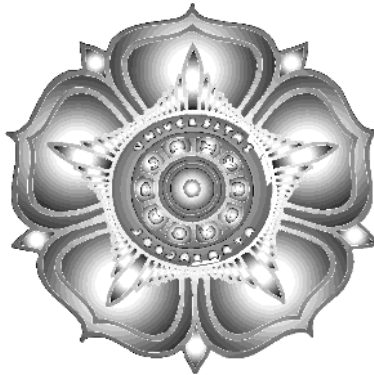


TUGAS MATAKULIAH KRIPTOGRAFI

**PROGRAM Mencari Invers Perkalian Modulo  $n$   
Menggunakan Perluasan Algoritma Euclid  
(Extended Euclid Algorithm)**



DOSEN:  
Dra. Diah Junia Eksi Palupi, M.S

DISUSUN OLEH :  
Hedri Wahyudi  
(07/259575/PPA/2248)

**PROGRAM S2 MAGISTER ILMU KOMPUTER  
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS GADJAH MADA  
YOGYAKARTA  
2008**

# TUGAS KRIPTOGRAFI

## PROGRAM INVERS PERKALIAN BILANGAN MODULO $n$ MENGUNAKAN PERLUASAN ALGORITMA EUCLID

---

### A. Permasalahan

Salah satu sifat dari operasi perkalian bilangan modulo, yaitu : misalkan  $\bar{a} \in \mathbb{Z}_n$ , jika  $(\bar{a}, n) = 1$  maka  $\forall \bar{a}$  memiliki invers perkalian yaitu  $(\bar{a})' \in \mathbb{Z}_n$  sehingga

$$\bar{a} \times (\bar{a})' = (\bar{a})' \times \bar{a} = \bar{e}.$$

$\bar{e}$  merupakan identitas dalam operasi perkalian bilangan modulo  $n$ . Buatlah program untuk mencari invers perkalian bilangan modulo  $n$  menggunakan Perluasan Algoritma Euclid (Extended Euclid Algorithm). Program meminta masukan (input) berupa : dua bilangan bulat yaitu bilangan modulo  $n$  dan bilangan  $a$  anggota bilangan modulo  $n$ . Hasil (output) program adalah invers perkalian dari  $a$  dalam modulo  $n$ .

### B. Analisis

Berdasarkan permasalahan yang dikemukakan tersebut diatas, dilakukan analisis permasalahan. Hasil analisis tersebut adalah sebagai berikut :

1. Program menggunakan bahasa pascal.
2. Data yang dimasukkan (input) adalah berupa angka. Angka yang dimasukkan adalah dua buah bilangan bulat.
3. Setiap anggota bilangan modulo  $n$  selain 0 (nol), memiliki invers jika  $n$  merupakan bilangan prima.
4. Jika  $n$  tidak prima, anggota bilangan modulo  $n$  yang memiliki invers perkalian adalah bilangan-bilangan yang relatif prima dengan  $n$ .
5. Untuk menguji kerelatifprimaan kedua bilangan bulat yang dimasukkan, dilakukan dengan mencari nilai pembagi bersama terbesar kedua bilangan tersebut menggunakan Algoritma Euclid. Jika pembagi bersama terbesar kedua bilangan adalah 1 maka kedua bilangan tersebut relatif prima. Jika pembagi bersama terbesar dari kedua bilangan tidak sama dengan 1 maka kedua bilangan tidak relatif prima.

6. Untuk memperoleh nilai invers perkalian bilangan  $a$  dalam modulo  $n$  dilakukan menggunakan Algoritma Euclid yang diper luas (Extended Euclid Algorithm).

