

1. Caesar's cipher

$$x \equiv (y - k) \pmod{26}$$

Cipher: EXLBOKUKLVO

Shift: 10

Decoded msg: UNBREAKABLE

2. Modular calculation for double power

Calculate $2^{2024} \pmod{13}$ using Fermat's little theorem (key insight: when you're calculating powers mod some no; the results start repeating after a while)

$$2^{2024} \pmod{13} = 2^{2024} \pmod{13}$$

We only need to find remainder of $2^{2024} \pmod{3}$ but it is HUGE!
So, we find cycle of powers of 2 mod 3

$$2^1 \equiv 2$$

$$2^2 \equiv 1$$

$$2^3 \equiv 2$$

$$2^4 \equiv 1$$

$$2^5 \equiv 2$$

:

The cycle repeats after every 2 steps
the remainder of $2^{2024} \pmod{3}$ is 1 (since 2024 is even).

So, remainder of $2^{2024} \pmod{3} = 1$

$$2^{2024} \pmod{3} = 9^1 \equiv 9$$

SOLUTION

$$\begin{aligned} 2^{2024} \pmod{13} &= 9^{2024} \pmod{13} \\ &= 9^{2020+4} \pmod{13} \\ &= (9^4)^{2020} \cdot 9^4 \pmod{13} \\ &\stackrel{\text{NOTE: } (a^m)^n = a^{mn}}{=} 1^{2020} \cdot 9^4 \pmod{13} \\ &= 9^4 \pmod{13} \\ &= 9^2 \pmod{13} \\ &= 81 \pmod{13} \\ &= 9 \end{aligned}$$

3. Divisibility by 9

ring \mathbb{Z}_{10}

Rule?

non-negative integer = sum of its decimal digits

9

SOLUTION

Checking divisibility by 9 is based on the sum of

The rule for checking if a number is divisible by 9 is to sum the digits of the number. Specifically, a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Why does this work?
Consider an arbitrary number ABC. This ABC can be expressed as:

$$100A + 10B + C$$

Rewriting this expression using the fact that $10 \equiv 1 \pmod{9}$:

$$100A + 10B + C \equiv (99+1)A + (9+1)B + C \equiv 99A + A + 9B + B + C \equiv A + B + C \pmod{9}$$

4. How to define functions well?

$f: \mathbb{R} \rightarrow \mathbb{R}$ \nexists \Rightarrow not well defined

$$y^2 = x$$

ring $(\mathbb{Z}_n, +, \cdot)$ $x \in \mathbb{Z}, y \in \mathbb{Z}$

↑ suppose we have 2 cosets in \mathbb{Z}_n i.e. x, y . We define their sum as the coset $[x+y]$

↑ Now, suppose we choose diffⁿ representatives x' and y' s.t. $x' \equiv x \pmod{n}$ and $y' \equiv y \pmod{n}$

↑ we want to show that the coset contains $[x'+y'] = [x+y]$

↑ since $x' \equiv x \pmod{n}$
 $y' \equiv y \pmod{n}$

$$[x'+y'] \equiv [x+y] \pmod{n}$$

it follows $[x'+y'] \equiv [x+y]$ belong to the same coset.

Hence, $[x'+y'] \equiv [x+y]$

2. Fermat's Little theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\begin{aligned} 2^{2024} &\pmod{12} \\ 9^{2024} &\equiv 9^2 - 12 \end{aligned}$$

$$12 \pmod{13}$$

3. Divisibility by 9

$$10^k \equiv 1 \pmod{9}$$

$$\sum_{k=0}^{n-1} 10^k a_k = \sum_{k=0}^{n-1} a_k \pmod{9}$$

$\{0, 1, 2, \dots, 9\}$

Every number with n digits can be written in the form:

$$\sum_{k=0}^{n-1} 10^k a_k$$

for $a_k \in \{0, 1, 2, \dots, 9\}$

for all $k = 0, 1, \dots, n-1$

$$a^{n-1} \neq 0$$

4. Functions

$$[x]_n + [y]_n := [x+y]_n$$

x' - x divided by $n \Rightarrow \exists k \in \mathbb{Z}$

y' - y divided by $n \Rightarrow \exists l \in \mathbb{Z}$

$$x' - x = kn \Rightarrow x' = x + kn$$

$$y' - y = ln \Rightarrow y' = y + ln$$

$$(x+y') - (x+y) = x+kn+y+ln - x-y$$

$$= kn + ln$$

$(x+y') - (x+y)$ is divided by n

$$\Leftrightarrow x+y' \in [x+y]$$

Show that \cdot is well-defined on \mathbb{Z}_n for some $n \in \mathbb{N}$

Let $x, y \in \mathbb{Z}$. we take diffⁿ representatives $x', y' \in \mathbb{Z}$ with $x' \in [x]$ & $y' \in [y]$

To Prove: $x' \cdot y' \in [x \cdot y]_n$

$$x' \in [x]_n \text{ and } y' \in [y]_n$$

$x' \in [x]_n$ and $y' \in [y]_n$, we get n divides $x' - x$ and $y' - y$

By definition of \mathbb{Z}_{7n} .
Therefore there exists $k, l \in \mathbb{Z}$ such that
 $x' - x = kn$, $y' - y = ln$

this yields
 $x' = x + kn$, $y' = y + ln$ - ①

we consider

$$\begin{aligned}x' \cdot y' - xy &= (x + kn)(y + ln) - xy \\&= xy + xln + kny + kln^2 - xy \\&= (n)(xk + ly + kln)\end{aligned}$$

therefore x divides $x' \cdot y' - xy$ and hence we proved that \cdot on \mathbb{Z}_5 is well defined.

1) Caesar strikes back

The function

$$f(x) = ax + b \pmod{26}$$

is a linear function over the finite field of integers modulo 26 i.e. \mathbb{Z}_{26}

For this function to be bijective, it must be invertible. This means,
the inverse function $f^{-1}(x)$ such that,

$$f(f^{-1}(x)) = f^{-1}(f(x)) = x$$

for $x \in \mathbb{Z}_{26}$.

The inverse function of $f(x)$ is

$$f^{-1}(x) = a^{-1}(x - b) \pmod{26}$$

where a^{-1} is the multiplicative inverse of a in \mathbb{Z}_{26} .

The Multiplicative inverse of a exists if and only if a and 26 are coprime i.e. $\gcd(a, 26) = 1$

This is because only then we can find an integer a^{-1} such that

$$(a * a^{-1}) \pmod{26} = 1$$

The possible values of a that are coprime with 26 are:

$$a = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

The value of b can be any integer in \mathbb{Z}_{26} i.e. 0 to 25 because adding does not affect the bijectiveness of the function.

So, all pairs (a, b) where $a = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$$b = \{0, 1, 2, 3, \dots, 24, 25\}$$

will give a bijective function.

2) Asterix never gives up.

Cipher = "UQPFXFUBSUQPFU"

$$f(x) = ax + b$$

Let's call the repeating triple in the cipher is xyz. We can form a set of equations assuming x, y, z represent t, h, e:

$$a*t + b \equiv x \pmod{26}$$

$$a*h + b \equiv y \pmod{26}$$

$$a*e + b \equiv z \pmod{26}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Encoding English capital letters using integers from \mathbb{Z}_{26} .

$$19a + b \equiv 20 \pmod{26} \quad \text{①}$$

$$7a + b \equiv 16 \pmod{26} \quad \text{②}$$

$$4a + b \equiv 15 \pmod{26} \quad \text{③}$$

Using ① - ②

$$(19a + b) - (7a + b) \equiv (20 - 16) \pmod{26}$$

$$12a \equiv 4 \pmod{26}$$

$$(\div 4) \quad 3a \equiv 1 \pmod{26}$$

Using Euclid's algorithm,

$$26 = 3(8) + 2$$

$$3 = 2(1) + 1$$

$$\text{Backward substitution} \quad 1 = 3 - 2(1)$$

$$1 = 3 - (26 - 3(8))$$

$$1 = 3(9) - 26$$

$$S_0, \boxed{a = 9}$$

sub $a = 9$ in ①

$$19a + b \equiv 20 \pmod{26}$$

$$19(9) + b \equiv 20 \pmod{26}$$

$$171 + b \equiv 20 \pmod{26}$$

$$15 + b \equiv 20 \pmod{26} \quad (\text{because } 171 \pmod{26} = 15)$$

(-15)

$$\boxed{b = 5}$$

	U	Q	P	X	F	U	B	S	U	Q	P	J	F	U
X	20	16	15	23	5	20	1	18	20	16	15	9	5	20
$x - 5$	15	11	10	18	0	15	-4	13	15	11	10	4	0	15
$3(x - 5)$	45	33	30	54	0	45	-12	39	45	33	30	12	0	45
$\pmod{26}$	19	7	4	2	0	19	14	13	19	7	4	12	0	19
	T	H	E	C	A	T	O	N	T	H	E	M	A	T

