Example: $\mathbb{Z}_{41}$. Let's invert x^{33}. It is indeed invertible by Corollary 8 since $\gcd(33, 41-1) = 1$. We do EEA on $(33, 40)$.

$$\begin{cases} e = 33 & (1) \\ \tilde{p} = 40 & (2) \end{cases} \qquad (2) := (2) - (1)$$

$$\begin{cases} e = 33 & (1) \\ -e + \tilde{p} = 7 & (2) \end{cases} \qquad (1) := (1) - 5\cdot(2)$$

← Deviation from the standard EEA. But it still works.

$$\begin{cases} 6e - 5\tilde{p} = -2 & (1) \\ -e + \tilde{p} = 7 & (2) \end{cases} \qquad (2) := (2) + 3(1)$$

$$\begin{cases} 6e - 5\tilde{p} = -2 & (1) \\ 17e - 14\tilde{p} = 1 & (2) \end{cases} \qquad (1) := (1) + 2(2)$$

← Let's do it, even though we don't strictly need this

$$\begin{cases} 40e - 33\tilde{p} = 0 & (1) \\ 17e - 14\tilde{p} = 1 & (2) \end{cases}$$

$$\Downarrow$$

$$17 \cdot e \equiv 1 \pmod{40}$$

$\Rightarrow$ By Corollary 8, the inverse of x^{33} is x^{17}.

Computational issue: How do we compute powers quickly?

We want to compute x^e for $e \in \mathbb{N}_0$ for x in a unitary commutative ring $(R, +, \cdot)$. Can we save multiplications?

```
Naive_power(x, e):
    p := 1
    for i := 1, ..., e:
        p := p · x
    return p
```

$$x \xmapsto{\cdot x} x^2 \xmapsto{\cdot x} x^3 \mapsto \dots \xmapsto{\cdot x} x^e$$

This way we spend $e-1$ multiplications to compute x^e.

This is way too much if e has many digits.

$$x^{183487553\,11}$$

Example We want to compute x^{23} quickly.

23 in the binary is 10111

$$23 = 16 + 4 + 2 + 1 \Rightarrow$$

$$x^{23} = x^{16} \cdot x^4 \cdot x^2 \cdot x^1$$

$$x \xrightarrow[\text{square}]{} x^2 \xrightarrow[\text{square}]{} x^4 \xrightarrow[\text{square}]{} x^8 \xrightarrow[\text{square}]{} x^{16}$$

4 multiplications for creating the necessary squares

4 multiplications for multiplying the powers x^1, x^2, x^4, x^{16} relevant to calculation of x^{23}.

Let's implement this idea recursively!

$$x^e = \begin{cases} x & \text{if } e = 1 \\ (x^2)^{\frac{e}{2}} & \text{if } e \text{ is even and at least two.} \\ (x^2)^{\frac{e-1}{2}} \cdot x & \text{if } e \text{ is odd and at least three} \end{cases}$$

This recursive formulation of the power function is essentially a recursive algorithm.

How to implement this iteratively?

You can start with $s := x$ and $p := 1$ and maintain $s^e \cdot p$ as an invariant.

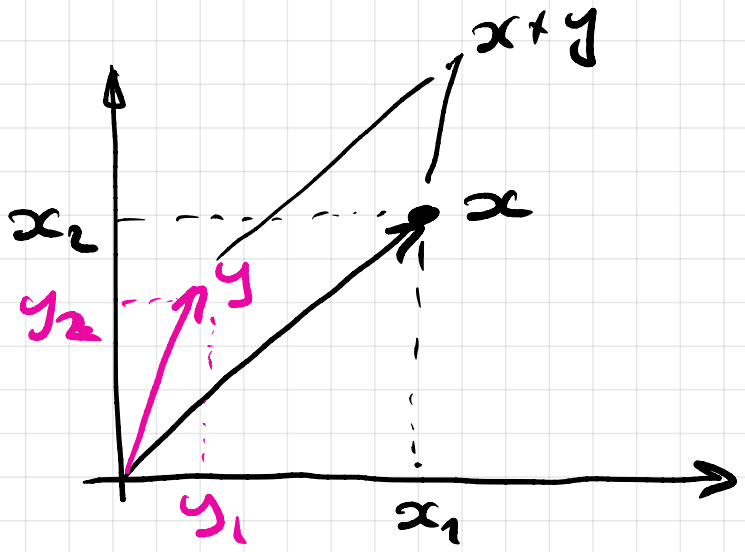
The algorithm would make e smaller in each iteration, maintaining the value of $s^e \cdot p$. And this value is x^e for the e in the input.

```
fast-exponentiation(x, e):
    p := 1
    s := x
    ▷ Invariant: s^e · p is our result.
    while e > 0:
        if e is odd:
            p := p · s          ▷ s^(e-1) · p.
            s := s^2
            e := (e-1)/2
            ▷ Invariant: s^e · p is our result.
        else:
            s := s^2
            e := e/2
            ▷ Invariant: s^e · p is our result.

    return p.
```

1.4. The Chinese Remainder Theorem

Can we model $\mathbb{Z}_n$ (that is, implement computations in $\mathbb{Z}_n$) by two smaller structures $\mathbb{Z}_{n_1}$ and $\mathbb{Z}_{n_2}$ with $n_1 n_2 < n$?



$$x + y = (x_1 + y_1,\ x_2 + y_2)$$

$x+y$ splits into two independent calculations.

