Assignment 1 Question 4

Part (a)

```
> EEA := proc(A,B)
  local r,s,t,k,q;
     r[0] := A;
     r[1] := B;
     s[0] := 1; s[1] := 0;
     t[0] := 0; t[1] := 1;
     printf("%6s %8s %8s %8s %8s \n","k","r[k]","q[k]","s[k]","t[k]");
     printf("%6d %8d %8s %8d %8d \n",0,r[0],"",s[0],t[0]);
     printf("%6d %8d %8s %8d %8d \n",1,r[1],"",s[1],t[1]);
     for k from 1 while r[k] <> 0 do
        q := iquo(r[k-1],r[k]);
        r[k+1] := r[k-1]-q*r[k];
        s[k+1] := s[k-1]-q*s[k];
        t[k+1] := t[k-1]-q*t[k];
        printf("%6d %8d %8d %8d %8d\n",k+1, r[k+1],q,s[k+1],t[k+1]);
     od; printf("\n");
     r[k-1],s[k-1],t[k-1];
  end:
> EEA(99,28);
```

k	r[k]	q[k]	s[k]	t[k]
0	99		1	0
1	28		0	1
2	15	3	1	-3
3	13	1	-1	4
4	2	1	2	-7
5	1	6	-13	46
6	0	2	28	-99

$$1, -13, 46$$

Hence the gcd(m,u) = $r_5 = 1$ and the inverse of u is t_5 = 46.

Part (b)

In Maple mods(a,b) returns the remainder in the symmetric representation

```
> seq( mods(a,8), a=0..7 );
```

$$0, 1, 2, 3, 4, -3, -2, -1$$

So if a = b q + r and we know r we can compute q = (a-r)/b .

```
> EEA := proc(A,B)
  local r,s,t,k,q;
     r[0] := A;
     r[1] := B;
     s[0] := 1; s[1] := 0;
     t[0] := 0; t[1] := 1;
     printf("%6s %8s %8s %8s %8s \n","k","r[k]","q[k]","s[k]","t[k]");
```

```
    printf("%6d %8d %8s %8d %8d \n",0,r[0],"",s[0],t[0]);
    printf("%6d %8d %8s %8d %8d \n",1,r[1],"",s[1],t[1]);
    for k from 1 while r[k] <> 0 do
       r[k+1] := mods(r[k-1],r[k]);
# Maple uses [-2,+3] for mods(x,6) and I asked you to use [-3,+2] so
I need to fix this
       if( r[k+1]=r[k]/2 ) then r[k+1] := -r[k+1] fi;
       q := iquo(r[k-1]-r[k+1],r[k]);
       s[k+1] := s[k-1]-q*s[k];
       t[k+1] := t[k-1]-q*t[k];
       printf("%6d %8d %8d %8d %8d\n",k+1,r[k+1],q,s[k+1],t[k+1]);
    od;
    printf("\n");
    r[k-1],s[k-1],t[k-1];
end:
> EEA(99,28);

     k     r[k]     q[k]     s[k]     t[k]
     0       99                1        0
     1       28                0        1
     2      -13        4       1       -4
     3        2       -2       2       -7
     4       -1       -6      13      -46
     5        0       -2      28      -99

                                  -1, 13, -46
```

The inverse of u is $t_4 + m = -53 + 99 = 46$. The difference is that by using the symmetric remainder, the Euclidean algorithm takes fewer steps.