1. Caesar's cipher

$x \equiv (y - k) \bmod 26$

Cipher: EXL BOK UIKLVO

Shift: 10

decoded msg: UNBREAKABLE

2. Modular calculation for double power

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

$$2024^{2^{2024}} \bmod 13 = 9^{2^{2024}} \bmod 13$$

we only need to find remainder of 2^{2024} but it is HUGE!

so, we find cycle of powers of 2 mod 3

$2^1 = 2$

$2^2 = 1$

$2^3 = 2$

$2^4 = 1$

$2^5 = 2$

⋮

the cycle repeats after every 2 steps

So, remainder of $2^{2024} \bmod 3$ is 1 (since 2024 is even).

$$2024^{2^{2024}} = 9^1 = 9$$

SOLUTION

$$2024^{2^{2024}} \bmod 13 = 9^{2^{2024}} = 9^{(2^{2022})(4)} = (9^4)^{2^{2022}}$$

$$= 9^{2^{2022}} = 9^{2^{2020} \cdot 4} = (9^4)^{2^{2020}} = 9^{2^{2020}} = 9^{2^0} = 9^1 = 9$$

NOTE: $(a^m)^n = a^{mn}$

3. Divisibility by 9

ring 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 ... g
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 $10 \equiv 1 \bmod 9$:

$$100A+10B+C \equiv (99+1)A + (9+1)B + C \equiv 99A + A + 9B + B + C \equiv A+B+C \bmod 9$$

4. How to define Functions well?

$f: R \to R$, $y^2 = x$ $\Rightarrow$ not well defined

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 diff^n representatives x' and y' s.t. $x' \equiv x \bmod n$ and $y' \equiv y \bmod n$

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

↑ since $x' \equiv x \bmod n$
$y' \equiv y \bmod n$
it follows $[x'+y'] \equiv [x+y] \bmod n$

Hence, $[x'+y']$ and $[x+y]$ belong to the same coset.

---

2. Fermat's little theorem

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

$$2^{2024} \bmod 12$$

$$a^{2^{2024}} \equiv a^{2^{2024}-12}$$

$$\equiv \bmod 13$$

$q^{12} \equiv 1 \mod$

3. Divisibility by 9

$$10^k \equiv 1^k \equiv 1 \mod 9$$

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

$a_k \in \{0, 1, 2, \ldots, 9\}$

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

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

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

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

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

4. Functions

$x, y \in \mathbb{Z}$

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

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

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

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

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

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

$= kn + ln$

$\Leftrightarrow (x'+y') - (x+y)$ 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 diff" representatives $x', y' \in \mathbb{Z}$ with $x' \in [x]$ & $y' \in [y]$

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

$x' \in [x]_n$ and $y' \in [y]_n$

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

By definition of $[x]_n$

Therefore there exists $k, l \in \mathbb{Z}$ such that

$x' - x = kn, \quad y' - y = ln$

this yields

$x' = x + kn \;, \; y' = y + ln \quad -①$

we consider

$x'.y' - xy \overset{①}{=} (x+kn)(y+ln) - x.y$

$= xy + xln + kny + kln^2 - xy$

$= n(xl + ky + kln)$

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

---

1) Caesar strikes back

The function

$f(x) = ax + b \mod 26$

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

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

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

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

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

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

will give a bijective function.

2) Asterix never gives up.

Cipher = "UQPXFUBSUQPJFU"

$f(x) = ax + b$

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 :

$$a*t + b \equiv x \bmod 26$$
$$a*h + b \equiv y \bmod 26$$
$$a*e + b \equiv z \bmod 26$$

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 $\mathbb{Z}_{26}$.

$$19a + b \equiv 20 \bmod 26 \quad -①$$
$$7a + b \equiv 16 \bmod 26 \quad -②$$
$$4a + b \equiv 15 \bmod 26 \quad -③$$

Using ① - ②

$$(19a + b) - (7a + b) \equiv (20 - 16) \bmod 26$$
$$12a \equiv 4 \bmod 26$$
$$(\div 4) \quad 3a \equiv 1 \bmod 26$$

