Sifat Modulo

🔢 Sifat Dasar Modulo

Misal a≡bmod ma \equiv b \mod ma≡bmodm, maka berlaku:

1. **Penjumlahan:**
   a+c≡b+c mod ma + c \equiv b + c \mod ma+c≡b+cmodm
2. **Pengurangan:**
   a−c≡b−cmod ma - c \equiv b - c \mod ma−c≡b−cmodm
3. **Perkalian:**
   a⋅c≡b⋅cmod ma \cdot c \equiv b \cdot c \mod ma⋅c≡b⋅cmodm
4. **Pangkat (Eksponen):**
   an≡bnmod ma^n \equiv b^n \mod man≡bnmodm

🔁 Mod Operasi Langsung

- (amod m)+(bmod m)≡(a+b)mod m(a \mod m) + (b \mod m) \equiv (a + b) \mod m(amodm)+(bmodm)≡(a+b)modm

- (amod m)⋅(bmod m)≡(a⋅b)mod m(a \mod m) \cdot (b \mod m) \equiv (a \cdot b) \mod m(amodm)⋅(bmodm)≡(a⋅b)modm

---

📉 Modular Inverse (Invers Modulo)

Kalau a⋅x≡1mod ma \cdot x \equiv 1 \mod ma⋅x≡1modm, maka xxx disebut **invers modulo** dari aaa.

> Invers hanya ada jika gcd(a,m)=1\gcd(a, m) = 1gcd(a,m)=1

📚 Sifat Khusus

1. **Fermat's Little Theorem:** Jika ppp adalah bilangan prima dan a≢0mod pa \not\equiv 0 \mod pa≡0modp, maka:
   ap−1≡1mod pa^{p-1} \equiv 1 \mod pap−1≡1modp
2. **Euler's Theorem:** Jika gcd(a,m)=1\gcd(a, m) = 1gcd(a,m)=1, maka:
   aϕ(m)≡1mod ma^{\phi(m)} \equiv 1 \mod maϕ(m)≡1modm
   di mana ϕ(m)\phi(m)ϕ(m) adalah fungsi Euler (jumlah bilangan < m yang relatif prima terhadap m).

Mencari inverse multip step by step:

multiplicative inverse 683 utk GF(887)

gcd

$887=1\cdot 683+204$

$683=3\cdot 204+71$

$204=2\cdot 71+62$

$71=1\cdot 62+9$

$62=6\cdot 9+8$

$9=1\cdot 8+1$

$8=8\cdot 1+0$

extended euclidian (back sub)

$1=9-1\cdot 8$

$1=9-1(62-6\cdot 9)=9\text{-}1.62+6.9=7\cdot 9-1\cdot 62$

$1=7(71-1\cdot 62)-1\cdot 62=7\cdot 71-8\cdot 62$

$1=7\cdot 71-8(204-2\cdot 71)=23\cdot 71-8\cdot 204$

$1=23(683-3\cdot 204)-8\cdot 204=23\cdot 683-77\cdot 204$

$1=23\cdot 683-77(887-1\cdot 683)=100\cdot 683-77\cdot 887$

```
def extended_gcd(a, b):
    if b == 0:
        return a, 1, 0
    else:
        gcd, x1, y1 = extended_gcd(b, a % b)
        x = y1
        y = x1 - (a // b) * y1
        return gcd, x, y

def mod_inverse(a, m):
    gcd, x, _ = extended_gcd(a, m)
    if gcd != 1:
        return None
    else:
        return x % m
```

```python
a = 683
m = 887
inverse = mod_inverse(a, m)
print(f"Invers dari {a} modulo {m} adalah: {inverse}")
```

Tinjau GF(2^4) dengan m(x) = $x^4 + x + 1$.

Andaikan g adalah sebuah generator dari GF(2^4) tersebut. Representasi hexadesimal untuk g^{10} adalah ....

Select one:

- a. A
- b. 7
- c. 9 ✖
- d. F

Your answer is incorrect.

The correct answer is: 7

x^4+x+1 = 0
x^4=-(x+1)=x+1

g = x = 0010 = 2
g^2 = g*g = x^2 = 0100 = 4
g^3 = g^2*g = x^2*x = x^3 = 1000 = 8
g^4 = g^3*g = x^3*x = x^4 = x+1 = 0011 = 3
g^5 = g^4*g = (x+1)x = x^2+x = 0110 = 6
g^6 = g^5*g = (x^2+x)x = x^3+x^2 = 1100 = 12
g^7 = g^6*g = (x^3+x^2)x = x^4+x^3 = x^3+x+1 = 1011 = 11
g^8 = g^7*g = (x^3+x+1)x = x^4+x^2+x = x^2+2x+1 = x^2+1 = 0101 = 5
g^9 = g^8*g = (x^2+1)x = x^3+x = 1001 = 9
g^10 = g^9*g = (x^3+x)x = x^4+x^2 = x^2+x+1 = 0111 = 7

- Exercise: Find the last three digits of 7^{803}.

last 3 digits -> n mod 1000
7^803 = 7^400*2+3 = (7^400)^2 * 7^3
we know that 7^u(1000) === 1 mod 1000
7^400 === 1 mod 1000

(7^400)^2 === 1^2 mod 1000
(7^400)^2 * 7^3 === 1^2 * 7^3 mod 1000
= 343

Untuk data dalam notasi hex berikut:

ABABCDCDEFEF3388

padding menurut PKCS#5 agar menjadi 10 byte adalah ....

Select one:

- a. 01
- b. 030303
- c. 0202
- d. Tidak perlu padding. ✖

Your answer is incorrect.

The correct answer is: 0202

ABABCDCDEFEF3388

1 byte = 8 bit biner = 2 bit hex
AB AB CD CD EF EF 33 88 = 8 byte = kurang 2 byte
padding PKCS#5 nambahin byte sesuai jumlah byte yang kurang -> kurang 2 byte -> 02 (hex)
jadi padd 02 02

Tinjau GF(2^4) dengan m(x) = $x^4 + x + 1$.

Dalam representasi polinomial, hasil perkalian antara $x^3 + x$ dan $x^3 + 1$ adalah

Select one:

- a. $x^4 + x^3 + x$
- b. $x^3 + x + 1$
- c. $x^6 + x^4 + x^3 + x$ ✖
- d. $x^2 + 1$

Your answer is incorrect.

The correct answer is: $x^2 + 1$

x^4+x+1 = 0
x^4 = -(x+1) = x+1

$(x^3+x)(x^3+1) = x^6+x^4+x^3+x$
subs x^4
$x^6+x^4+x^3+x = x^6+x^3+2x+1 = x^6+x^3+1$
subs x^6
$x^6+x^3+1 = x^4*x^2+x^3+1 = (x+1)x^2+x^3+1 = x^3+x^2+x^3+1 = 2x^3+x^2+1 = x^2+1$