Problem

Given: a matrix $A \in \mathbb{Q}^{n \times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

Problem

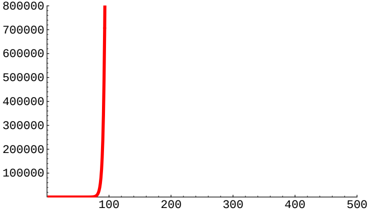
Given: a matrix $A \in \mathbb{Q}^{n \times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

This can be done with Gaussian elimination.

Problem

Given: a matrix $A \in \mathbb{Q}^{n\times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

This can be done with Gaussian elimination.

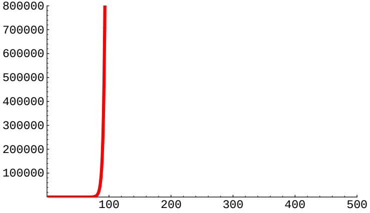


But this is very slow. . .

Problem

Given: a matrix $A \in \mathbb{Q}^{n\times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

This can be done with Gaussian elimination.



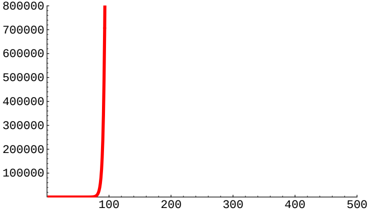
But this is very slow...

Observation:
This seems to be exponential.

Problem

Given: a matrix $A \in \mathbb{Q}^{n \times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

This can be done with Gaussian elimination.



But this is very slow...

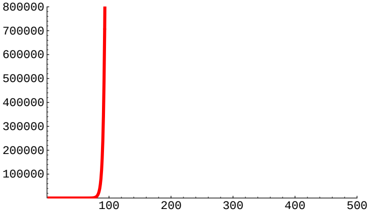
Observation:
This seems to be exponential.

Ex: expected runtime for solving a 300×300 system: 10^{33} years.

Problem

Given: a matrix $A \in \mathbb{Q}^{n \times n}$
Find: all $x \in \mathbb{Q}^n$ such that $A \cdot x = 0$.

This can be done with Gaussian elimination.



But this is very slow...

Observation:
This seems to be exponential.

Ex: expected runtime for solving a 300×300 system: 10^{33} years.
(If you are 100 000 times faster, you still have to wait 10^{27} years.)

Problem

Why is this?

Problem

Why is this? Gaussian elimination should run in polynomial time.

Problem

Why is this? Gaussian elimination should run in polynomial time.

Indeed it does, but let's have a close look.

Problem

Why is this? Gaussian elimination should run in polynomial time.

Indeed it does, but let's have a closer look.

Time for arithmetic in $\mathbb{Q}$ depends on the *bitsize* of the input.

Problem

Why is this? Gaussian elimination should run in polynomial time.

Indeed it does, but let's have a closer look.

Time for arithmetic in $\mathbb{Q}$ depends on the *bitsize* of the input.

The bitsize doubles with addition or multiplication:

$$\frac{1245343545245}{5902739457324} + \frac{3457293579639}{9372394567964}$$

Problem

Why is this? Gaussian elimination should run in polynomial time.

Indeed it does, but let's have a closer look.

Time for arithmetic in $\mathbb{Q}$ depends on the *bitsize* of the input.

The bitsize doubles with addition or multiplication:

$$\frac{1245343545245}{5902739457324} + \frac{3457293579639}{9372394567964} = \frac{2004959644174458006084826}{3457675201620639174723021}$$

Problem

Why is this? Gaussian elimination should run in polynomial time.

Indeed it does, but let's have a closer look.

Time for arithmetic in $\mathbb{Q}$ depends on the *bitsize* of the input.

The bitsize doubles with addition or multiplication:

$$\frac{1245343545245}{5902739457324} + \frac{3457293579639}{9372394567964} = \frac{2004959644174458006084826}{3457675201620639174723021}$$

Therefore, we have

- exponential *"bit complexity"* despite of the
- polynomial *"arithmetic complexity"*.

