

TP6B : courbes elliptiques et groupe de Mordell

Eléments de corrigé

```
> restart;
```

Question 1

```
> arc1:=plot({sqrt(x^3-36*x),-sqrt(x^3-36*x)},x=-6..0):
arc2:=plot({sqrt(x^3-36*x),-sqrt(x^3-36*x)},x=6..10):
plots[display]({arc1,arc2}):
```

Un point (x,y) sur C et sur la droite de pente alpha passant par P(x1,y1) et Q(x2,y2) doit vérifier les deux équations ; on remplace y par son expression en fonction de x : alors x3 est la troisième racine du polynôme obtenu ; on utilise les relations entre coefficients et racines.

```
> f:=y^2-(x^3+a*x+b): beta:=y1-alpha*x1:
f1:=subs(y=alpha*x+beta,f): collect(f1,x):
x3:=coeff(f1,x,2)-x1-x2;
```

$$-x^3 + \alpha^2 x^2 + (-a + 2(y1 - \alpha x1)\alpha)x + (y1 - \alpha x1)^2 - b$$

$$x3 := \alpha^2 - x1 - x2$$

cette formule est valable dans les deux cas (P=Q et P différent de Q) ; la pente alpha vaut dans le second cas :

```
> alpha:=normal(-diff(f,x)/diff(f,y));
```

$$\alpha := \frac{3x^2 + a}{2y}$$

Question 2

les procédures suivantes résultent directement des formules trouvées précédemment :

```
> appart:=proc(E,P):
  if P=0 then return(true);fi;
  if P[2]^2=P[1]^3+E[1]*P[1]+E[2] then return(true) else
  return(false);fi;
end:
> sommel:=proc(E,P,Q) local alpha,x3,y3;
  alpha:=(Q[2]-P[2])/(Q[1]-P[1]);
  x3:=alpha^2-P[1]-Q[1];
  y3:=-P[2]+alpha*(P[1]-x3);
  return([x3,y3]);end:
> somme2:=proc(E,P) local alpha,x3,y3;
  alpha:=(3*P[1]^2+E[1])/(2*P[2]);
  x3:=alpha^2-2*P[1];
  y3:=-P[2]+alpha*(P[1]-x3);
  return([x3,y3]);end:
> somme:=proc(E,P,Q) local d,alpha,x3,y3;
  d:=4*E[1]^3+27*E[2]^2;
  if d=0 then error("ceci n'est pas une courbe elliptique")
  else
  if (P=0 or appart(E,P)=true)
  and (Q=0 or appart(E,Q)=true)
  then
```

```
  if P<>0 and Q<>0 then
    if P[1]<>Q[1] then return(sommel(E,P,Q));
    elif P[2]=Q[2] and Q[2]<> 0 then return(somme2(E,P));
    else return(0)
    fi;
  elif P=0 then return(Q);
  else return(P);
  fi;
else error("l'un des points au moins n'est pas sur la
courbe");
fi;
fi;
end:
```

[Test :

```
> E:=[-36,0]: P:=[-3,9]: Q:=[-2,8]: R:=[-3,8]: F:=[0,0]:
> somme(E,P,Q); somme(E,P,P); somme(E,Q,Q);
```

$$\begin{bmatrix} 6, 0 \\ \frac{25}{4}, \frac{35}{8} \\ \frac{25}{4}, \frac{35}{8} \end{bmatrix}$$

[2P=-2Q, ce qui n'a rien d'étonnant car P+Q a pour ordonnée 0, donc est d'ordre 2.

```
> somme(E,O,O); somme(E,P,O);
```

$$\begin{bmatrix} 0 \\ -3, 9 \end{bmatrix}$$

```
> somme(E,P,R);
Error, (in somme) l'un des points au moins n'est pas sur la courbe
```

```
> somme(F,P,R);
Error, (in somme) ceci n'est pas une courbe elliptique
```