Using Euclid's algorithm,

$$26 = 3(8) + 2$$
$$3 = 2(1) + 1$$

Backword substitution

$$1 = 3 - 2(1)$$
$$1 = 3 - (26 - 3(8))$$
$$1 = 3(9) - 26$$

So, $\boxed{a = 9}$

sub $a = 9$ in ①

$$19a + b \equiv 20 \bmod 26$$
$$19(9) + b \equiv 20 \bmod 26$$

$171 + b \equiv 20 \bmod 26$

$15 + b \equiv 20 \bmod 26$ (because $171 \bmod 26 = 15$)

(-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	$a^{-1} \bmod 26 = 3$
3(x-5)	45	33	30	54	0	45	-12	39	45	33	30	12	0	45	
mod 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	

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

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

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

$a = 2$

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

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

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

$f(x) = ax+b$, a 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) UQPXFUBSUQPJFU

$f(x) = ax+b$

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

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

19 T → U 20

7 H → Q 16

4 E → P 15

$19a + b = 20$

$7a + b = 16$

$4a + b = 15$

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

$3a = 1$

$\Rightarrow \boxed{a = 9}$

$9 \cdot 4 + b = 15$

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

$\boxed{b = 5}$

3) $a \in R$ show that negative of a 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 $* : G \times G \to G$

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

i) Show that neutral element is unique

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

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

$e'*a = a = a*e'$

$e = e*e' = e'$

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

$a*(b*a')$

$a*e$

$a * e$

a

$b * a' = e$ — ②

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

$\overset{①}{=} b * (e * a')$

$\overset{(N)}{=} b * a$

$\overset{②}{=} e$

Show that inverse is unique $a * b = e$ — ④

we assume that b, c exist with $a * b = a * c = e \Rightarrow c * a = e$ — ③

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

Excercise sheet 3

1) f encryption fct $f: X \to Y$

g decryption fct $g: Y \to X$

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

(i) Is f necessarily injective?

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?

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

Assume $f(0) = 0$ $g(0) = g(1) = 0$

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 $\cdot$

$G_1 = R^\times = \{ a \in R \mid \text{there exists an inverse} \}$

$(G_1, \cdot)$

Take $a, b \in G_1$. There exist inverses $a^{-1}, b^{-1} \in R$

$(b^{-1}a^{-1})(ab) \overset{+}{=} b^{-1}(a^{-1}(ab)) = b^{-1} 1 b = 1$

we have shown by this that products of invertible elements are invertible, hence $\cdot : G_1 \times G_1 \to G_1$ holds.

We need to show that $(G_1, \cdot)$ is Abelian group.

Commutativity:

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

Invertibility:

$a \in G_1$ want to show that $a^{-1} \in G_1$

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

$\Rightarrow a$ is invertible

$\Rightarrow a^{-1} \in G_1$

Neutral element

$1 \in G_1$ as $1 \cdot 1 = 1$ hence 1 is invertible

Associativity

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

3. power functions in finite groups.

[in $\mathbb{Z}_p$ $a^{\cdot} \equiv 1 \mod p$]

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

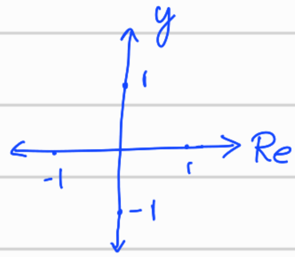
$ax_1 = f(x_1) = f(x_2) = ax_2$

$f : G \to G$

$\overset{I}{\Longrightarrow} a^{-1}(ax_1) = a^{-1} \cdot (ax_2) = x_2$
$\quad\quad\; \shortparallel$
$\quad\quad\; x_1$

Because $|G| = h$ is finite
injectivity is the same as bijectivity

$\prod_{x \in G} x = \prod_{x \in G} (ax) \overset{\text{Abelian}}{=} a^h \underbrace{\prod_{x \in G} x}_{\text{invertible}}$ $\quad \left[\prod_{x \in G} x = \prod_{x \in G} \underbrace{f(x)}_{ax}\right]$