We want to do something like this with $\mathbb{Z}_n$ that is, split computations in $\mathbb{Z}_n$ into independent threads.

Remark. If $n, d \in \mathbb{N}$, $n, d \geq 2$ and n is divisible by d, then the map

$\mathbb{Z}_n \longrightarrow \mathbb{Z}_d$ acting by

$[z]_n \longmapsto [z]_d$ is well-defined. That is, if you know the remainder of the division by n, then you also know the remainder of the division by d when d is a factor of n.

Example $\mathbb{Z}_6 \longrightarrow \mathbb{Z}_3$

$[0]_6 \longmapsto [0]_3$

$[1]_6 \longmapsto [1]_3$

$[2]_6 \longmapsto [2]_3$

$[3]_6 \longmapsto [0]_3$

$[4]_6 \longmapsto [1]_3$

$[5]_6 \longmapsto [2]_3$

Example

$\mathbb{Z}_{35} \to \mathbb{Z}_5$ $\quad [z]_{35} \longmapsto [z]_5$

$\mathbb{Z}_{35} \to \mathbb{Z}_7$ $\quad [z]_{35} \longmapsto [z]_7$

that gives a map: $[z]_{35} \longmapsto ([z]_5, [z]_7)$.

$\mathbb{Z}_7$

$\mathbb{Z}_5$	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

this map $\mathbb{Z}_{35} \to \mathbb{Z}_5 \times \mathbb{Z}_7$ is bijective!

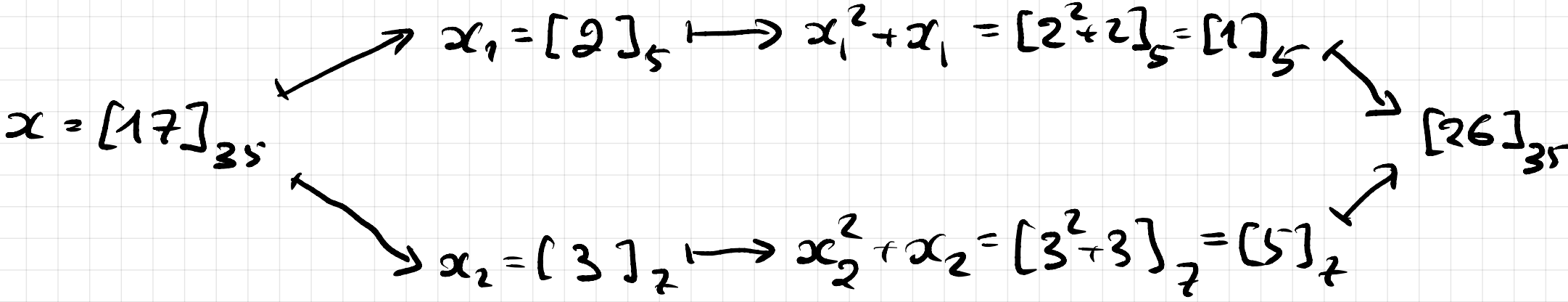
It's not only that

It also respects calculations.

Instead of doing algebra in $\mathbb{Z}_{35}$ we can do the same algebra independently twice,

once in $\mathbb{Z}_5$ and once in $\mathbb{R}_7$.

For example: assume we want to evaluate x^2+x at $x=[17]_{35}$



Def. Let R_1, R_2 be unitary commutative rings. Then the direct product of rings R_1 and R_2 is defined as the Cartesian product $R_1 \times R_2$ with the $+$ and $\cdot$ defined by:

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot b_1, a_2 \cdot b_2)$$

$R_1 \times R_2$ represents doing the "same algebra" in R_1 and R_2 independently.

Example $x = (x_1, x_2)$ with $x_1 \in R_1$ and $x_2 \in R_2$

What is $x^2 + x$? It's

$$x^2 + x = x \cdot x + x = (x_1, x_2) \cdot (x_1, x_2) + (x_1, x_2)$$

$$= (x_1^2, x_2^2) + (x_1, x_2)$$

$$= (x_1^2 + x_1, x_2^2 + x_2).$$

Rem. Clearly, $R_1 \times R_2$ is a unitary commutative ring with the $1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$.

