TD4 : WHAT IS THIS CODE DOING ?

1. WHAT IS THIS CODE DOING ?

What is this code doing ? Explain the contribution of each function and the meaning of every variable. Run this code on various numerical examples. Which is the running time ?

```
default(colors,darkbg)

p = nextprime(random(10^10));
p= 9161878381;
g = Mod(7,p);

o = p-1;
r=truncate(sqrt(o))+1;
G = g^r;

h=Mod(11,p);

baby=vector(r,k,[0,k,lift(h*g^(-k))]);
GIANT=vector(r,k,[1,k,lift(G^k)]);
merge=concat(baby,GIANT);
merge=vecsort(merge,3);
k=1;until(merge[k][3]==merge[k+1][3],k=k+1);
if(merge[k][1]==0,rep=merge[k][2]+r*merge[k+1][2],
rep=merge[k+1][2]+r*merge[k][2]);
```

2. WHAT IS THIS CODE DOING ?

What is this code doing ? Explain the contribution of each function and the meaning of every variable. Run this code on various numerical examples. Which is the running time ?

```
default(colors,darkbg)

p = nextprime(random(2*10^3));
g = Mod(3,p);
h = Mod(5,p);

b=5;
B=prime(b);
```

```
{smooth(n,B)=
local(q);
q=n;
forprime(p=2,B,while(q%p==0,q=q/p));
return((q==1));
}

{relation(p,g,h,B)=
local(a,x);
until(smooth(x,B),a=random(p-1);x=lift(g^a*h));
return([a,x]);
}

{exponents(x,b,B)=
local(i,y,ex);
y=x;
ex=vector(b);
i=0;
forprime(p=2,B,i=i+1;while(y%p==0,y=y/p;ex[i]=ex[i]+1));
return(ex);
}

{line(p,g,h,b,B)=
local(rel,l);
rel=relation(p,g,h,B);
l=[rel[1],1];
return(concat(l,exponents(rel[2],b,B)));
}

M=[];
for(k=1,b+6,M=concat(M,[line(p,g,h,b,B)]~));
M=Mat(M);

K=matrix(b+2,b+2,i,j,(i==j)*(p-1))

N= concat(M~,K)

mathnf(N)
```

3. TD4 : WHAT IS THIS CODE DOING ?

What is this code doing ? Explain the contribution of each function and the meaning of every variable. Run this code on various numerical examples. Which is the running time ?

```
default(colors,darkbg)

p = 171962010545840643348334056831754301958457563589574256043877110505832165523856261308397965147955578800999455782202456522693290629520826275682275663694111;

factors=factor(p-1);
factors=factors[,1];
Nf=length(factors);

{isgenerator(x)=
local(rep);
rep=1;
for(k=1,Nf,if(x^((p-1)/factors[k])==Mod(1,p),rep=0));
return(rep);
}

biggene=Mod(19,p);

cofactors=vector(Nf,k,(p-1)/factors[k]);
smallgene=vector(Nf,k,biggene^cofactors[k]);

bez = mathnf(Mat(cofactors),1);
bez=bez[2];
bez=bez[,Nf];

{DL(x)=
local(l,xk);
l=vector(Nf);
for(k=1,Nf,
xk=x^(cofactors[k]*bez[k]);
l[k]=0;
while(xk!=smallgene[k]^l[k],l[k]=l[k]+1);
);
return(sum(k=1,Nf,l[k]*cofactors[k])%(p-1));
}
```