### C. Desain Program

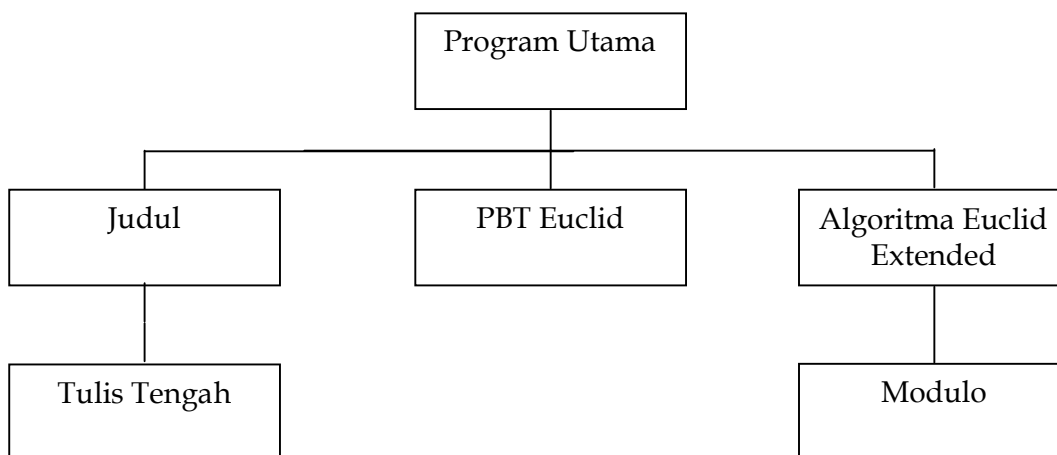
#### C. 1. Struktur Program

Pada program yang dibuat terdapat beberapa modul. Pada *Tabel Modul Program* dibawah diterangkan nama modul, fungsi dan bentuk implementasinya :

*Tabel Modul Program*

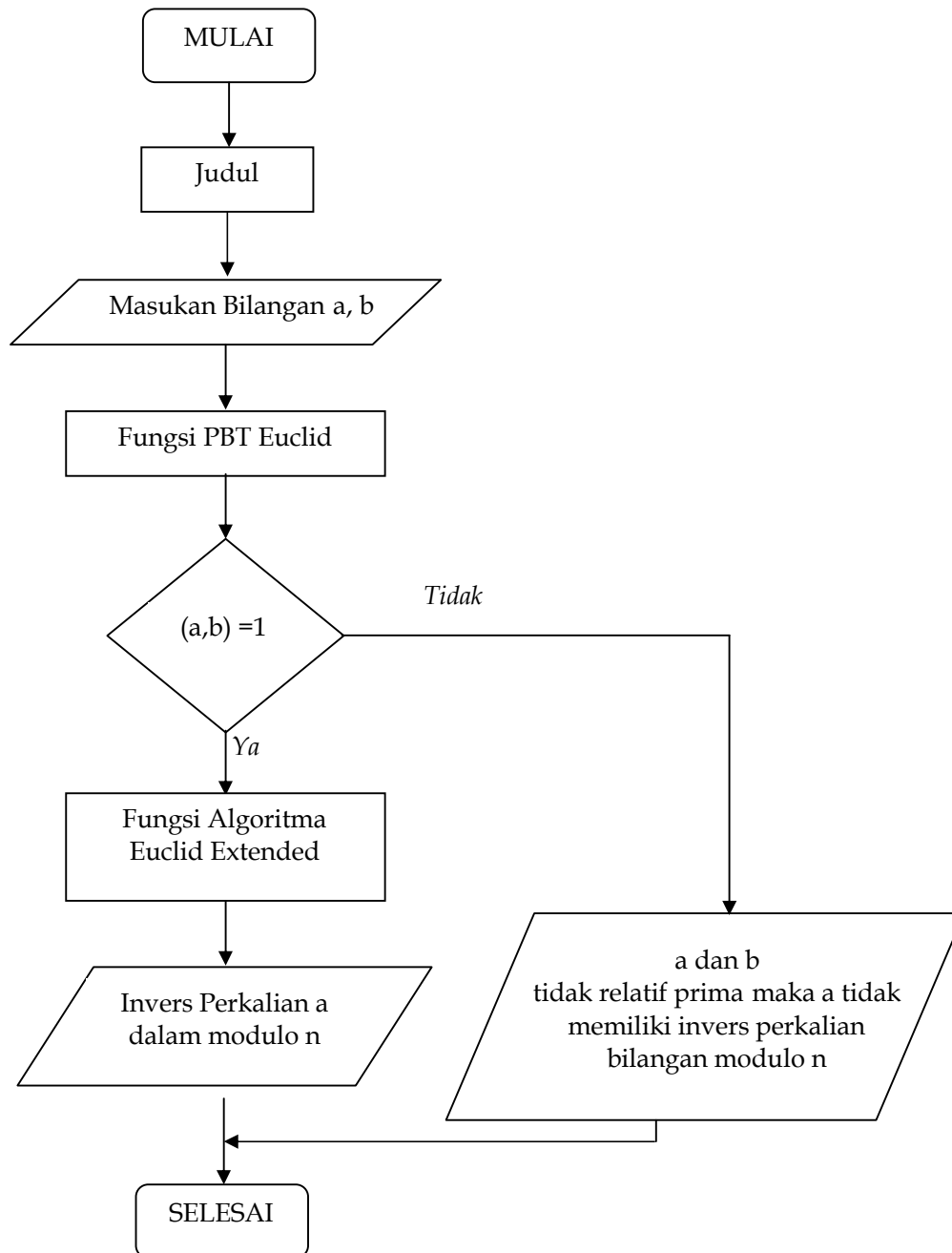
No	Nama Modul	Fungsi	Bentuk Implementasi
1	Judul	Menuliskan judul program	Prosedur
2	Tulis Tengah	Menuliskan sebuah string pada posisi tengah secara horisontal	Prosedur
3	PBT Euclid	Mencari nilai pembagi bersama terbesar menggunakan Algoritma Euclid	Fungsi
4	Modulo	Mencari nilai modulo $n$	Fungsi
5	Algoritma Euclid Extended	Mencari invers perkalian bilangan modulo $n$ menggunakan Perluasan Algoritma Euclid	Fungsi

