FINITE FIELDS

--Dr. Mike Yuliana--

Mata Kuliah : Keamanan Jaringan

Politeknik Elektronika Negeri Surabaya (PENS)

Outline

- Aritmatika Modular
- Algoritma Euclidian
- Multiplicative inverse
- Polinomial Aritmatika

Aritmatika Modular

Jika a adalah integer dan n adalah integer positif , maka $a \ mod \ n$ akan menjadi sisa jika a dibagi dengan n

$a = \lfloor a/n \rfloor \times n + (a \bmod n)$

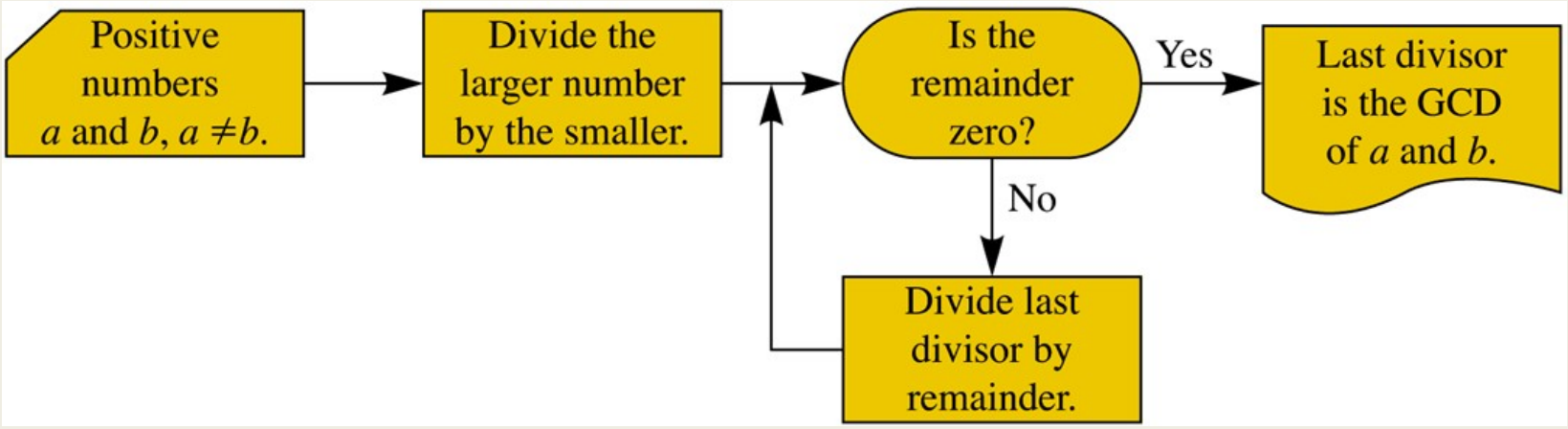
11 mod 7 = 4;	-11 mod 7 = 3

$a = 11;$	$n = 7;$	$11 = 1 \times 7 + 4;$	$r = 4$	$q = 1$
$a = -11;$	$n = 7;$	$-11 = (-2) \times 7 + 3;$	$r = 3$	$q = -2$

Dua integer a dan b dikatakan kongruen modulo n, jika $a \ mod \ n = b \ mod \ n$. Hal ini bisa ditulis sebagai $a \equiv b \ mod \ n$

$73 \equiv 4 \ (mod \ 23);$	$21 \equiv -9 \ (mod \ 10)$

Algoritma Euclidian (1)



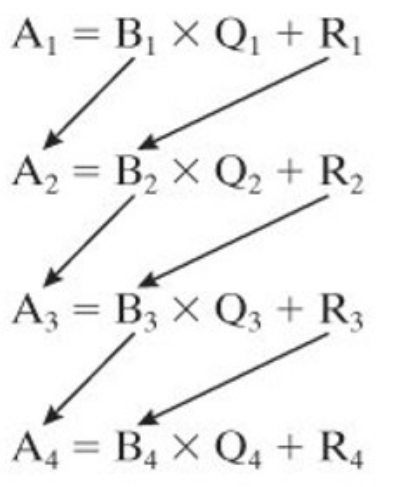
Algoritma ini mengasumsikan $a > b > 0$ sehingga $\gcd(a, b) = \gcd(|a|, |b|)$