Rem $R_1 \times R_2$ is never a field, because

$$(1,0) \cdot (0,1) = (1 \cdot 0, 0 \cdot 1) = (0,0)$$

$\Rightarrow$ $(1,0)$ and $(0,1)$ are zero divisors.

Def. Let S, T be unitary commutative rings. Then a map $f: S \to T$ is called a unitary homomorphism if the following hold:

$f(1_S) = 1_T$ and

$$\left.\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b) \end{aligned}\right\} \text{for every } a, b \in S$$

If additionally, f is bijective, then f is called a unitary isomorphism and the respective S and T are called isomorphic unitary commutative rings.

Example Let $n, d \in \mathbb{N}$ with $n, d \geq 2$ and let n be divisible by d. Then the map

$f : \mathbb{Z}_n \to \mathbb{Z}_d$ given by

$$f([z]_n) = [z]_d \quad \text{for } z \in \mathbb{Z}$$

is well defined and is a unitary homomorphism.

Why well defined? If $u, v \in \mathbb{Z}$ define the same coset, i.e. $u \equiv v \pmod{n}$, then $u - v$ is divisible by n. But n is divisible by d. So, $u - v$ is divisible by d. $\Rightarrow$

$u \equiv v \pmod{d} \Rightarrow [u]_d = [v]_d$.

Why is f a unitary homomorphism?

$$f([1]_n) = [1]_d$$

$[1]_n$: the one in $\mathbb{Z}_n$

$[1]_d$: the one in $\mathbb{Z}_d$

$$f([a]_n + [b]_n) = f([a+b]_n) = [a+b]_d$$
$$= [a]_d + [b]_d$$
$$= f([a]_n) + f([b]_n)$$

It's just the same for multiplication:

$$f([a]_n \cdot [b]_n) = f([a \cdot b]_n) = [a \cdot b]_d = [a]_d \cdot [b]_d$$
$$= f([a]_n) \cdot f([b]_n)$$

Remark. If S and T (unitary commutative rings), then one can "translate" between the calculations in these structures. Let f be a unitary isomorphism $f: S \to T$. And assume in S we have found some $x \in S$ satisfying $x^2 + x = 1$. We can apply f to this relation and obtain

$$
\begin{array}{l}
\Downarrow \quad f(x^2 + x) = f(1) \\
\Downarrow \quad f(x^2) + f(x) = 1 \\
\Downarrow \quad f(x \cdot x) + f(x) = 1 \\
\quad\; f(x) \cdot f(x) + f(x) = 1
\end{array}
$$

$y^2 + y = 1$ for $y = f(x)$.

so, y is a "translation of" $x \in S$ in the "world" of T.

Theorem 9 Let $n \in \mathbb{N}$ be a product of two relatively prime numbers $n_1, n_2 \geq 2$, that is

$$n = n_1 \cdot n_2 \quad \text{and} \quad \gcd(n_1, n_2) = 1.$$

Then the unitary commutative rings $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ are isomorphic.

Proof: Let's consider the unitary homomorphism

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \text{ given by}$$

$$f([z]_n) := ([z]_{n_1}, [z]_{n_2})$$

By the above discussion, it is indeed a unitary homomorphism.

We need to show that it is bijective.

Let's show that f is injective

Let's take cosets $[u]_n$ and $[v]_n$ with $u, v \in \mathbb{Z}$ such that $f([u]_n) = f([v]_n) \Rightarrow$

$$([u]_{n_1}, [u]_{n_2}) = ([v]_{n_1}, [v]_{n_2}) \Rightarrow$$

$$\begin{cases} [u]_{n_1} = [v]_{n_1} \\ [u]_{n_2} = [v]_{n_2} \end{cases} \Rightarrow$$

$$\begin{cases} u - v \text{ is divisible by } n_1 \\ u - v \text{ is divisible by } n_2 \end{cases}$$

But since $\gcd(n_1, n_2) = 1$, the difference $u - v$ is divisible by $n_1 n_2 = n$

$\Rightarrow [u]_n = [v]_n$.

$\Rightarrow f$ is injective.

Since $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ have the same number $n = n_1 \cdot n_2$ of elements, f is surjective, too.

$\Rightarrow f$ is bijective.

□

Theorem 9 is the Chinese Remainder Theorem in a very basic formulation.

Lemma 10 Let p and q be prime numbers with $p \neq q$ and let $n = p \cdot q$. Let $e \in \mathbb{N}$ be a natural number satisfying $\gcd(e, (p-1)\cdot(q-1)) = 1$

Then there exists $d \in \{1, \dots, (p-1)\cdot(q-1)\}$ such that x^d is the inverse function of x^e on $\mathbb{Z}_n$. That means,

$$(x^e)^d = (x^d)^e = x \quad \text{for every } x \in \mathbb{Z}_n.$$