Struktur program dapat digambarkan sebagai berikut:



*Gambar 1 Struktur Modul*

## C. 2. Algoritma



*Gambar 1. Algoritma Program*

## D. Kode Program

```
1  {
2  Nama Program      : PROGRAM INVERS PERKALIAN MODULO N MENGGUNAKAN PERLUASAN
3                    ALGORITMA EUCLID
4  Nama File        : aleuclid.pas
5  Tanggal Dibuat   : 26 April 2008
6  Pembuat          : Hedri Wahyuudi
7  Deskripsi        : Program ini meminta input berupa nilai n (modulo)
8                    dan bilangan dalam modulo n yang akan dicari invers
9                    perkaliannya. Selanjutnya Program akan memberikan output
10                   berupa bilangan yang menjadi inversnya
11
12 }
13
14 Program PerluasanAlgoritmaEuclid;
15 uses wincrt;
16 var a, b : integer;
17     lagi : char;
18
19
20 {PROSEDUR UNTUK MENULIS STRING DI TENGAH WINDOW}
21 Procedure Tulistengah(x,y:byte;kata:string);
22 begin
23     x := (80-length(kata)) div 2;
24     gotoxy(x,y);
25     write(kata);
26 end;
27
28 {PROSEDUR MENULIS JUDUL}
29 Procedure Judul;
30 begin
31     tulistengah(0, 2, '+=====+' );
32     tulistengah(0, 3, '|                                     |');
33     tulistengah(0, 4, '|                                     |');
34     tulistengah(0, 5, '|                                     |');
35     tulistengah(0, 6, '|-----|');
36     tulistengah(0, 7, '|                                     |');
37     tulistengah(0, 8, '|                                     |');
38     tulistengah(0, 9, '|                                     |');
39     tulistengah(0,10, '|                                     |');
40     tulistengah(0,11, '|                                     |');
41     tulistengah(0,12, '|                                     |');
42     tulistengah(0,13, '|                                     |');
43     tulistengah(0,14, '+=====+' );
44     tulistengah(0, 4, 'PROGRAM Mencari Invers Perkalian Modulo N');
45     tulistengah(0,5, 'MENGUNAKAN PERLUASAN ALGORITMA EUCLID');
46     tulistengah(0, 8, 'TUGAS MATA KULIAH KRIPTOGRAFI');
47     tulistengah(0,10, 'DISUSUN OLEH');
48     tulistengah(0,10, 'HEDRI WAHYUDI');
49     tulistengah(0,12, '(07/259575/PPA/2248)');
50     tulistengah(0,16, '<< Tekan Enter >>');
51     readln;
52     clrscr;
53 end;
54
55
56 {FUNGSI UNTUK Mencari Nilai Pembagi Bersama Terbesar Menggunakan Algoritma
57 EUCLID}
58 Function PBTEuclid (a,b : integer):integer;
59 var R, Q : array [0..10] of integer;
60     m     : integer;
61 begin
62     R[0]:=a;
```

```

63     R[1]:=b;
64     m:=1;
65     while R[m]<>0 do
66     begin
67         Q[m]:=R[m-1] div R[m];
68         R[m+1]:=R[m-1] - Q[m] * R[m];
69         m:= m + 1;
70     end;
71     m:= m - 1;
72     PBTEuclid:=R[m];
73 end;
74
75
76 {FUNGSI UNTUK MENCARI NILAI A MODULO N}
77 Function Modulo (a, e : integer): integer;
78 var b, c, d : integer;
79 begin
80     if a < 0 then
81     begin
82         a:=abs(a);
83         c:=a div e;
84         c:=c+1;
85         d:=c * e;
86         b:= d - abs(a);
87     end
88     else b:= a mod e;
89     Modulo:=b;
90 end;
91
92 {FUNGSI UNTUK MENCARI INVERS PERKALIAN MODULO N MENGGUNAKAN PERLUASAN
93 ALGORITMA EUCLID}
94 Function AlgoritmaEuclidExtended (y,x:integer):integer;
95 var r, q, t, temp : integer;
96     A, B, C      : array [0..10] of integer;
97 begin
98     A[0]:=x;
99     B[0]:=y;
100    C[0]:=0;
101    t  :=1;
102    q  := A[0] div B[0];
103    r  := A[0] - q * B[0];
104    while r > 0 do
105    begin
106        temp:=C[0] - q * t;
107        temp:= Modulo (temp,x);
108        C[0]:=t;
109        t:=temp;
110        A[0]:=B[0];
111        B[0]:=r;
112        q:= A[0] div B[0];
113        r:=A[0] - q * B[0];
114    end;
115    AlgoritmaEuclidExtended:=t;
116 end;
117
118 {-----PROGRAM UTAMA-----}
119 begin
120     judul;
121     lagi:='Y';
122     repeat
123     clrscr;
124     gotoxy (13,5);
125     write ('Masukkan Bilangan Bulat Yang Akan Dicari Inversnya: ');
126     readln (b);
127     gotoxy (18, 7);write ('Invers ', b, ' dalam Bilangan Modulo Berapa ? ');