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.

$$\mathbb{Q} \rightsquigarrow \mathbb{Q}$$

Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.

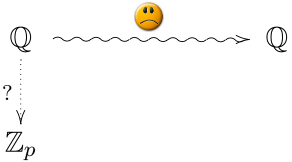
Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.



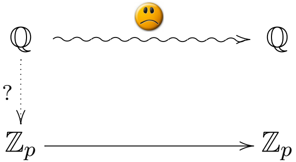
Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.



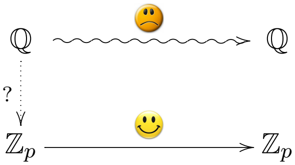
Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.



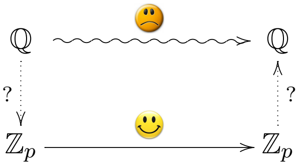
Problem

In short: Not Gaussian elimination is bad, but $\mathbb{Q}$ is bad.

For example, Gauss in a prime field $\mathbb{Z}_p$ is fast.

Reason: Elements in $\mathbb{Z}_p$ have a fixed size.

Idea: Do the computation in $\mathbb{Z}_p$ and recover the result for $\mathbb{Q}$ from the result for $\mathbb{Z}_p$.



$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_\sim$ where $a \sim b :\Leftrightarrow p \mid a - b$.

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_\sim$ where $a \sim b :\Leftrightarrow p \mid a - b$.

For example $\mathbb{Z}_{71} = \{[0]_\sim, [1]_\sim, [2]_\sim, \ldots, [70]_\sim\}$

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_\sim$ where $a \sim b :\Leftrightarrow p \mid a - b$.

For example $\mathbb{Z}_{71} = \{[0]_\sim, [1]_\sim, [2]_\sim, \ldots, [70]_\sim\}$ where, .e.g,

$$[18]_\sim = \{\ldots, -124, -53, 18, 89, 160, 231, \ldots\} \subseteq \mathbb{Z}$$

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_{\sim}$ where $a \sim b :\Leftrightarrow p \mid a - b$.

For example $\mathbb{Z}_{71} = \{[0]_\sim, [1]_\sim, [2]_\sim, \ldots, [70]_\sim\}$ where, .e.g,

$[18]_\sim =$ 

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_\sim$ where $a \sim b :\Leftrightarrow p \mid a - b$.

For example $\mathbb{Z}_{71} = \{[0]_\sim, [1]_\sim, [2]_\sim, \dots, [70]_\sim\}$ where, .e.g,

$[18]_\sim =$ 

$\mathbb{Z}_p$ is a ring and

$$\operatorname{mod}\colon \mathbb{Z} \to \mathbb{Z}_p \quad x \mapsto [x]_\sim$$

is a ring homomorphism.

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

Recall: $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} := \mathbb{Z}/_\sim$ where $a \sim b :\Leftrightarrow p \mid a - b$.

For example $\mathbb{Z}_{71} = \{[0]_\sim, [1]_\sim, [2]_\sim, \dots, [70]_\sim\}$ where, .e.g,

$[18]_\sim =$ 

$\mathbb{Z}_p$ is a ring and

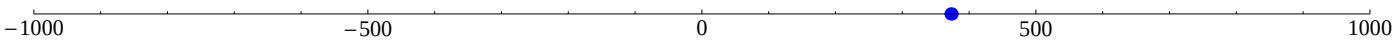
$$\operatorname{mod}: \mathbb{Z} \to \mathbb{Z}_p \quad x \mapsto [x]_\sim$$

is a ring homomorphism. Therefore:

$$\boxed{\operatorname{mod}(\text{solution}(\text{problem})) = \text{solution}(\operatorname{mod}(\text{problem}))}$$

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Suppose the solution to a problem is $x \in \mathbb{Z}$.



$\mathbb{Z} \longleftarrow \mathbb{Z}_p$

Suppose the solution to a problem is $x \in \mathbb{Z}$.