$$a^{-1} \pmod{26} = 3$$

3) Unique negative

$$a + b = a + c = 0$$

additive inverse = $-a$

$$a + b = a + c$$

adding additive inverse

$$a + b - a = a + c - a$$

$$b = c = 0$$

4) Groups

$$(G, *) \quad * : G \times G \rightarrow G$$

G has an element e satisfying $a * e = e * a = a$

$\forall a \in G$

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$$

$$\forall a \in G \quad \exists a, b \in G \quad a * b = e$$

EXERCISE CLASS SOLUTION

1) $f(x) = ax + b \quad a, b \in \mathbb{Z}_{26}$

$$a = 2$$

$$x_1 = 0 \quad f(x_1) = b$$

$$x_2 = 2 \quad f(x_2) = 2(13) + b$$

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

$$f(x) = ax + b, a \text{ invertible}$$

want to show f is bijective

- injectivity

$$x', x'' \in \mathbb{Z}_{26}$$

$$f(x') = f(x'')$$

$$ax' + b = ax'' + b$$

$$ax' = ax''$$

$$a^{-1}(ax') = a^{-1}(ax'')$$

$$\Rightarrow x' = x''$$

- Surjectivity is a result of the input space \mathbb{Z}_{26} having the same no. of elements as the output space \mathbb{Z}_{26}

Hence, Bijectivity has been shown.

$$2) U Q P X F U B S U Q P J F U$$

$$f(x) = ax + b$$

$$b \in \mathbb{Z}_{26}^*$$

$$a \in \mathbb{Z}_{26}, a \text{ invertible}$$

$$19T \rightarrow U_{20}$$

$$7H \rightarrow Q_{16}$$

$$4E \rightarrow P_{15}$$

$$19a + b = 20$$

$$7a + b = 16$$

$$4a + b = 15$$

$$7a + b - 4a - b = 1$$

$$3a = 1$$

$$\Rightarrow a = 9$$

$$9 \cdot 4 + b = 15$$

$$b = 15 - 36 = -21 = 5$$

$$b = 5$$

$$3) a \in \mathbb{R} \text{ show that negative of } a \text{ is unique}$$

+ properties

→ Zero element $0 : \forall a \in R \quad 0+a=a+0=a$

→ Commutativity $\forall a, b \in R \quad a+b=b+a$

→ Additive inverse $\forall a \in R \exists b \in R \quad a+b=0$

→ Associativity $\forall a, b, c \in R \quad a+(b+c)=(a+b)+c$

We take $b, c \in R \quad a+b=0, a+c=0$

using zero element, $c = c+0$

using $a+b=0$, $c = c+(a+b)$

using Associativity, $c = (c+a)+b$

using commutativity, $c = (a+c)+b$

using $a+c=0$ $c = 0+b$

using zero element, $c = b$

4) $(G, *)$

closure

$$*: G \times G \rightarrow G$$

neutral element $e : a * e = e * a = a \quad \forall a \in G$

Associative $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$

inverse $\forall a \in G \exists b \in G \quad a * b = e$

If additional $x \quad \forall a, b \in G \quad a * b = b * a$ (commutative), then G is called Abelian

i) Show that neutral element is unique

We take neutral elements $e, e' \in G$

i.e. $e * a = a = a * e \quad \forall a \in G$

$$\begin{array}{l} e' * a = a = a * e' \\ \downarrow \qquad \downarrow \\ e = e * e' = e' \end{array}$$

ii) Show that if $b = a^{-1}$ i.e. $a * b = e$, then also $b * a = e$

$$a * b = e \Rightarrow (a * b) * a' = e * a' = a'$$

①

$$a * (b * a')$$

a

$$b * a' = e - \textcircled{2}$$

$$b * a \stackrel{(N)}{=} (b * a) * e \stackrel{\textcircled{2}}{=} (b * a) * (b * a') \stackrel{(A)}{=} b * (a * (b * a')) \stackrel{(A)}{=} b * ((a * b) * a')$$

$$\textcircled{1} b * (e * a')$$

$$(N) b * a$$

$$\textcircled{2} e$$

Show that inverse is unique $a * b = e - \textcircled{4}$

We assume that b, c exist with $a * b = a * c = e \Rightarrow c * a = e - \textcircled{3}$

$$b \stackrel{(N)}{=} e * b \stackrel{\textcircled{3}}{=} (c * a) * b \stackrel{(A)}{=} c * (a * b) \stackrel{\textcircled{4}}{=} c * e \stackrel{(N)}{=} c$$

Exercise sheet 3

I) f encryption fct $f: X \rightarrow Y$

g decryption fct $g: Y \rightarrow X$

$$\forall x \in X : g(f(x)) = x$$

(i) Is f necessarily injective?

$$\text{Suppose } x', x'' : f(x') = f(x'')$$

$$\Rightarrow x' = g(f(x')) = g(f(x'')) = x''$$

This means that f has to be injective

(ii) Is f necessarily surjective?

$$f: \{0\} \rightarrow \{0, 1\}, g: \{0, 1\} \rightarrow \{0\}$$

$$\text{Assume } f(0) = 0 \quad \underbrace{g(0) = g(1) = 0}_{\text{This contradicts injectivity of } g}$$

$$g(f(0)) = g(0) = 0$$

f is not necessarily surjective

(iii)



(iv) Is g necessarily surjective?

If g were not surjective, then there is $x \in X$ s.t.

$\forall y \in Y : g(y) \neq x$

$$\underbrace{g(f(x))}_{\in Y} = x$$

g has to be surjective

2. Structure of invertible elements in rings

$(R, +, \cdot)$ is an abelian group wrt \cdot .

$$G = R^\times = \{ n \in R \mid \text{there exists an inverse} \}$$
$$(G, \cdot)$$

Take $a, b \in G$. There exist inverses $a^{-1}, b^{-1} \in R$

$$(b^{-1}a^{-1})(ab) \stackrel{?}{=} b^{-1}(a^{-1}(ab)) = b^{-1} \cdot b = 1$$

We have shown by this that products of invertible elements are invertible, hence $\cdot : G \times G \rightarrow G$ holds.

We need to show that (G, \cdot) is Abelian group.

Commutativity:

It is inherited because of commutativity of (R, \cdot)

Invertibility:

$a \in G$ want to show that $a^{-1} \in G$

$$a \cdot a^{-1} = 1 \Rightarrow a \text{ is the inverse of } a^{-1}$$

$\Rightarrow a$ is invertible

$$\Rightarrow a^{-1} \in G$$

Neutral element

$1 \in G$ as $1 \cdot 1 = 1$ hence 1 is invertible

Associativity

Property is inherited by associativity of (R, \cdot)

3. Power functions in finite groups.

$\lim_{p \rightarrow \infty} a^p \equiv 1 \pmod{p}$

we want to show $a^h = 1$ in (G, \cdot) with $|G| = h$
for all $a \in G$ Abelian group

Take $f(x) = ax$

we show that f is injective

$$ax_1 = f(x_1) = f(x_2) = ax_2$$

$$f: G \rightarrow G$$

$$\xrightarrow{\text{I}} a^{-1}(ax_1) = a^{-1}(ax_2) = x_2$$

$\begin{matrix} \text{||} \\ x_1 \end{matrix}$

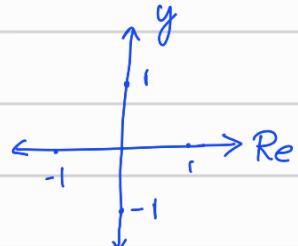
Because $|G| = h$ is finite

injectivity is the same as bijectivity

$$\prod_{x \in G} x = \prod_{x \in G} (ax) \xrightarrow{\text{Abelian}} a^h \prod_{x \in G} x$$

$\underbrace{x \in G}_{\text{invertible}}$

$$\left[\prod_{x \in G} x = \prod_{x \in G} f(x) \right]$$



$$\Rightarrow i = a^h$$

$$f(x) = ix$$

$$1 \quad f(1) = i$$

$$i \quad f(i) = -1$$

$$-1 \quad f(-1) = -i$$

$$-i \quad f(-i) = 1$$

4. Beancrypt

$a \in \mathbb{Z}_p \setminus \{0\}$, $b \in \mathbb{Z}_p$, $e \in \mathbb{N}$, $\gcd(e, p-1) = 1$

encryption $f(x) = ax^e + b$

decryption $g(x) = (ux + v)^d$

(a, b, e, p) public key

(u, v, d, p) private key

$$x = g(f(x)) = (u(ax^e + b) + v)^d$$
$$x^e = (u(ax^e + b) + v)^{ed}$$

Extended Euclidean Algorithm

$$\exists d, \beta \in \mathbb{Z}: \alpha e + \beta(p-1) = \gcd(e, p-1) = 1$$

$$\stackrel{\text{mod } p-1}{\Rightarrow} \alpha e \equiv 1 \pmod{p-1} \Rightarrow d = \alpha$$

By EEA we can compute d in polynomial time

$$x^e = u \alpha^e + v b + v$$

$$\Rightarrow 1 = u \alpha \quad \Rightarrow u = \underbrace{\alpha^{-1}}$$

$$0 = u b + v \quad \Rightarrow v = -u b \quad \Rightarrow v = -\alpha^{-1} b$$

$$x^{ed} = x \quad \text{corollary 8}$$

5. Caesar's new idea

$$f(x) = ax^e + b, \quad e \in \mathbb{N}$$

$$x^1, x^2, x^3, x^4, \dots$$

$$f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

n inputs

$$|\{f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n\}| = n^n$$

There is only finite number of functions mapping from \mathbb{Z}_n to \mathbb{Z}_n .

