

1

art;maple\_mode(0);cas\_setup(0,0,0,1,0,1e-10,10,[1,50,0,25],0,0,0); //radians,pas de cmplx, pas de Sqrt

M

2

-----Exercice-----

3

4

n:=nextprime(10^13)\*nextprime(12^14)\*nextprime(10^7);

128392090399872015023007768767867561

M

5

6

Prog Edit Add

1

nxt

OK (F9)

Save

```

rabmil1:proc(n)
local m,j0,a,b,retour;
//retour vaut 0 si l'on ne sait pas si n est premier.
//retour=1 implique que l'on est sur que n n'est pas premier.
retour:=0;
j0:=0;m:=n-1;a:=2;
while(irem(m,2)==0){m:=m/2;j0++;}
b:=powmod(a,m,n);j:=0;
while((irem((b-1)*(b+1),n) <> 0)and j<j0){b:=irem(b*b,n);j++;};
if (b==1 and j>0)then retour:=1;
    else if (j==j0) then retour:=1; fi;
fi;

retour;
end;

```

// Warning: j, declared as global variable(s)

// End defining rabmil1

```

(n)->
{ local m,j0,a,b,retour;
retour:=0;
j0:=0;
m:=n-1;
a:=2;
while(((irem(m,2))==0)){
    m:=m/2;
    j0++;
};
b:=powmod(a,m,n);
j:=0;
while((((irem((b-1)*(b+1),n))!=0) && (j<j0))){
    b:=irem(b*b,n);
    j++;
};
if (((b==1) && (j>0))) {

```

8	Prog	Edit	Add	1	nxt	OK (F9)	Save
---	------	------	-----	---	-----	---------	------

```

rabmil2:=proc(n)
local m,j0,a,b,retour;
//retour vaut 0 si l'on ne sait pas si n est premier.
//retour=1 implique que l'on est sur que n n'est pas premier.
retour:=0;
j0:=0;m:=n-1;a:=2 % n;
while(irem(m,2)==0){m:=m/2;j0++;};
b:=a^m;j:=0;
while((b != 1 % n) and (b!=-1 % n) and j<j0){b:=(b*b);j++;};
if (b==1 % n and j>0)then retour:=1;
else if (j==j0) then retour:=1; fi;
fi;
retour;
end;

// End defining rabmil2

```

9							
---	--	--	--	--	--	--	--

```

(n)->
{ local m,j0,a,b,retour;
retour:=0;
j0:=0;
m:=n-1;
a:=2 % n;
while(((irem(m,2))==0)){
m:=m/2;
j0++;
};
b:=a^m;
j:=0;
while((((b!=(1 % n)) && (b!=((-1) % n)))) && (j<j0)){
b:=b*b;
j++;
};
if (((b==(1 % n)) && (j>0))) {
retour:=1;
}
else {
if ((j==j0)) {
retour:=1;
}
}
}

```

10	Prog	Edit	Add	1	nxt	OK (F9)	Save
----	------	------	-----	---	-----	---------	------

```

testa:=proc(n)
local m,j0,a,b,retour;
//retour vaut 0 si l'on ne sait pas si n est premier.
//retour=1 implique que l'on est sur que n n'est pas premier.
retour:=0;
j0:=0;m:=n-1;
while(irem(m,2)==0){m:=m/2;j0++;};
l:=[ ];
for(a:=2;a<n;a++)
{
retour:=0;
b:=(a % n )^m;j:=0;
while((b != 1 % n) and (b!=-1 % n) and j<j0){b:=(b*b);j++;};
if (b==1 % n and j>0)then retour:=1;
else if (j==j0) then retour:=1; fi;
fi;
if(retour==0){l:=augment(l,a)};
}
l;
end;

// End defining testa

```

--	--	--	--	--	--	--	--

```

(n)->
{ local m,j0,a,b,retour;
retour:=0;
j0:=0;
m:=n-1;

```

```

        m:=m/2,
        j0++;
    };
    l:=[];
    for (a:=2;a<n;a++) {
        retour:=0;
        b:=(a % n)^m;
        j:=0;
        while((((b!=(1 % n)) && (b!=((-1) % n)))) && (j<j0)){
            b:=b*b;
            j++;
        };
        if (((b==(1 % n)) && (j>0))) {
            retour:=1;
        }
        else {
            if ((j==j0)) {
                retour:=1;
            };
        };
    };
};

```

11

12 Il faut n tel que:  $(0.25)^n < 0.001$  et donc n superieur a:

13  $\ln(0.001)/\ln(0.25)$

4.982892142

14

15 Prog Edit Add 1 nxt OK (F9) Save

```

rabmil:=proc(n)
local m,j0,a,b,retour;
//retour vaut 0 si l'on ne sait pas si n est premier.
//retour=1 implique que l'on est sur que n n'est pas premier.
retour:=0;
j0:=0;m:=n-1;
while(iirem(m,2)==0){m:=m/2;j0++;};
l:=[2,101,55,23,177];
for(ia:=0;ia<5;ia++)
{
    retour:=0;a:=l[ia];
    b:=(a % n )^m;j:=0;
    while((b != 1 % n) and (b!=-1 % n) and j<j0){b:=(b*b);j++;};
    if (b==1 % n and j>0)then retour:=1;ia:=5
        else if (j==j0) then retour:=1; ia:=5fi;
    fi;
}
retour;
end;

```

// Warning: iia,j, declared as global variable(s)  
 // End defining rabmil

```

(n)->
{ local m,j0,a,b,retour;
retour:=0;
j0:=0;
m:=n-1;
while(((iirem(m,2)==0)){
    m:=m/2;
    j0++;
};
l:=[2,101,55,23,177];
for (ia:=0;ia<5;ia++) {
    retour:=0;
    a:=l[ia];
    b:=(a % n)^m;
    j:=0;
    while((((b!=(1 % n)) && (b!=((-1) % n)))) && (j<j0)){
        b:=b*b;
        j++;
    };
    if (((b==(1 % n)) && (j>0))) {
        retour:=1;
        ia:=5;
    };
};
}

```

	else {	M
16	rabmil(561)	
	1	M
17	n:=nextprime(10^13)*nextprime(5^22)*nextprime(9^11);	
	748182764366062804213405779753545467883	M
18	rabmil(n);	
	1	M
19	rabmil(nextprime(4444444444444444))	
	0	M
20		