$\Longrightarrow 1 = a^h$

$f(x) = ix$

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

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

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

$\overset{\text{mod } p-1}{\Longrightarrow} de \equiv 1 \pmod{p-1} \Rightarrow d = d$

By EEA we can compute d in polynomial time

$x^e = uax^e + ub + v$

$\Rightarrow 1 = ua \Rightarrow u = a^{-1}$

$0 = ub + v \Rightarrow v = -ub \Rightarrow v = -a^{-1}b$

$x^{ed} = x$ corollary 8

5. Caesar's new idea

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

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

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

n inputs

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

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 $m \in \mathbb{N}$, $t \in \mathbb{N}$

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

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

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

Excercise sheet 4

1) Caesar variation

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

△ (a, b) choices

a should be invertible

$ax_1' + b = ax_1'' + b$

↳ case 1 : a invertible ⇒ injective ⇒ is also bijective (encryption fn is)

↳ case 2 : a is not invertible ⇒ not injective

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

△ decryption

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

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

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

$\vdots$

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

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

△ determine a

T $\quad 19a = y_{100} - y_{99}$

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

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

$y_{100} = a(\underbrace{x_1 + \ldots + x_{99}}_{S} + x_{100}) + b$

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

$y_{101} = aS + b + ax_{100} + ax_{101}$

$y_{102} = aS + b + ax_{100} + ax_{101} + ax_{102}$

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 atleast zero multiplications

Δ Induction step

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

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

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

$e = a + b$

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

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

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

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

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

$x^e = x^a \cdot x^b$

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

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

$103 = 101(1) + 2$	$1 = 101 - 2(50)$
$101 = 2(50) + 1$	$1 = 101 - 50(103 - 101)$
	$= 51 \times 101 - 50 \times 103$

$\Rightarrow 5151 \equiv 0 \bmod 101 \quad -5150 \equiv 1 \bmod 101$

$5151 \equiv 1 \bmod 103 \quad -5150 \equiv 0 \bmod 103$

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

4) quadratic equations & Modular arithmetic

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

$217 = 7 \cdot 31$

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

$1^2+1+1 = 3$ ×

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

$3^2+3+1 = 13 \bmod 7 = 6$ ×

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

$5^2+5+1 = 31$ ×

$6^2+6+1 = 43$ ×

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

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

$p_1 = 5$

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

$= x^2 + \underbrace{(-p_1-p_2)}_{1} x + p_1 p_2$

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

$\mathbb{Z}_5$ 2 $\quad$ $\mathbb{Z}_{31}$ 5

4 $\quad$ 25

$31 = 7(4)+3$ | $1 = 7-3(2)$

$7 = 3(2)+1$ | $= 7-2(31-7(4))$

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

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

$63 \equiv 0 \bmod 7$ $\quad$ $-62 \equiv 1 \bmod 7$

$63 \equiv 1 \bmod 31$ $\quad$ $-62 \equiv 0 \bmod 31$

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

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

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

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

5) CRT

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

there is a bijection

(1)

$f: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$

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

Lecture says (2) $\Rightarrow$ (1)

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

Non-bijective

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

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

$n = n_1 n_2$ $\quad g \mid n_1, g \mid n_2$ ×

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

$\in \mathbb{Z}$

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

$\Rightarrow f$ is not bijective

Exercise sheet 5

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

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

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

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

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

we show bijectivity by showing injectivity

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

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

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

$n \mid (u-v) \iff [u]_n = [v]_n$

$\Rightarrow$ 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

$\Rightarrow \quad 21 * d = 1 \bmod \phi(n)$

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

$= 381$

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

$x = [z]_{1111}$

① get $[z]_{11}$, $[z]_{101}$
② calculate $[z]_{11}^d$, $[z]_{101}^d$
③ get back $[z]_{1111}^d$ by (*)

EEA(11, 101)

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

$506 = 46 \cdot 11 \equiv 1 \bmod 101 \qquad -505 \equiv 0 \bmod 101$

$46 \cdot 11 \equiv 0 \bmod 11 \qquad -505 \equiv 1 \bmod 11$

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

$[z]_{1111} \to [z]_{101}$

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

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

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

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

$z^{q-1} \equiv 1 \bmod q$

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

$x \rightsquigarrow x^e$

what if $x^e = x$?