But the above sequence contains infinitely many elements.

Hence, there exists some $m \in \mathbb{N}, t \in \mathbb{N}$

$$x^m = x^{m+t}$$

$$x^{m+1} = x^{m+1+t}$$

$$\forall i \geq m: x^i = x^{i+t}$$

Exercise sheet 4

1) Caesar variation

$$y_i := a(x_1 + \dots + x_i) + b, \quad i = 1, \dots, n$$

$\Delta(a, b)$ choices

a should be invertible

$$ax_1 + b = ax_1'' + b \quad \text{encryption fn is}$$

\hookrightarrow case 1: a invertible \Rightarrow injective \Rightarrow is also bijective

\hookrightarrow case 2: a is not invertible \Rightarrow not injective

$$a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}$$

△ decryption

$$y_1 = ax_1 + b \Rightarrow x_1 = a^{-1}(y_1 - b)$$

$$y_2 = a(x_1 + x_2) + b$$

$$y_3 = a(x_1 + x_2 + x_3) + b$$

:

$$y_3 - y_2 = ax_3 \Rightarrow x_3 = a^{-1}(y_3 - y_2)$$

$$\boxed{x_i = a^{-1}(y_i - y_{i-1}) \quad \forall i=2, \dots, n}$$

△ determine a

$$T \quad 19a = y_{100} - y_9$$

$$H \quad 7a = y_{101} - y_{100} \rightarrow a = [7]^{-1}(y_{101} - y_{100})$$

$$E \quad 4a = y_{102} - y_{101} \quad a = 15(y_{101} - y_{100})$$

△ determine b

$$S := x_1 + \dots + x_{99}$$

$$y_{100} = a(\underbrace{x_1 + \dots + x_{99}}_S + x_{100}) + b$$

$$y_{100} = aS + b + a \cdot x_{100}$$

$$y_{101} = aS + b + a \cdot x_{100} + a \cdot x_{101}$$

$$y_{102} = aS + b + a \cdot x_{100} + a \cdot x_{101} + a \cdot x_{102}$$

we cannot determine x_1 and b

2) Fast exponentiation

let $e \geq 2^k$ be given

prove that x^e cannot be computed using just x and e with less than k multiplications

△ Induction

consider $k=0$, $e \geq 2^0 = 1$

that is trivial.

You always need at least n multiplications.

new always new want you manipulations.

△ Induction step

Assume the property already holds for some $k \in \mathbb{N}$.

Now show that it holds for $k+1$ too.

$$\Delta e \geq 2^{k+1} \quad x^e = \underbrace{x^a \cdot x^b}_{e=a+b}$$

$$e = a + b$$

* what if $a, b > 2^k$

$$a+b < 2^{k+k} = 2^{k+1}$$

$$(*) \Rightarrow a \geq 2^k \quad ab \geq 2^{2k}$$

w.l.o.g. = without loss of generality

w.l.o.g. assume $a \geq 2^k$

$$x^e = \underbrace{x^a \cdot x^b}_{e=a+b}$$

by assumption x^a cannot be computed in less than k steps.

$\Rightarrow x^e$ needs $s \geq k+1$ multiplications.

3) EEA & CRT

what $[z]_{10403}$ fulfills

$$[z]_{101} = [20]_{101}, [z]_{103} = [15]_{103} ?$$

$$\begin{array}{l|l} 103 = 101(1) + 2 & 1 = 101 - 2(50) \\ 101 = 2(50) + 1 & 1 = 101 - 50(103 - 101) \\ & = 51 \times 101 - 50 \times 103 \end{array}$$

$$\Rightarrow 5151 \equiv 0 \pmod{101} \quad -5150 \equiv 1 \pmod{101}$$

$$5151 \equiv 1 \pmod{103} \quad -5150 \equiv 0 \pmod{103}$$

$$\Rightarrow 20(-5150) + 15(5151) = 5474$$

4) quadratic equations & modular arithmetic

which $x \in \mathbb{Z}_{217}$ fulfills $x^2 + x + 1 \equiv 0 \pmod{217}$

$$217 = 7 \cdot 31$$

$$\mathbb{Z}_7 \quad 0^2 + 0 + 1 = 1$$

$$1^2 + 1 + 1 = 3 \times$$

$$2^2 + 2 + 1 = 7 \bmod 7 = 0$$

$$3^2 + 3 + 1 = 13 \bmod 7 = 6 \times$$

$$4^2 + 4 + 1 = 21 \bmod 7 = 0$$

$$5^2 + 5 + 1 = 31 \times$$

$$6^2 + 6 + 1 = 43 \times$$

$$\Rightarrow x = 2, x = 4$$

$$\mathbb{Z}_{31} \quad 5^2 + 5 + 1 = 31 \bmod 31 = 0$$

$$p_1 = 5$$

$$x^2 + ax + b = (x - p_1)(x - p_2)$$

$$= x^2 + (-p_1 - p_2)x + p_1 p_2$$

$$\Rightarrow -5 - p_2 = 1 \Rightarrow p_2 = -6 \equiv 25 \bmod 31$$

$$\mathbb{Z}_5 \quad 2$$

$$\mathbb{Z}_{31} \quad 5$$

$$4$$

$$25$$

$$31 = 7(4) + 3$$

$$1 = 7 - 3(2)$$

$$7 = 3(2) + 1$$

$$= 7 - 2(31 - 7(4))$$

$$= 7 - 2(31) + 8(7)$$

$$1 = 9(7) - 2(31)$$

$$63 \equiv 0 \bmod 7$$

$$-62 \equiv 1 \bmod 7$$

$$63 \equiv 1 \bmod 31$$

$$-62 \equiv 0 \bmod 31$$

$$2 \cdot (-62) + 5 \cdot (63) \equiv 191 \quad \mathbb{Z}_1, \mathbb{Z}_2$$

$$4 \cdot (-62) + 5 \cdot (63) \equiv 67 \quad [a]_{z_1, z_2} = ([a]_{z_1}, [a]_{z_2})$$

$$2 \cdot (-62) + 25 \cdot (63) \equiv 149$$

$$4 \cdot (-62) + 25 \cdot (63) \equiv 25$$

5) CRT

$$n = n_1 n_2 \quad n, n_1, n_2 \in \mathbb{N}$$

there is a bijection

$$(1) f: \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

if and only if (2) $\gcd(n_1, n_2) = 1$

Lecture says (2) \Rightarrow (1)

		\mathbb{Z}_6					
		0	1	2	3	4	5
\mathbb{Z}_2	0	0, 6		2, 8		4, 10	
	1		1, 7		3, 9		5, 11

Non-bijective

$$\gcd(n_1, n_2) = g > 1$$

$$f([0]_n) = ([0]_{n_1}, [0]_{n_2})$$

$$n = n_1 n_2 \quad g | n_1, g | n_2 \quad \text{X}$$

$$f\left(\left[\frac{n}{g}\right]_n\right) = \left(\left[\frac{n}{g}\right]_{n_1}, \left[\frac{n}{g}\right]_{n_2}\right) = \left(\left[n_1 \cdot \frac{n_2}{g}\right]_{n_1}, \left[n_2 \cdot \frac{n_1}{g}\right]_{n_2}\right)$$

$$= ([0]_{n_1}, [0]_{n_2})$$

$\Rightarrow f$ is not bijective

Exercise sheet 5

1. Breaking \mathbb{Z}_n into more than two pieces (Pls also prove homomorphism?)

$$n \in \mathbb{N}, n = n_1 \dots n_k, n_i \geq 2, \gcd(n_i, n_j) = 1 \text{ for } i \neq j$$