```

```

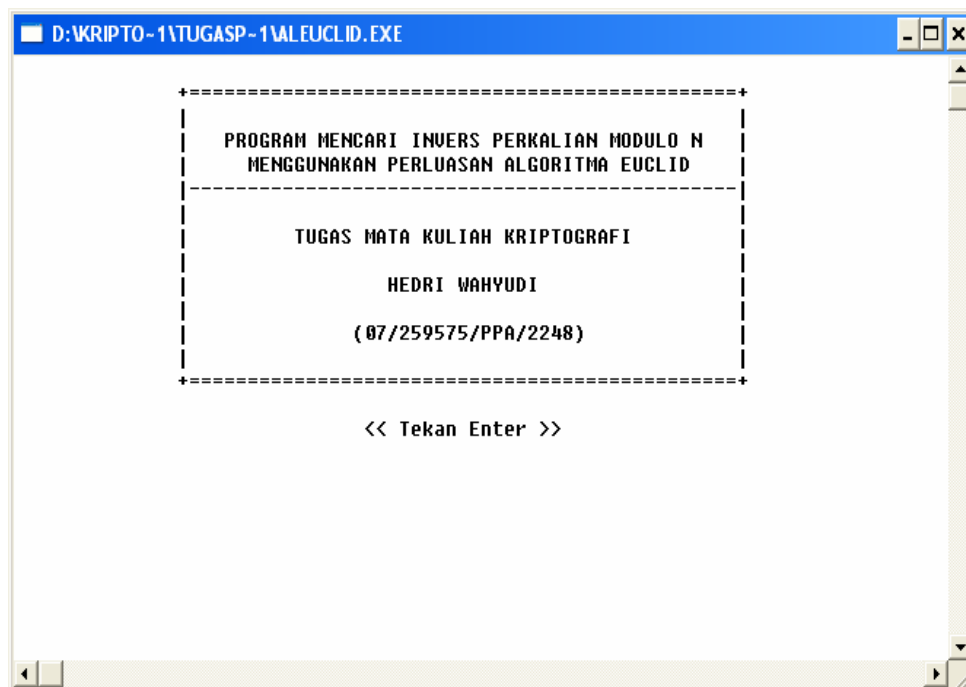
128     readln (a);
129     if (PBTEuclid(b,a)<>1) then
130     begin
131         gotoxy (23, 10);
132         write (b, ' dan ', a, ' tidak relatif prima, maka');
133         gotoxy (16, 12);
134         write ( b,' tidak memiliki invers dalam bilangan modulo ', a);
135     end
136     else
137     begin
138         gotoxy (19, 10);
139         writeln ('Invers ', b,' dalam bilangan modulo ', a, ' adalah ',
140             AlgoritmaEuclidExtended(b, a));
141     end;
142     gotoxy (31,15); write ('Coba Lagi [Y/T] ?'); readln (lagi);
143     lagi:=upcase(lagi);
144     until (lagi='T');
145     clrscr;
146 end.
147
148 {-----AKHIR PROGRAM UTAMA-----}
149