Algoritma Euclidian:

```
EUCLID(a, b)
1.   A ← a; B ← b
2.   if B = 0  return  A = gcd(a, b)
3.   R = A mod B
4.   A ← B
5.   B ← R
6.   goto 2
```

Algoritma Euclidian (2)

Detil cara kerja Algoritma :



To find gcd(1970, 1066)		
1970	= 1 x 1066 + 904	gcd(1066, 904)
1066	= 1 x 904 + 162	gcd(904, 162)
904	= 5 x 162 + 94	gcd(162, 94)
162	= 1 x 94 + 68	gcd(94, 68)
94	= 1 x 68 + 26	gcd(68, 26)
68	= 2 x 26 + 16	gcd(26, 16)
26	= 1 x 16 + 10	gcd(16, 10)
16	= 1 x 10 + 6	gcd(10, 6)
10	= 1 x 6 + 4	gcd(6, 4)
6	= 1 x 4 + 2	gcd(4, 2)
4	= 2 x 2 + 0	gcd(2, 0)
Therefore, gcd(1970, 1066) = 2		

Algoritma Euclidian (3)

Tentukan :

1. gcd(24140, 16762)
2. gcd(4655, 12075)

H1

Multiplicative Inverse (1)

Algoritma extended Euclidian:

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3) ← (1, 0, m); (B1, B2, B3) ← (0, 1, b)
2. if B3 = 0 return A3 = gcd(m, b); no inverse
3. if B3 = 1 return B3 = gcd(m, b); B2 = b^1 mod m
```

4. $Q = \left\lfloor \frac{A3}{B3} \right\rfloor$

```
5. (T1, T2, T3) ← (A1  QB1, A2  QB2, A3  QB3)
6. (A1, A2, A3) ← (B1, B2, B3)
7. (B1, B2, B3) ← (T1, T2, T3)
8. goto 2
```

➡ Mencari multiplicative inverse di GF (p)

Hitunglah gcd (1759,550)

Q	A1	A2	A3	B1	B2	B3
	1	0	1759	0	1	550
3	0	1	550	1	3	109
5	1	3	109	5	16	5
21	5	16	5	106	339	4
1	106	339	4	111	355	1

Slide 7

H1 HP, 15/03/2020

H1

Aritmatika Polinomial (1)

$$\begin{array}{l} x^3 + x^2 \quad\quad + 2 \\ +\ (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

penambahan

$$\begin{array}{l} x^3 + x^2 \quad\quad + 2 \\ -\ (x^2 - x + 1) \\ \hline x^3 \quad\quad + x + 1 \end{array}$$

pengurangan

$$\begin{array}{r} x^3 + x^2 \quad\quad + 2 \\ \times\ (x^2 - x + 1) \\ \hline x^3 + x^2 \quad\quad + 2 \\ -x^4 - x^3 \quad\quad - 2x \\ x^5 + x^4 \quad\quad + 2x^2 \\ \hline x^5 \quad\quad + 3x^2 - 2x + 2 \end{array}$$

perkalian

$$\begin{array}{r|l} & x + 2 \\ \hline x^2 - x + 1 & x^3 + x^2 \quad\quad + 2 \\ & x^3 - x^2 + x \\ \hline & 2x^2 - x + 2 \\ & 2x^2 - 2x + 2 \\ \hline & x \end{array}$$

pembagian

Slide 8

H1 HP, 15/03/2020

Aritmatika Polinomial (2)

$$
\begin{array}{l}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\quad + (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}
$$

penambahan

$$
\begin{array}{l}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\quad - (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}
$$

pengurangan

$$
\begin{array}{l}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\quad \times (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 + x^3 + x + 1 \\
x^8 + x^6 + x^5 + x^4 + x^2 + x \\
x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\
\hline
x^{10} + x^4 + x^2 + 1
\end{array}
$$

perkalian

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\cline{2-2}
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
\end{array}
$$

pembagian

Aritmatika Polinomial (3)

Polinomial $f(x) = x^4 + 1$ di GF (2) adalah reducible karena $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$

$$
\begin{array}{r}
x^2 + x \\
x + 1 \overline{)\, x^3 \quad + x + 1} \\
\underline{x^3 + x^2} \\
x^2 + x \\
\underline{x^2 + x} \\
1
\end{array}
$$

⇨ irreducible

Algoritma Euclidian untuk Polinomial (1)