Show there is a bijection between \mathbb{Z}_n and $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \dots \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3} \dots \mathbb{Z}_{n_k} \cong \dots \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$$

$$f([u]_n) = ([u]_{n_1}, [u]_{n_2}, \dots, [u]_{n_k})$$

We show bijectivity by showing injectivity

$$f([u]_n) = f([v]_n) \Leftrightarrow [u]_{n_i} = [v]_{n_i} \quad \forall i = 1, \dots, k$$

$$\Leftrightarrow [u - v]_{n_i} = [0]_{n_i} \quad \forall i \Leftrightarrow n_i | (u - v) \quad \forall i$$

$$\Downarrow \gcd(u_i, v_i) = 1, i \neq j$$

$$n | (u - v) \Leftrightarrow [u]_n = [v]_n$$

\Rightarrow injectivity

Surjectivity

$$|\mathbb{Z}_n| = n$$

$$|\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}| = n_1 \dots n_k = n$$

2. RSA example that reveals a lot of messages.

$$p=11, q=101, e=21$$

- $d = ?$

$$n = p \cdot q = 11 \cdot 101 = 1111$$

$$\phi(n) = (p-1) \cdot (q-1) = 10 \cdot 100 = 1000$$

find d

$$\Rightarrow 21 \cdot d \equiv 1 \pmod{\phi(n)}$$

$$d = 21^{-1} \pmod{1000}$$

$$= 381$$

- $\mathbb{Z}_{1111} \rightarrow \mathbb{Z}_{11} \times \mathbb{Z}_{101}$

$$x = [z]_{1111}$$

$$\text{EEA}(11, 101)$$

$$(46) \cdot 11 + (-5) \cdot 101 = 1$$

$$506 = 46 \cdot 11 \equiv 1 \pmod{101}$$

$$46 \cdot 11 \equiv 0 \pmod{11}$$

$$-505 \equiv 0 \pmod{101}$$

$$-505 \equiv 1 \pmod{11}$$

$$[z]_{1111} \xrightarrow{} [z]_{11} \xrightarrow{} \dots \xrightarrow{} [z]_{1111}^d$$

$$(*) ([z]_{11}, [z]_{101}) \rightarrow [-505z_1 + 506z_2]_{1111}$$

$$f([z]_{1111}) = ([z]_{11}, [z]_{101})$$

$$[z]_{11}^{381} = z^{381} \equiv z^1 \pmod{11} \quad \text{because } 381 = 38 \cdot 10 + 1 \quad (10 = p-1)$$

$$[z]_{101}^{381} = [z]_{101}^{81}$$

$$z^{81} = z(((z(z^2)^2)^2)^2)^2$$

$$x \xrightarrow{} x^e$$

$$\text{what if } x^e = x?$$

3. prime numbers

$$\ln(a \cdot b) = \ln a + \ln b$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$$

$$\pi(n) \approx \frac{\ln n}{n}$$

$$\frac{\pi(n)}{n \ln n} \rightarrow 1 \text{ for } n \rightarrow \infty$$

$$\pi(n) = \frac{n}{\ln n} \alpha(n), \quad \alpha(n) \rightarrow 1 \text{ for } n \rightarrow \infty$$

$$\ln(a^k) = k \ln(a)$$

$$10^k - 10^{k-1} = 10^{k-1} (10 - 1)$$

$$\begin{aligned} \frac{\pi(10^k) - \pi(10^{k-1})}{10^k - 10^{k-1}} &= \frac{\frac{10^k}{\ln(10^k)} \alpha(10^k) - \frac{10^{k-1}}{\ln(10^{k-1})} \alpha(10^{k-1})}{10^k - 10^{k-1}} \\ &= \frac{\frac{10}{\ln(10^k)} \alpha(10^k) - \frac{1}{\ln(10^{k-1})} \alpha(10^{k-1})}{10^k - 10^{k-1}} \\ &= \frac{\frac{10}{k \ln 10} \alpha(10^k) - \frac{1}{(k-1) \ln 10} \alpha(10^{k-1})}{10^k - 10^{k-1}} \\ &= \frac{1}{k} \left[\underbrace{\frac{10}{\ln 10} \alpha(10^k)}_1 - \underbrace{\frac{1}{\ln 10} \cdot \frac{k}{k-1} \alpha(10^{k-1})}_1 \right] \\ &\approx \frac{1}{k \ln 10} \end{aligned}$$

4. variant on Caesar

$$d(e(x)) = x$$

$$S_1 S_2 | S_3 S_4 | S_5 S_6 | \dots$$

$$T(x, y) = (ax + by, cx + dy)$$

$$T(S_1, S_2) T(S_3, S_4) T(S_5, S_6)$$

$$\begin{aligned} ad - bc &\\ T(x, y) &= \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

$\det() = ad - bc$ should be invertible in \mathbb{Z}_{26}

$$\frac{1}{ad - bc} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\text{when } ad - bc = 4, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\text{also } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 13 \end{pmatrix} = \begin{pmatrix} 4 \cdot 13 + 12 \cdot 13 \\ 11 \cdot 13 + 7 \cdot 13 \end{pmatrix} = \begin{pmatrix} 8 \cdot 26 \\ 9 \cdot 26 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

If $a=4, b=12, c=11, d=7$

$$ad - bc = 28 - 14 \cdot 2 = -104 = -4 \cdot 26 \Rightarrow \text{not invertible in } \mathbb{Z}_{26}$$

If $a=7, b=5, c=8, d=15$

$$ad - bc = 7 \cdot 15 - 5 \cdot 8 = 105 - 40 = 65 \Rightarrow \text{not invertible}$$

choice 3

$$ad - bc = 3 \cdot 19 - 17 \cdot 6 = -45 \equiv 7 \Rightarrow \text{invertible}$$

Exercise sheet 6

1. Rings and non-rings

(i) $\{\text{False, True}\}$ XOR $\hat{+}$ and $\hat{\cdot}$

$f: 0 \rightarrow F$	$(\mathbb{Z}_2, +, \cdot)$	$+ \mid \begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}$	$\cdot \mid \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}$
$1 \rightarrow T$		$1 \mid \begin{array}{cc} 1 & 0 \\ 1 & 0 \end{array}$	

XOR	F	T	AND	F	T
F	F	T	F	F	F
T	T	F	T	F	T



is an isomorphism between $(\mathbb{Z}_2, +, \cdot)$ and $(\{\text{F, T}\}, \text{XOR, AND})$ and $(\mathbb{Z}_2, +, \cdot)$ is a unitary commutative ring $\Rightarrow (\{\text{F, T}\}, \text{XOR, AND})$ is also a unitary commutative ring.

(ii) $\{\text{False, True}\}$ OR

OR	F	T	$a \in \{\text{F, T}\}$
F	F	T	$F \text{ on } a = a \Rightarrow F \text{ is neutral}$
T	T	T	$T \text{ on } a = T \Rightarrow T \text{ has no inverse w.r.t. on}$

(iii) $(\mathbb{N}_0, +, \cdot)$ 0 is neutral

Consider $1 \in \mathbb{N}_0$

$\forall n \in \mathbb{N}_0 : 1+n \neq 0 \Rightarrow$ no inverse exists for 1.

(IV) $(2\mathbb{Z}, +, \cdot)$

Assume there is a neutral element $\mathbb{Z} \in 2\mathbb{Z}$, then we should have

$$2\mathbb{Z} = \{ \dots -6, -4, -2, 0, 2, 4, 6, \dots \}$$

$$2\mathbb{Z} = \mathbb{Z} \Rightarrow \underbrace{4k}_{\in 2\mathbb{Z}} = \underbrace{\mathbb{Z}}_{\in 2\mathbb{Z}}$$

Hence, there is no neutral element.

(V) $(\{f: \mathbb{N} \rightarrow \mathbb{Z}\}, +, \circ)$

Associativity $(f+g)+h \stackrel{?}{=} f+(g+h)$

$$\Leftrightarrow \forall n \in \mathbb{N} \quad (f(n) + g(n)) + h(n) = f(n) + (g(n) + h(n)) \quad \checkmark \text{ because } \mathbb{Z} \text{ is associative}$$

Neutral $e: n \mapsto 0$

$$f(n) + e(n) = f(n) \Rightarrow e \text{ is neutral}$$

Inverse $f: n \mapsto -f(n)$

$$f(n) + (-f(n)) = 0 \Rightarrow \text{inverse exists}$$

Commutativity $f+g = g+f$

$$\Rightarrow \forall n \in \mathbb{N}: f(n) + g(n) = g(n) + f(n) \quad \checkmark \text{ because } f(n), g(n) \in \mathbb{Z}, \\ \mathbb{Z} \text{ is associative}$$

Associativity and commutativity for \cdot are done completely analogous.