Suppose we know $[x]_\sim \in \mathbb{Z}_p$.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Suppose the solution to a problem is $x \in \mathbb{Z}$.

Suppose we know $[x]_\sim \in \mathbb{Z}_p$.

How to choose p such that x can be recovered from its homomorphic image $[x]_\sim \in \mathbb{Z}_p$?

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Suppose the solution to a problem is $x \in \mathbb{Z}$.

Suppose we know $[x]_\sim \in \mathbb{Z}_p$.

How to choose p such that x can be recovered from its homomorphic image $[x]_\sim \in \mathbb{Z}_p$?

Observation: If $p >> 0$, then x is the element of $[x]_\sim$ with least absolute value.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Two typical scenarios:

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Two typical scenarios:

- There is an a priori bound M on the final result.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M$.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M$.
- There is an efficient way to check whether a solution candidate is correct.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M$.
- There is an efficient way to check whether a solution candidate is correct.
  - Then redo the computation with larger and larger choices of p until the correct solution is found.

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

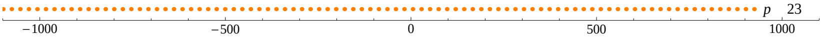
In the second scenario, it can be exploited that

$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

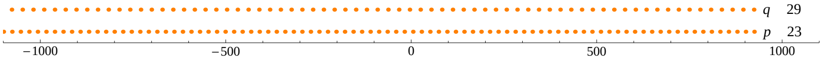
$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$



$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

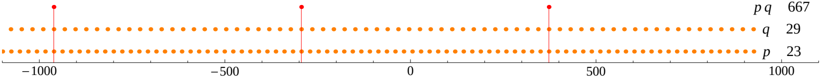
$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$



$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

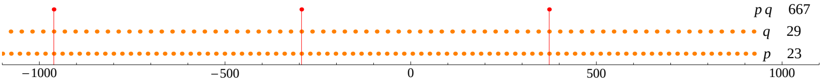
$$x \in [x]_p \cap [x]_q = [x]_{\text{lcm}(p,q)}.$$



$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$



A representative for $[x]_{\mathrm{lcm}(p,q)}$ can be computed from representatives of $[x]_p$ and $[x]_q$ by the *Chinese Remainder Algorithm.*

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$

Two features:

$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$

Two features:

- We don't need to throw away the results of trial computation for p that turned out to be too small.

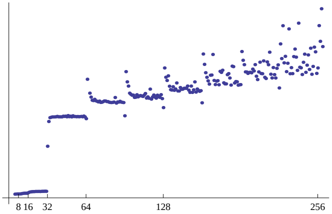
$$\mathbb{Z} \longleftarrow \mathbb{Z}_p$$

In the second scenario, it can be exploited that

$$x \in [x]_p \cap [x]_q = [x]_{\mathrm{lcm}(p,q)}.$$

Two features:

- We don't need to throw away the results of trial computation for p that turned out to be too small.
- We don't need to ever choose a $p > 2^{32}$ for which arithmetic would be considerably slower.



$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

Then there exist $s, t \in \mathbb{Z}$ with

$$1 = \gcd(p, v) = sp + tv$$

$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

Then there exist $s, t \in \mathbb{Z}$ with

$$1 = \gcd(p, v) = sp + tv$$

So $[1]_\sim = [tv]_\sim = [t]_\sim [v]_\sim$ in $\mathbb{Z}_p$

$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

Then there exist $s, t \in \mathbb{Z}$ with

$$1 = \gcd(p, v) = sp + tv$$

So $[1]_\sim = [tv]_\sim = [t]_\sim [v]_\sim$ in $\mathbb{Z}_p$

We can therefore define $[\frac{u}{v}]_\sim := [ut]_\sim$

$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

Then there exist $s, t \in \mathbb{Z}$ with

$$1 = \gcd(p, v) = sp + tv$$

So $[1]_\sim = [tv]_\sim = [t]_\sim [v]_\sim$ in $\mathbb{Z}_p$

We can therefore define $[\frac{u}{v}]_\sim := [ut]_\sim$

Examples:

- $[\frac{1}{3}]_\sim = [2]_\sim$ in $\mathbb{Z}_5$
- $[-\frac{124}{11}]_\sim = [29771]_\sim$ in $\mathbb{Z}_{65521}$
- etc.