```
EUCLID[a(x), b(x)]
1. A(x) ← a(x); B(x) ← b(x)
2. if B(x) = 0 return A(x) = gcd[a(x), b(x)]
3. R(x) = A(x) mod B(x)
4. A(x) ← B(x)
5. B(x) ← R(x)
6. goto 2
```

Soal :

Carilah gcd [a(x),b(x)] untuk $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ dan $b(x) = x^4 + x^2 + x + 1$

A(x) = a(x); B(x) = b(x)

$$
\begin{array}{r}
x^2 + x \\
x^4 + x^2 + x + 1 \overline{)\, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\underline{x^6 \quad + x^4 + x^3 + x^2} \\
x^5 \quad + x + 1 \\
\underline{x^5 \quad + x^3 + x^2 + x} \\
x^3 + x^2 \quad + 1
\end{array}
$$

Algoritma Euclidian untuk Polinomial (2)

$R(x) = A(x) \bmod B(x) = x^3 + x^2 + 1$

$A(x) = x^4 + x^2 + x + 1$; $B(x) = x^3 + x^2 + 1$

$$
\begin{array}{r}
x + 1 \\
x^3 + x^2 + 1 \overline{)\, x^4 + x^2 + x + 1} \\
\underline{x^4 + x^3 \quad + x} \\
x^3 + x^2 + 1 \\
\underline{x^3 + x^2 + 1} \\
0
\end{array}
$$

$R(x) = A(x) \bmod B(x) = 0$

$\gcd[a(x), b(x)] = A(x) = x^3 + x^2 + 1$

Algoritma Euclidian untuk Polinomial (3)

<u>Tentukan :</u>

gcd dari polynomial $x^3 + x + 1$ dan $x^2 + x + 1$ di GF (2)

Multiplicative inverse (1)

Algoritma extended Euclidian algorithm untuk Polinomial Aritmatika

```
EXTENDED EUCLID[m(x), b(x)]
1. [A1(x), A2(x), A3(x)] ← [1, 0, m(x)]; [B1(x), B2(x),
   B3(x)] ← [0, 1, b(x)]
2. if B3(x) = 0   return  A3(x) = gcd[m(x), b(x)]; no
   inverse
3. if B3(x) = 1   return  B3(x) = gcd[m(x), b(x)];
   B2(x) = b(x)^1 mod m(x)
```

```
4. Q(x) = quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)] ← [A1(x)  Q(x)B1(x), A2(x)
   Q(x)B2(x), A3(x)  QB3(x)]
6. [A1(x), A2(x), A3(x)] ← [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)] ← [T1(x), T2(x), T3(x)]
8. goto 2
```

Multiplicative inverse (2)

Soal :
Tentukan multiplicative inverse dari (x^7+x+1) mod ($x^8 + x^4 + x^3 + x + 1$)

Initialization	A1(x) = 1; A2(x) = 0; A3(x) = $x^8 + x^4 + x^3 + x + 1$ B1(x) = 0; B2(x) = 1; B3(x) = $x^7 + x + 1$
Iteration 1	Q(x) = x A1(x) = 0; A2(x) = 1; A3(x) = $x^7 + x + 1$ B1(x) = 1; B2(x) = x; B3(x) = $x^4 + x^3 + x^2 + 1$
Iteration 2	Q(x) = $x^3 + x^2 + 1$ A1(x) = 1; A2(x) = x; A3(x) = $x^4 + x^3 + x^2 + 1$ B1(x) = $x^3 + x^2 + 1$; B2(x) = $x^4 + x^3 + x + 1$; B3(x) = x
Iteration 3	Q(x) = $x^3 + x^2 + x$ A1(x) = $x^3 + x^2 + 1$; A2(x) = $x^4 + x^3 + x + 1$; A3(x) = x B1(x) = $x^6 + x^2 + x + 1$; B2(x) = x^7; B3(x) = 1
Iteration 4	B3(x) = gcd[($x^7 + x + 1$), ($x^8 + x^4 + x^3 + x + 1$)] = 1 B2(x) = $(x^7 + x + 1)^1$ mod ($x^8 + x^4 + x^3 + x + 1$) = x^7