Neutral for multiplication: $i(n) = 1 \quad \forall n \in \mathbb{N}$

$$f: -f \Leftrightarrow \forall n \in \mathbb{N} \quad \underbrace{f(n) \cdot i(n)}_1 = f(n) \Rightarrow \text{u or}$$

2. Zero divisors

$$(a, b, c) \neq 0$$

(i) if $a^2 = 0$, is a a zero divisor?

$$a^2 = 0 = a \cdot a$$

Yes

(ii) $a^3 = 0$

$$\Rightarrow a^2 \cdot a \quad \text{case 1: } a^2 \neq 0 \Rightarrow a \text{ is a zero divisor (ZD)}$$

$$\text{case 2: } a^2 = 0 \Rightarrow a \cdot a = 0 \Rightarrow a \text{ is ZD}$$

(iii) $ab=0$

$\Rightarrow a$ is ZD

(iv) $abc=0$

a is not necessarily ZD because $abc=0$ is possible.

(v) $abc=0$ if any a,b,c are ZD's

case $ab=0 \Rightarrow a$ is ZD

case $ab \neq 0 \Rightarrow c$ is ZD

(vi) If a is ZD, $ab \neq 0$ is ab ZD?

↓

$$y \neq 0, ay=0 \Rightarrow yab = \underbrace{(ay) \cdot b}_0 = 0 \Rightarrow ab \text{ is ZD}$$

3. Group Homomorphisms

$f: G \rightarrow H \quad (G, *) \quad (H, \circ)$

f is a homomorphism, e_G, e_H neutral

$$e_G * e_G = e_G$$

$$\underbrace{f(e_G)}_{\in H} = f(e_G * e_G) = f(e_G) \circ f(e_G)$$

$f(e_G)$ is invertible as H is a group.

$$\Rightarrow e_H = (f(e_G))^{-1} \cdot f(e_G) = (f(e_G))^{-1} \circ (f(e_G) \circ f(e_G)) = f(e_G)$$

$$e_H = f(e_G) = f(a * a^{-1}) = f(a) \circ f(a)^{-1} \Rightarrow f(a^{-1}) = f(a)^{-1}$$

$$f(a)^{-1} \cdot e_H = f(a)^{-1} \circ f(a) \circ f(a)^{-1} \Rightarrow e_H \circ f(a)^{-1} = f(a^{-1})$$

4) Group automorphisms for $(\mathbb{Z}_6, +)$

$(G_1, *)$ $f: G \rightarrow G$

need: $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$

$$f(a+b) = f(a) + f(b)$$

$$\mathbb{Z}_6 = \{1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1, 1+1+1+1+1+1\}$$

$f(a) := a$ is an automorphism

$$f(1) = 1$$

$$f(1+1+1) = 1+1+1$$

$$\text{where } f : f(1) = 1$$

$$f(0) = 0$$

$$f(3) = f(1+1+1) = 1+1+1 = 3$$

$\Rightarrow f$ is not an isomorphism \Rightarrow not an automorphism

if $b \in \{2, 3, 4, c=0\}$ then it is not an automorphism

if $f(1) = 5 \equiv -1$ we get $f(a) = -a \Rightarrow$ automorphism

$\{f(x) = x, f(x) = -x\}$ is the set of all automorphisms

$$n \cdot f(a) := \underbrace{f(a) + \dots + f(a)}_{n \text{ times}}$$

$$\{f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_6, x \mapsto x\}, \{f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_6, x \mapsto -x\}.$$

5)

$$e(x, y) = (x, y)$$

$$a(x, y) = (-y, x)$$

$$b(x, y) = (-x, -y)$$

$$c(x, y) = (y, -x)$$

$$h(x, y) = (-x, y)$$

$$v(x, y) = (x, -y)$$

$$s(x, y) = (y, x)$$

$$t(x, y) = (-y, -x)$$

$$H = \{e, h\}$$

$$e \circ e = e$$

$$e \circ h = h$$

$$h \circ e = h$$

$$h \circ h = e$$

$$gH \quad g=e \quad eH=H \quad hH=H$$

$$aH \quad a \circ e = a$$

$$a \circ h \sim a(h(x, y)) = a(-x, y) = (-y, -x) = t(x, y) \Rightarrow aH = \{a, t\}$$

$$tH \quad t \circ e = t$$

$$t(h(x, y)) = t(-x, y) = (-y, -x) = e$$

$$aH = tH = \{a, t\}$$

$$\begin{array}{ll} \text{H} & h(-x, y) = h(-x, -y) = (-y, x) = a \\ \text{bH} & b \circ e = b \quad b \circ h \quad b(h(x, y)) = b(-x, y) = (x, -y) = v(x, y) \\ \text{vH} & v \circ e = v \quad v \circ h = b \\ \text{cH} & c \circ e = c \quad c \circ h \quad c(h(x, y)) = c(-x, y) = (y, x) = b(x, y) \\ \text{dH} & d \circ e = d \quad d \circ h = c \end{array} \quad \left. \begin{array}{l} \text{bH} = \{v\}, \text{cH} = \{b\} \end{array} \right\} \text{CH} = \{b, c\}$$

Exercise sheet 7

1) Long division in \mathbb{Z}

$\forall a \in \mathbb{Z}, b \in \mathbb{Z}: \exists q \in \mathbb{Z}, n \in \{0, \dots, b-1\}$ s.t. $a = qb + n$

Induction start $a=0 \Rightarrow q=n=0$

step let it be true for a , i.e. $a = qb + n$

$$a+1 = \underbrace{qb}_{q'} + \underbrace{n+1}_{n'}$$

Case 1: $n \in \{0, \dots, b-2\}$

$$a+1 = q' b + n'$$

$$q' = q, n' = n+1 \Rightarrow 0 \leq n' \leq b-1$$

Case 2: $n = b-1$

$$a+1 = qb + b-1 + 1 = \underbrace{(q+1)b}_{q'} + \underbrace{0}_{n'}$$

$$0 \leq n' \leq b$$

We still have to consider the negative numbers

Let $a \in \mathbb{Z}, a < 0, b \in \mathbb{N}$

Then $-a \in \mathbb{N}$. By the induction, there exist $q \in \mathbb{Z}, n \in \{0, \dots, b-1\}$

$$\text{s.t. } -a = qb + n \Rightarrow a = -qb - n$$

$$\text{Case 1: } n=0 \Rightarrow a = -qb + 0$$

$$-q \in \mathbb{Z} \quad \hookrightarrow 0 \leq 0 < b$$

$$\text{Case 2: } n > 0$$

$$-n \in \{-b+1, \dots, -1\}$$

$$b-n \in \{1, \dots, b-1\}$$

$$a = \underbrace{(q+1)b}_{\in \mathbb{Z}} + \underbrace{(b-a)}_{0 \leq b-a < b}$$

Hence, it also holds for the negative numbers.

2) Order of elements in cyclic group.

$$(\mathbb{Z}_n, +) \quad n \in \mathbb{N}, z \in \mathbb{Z}$$

Show that the order of $[z]_n$ is $\frac{n}{\gcd(z, n)}$

Let s be the order of $[z]_n$

s is the number of elements in the subgroup generated by $[z]_n$

By Lagrange's theorem s divides n .

$$\text{Let } t := \frac{n}{s} \in \mathbb{N}$$

$$st = n \Rightarrow \frac{t}{s} n \quad sz \equiv 0$$

It holds

$$t \leq \gcd(z, n) \Rightarrow s = \frac{n}{t} \geq \frac{n}{\gcd(z, n)}$$

$$\left[z \cdot \frac{n}{\gcd(z, n)} \right]_n = \left[n \cdot \underbrace{\frac{z}{\gcd(z, n)}}_{\in \mathbb{Z}} \right]_n = [0]_n$$

This shows the other inequality, hence $s = \frac{n}{\gcd(z, n)}$

3) Number of generators $(\mathbb{Z}_{17}^*, \cdot)$

$$(\mathbb{Z}_{17} \setminus \{0\}, \cdot)$$

In the lecture $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is cyclic, $p \in \mathbb{P}$

$$|\mathbb{Z}_{17} \setminus \{0\}| = 16$$

$$g^1, g^2, g^3, \dots, g^{16}$$

$$(\mathbb{Z}_{16}, +)$$

We know that $(\mathbb{Z}_{17} \setminus \{0\}, \cdot)$ and $(\mathbb{Z}_{16}, +)$ have the same number of generators.