3. prime numbers

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

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

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

$10^k - 10^{k-1}$
$= 10^{k-1}(10-1)$
$= 9$

$\frac{\pi(n)}{n \ln n} \longrightarrow 1$ for $n \to \infty$

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

$$\frac{\pi(10^k) - \pi(10^{k-1})}{10^k - 10^{k-1}} = \frac{\frac{10^k}{\ln(10^k)} \alpha(10^k) - \frac{10^{k-1}}{\ln(10^{k-1})} \alpha(10^{k-1})}{9 \cdot 10^{k-1}}$$

$$= \frac{\frac{10}{\ln(10^k)} \alpha(10^k) - \frac{1}{\ln(10^{k-1})} \alpha(10^{k-1})}{9}$$

$$= \frac{\frac{10}{k \ln 10} \alpha(10^k) - \frac{1}{(k-1)\ln 10} \alpha(10^{k-1})}{9}$$

$$= \frac{1}{k}\left[\underbrace{\frac{10}{\ln 10} \alpha(10^k)}_{1} - \underbrace{\frac{1}{\ln 10} \cdot \frac{k}{k-1}}_{1} \underbrace{\alpha(10^{k-1})}_{1}\right]$$

$$\simeq \frac{1}{k \ln 10}$$

4. variant on Caesar

$d(e(x)) = x$

$S_1\ S_2 \mid S_3\ S_4 \mid S_5\ S_6 \mid \ldots$

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

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

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

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

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

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

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

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

$ad-bc = 28-142 = -104 = -4\cdot 26 \Rightarrow$ not invertible in $\mathbb{Z}_{26}$

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

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

choice 3

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

---

Exercise sheet 6

1. Rings and non-rings

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

$f: 0 \to F$, $1 \to T$ $\quad (\mathbb{Z}_2, +, \cdot)$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

XOR	F	T
F	F	T
T	T	F

AND	F	T
F	F	F
T	F	T

$0 \rightsquigarrow F$
$1 \rightsquigarrow T$

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

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

OR	F	T
F	F	T
T	T	T

$a \in \{T, F\}$

F on $a = a \Rightarrow$ F is neutral

T on $a = T \Rightarrow$ T 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

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

$2\mathbb{Z} = \mathbb{Z} \Rightarrow 4k = \mathbb{Z} \Rightarrow \underbrace{2k}_{\in 2\mathbb{Z}} = \underbrace{1}_{\notin 2\mathbb{Z}}$

Hence, there is no neutral element.

(v) $(\{f : \mathbb{N} \to \mathbb{Z}\}, +, \cdot)$

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

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

Neutral $e : n \longmapsto 0$

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

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

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

Commutativity $f+g = g+f$

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

Associativity and Commutativity for $\cdot$ are done completely analogous.

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

$f : -f \Leftrightarrow \forall n \in \mathbb{N} \quad \underbrace{f(n) \cdot i(n)}_{1} = f(n) \Rightarrow$ ucr

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) $a^3 = 0$

$\Rightarrow a^2 \cdot a$ case 1 : $a^2 \neq 0 \Rightarrow a$ is a Zero Divisor ($\mathbb{Z}D$)

case 2 : $a^2 = 0 \Rightarrow a \cdot a = 0 \Rightarrow a$ is $\mathbb{Z}D$

(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?

