$$

where $g = \gcd(a, b)$, $u, v, s, t \in \mathbb{Z}$

and the two equations you obtain are valid for $x = a$, $y = b$ which you had in the input.