The order of generator z in $(\mathbb{Z}_{16}, +)$ has to be 16.

and by task 2 $\frac{16}{\gcd(z, 16)}$ is the order

that means z is a generator $\Leftrightarrow 16 = \frac{16}{\gcd(z, 16)} \Leftrightarrow \gcd(z, 16) = 1 \Leftrightarrow z$ is odd.

There are 8 odd numbers in $(\mathbb{Z}_{16}, +)$

4) Baby step giant step algorithm

solve $5^i \equiv 9 \pmod{17} \quad i = 0, \dots, 16$

$$g^i \equiv h \pmod{p}$$

$$|\sqrt{p-1}| = |\sqrt{16}| = 4 \quad i = \{0, \dots, p-1\}$$

$$i = s + 4t$$

$$s, t \in \{0, \dots, 3\}$$

$$h \equiv g^{s+4t}$$

$$h, g^{-1} \equiv g^s$$

Incomplete solution

5) solving DLP

Exercise sheet 8

1) finite field $\mathbb{Z}_2[t]/(t^3 + t^2 + 1)$

For $\mathbb{Z}_2[g]$ to be a field, it needs to be irreducible

If g is not irreducible, then there exist $g_1, g_2 \in \mathbb{Z}_2[t]$, $\deg(g_1), \deg(g_2) \geq 1$ with $g = g_1 g_2$

\Rightarrow one of the polynomials has degree one, the other has degree two.

$$\text{W.l.o.g } \deg(g_1) = 1, \deg(g_2) = 2$$

$$1 = g(0) = g_1(0)g_2(0) \rightarrow g_1 \text{ has no zero}$$

$$1 = g(1) = g_1(1)g_2(1) \rightarrow \text{but } g_1 \text{ is linear, and linear polynomials always have a zero.}$$

By that g is irreducible $\Rightarrow F$ is a field.

Every element in F has the form $[a + bt + ct^2]a$

There are 3 coefficients with two possible values (α_2) \Rightarrow 8 elements

$$f = t+1$$

$$x = [f]_g$$

$$x^{2024}$$

$$a + b\alpha + c\alpha^2$$

$$\alpha = [t]_g$$

$$a, b, c \in \mathbb{Z}_2$$

$$[t+1]_g^{2024}$$

$F \setminus \{0\}$ has 7 elements

$(F \setminus \{0\}, \cdot)$ is a group as F is a field

$$[t+1]_g \in F \setminus \{0\}$$

$$[t+1]_g^{2024} = [t+1]_g^{7 \cdot 289 + 1} = ([t+1]_g^7)^{289} \cdot [t+1]_g = 1[t+1]_g = 1 + \alpha$$

2) Understanding $\mathbb{Q}[t]/(t^2 - 1)$

S''

\underbrace{g}

$$T = \mathbb{Q} \times \mathbb{Q}$$

$$\phi([f]_g) = (f(1), f(-1))$$

well-definedness: Let $f_1, f_2 \in \mathbb{Q}[t]$, $[f_1]_g = [f_2]_g$

Then, there exists $q \in \mathbb{Q}[t]$ with $f_1 - f_2 = q \cdot g$

$$\text{Hence } f_1(1) - f_2(1) = q(1) \underbrace{g(1)}_0 = 0$$

$$f_1(-1) - f_2(-1) = q(-1) \underbrace{g(-1)}_0 = 0$$

we show that ϕ is injective

we take $f_1, f_2 \in S$ with $\phi([f_1]_g) = \phi([f_2]_g)$

$$(f_1(1), f_1(-1))$$

$$(f_2(1), f_2(-1))$$

$$\left. \begin{array}{l} f_1(1) - f_2(1) = 0 \\ f_1(-1) - f_2(-1) = 0 \end{array} \right\} f_1 - f_2 = q(t-1)(t+1) = q(t^2 - 1) = qg \Rightarrow [f_1]_g = [f_2]_g \Rightarrow \text{injectivity}$$

Surjectivity

Let $(y_1, y_2) \in T$ be given

We need f s.t.

$$f(1) = y_1, f(-1) = y_2$$

$$f(t) = y_1 \frac{t+1}{2} - y_2 \frac{t-1}{2}$$

$$f(1) = y_1$$

$$f(-1) = y_2$$

$$(t-1)(t+1) = 1$$

Zero divisors are all multiples of $k(t-1)$ and $k(t+1)$, $k \in \mathbb{Q} \setminus \{0\}$

3) Understanding $\mathbb{Q}[t]/t^2 - 2$

$$f(t) = \sum_{i \in \mathbb{N}_0} c_i t^i \in K[t]$$

$$f(A) = \sum_{i \in \mathbb{N}_0} c_i A^i$$

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

$$\mathbb{Q}[A] = \{f(A) \mid f \text{ in } K[t]\}$$

$$A^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2I$$

$$\phi([f]_g) = f(A)$$

well-definedness

$$\text{Let } f_1, f_2 \in \mathbb{Q}[t], [f_1]_g = [f_2]_g \Rightarrow f_1 - f_2 = g \cdot g \text{ for some } g \in \mathbb{Q}[t]$$

$$f_1(A) - f_2(A) = \underbrace{g(A)}_{\substack{\sim \\ A^2 - 2I}} \underbrace{g(A)}_{\sim 0} = 0$$

It is clear that ϕ preserves addition and multiplication and 1 is mapped to I.

Injectivity: $[f_1]_g \neq [f_2]_g \Rightarrow f_1 - f_2 = g \cdot g + n, g, n \in \mathbb{Q}[t], n(t) = at+b$
 $(a, b) \neq (0, 0)$

$$\text{we get } \phi([f_1]_g) - \phi([f_2]_g) = f_1(A) - f_2(A) = \underbrace{g(A)}_{\neq 0} \underbrace{g(A)}_{\sim 0} + n(A) = n(A)$$

$$= aA + bI = \begin{pmatrix} b & a \\ 2a & b \end{pmatrix} \neq 0 \text{ because } (a, b) \neq (0, 0)$$

\Rightarrow injectivity holds.

Injectivity is clear

$$A^2 = 2I \quad \begin{pmatrix} 0 & x \\ x & 0 \end{pmatrix} \quad \begin{pmatrix} b & a \\ 2a & a \end{pmatrix}$$

$$A^3 = 2A$$

$$A^4 = 4I$$

4) Modulo $t^2 - 1$ vs Modulo $t^2 - 2t$

or $\begin{cases} S = \mathbb{Q}[t]/t^2 - 1 \\ T = \mathbb{Q}[t]/t^2 - 2t \end{cases}$ Isomorphic?

$$g(t) = t^2 - 1 = (t - (-1))(t + 1)$$

$$h(t) = t^2 - 2t = (t - 0)(t - 2)$$

$$\phi([f]_g) = [f(t-1)]_h$$

$$\phi([f]_h) = [f(t+1)]_g$$

Exercise sheet 9

$$1) f(t) = \sum_{i=0}^d a_i t^i \quad d \in \mathbb{N}, a_i \in \mathbb{Z}$$

$a_0, a_d \neq 0$

$$n = \frac{m}{n} \quad m \in \mathbb{Z} \setminus \{0\}, n \in \mathbb{N}, \gcd(m, n) = 1$$

$$\text{As } n \text{ is a root: } 0 = f(n) = f\left(\frac{m}{n}\right) = \sum_{i=0}^d a_i m^i n^{i-1}$$

multiply with n^d gives

$$0 = \sum_{i=0}^d a_i m^i n^{d-i}$$

Apply mod n gives $0 \equiv a_d m^d \underbrace{n^{d-d}}_{=1} \pmod{n}$

Analogously mod m gives $0 \equiv a_0 m^0 n^{d-0} \pmod{m}$

$$a_d m^d \equiv 0 \pmod{n}, a_0 n^d \equiv 0 \pmod{m}$$

As $\gcd(m, n) = 1$ holds, we get the wanted, $a_d \equiv 0 \pmod{n}$ and $a_0 \equiv 0 \pmod{m}$

2) GCD

$$f(t) = (t^2 - 1)^{100}$$

$$g(t) = (t^3 - 1)^{200} \text{ in } \mathbb{Q}[t]$$

we factorize:

$$f(t) = (t-1)^{100} (t+1)^{100}$$

$$g(t) = (t-1)^{200} (t^2 + t + 1)^{200}$$

for g : we see $t^3 - 1 = 0 \Rightarrow 1$ is a root of g

$\Rightarrow (t-1)$ divides $t^3 - 1$

$$(t^3 - 1)(t-1) = t^2 + t + 1$$

$$\begin{array}{r} -t^2(t+1) \\ \hline 0t^3 + t^2 - 1 \\ -t(t-1) \\ \hline 0t^2 + t - 1 \end{array}$$

$t^2 + t + 1$ has no rational roots

in \mathbb{C} the roots are $\frac{-1}{2} \pm \sqrt{\frac{-3}{4}} \notin \mathbb{Q}$
 $\Rightarrow t^2 + t + 1$ is irreducible

Now we compare the factorization and gcd

$$\gcd(f, g) = (t-1)^{\min(100, 200)} (t+1)^{\min(100, 0)} (t^2 + t + 1)^{\min(0, 200)} = (t-1)^{100}$$

3) Finite field formula

F is a finite field. $a \in F$. Determine $a^{|F|}$.