$\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Let $\frac{u}{v} \in \mathbb{Q}$ and choose $p \in \mathbb{Z}$ such that $\gcd(p, v) = 1$.

Then there exist $s, t \in \mathbb{Z}$ with

$$1 = \gcd(p, v) = sp + tv$$

So $[1]_\sim = [tv]_\sim = [t]_\sim [v]_\sim$ in $\mathbb{Z}_p$

We can therefore define $[\frac{u}{v}]_\sim := [ut]_\sim$

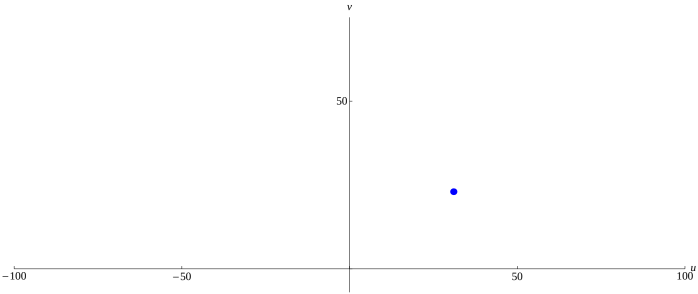
With this extended definition we still have

$$\boxed{\text{mod}(\text{solution}(\text{problem})) = \text{solution}(\text{mod}(\text{problem}))}$$

provided that p is coprime with all the denominators appearing in the problem. (Almost all primes p will work.)

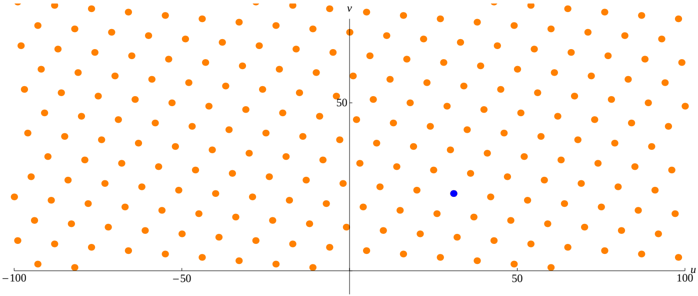
$$\mathbb{Z}_p \longrightarrow \mathbb{Q}$$

Suppose the solution to a problem is $x = \frac{u}{v} \in \mathbb{Q}$. with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$.



$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

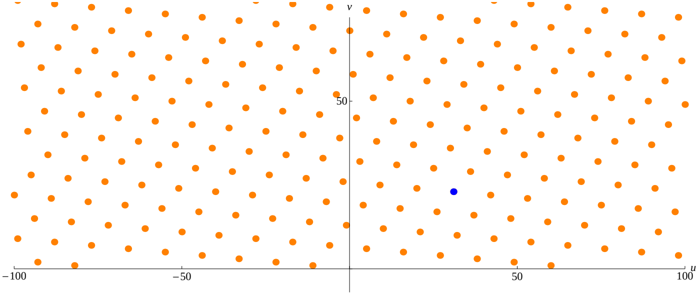
Suppose the solution to a problem is $x = \frac{u}{v} \in \mathbb{Q}$. with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$.



