

## FUNGSI BALIKAN MODULO (invers modulo)

Terorema modular atau sisa pembagia adalah sebagai berikut :

Jika  $a$  adalah suatu bilangan dalam  $Z_m$  maka bilangan  $a^{-1}$  dalam  $Z_m$  disebut balikan atau invers perkalian dari  $a$  modulo  $m$  jika  $a a^{-1} = a^{-1} a = 1 \pmod{m}$

Dapat dibuktikan bahwa jika  $a$  dan  $m$  **tidak mempunyai faktor prima bersama**, maka  $a$  mempunyai balikan modulo  $m$  unik.

Sebaliknya jika  $a$  dan  $m$  mempunyai faktor prima bersama maka  $a$  tidak mempunyai balikan modulo  $m$ .

### Source Code (Pascal / Delphi)

```
function bilanganPrima(i: integer):boolean;
var k : integer;
    prima : boolean;
begin
    prima := true;
    for k:=2 to (i div 2) do
        if (i mod k = 0) then
            begin
                prima := false;
                break;
            end;

    bilanganPrima := prima;
end;
```

```
function bukanFaktorPrimaBersama(a,m : integer): boolean;
var i, batas : integer;
    ada : boolean;
begin
    ada := false;

    if a <= m then batas := a
    else batas := m;

    for i:=1 to batas do
        if bilanganPrima(i) then
            if (a mod i = 0) and (m mod i = 0) then
                begin
                    ada := true;
                    break;
                end;

    bukanFaktorPrimaBersama := ada;
end;
```

```
function balikanModulo(a,m : integer): integer;
var i, aI : integer;
begin
  aI := 0;
  if bukanFaktorPrimaBersama(a,m) then
    for i:=1 to m do
      if (a*i) mod m = 1 then
        begin
          aI := i;
          break;
        end;
    end;

  balikanModulo := aI;
end;
```

*Ditulis oleh* : **Mahendra Data**

*Referensi* :  
Penerapan Aljabar Linier (Elementary Linier Algebra With Applications),  
AntonTextbooks, Inc