$\Downarrow$

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

3. Group Homomorphisms

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

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 $(\mathbb{Z}_6, +)$

$(G, *)$ $f: G \to G$

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

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

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

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

$f(1) = b$

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

where f : $f(1) = 2$

$f(0) = 0$

$f(3) = f(1+1+1) = 2+2+2 = 0$

$\Rightarrow f$ 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

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

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

5)

$e(x,y) = (x,y)$
$a(x,y) = (-y,x)$
$b(x,y) = (-x,-y)$
$c(x,y) = (y,-x)$
$h(x,y) = (-x,y)$
$v(x,y) = (x,-y)$
$s(x,y) = (y,x)$
$t(x,y) = (-y,-x)$

$H = \{e, h\}$

$e \circ e = e$

$e \circ h = h$

$h \circ e = h$

$h \circ h = h$

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

aH $a \circ e = a$

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

tH $t \circ e = t$

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

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

bH $be = b$ bh $b(h(x,y)) = b(-x,y) = (x,-y) = v(x,y)$ } $bH = vH = \{v, b\}$

vH $ve = v$ $vh = b$

cH $ce = c$ ch $c(h(x,y)) = c(-x,y) = (y,x) = s(x,y)$ } $cH = sH = \{s, c\}$

sH $se = s$ $sh = c$

Exercise sheet 7

1) Long division in $\mathbb{Z}$

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

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

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

$a+1 = \underbrace{q}_{q'} b + \underbrace{r+1}_{r'}$

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

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

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

Case 2: $r = b-1$

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

$0 \leq r' < b$

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 $q \in \mathbb{Z}, r \in \{0, \dots, b-1\}$

s.t $-a = qb + r \Rightarrow a = -qb - r$

Case 1: $r = 0 \Rightarrow a = \underbrace{-q}_{-q \in \mathbb{Z}} b + 0$ $\hookrightarrow 0 \leq 0 < b$

Case 2: $r > 0$

$-r \in \{-(b-1), \dots, -1\}$

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

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

Hence, it also holds for the negative numbers.

2) Order of elements in cyclic group.

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

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.

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

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

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 $(\mathbb{Z}_{17}^{\times}, \cdot)$

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

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

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

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

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

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 $5^i \equiv q \bmod 17 \quad i = 0, \dots, 16$

$g^i \equiv h \bmod p$

$\lfloor \sqrt{p-1} \rfloor = \lfloor \sqrt{16} \rfloor = 4 \qquad i = \{0, \dots, p-1\}$

$i = s + 4t$

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

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

$h \cdot g^{-1t} \equiv g^s$

Incomplete solution

5) solving DLP

Exercise sheet 8

1) Finite field $\mathbb{Z}_2 / (\underbrace{t^3 + t^2 + 1}_{g(t)})$

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.

w.l.o.g $\deg(g_1) = 1$, $\deg(g_2) = 2$

$1 = g(0) = g_1(0) g_2(0)$ $\longrightarrow$ g_1 has no zero

$1 = g(1) = g_1(1) g_2(1)$ $\longrightarrow$ but g_1 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 $[a + bt + ct^2]_g$

There are 3 coefficients with two possible values ($\mathbb{Z}_2$) $\Rightarrow$ 8 elements

$f = t+1$
$x = [f]_g$
x^{2024}
$a + b\alpha + c\alpha^2$
$\alpha = [t]_g$
$a, b, c \in \mathbb{Z}_2$

$[t+1]_g^{2024}$
$F/\{0\}$ has 7 elements
$(F/\{0\}, \cdot)$ 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 $\quad$ 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 $f_1 - f_2 = q\cdot g$
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 $\phi([f_1]_g) = \phi([f_2]_g)$
$(f_1(1), f_1(-1))$ $\quad$ $(f_2(1), f_2(-1))$

$f_1(1) - f_2(1) = 0$
$f_1(-1) - f_2(-1) = 0$
$\Big\}$ $f_1 - f_2 = q(t-1)(t+1) = q(t^2-1) = qg \Rightarrow [f_1]_g = [f_2]_g$
$\Rightarrow$ injectivity

Surjectivity
Let $(Y_1, Y_2) \in T$ be given
We need F s.t
$f(1) = Y_1$, $f(-1) = Y_2$
$f(t) = Y_1\frac{t+1}{2} - Y_2\frac{t-1}{2}$

$f(1) = Y_1$
$f(-1) = Y_2$
$(t-1)(at+\alpha) = 1$

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

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

$f(t) = \sum_{i \in N_0} c_i t^i \in K[t]$

$f(A) = \sum_{i \in N_0} c_i A^i$

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

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

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

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

well-definedness

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

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

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

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

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

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

$\Rightarrow$ injectivity holds.