Suppose we know $[x]_\sim \in \mathbb{Z}_p$.

$$\mathbb{Z}_p \longrightarrow \mathbb{Q}$$

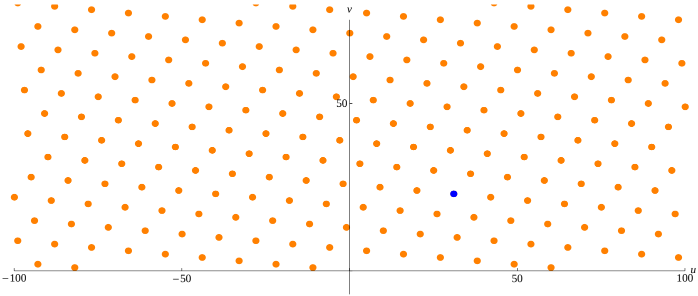
Suppose the solution to a problem is $x = \frac{u}{v} \in \mathbb{Q}$. with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$.



How to choose p such that x can be recovered from its homomorphic image $[x]_\sim \in \mathbb{Z}_p$? 

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

Suppose the solution to a problem is $x = \frac{u}{v} \in \mathbb{Q}$. with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$.



Observation: If $p >> 0$, then x is the element of $[x]_\sim$ where $u^2 + v^2$ is minimal.

$$\mathbb{Z}_p \longrightarrow \mathbb{Q}$$

Two typical scenarios:

$$\mathbb{Z}_p \longrightarrow \mathbb{Q}$$

Two typical scenarios:

- There is an a priori bound M on the final result.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M^2$.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M^2$.
- There is an efficient way to check whether a solution candidate is correct.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

Two typical scenarios:

- There is an a priori bound M on the final result.
  - Then choose $p \geq 2M^2$.
- There is an efficient way to check whether a solution candidate is correct.
  - Then redo the computation with larger and larger choices of p until the correct solution is found.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

g	t	s

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) \\ = 65521s + 29771t.$$

g	t	s
65521	0	1

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771)$$
$$= 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771)$$
$$= 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771)$$
$$= 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1
5855	9	-4
124	-11	5
27	526	-239

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771)$$
$$= 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771)$$
$$= 65521s + 29771t.$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1
5855	9	-4
124	-11	5
27	526	-239
16	-2115	961
11	2641	-1200

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1
5855	9	-4
124	-11	5
27	526	-239
16	-2115	961
11	2641	-1200
5	-4756	2161
1	12153	-5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [\tfrac{29771}{1}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [-\frac{5979}{2}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [\frac{5855}{9}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [-\frac{124}{11}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [\tfrac{27}{526}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1
5855	9	-4
124	-11	5
27	526	-239
16	-2115	961
11	2641	-1200
5	-4756	2161
1	12153	-5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [-\frac{16}{2115}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [\frac{11}{2641}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	-2	1
5855	9	-4
124	-11	5
27	526	-239
16	-2115	961
11	2641	-1200
5	-4756	2161
1	12153	-5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$\begin{aligned} g &= \gcd(65521, 29771) \\ &= 65521s + 29771t. \end{aligned}$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [-\frac{5}{4756}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [\frac{1}{12153}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

Example: Compute g, s, t with

$$g = \gcd(65521, 29771) = 65521s + 29771t.$$

Then in $\mathbb{Z}_{65521}$ we have:

$$[29771]_\sim = [-\frac{124}{11}]_\sim$$

g	t	s
65521	0	1
29771	1	0
5979	−2	1
5855	9	−4
124	−11	5
27	526	−239
16	−2115	961
11	2641	−1200
5	−4756	2161
1	12153	−5522

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

More precisely, it appears exactly in the middle line of the E.E.A.

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

More precisely, it appears exactly in the middle line of the E.E.A.

Hence the name: *Half-GCD-algorithm* (method-oriented)

$\mathbb{Z}_p \longrightarrow \mathbb{Q}$

But how to find for a given $[x]_\sim \in \mathbb{Z}_p$ the pair (u, v) such that $[x]_\sim = [\frac{u}{v}]_\sim$ and $u^2 + v^2$ is minimal?

Answer: It appears as intermediate result in the E.E.A.

More precisely, it appears exactly in the middle line of the E.E.A.

Hence the name: *Half-GCD-algorithm* (method-oriented)

Alternative name: *rational reconstruction* (problem-oriented)

$$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u \rangle$$

Other domains can be handled analogously.

$$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u \rangle$$

Other domains can be handled analogously.