```

### E. Hasil Program

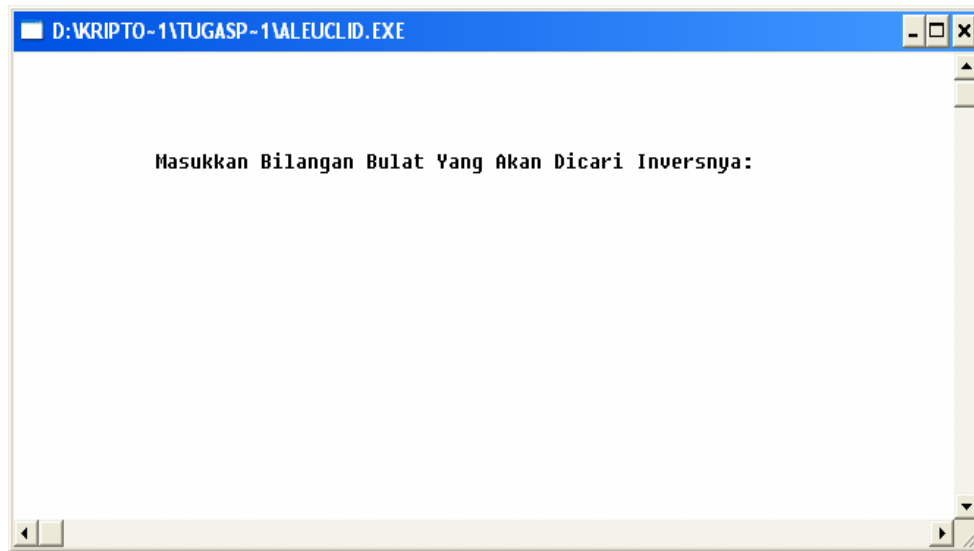
Contoh output program :

1. Setelah program mulai dijalankan akan muncul tampilan awal program seperti gambar 2.



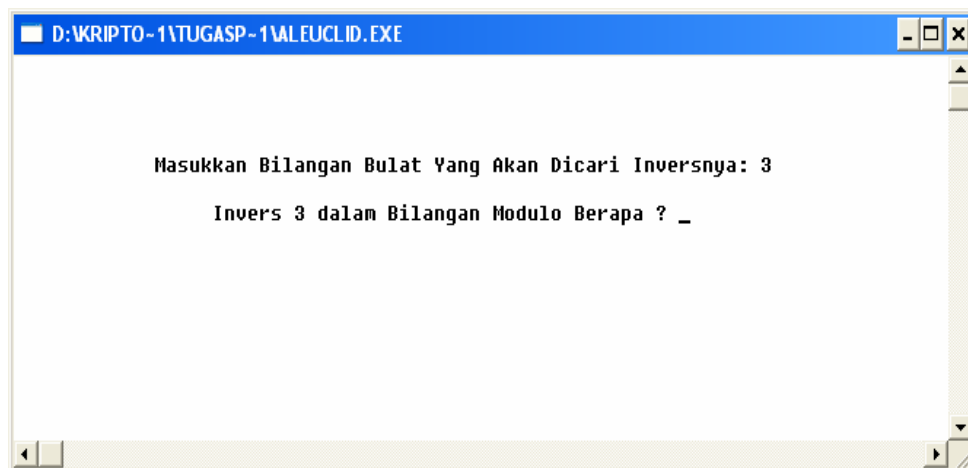
*Gambar 2. Tampilan Awal Program*

- Setelah menekan tombol keyboard akan muncul tampilan seperti gambar 3.