Surjectivity is clear.

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

$A^3 = 2A$

$A^4 = 4I$

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

w.o.l.g. $\begin{cases} S = \mathbb{Q}[t]/t^2-1 \\ T = \mathbb{Q}[t]/t^2-2t \end{cases}$ 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) $f(t) = \sum_{i=0}^{d} a_i t^i$ $d \in \mathbb{N}$, $a \in \mathbb{Z}$

$a_0, a_d \neq 0$

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

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

multiply with n^d gives

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

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

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

$a_d m^d \equiv 0 \bmod n$, $a_0 n^d \equiv 0 \bmod m$

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

2) GCD

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

$g(t) = (t^3-1)^{200}$ 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 $1^3-1=0 \Rightarrow 1$ is a root of g

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

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

$-t^2(t+1)$

$0t^3+t^2-1$

$-t(t-1)$

$0t^2+t-1$

t^2+t+1 has no rational roots

[in $\mathbb{C}$ the roots are $-\frac{1}{2} \pm \sqrt{-\frac{3}{4}}$ & $\mathbb{Q}$

$\Rightarrow t^2+t+1$ is irreducible

Now we compare the factorization and gcd

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

3) Finite field formula

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

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

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

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

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

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

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

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

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}?

$b = y_0 + y_1\alpha$

$$1 = ab = x_0y_0 + (x_0y_1 + x_1y_0)\alpha + x_1y_1\alpha^2$$
$$= x_0y_0 + (x_0y_1 + x_1y_0)\alpha + x_1y_1(\alpha+1)$$
$$= \underbrace{x_0y_0 + x_1y_1}_{1} + \underbrace{(x_0y_1 + x_1y_0 + x_1y_1)}_{0}\alpha$$

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

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

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

$$= \left(x_0^2 + x_0x_1 + x_1^2\right)^{-1} \begin{pmatrix} x_0+x_1 \\ +x_1 \end{pmatrix} \qquad \begin{matrix} 0^2 = 0 \\ 1^2 = 1 \end{matrix}$$

$$= \left(x_0 + x_0x_1 + x_1\right)^{-1} \begin{pmatrix} x_0+y_1 \\ x_1 \end{pmatrix}$$

By the idea

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

$|\mathbb{Z}_2[t]/(t^2+t+1)| = 4$ 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

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

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

$= x_0^2 + 2x_0x_1\alpha + x_1^2\alpha^2$

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

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

$[\ \alpha^2 \equiv -1\alpha - 1 \bmod g$

$\equiv +1\alpha + 1 \bmod g$

$= \alpha + 1\ ]$

5) Invertability 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?

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

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

$-t^2(t+1)$

$0t^3+t^2$

$-t(t+1)$

$0t^2+t$

$-1(t+1)$

$0t+0$

t^2+t+1 irreducible in question 4

$\gcd(g(t), t+1) = t+1 \neq 1 \Rightarrow$ Not invertible

$\gcd(g(t), t^2+t+1) = t^2+t+1 \neq 1 \Rightarrow$ Not invertible

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

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

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

t^3+t^2+t+1

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

$0t^2+0t+1$

$\gcd(g(t), t^4+t+1) = 1 \Rightarrow [t^4+t+1]_g$ 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

$q, 1+q, 3+q, 4+q, 5+q, 9+q \not\equiv 0 \bmod 11$

$\Downarrow$

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

$g(t) \not\equiv 0$ for $t \in \mathbb{Z}_{11}$

$\Downarrow$

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

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 $[t+1]_g^2, [t+1]_g^4 \neq [1]_g$

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

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

$[t]_g = \alpha$

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

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

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

$\Rightarrow g$ is a generator