In particular, if $\mathbb{K}$ is a field, then there are variants with

$\mathbb{K}(x)$	playing the role of	$\mathbb{Q}$
$\mathbb{K}[x]$	playing the role of	$\mathbb{Z}$
$\mathbb{K}[x]/\langle u \rangle$	playing the role of	$\mathbb{Z}_p$

$$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u \rangle$$

Other domains can be handled analogously.

Recall: $\mathbb{K}[x]/\langle u \rangle := \mathbb{K}[x]/_{\sim}$ with $a \sim b :\Leftrightarrow u \mid a - b$.

$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u\rangle$

Other domains can be handled analogously.

Recall: $\mathbb{K}[x]/\langle u\rangle := \mathbb{K}[x]/_\sim$ with $a \sim b :\Leftrightarrow u \mid a - b$.

$\mathbb{K}[x]/\langle u\rangle$ is a ring and

$$\mathrm{mod}\colon \mathbb{K}[x] \to \mathbb{K}[x]/\langle u\rangle \qquad p \mapsto [p]_\sim$$

is a ring homomorphism.

$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u \rangle$

Other domains can be handled analogously.

Recall: $\mathbb{K}[x]/\langle u \rangle := \mathbb{K}[x]/_\sim$ with $a \sim b :\Leftrightarrow u \mid a - b$.

$\mathbb{K}[x]/\langle u \rangle$ is a ring and

$$\mathrm{mod}\colon \mathbb{K}[x] \to \mathbb{K}[x]/\langle u \rangle \qquad p \mapsto [p]_\sim$$

is a ring homomorphism.

Special case: if $u = x - c$ for some $c \in \mathbb{K}$, then $\mathbb{K}[x]/\langle u \rangle \cong \mathbb{K}$ and mod corresponds to evaluating of a polynomial at $x = c$.

$\mathbb{K}(x) \longrightarrow \mathbb{K}[x]/\langle u\rangle$

Other domains can be handled analogously.

Recall: $\mathbb{K}[x]/\langle u\rangle := \mathbb{K}[x]/_{\sim}$ with $a \sim b :\Leftrightarrow u \mid a - b$.

$\mathbb{K}[x]/\langle u\rangle$ is a ring and

$$\mathrm{mod}\colon \mathbb{K}[x] \to \mathbb{K}[x]/\langle u\rangle \qquad p \mapsto [p]_{\sim}$$

is a ring homomorphism.

Special case: if $u = x - c$ for some $c \in \mathbb{K}$, then $\mathbb{K}[x]/\langle u\rangle \cong \mathbb{K}$ and mod corresponds to evaluating of a polynomial at $x = c$.

The polynomials $x - c$ play the role of short primes.

$\mathbb{K}[x]/\langle u \rangle \longrightarrow \mathbb{K}(x)$

If we know $[p]_\sim$ in $\mathbb{K}[x]/\langle x - c_i \rangle$ for several $c_i \in \mathbb{K}$, how to we construct $[p]_\sim$ in $\mathbb{K}[x]/\langle (x - c_1)(x - c_2) \cdots (x - c_n) \rangle$?

$\mathbb{K}[x]/\langle u \rangle \longrightarrow \mathbb{K}(x)$

If we know $[p]_\sim$ in $\mathbb{K}[x]/\langle x - c_i \rangle$ for several $c_i \in \mathbb{K}$, how to we construct $[p]_\sim$ in $\mathbb{K}[x]/\langle (x - c_1)(x - c_2) \cdots (x - c_n) \rangle$?

In other words: Given $y_1, \ldots, y_n \in \mathbb{K}$, how to find $p \in \mathbb{K}[x]$ such that $p(c_i) = y_i$ for all i?