$\rightarrow F$ is a finite field, $(F \setminus \{0\}, \cdot)$ is a group

\rightarrow if $a \neq 0$ the order of the subgroup generated by a is a divisor of $|F|-1$ by Lagrange's theorem.

$$\text{By, this } a^{|F|-1} = 1$$

\rightarrow if k is the order of $a \Rightarrow a^k = 1 \Rightarrow a^{|F|-1} = (a^k)^{\frac{|F|-1}{k}} \in \mathbb{N}$

$$\Rightarrow \text{for } a \neq 0: a^{|F|} = 1 \cdot a = a$$

$$\text{for } a=0: a^{|F|} = a \text{ holds trivially}$$

$$a^{|F|} = a$$

4) Inversion in $\mathbb{Z}_2[t]/t^2+t+1$

$$F = \mathbb{Z}_2[t]/t^2+t+1$$

$$a = x_0 + x_1 \alpha$$

α is a coset of t
 $(x_0, x_1) \neq ([0]_2, [0]_2)$

what is a^{-1} ?

$$b = y_0 + y_1 \alpha$$

$$\begin{aligned} 1 = ab &= x_0 y_0 + (x_0 y_1 + x_1 y_0) \alpha + x_1 y_1 \alpha^2 \\ &= x_0 y_0 + (x_0 y_1 + x_1 y_0) \alpha + x_1 y_1 (\alpha + 1) \\ &= \underbrace{x_0 y_0}_{1} + \underbrace{x_1 y_1}_{0} + \underbrace{(x_0 y_1 + x_1 y_0 + x_1 y_1)}_{0} \alpha \end{aligned}$$

$$\begin{pmatrix} x_0 & x_1 \\ x_1 & x_0 + y_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 & x_1 \\ x_1 & x_0 + y_1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= (x_0(x_0 + y_1) - x_1^2)^{-1} \begin{pmatrix} x_0 + y_1 & -x_1 \\ -x_1 & x_0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= (x_0^2 + x_0 x_1 + x_1^2)^{-1} \begin{pmatrix} x_0 + x_1 \\ + x_1 \end{pmatrix} \quad 0^2 = 0 \quad 1^2 = 1$$

$$= (x_0 + x_0 x_1 + x_1)^{-1} \begin{pmatrix} x_0 + y_1 \\ x_1 \end{pmatrix}$$

By the idea

$\mathbb{Z}_2[t]/(t^2+t+1)$ is irreducible

Lecture. $\mathbb{Z}_2[t]/(t^2+t+1)$ is a field as g is irreducible and \mathbb{Z}_2 is a field

$$|\mathbb{Z}_2[t]/(t^2+t+1)| = 4 \quad \text{elements} = \{0+0\alpha, 0+1\alpha, 1+0\alpha, 1+1\alpha\}$$

By question 3 we get $a^4 = a$

$$a^4 = a$$

a is invertible

$$= a^2 = a \cdot a^{-2} = a^{-1}$$

$$\Rightarrow a^{-1} = a^2 = (x_0 + x_1 \alpha)^2$$

$$= x_0^2 + 2x_0 x_1 \alpha + x_1^2 \alpha^2$$

$$= x_0 + x_1 (\alpha + 1)$$

$$= (x_0 + x_1) + x_1 \alpha$$

$$\left[\begin{array}{l} \alpha^2 \equiv -1\alpha - 1 \pmod{g} \\ \equiv +1\alpha + 1 \pmod{g} \\ = \alpha + 1 \end{array} \right]$$

5) Invertibility in a quotient ring.

$$g = (t^3 + 1)^{10} \in \mathbb{Z}_2[t]$$

Are $[t+1]_g, [t^2+t+1]_g, [t^4+t+1]_g$ invertible?

$$g(t) = (t+1)^{10} (t^2+t+1)^{10}$$

$$\begin{array}{r} (t^3 + 1) : (t+1) = t^2 + t + 1 \\ \hline -t^2(t+1) \qquad \qquad \qquad \text{irreducible in question 4} \\ \hline 0t^3 + t^2 \\ \hline -t(t+1) \\ \hline 0t^2 + t \\ \hline -1(t+1) \\ \hline 0t + 0 \end{array}$$

$$\begin{aligned} \gcd(g(t), t+1) &= t+1 \neq 1 \Rightarrow \text{Not invertible} \\ \gcd(g(t), t^2+t+1) &= t^2+t+1 \neq 1 \Rightarrow \end{aligned}$$

$$t^4+t+1$$

It is not divisible by $t+1$ as 1 is a root of $t+1$ but not a root of t^4+t+1

$$(t^4+t+1) : (t^2+t+1) = t^2$$

$$\begin{array}{r} -t^2(t^2+t+1) \\ \hline A3+t^2+t+1 \end{array}$$

Remainder = 1

$$-t(t^2+t+1)$$

$$0t^2 + 0t + 1$$

$$\gcd(g(t), t^4+t+1) = 1 \Rightarrow [t^4+t+1]_g \text{ is invertible}$$

6) Field with 121 elements

$$121 = 11^2$$

$$\mathbb{Z}_{11}[t]/g, \deg(g) = 2$$

$$g(t) = t^2 + q$$

we want g to be irreducible

As $\deg(g) = 2$, this just means that g doesn't have a root.

$$[0]_{11}^2 = [0]_{11}$$

$$[1]_{11}^2 = [1]_{11}$$

$$[2]_{11}^2 = [4]_{11}$$

$$[3]_{11}^2 = [9]_{11}$$

$$[4]_{11}^2 = [5]_{11}$$

$$[5]_{11}^2 = [3]_{11}$$

$$[6]_{11}^2 = [3]_{11}$$

$$[7]_{11}^2 = [5]_{11}$$

$$[8]_{11}^2 = [9]_{11}$$

$$[9]_{11}^2 = [4]_{11}$$

$$[10]_{11}^2 = [1]_{11}$$

possible squares are $0, 1, 4, 9, 5, 3 \Rightarrow$ we choose $q \in \{0, 1, \dots, 10\}$ such that

$$q, 1+q, 3+q, 4+q, 5+q, 9+q \not\equiv 0 \pmod{11}$$



One choice is $g(t) = t^2 + 1$, as

$g(t) \neq 0$ for $t \in \mathbb{Z}_{11}$

$$\mathbb{Z}_{11}[t] / (t^2 + 1)$$

7) DHKE

$$F = \mathbb{Z}_3[t]/g$$

$$g = t^2 + 1$$

check if $[t+1]_g$ is a generator of the group $(F \setminus \{0\}, \cdot)$

By Lagrange's theorem, the group generated by g in $(F \setminus \{0\}, \cdot)$

divides $|F \setminus \{0\}| = 8$

\Rightarrow we just check $[t+1]_g^2, [t+1]_g^4 \neq [1]_g$

$$|\mathbb{Z}_3| = 3$$

$$|F \setminus \{0\}| = 3^2 - 1 = 8$$

$$[t]_g = \alpha$$

$$(\alpha+1)^2 = \underbrace{\alpha^2}_{\equiv 0} + 1 + 2\alpha = 2\alpha$$

$$(\alpha+1)^4 = [(1+\alpha)^2]^2 = (2\alpha)^2 = 4\alpha^2 = \alpha^2 \equiv -1 \equiv 2 \pmod{g}$$

\Rightarrow subgroup generated by g does not have 1, 2 or 4 elements \Rightarrow it has 8 elements
 $\Rightarrow g$ is a generator

Exercise sheet 10

1) \mathbb{Z}_2 -linear, \mathbb{F}_4 linear

$$g(t) = t^2 + t + 1 \in \mathbb{Z}_2[t], \quad \mathbb{F}_4 := \mathbb{Z}_2[t]/g$$

$$T: \mathbb{F}_4 \rightarrow \mathbb{F}_4$$

$$x_0 + x_1 \alpha \mapsto x_0 + (x_0 + x_1) \alpha$$

$$x_0, x_1 \in \mathbb{Z}_2$$

Is T \mathbb{Z}_2 linear? obvious

$$T(0x) = 0 + 0\alpha = 0T(x)$$

$$T(1x) = T(x) = 1T(x)$$

Is T \mathbb{F}_4 linear?