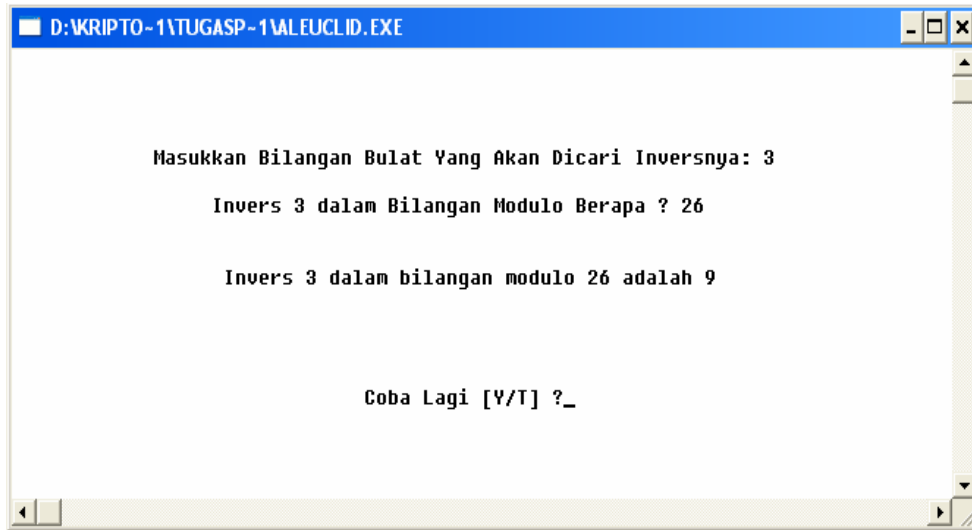


*Gambar 3. Menu Input Bilangan*

- Misalkan kita ingin mencari invers perkalian dari 3 dalam bilangan modulo 26. Saat program ditampilkan seperti pada gambar 2, masukkan angka 3 dengan menekan tombol angka 3 pada keyboard. Selanjutnya program akan tampil seperti gambar 4. Masukkan angka 26 dengan menekan tombol angka 2, lalu tombol dan angka 6 pada keyboard. Setelah menekan tombol enter, Hasil program akan tampil seperti gambar 5.

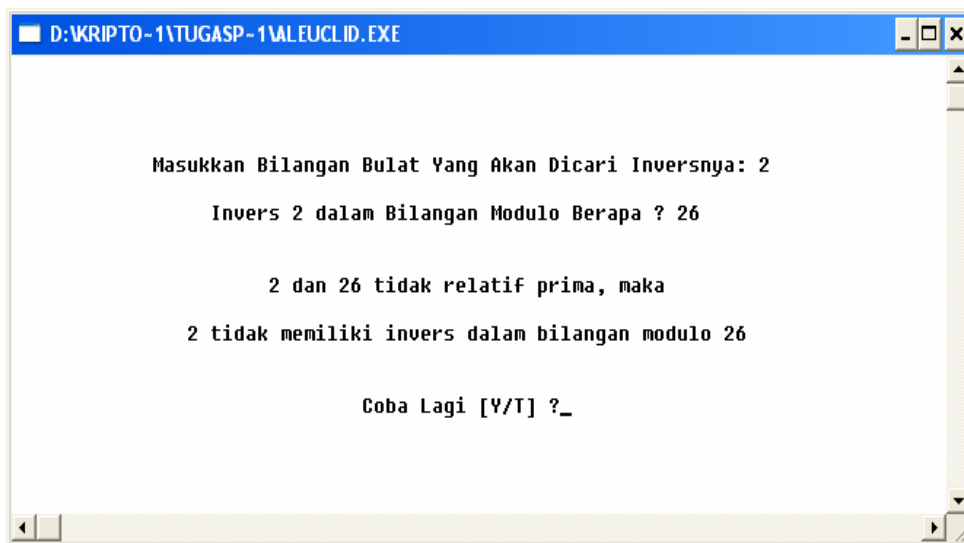


*Gambar 4. Menu Input Bilangan Modulo*



*Gambar 5. Tampilan hasil program*

4. Jika kita ingin mencari invers perkalian bilangan lainnya, saat program tampil seperti pada gambar 5, tekan tombol huruf 'Y' atau 'y' pada keyboard, lalu tekan tombol enter. Misalkan kita ingin mencari invers perkalian 2 pada bilangan modulo 26. Lakukan seperti langkah 3. Hasil program akan tampil seperti gambar 6. Pada gambar tersebut akan terlihat tampilan program jika bilangan yang ingin kita cari inversnya ternyata tidak memiliki invers perkalian.



*Gambar 6. Tampilan hasil program*

5. Jika anda ingin mengakhiri program, pada saat program tampil seperti pada gambar 5 atau gambar 6, tekan tombol huruf 'T' atau 't' pada keyboard.

----- ηεδρι ωαηψυδι -----