$\mathbb{K}[x]/\langle u \rangle \longrightarrow \mathbb{K}(x)$

If we know $[p]_\sim$ in $\mathbb{K}[x]/\langle x - c_i \rangle$ for several $c_i \in \mathbb{K}$, how to we construct $[p]_\sim$ in $\mathbb{K}[x]/\langle (x - c_1)(x - c_2) \cdots (x - c_n) \rangle$?

In other words: Given $y_1, \ldots, y_n \in \mathbb{K}$, how to find $p \in \mathbb{K}[x]$ such that $p(c_i) = y_i$ for all i?

- Polynomial interpolation plays the role of Chinese remaindering.

$\mathbb{K}[x]/\langle u \rangle \longrightarrow \mathbb{K}(x)$

If we know $[p]_\sim$ in $\mathbb{K}[x]/\langle x - c_i \rangle$ for several $c_i \in \mathbb{K}$, how to we construct $[p]_\sim$ in $\mathbb{K}[x]/\langle (x - c_1)(x - c_2) \cdots (x - c_n) \rangle$?

In other words: Given $y_1, \ldots, y_n \in \mathbb{K}$, how to find $p \in \mathbb{K}[x]$ such that $p(c_i) = y_i$ for all i?

- Polynomial interpolation plays the role of Chinese remaindering.

And since the Euclidean Algorithm also works for polynomials. . .

$\mathbb{K}[x]/\langle u \rangle \longrightarrow \mathbb{K}(x)$

If we know $[p]_\sim$ in $\mathbb{K}[x]/\langle x - c_i \rangle$ for several $c_i \in \mathbb{K}$, how to we construct $[p]_\sim$ in $\mathbb{K}[x]/\langle (x - c_1)(x - c_2) \cdots (x - c_n) \rangle$?

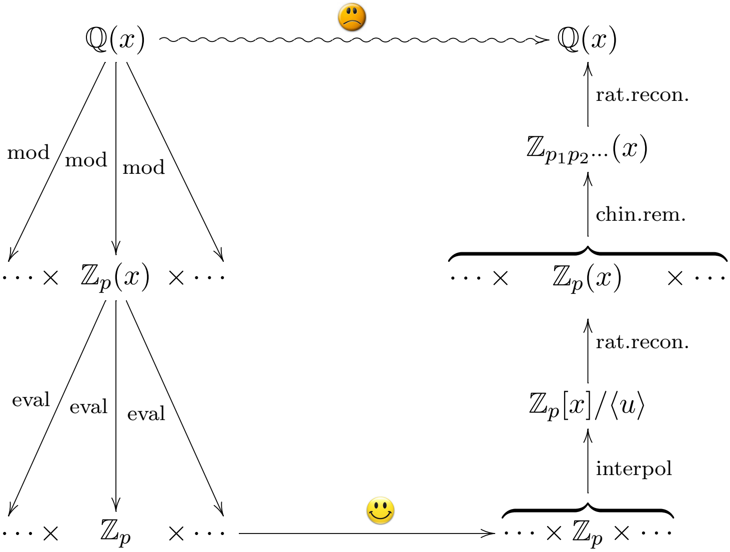
In other words: Given $y_1, \ldots, y_n \in \mathbb{K}$, how to find $p \in \mathbb{K}[x]$ such that $p(c_i) = y_i$ for all i?

- Polynomial interpolation plays the role of Chinese remaindering.

And since the Euclidean Algorithm also works for polynomials...

- ...we can also do rational (function) reconstruction

Summary



$\mathbb{Q}(x)$
$\mathbb{Q}(x)$
mod
mod
mod
rat.recon.
$\mathbb{Z}_{p_1 p_2 \cdots}(x)$
chin.rem.
$\cdots \times \; \mathbb{Z}_p(x) \; \times \cdots$
$\cdots \times \; \mathbb{Z}_p(x) \; \times \cdots$
eval
eval
eval
rat.recon.
$\mathbb{Z}_p[x]/\langle u \rangle$
interpol
$\cdots \times \; \mathbb{Z}_p \; \times \cdots$
$\cdots \times \mathbb{Z}_p \times \cdots$