If it is, then $x = x_0 + x_1 \alpha$

$$\begin{aligned} T(x) &= x \cdot T(1) = x \cdot (1+\alpha) = (x_0 + x_1 \alpha) \cdot (1+\alpha) \\ &\stackrel{!}{=} x_0 + (x_0 + x_1) \alpha + x_1 \alpha^2 \\ &= x_0 + (x_0 + x_1) \alpha + x_1 (1+\alpha) \\ &= x_0 + x_1 + (x_0 + x_1 + x_1) \alpha \\ &= (x_0 + x_1) + x_0 \alpha \end{aligned}$$

But $x_1 \neq x_0 \alpha$

$$T(1) = T(1+0\alpha) = 1+(1+0)\alpha = 1+\alpha$$

As the term $x_0 + (x_0 + x_1) \alpha$ is not $(x_0 + x_1) + x_0 \alpha$, we see that the map T is not \mathbb{F}_4 linear.

2) Linear maps, matrices, inversion

F is a field

$$T: F^n \rightarrow F^n$$

$$T(x_1, \dots, x_n) = (y_1, \dots, y_n)$$

$$y_i = \sum_{j=1}^i x_j$$

$$T(x) = A \cdot x$$

$$\begin{array}{ll} n=3 & y_1 = x_1 \\ & y_2 = x_1 + x_2 \\ & y_3 = x_1 + x_2 + x_3 \end{array} \quad \left. \right\}$$

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\text{In general: } A = (a_{ij})_{i,j=1}^n, \quad a_{ij} = \begin{cases} 1 & i \geq j \\ 0 & i < j \end{cases}$$

$$\text{We see: } x_1 = y_1,$$

$$\text{for } i \geq 2 : x_i = x_i - y_{i-1}$$

$$n=3 \quad \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$A^{-1} = B = (\beta_{ij})_{i,j=1}^n, \quad \beta_{ij} = \begin{cases} 1, & \text{if } i=j \\ -1, & \text{if } i=j+1 \\ 0, & \text{else} \end{cases}$$

3) Evaluation

$$V := \{ f \in \mathbb{Z}_7[t] \mid \deg f \leq 2 \}$$

$$\tau: V \rightarrow \mathbb{Z}_7^3$$

$$\tau(f) := (f(0), f(1), f(2))$$

Is τ linear?

$$\begin{aligned} \tau(\alpha f + \beta g) &= (\alpha f(0) + \beta g(0), \dots) \\ &= \alpha (f(0), \dots) + \beta (g(0), \dots) \end{aligned}$$

Invertibility of τ ?

$$\text{Ansatz: } V = \{ f \mid f(t) = x_0 + x_1 t + x_2 t^2, \quad x_0, x_1, x_2 \in \mathbb{Z}_7 \}$$

$$\tau(f) = \begin{pmatrix} f(0) \\ f(1) \\ f(2) \end{pmatrix} = \begin{pmatrix} x_0 + x_1 \cdot 0 + x_2 \cdot 0^2 \\ x_0 + x_1 \cdot 1 + x_2 \cdot 1^2 \\ x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 \end{pmatrix} = \begin{pmatrix} x_0 \\ x_0 + x_1 + x_2 \\ x_0 + 2x_1 + 4x_2 \end{pmatrix}$$

↓

$$\begin{aligned} (\Delta) \quad x_0 &= f(0) \\ f(1) - f(0) &= x_1 + x_2 \\ \underline{f(2) - f(0)} &= 2x_1 + 4x_2 \end{aligned}$$

-2 1

$$\begin{aligned} -2f(1) + 2f(0) + f(2) - f(0) &= -2x_1 - 2x_2 + 2x_1 - 4x_2 \\ f(0) - 2f(1) + f(2) &= 2x_2 \\ \Rightarrow 4f(0) - 8f(1) + 4f(2) &= 8x_2 \equiv 1x_2 = x_2 \quad (\square) \end{aligned}$$

-8 ≡ -1 ≡ 6

$$\begin{aligned} x_1 &= f(1) - f(0) - x_2 \\ &= f(1) - f(0) - [4f(0) + 6f(1) + 4f(2)] \\ &= -5f(0) - 5f(1) - 4f(2) \\ &= 2f(0) + 2f(1) + 3f(2) \quad (0) \end{aligned}$$

$$(\Delta), (0), (\square) \Rightarrow \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 3 \\ 4 & 6 & 4 \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ f(2) \end{pmatrix}$$

4) yet another map

F is a field

$$T: F^n \rightarrow F^n$$

$$T(x_0, \dots, x_{n-1}) = (y_0, \dots, y_{n-1})$$

$$x_1 = x_0 \quad y_1 = x_1 + x_0$$

$$x_{i+1} = x_i$$

• Is T linear? yes

$$\text{check if } T(\alpha x + \beta \tilde{x}) = \alpha T(x) + \beta T(\tilde{x})$$

• Consider $F = \mathbb{Z}_2$

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \vdots & 1 \end{pmatrix}$$

$$T(0) = 0$$

if $T(x) = 0$ for some $x \neq 0$, then T is not injective hence not bijective

$$T \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1+1 \\ 1+1 \\ \vdots \\ 1+1 \end{pmatrix} \stackrel{\mathbb{Z}_2}{=} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = T \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

even if $n=1$

indexing n modulo $n=1$

$0=1=2=3=\dots \Rightarrow T$ is not invertible in \mathbb{Z}_2

• Consider $F = \mathbb{Z}_3$

• n even

$$T(0) = 0$$

$$T \begin{pmatrix} 1 \\ 2 \\ \vdots \\ 2 \end{pmatrix} = \begin{pmatrix} 1+2 \\ 2+1 \\ \vdots \\ 2+1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\Rightarrow T$ is not invertible in \mathbb{Z}_3

• n odd

$$y_i - y_{i+1} + y_{i+2} - \dots + y_{i+n-1}$$

$$= (x_i + x_{i-1}) - (x_{i+1} + x_{i+2}) + (x_{i+2} + x_{i+3}) - \dots + (x_{i+n-1} + x_{i+n})$$

$$= x_i - x_{i+n}$$

$$= x_1 + x_{1+m} = 2x_1 = -x_1$$

$$\Rightarrow x_i = -y_i + y_{i+1} - y_{i+2} + \dots - y_{i+n-1}$$

Example: $n=4, i=2$

$$y_2 - y_3 + y_0 - y_1 = (\cancel{y_2} + \cancel{x_3}) - (\cancel{x_3} + \cancel{y_0}) + (\cancel{y_0} + \cancel{x_1}) - (\cancel{x_1} + \cancel{y_2}) = 0$$

\Rightarrow this idea of taking + and - (alternatively) does not work for even n

5) Matrix of the projection

$$T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

$$T(x) = y$$

y is the projection of $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ onto the plane $P = \{x \mid x_1 + x_2 + x_3 = 0\}$

along the direction $u = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$

look into direction u while staying in x

$$x + t u, t \in \mathbb{R}$$

$$x + t u, t \in \mathbb{R}$$

" y is the projection onto P " means $y \in P$



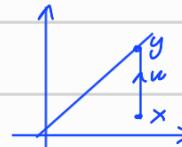
what $t \in \mathbb{R}$ gives $y = x + t u \in P$

$$x + t u = \begin{pmatrix} x_1 + t_1 \\ x_2 + t_2 \\ x_3 + t_3 \end{pmatrix}$$

$$\downarrow 0 = (x_1 + t_1) + (x_2 + 2t_2) + (x_3 + 3t_3)$$

$$\Rightarrow x_1 + x_2 + x_3 + 6t = 0$$

$$\Rightarrow t = -\frac{x_1 + x_2 + x_3}{6}$$



$$x + t u = \begin{pmatrix} x_1 - \frac{x_1 + x_2 + x_3}{6} \cdot 1 \\ x_2 - \frac{x_1 + x_2 + x_3}{6} \cdot 2 \\ x_3 - \frac{x_1 + x_2 + x_3}{6} \cdot 3 \end{pmatrix} = \begin{pmatrix} \frac{5}{6}x_1 - \frac{1}{6}x_2 - \frac{1}{6}x_3 \\ -\frac{1}{3}x_1 + \frac{2}{3}x_2 - \frac{1}{3}x_3 \\ -\frac{1}{2}x_1 - \frac{1}{2}x_2 + \frac{1}{2}x_3 \end{pmatrix} = \begin{pmatrix} \frac{5}{6} & -\frac{1}{6} & -\frac{1}{6} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$