Question 3

Dans cette procédure de simplification, on développe tous les termes, puis remplace les y_i^2 par leur expression en fonction des x_i (noter l'emploi de `algsubs` plutôt que `subs`) ; enfin, on normalise le résultat (afin de comparer les expressions par la suite).

```
> simplifier:=proc(expression) local temp,hyp1,hyp2,hyp3;
  hyp1:=P[2]^2=P[1]^3+a*P[1]+b; hyp2:=Q[2]^2=Q[1]^3+a*Q[1]+b;
  hyp3:=R[2]^2=R[1]^3+a*R[1]+b;
  temp:=normal(expression,expanded);
  temp:=algsubs(hyp1,temp); temp:=algsubs(hyp2,temp);
  temp:=algsubs(hyp3,temp);
  temp:=normal(temp);
  return(temp);
end:
```

C'est parti pour les vérifications (remplacer les : par ; pour voir les expressions, vous ne serez pas déçu ! Auriez-vous aimé faire les calculs à la main ?)

```
> P:='P': Q:='Q': R:='R': a:='a': b:='b':
PQ:=simplifier(sommel([a,b],P,Q));
QR:=simplifier(sommel([a,b],Q,R));
PetQR:=simplifier(sommel([a,b],P,QR));
```

```
PQetR:=simplifier(somme1([a,b],PQ,R)):
simplifier(PQetR-PetQR);
```

[0, 0]

```
> P2:=simplifier(somme2([a,b],P)):
PQ:=simplifier(somme1([a,b],P,Q)):
P2etQ:=simplifier(somme1([a,b],P2,Q)):
PetPQ:=simplifier(somme1([a,b],P,PQ)):
simplifier(P2etQ-PetPQ);
```

[0, 0]

```
> P2etP:=simplifier(somme1([a,b],P2,P)):
PetP2:=simplifier(somme1([a,b],P,P2)):
simplifier(P2etP-PetP2);
```

[0, 0]

Question 4

```
[ > E:=[-36,0]:
```

```
[ Les points d'ordre 2 sont clairement (-6,0), (0,0) et (6,0)
```

```
[ P est d'ordre 3 si et seulement si 2P=-P :
```

```
> x:='x': y:='y': P:=[x,y]:
temp:=normal(somme2(E,P)-[x,-y],expanded):
temp:=algsubs(y^2=x^3-36*x,temp): res:=normal(temp);
```

$$res := \left[-\frac{3(-72x^2 + x^4 - 432)}{4y^2}, \frac{9(-84x^4 + x^6 + 432x^2 + 5184)}{8y^3} \right]$$

```
> gcd(x^3-84*x^2+432*x+5184, -72*x+x^2-432);
```

$$-72x + x^2 - 432$$

```
[ Donc P(x,y) est d'ordre 3 si et seulement si x^2 est racine de -72*x+x^2-432
```

```
> solve(-72*x+x^2-432);
```

$$36 + 24\sqrt{3}, 36 - 24\sqrt{3}$$

```
[ En définitive, il y a 0 point d'ordre 3 dans E(Q), 4 tels points dans E(R) et 8 points dans E(C)
```

```
> P:=[-3,9]: P1:=P: i:=0: while P1<>0 and i<10 do
P1:=somme(E,P,P1): i:=i+1: print(i,P1): od:
```

$$1, \left[\frac{25}{4}, \frac{-35}{8} \right]$$

$$2, \left[\frac{-1587}{1369}, \frac{-321057}{50653} \right]$$

$$3, \left[\frac{1442401}{19600}, \frac{1726556399}{2744000} \right]$$

$$4, \left[\frac{-8264655507}{1646168329}, \frac{491678499730833}{66789987612517} \right]$$

$$5, \left[\frac{60473718955225}{6968554599204}, \frac{-339760634079313268605}{18395604368087917608} \right]$$

$$6, \left[\frac{-583552361658258723}{4023041763448204561}, \frac{-18433964971574382270849196761}{8069224743013821217381442809} \right]$$

$$7, \left[\frac{4386303618090112563849601}{233710164715943220558400}, \frac{8704369109085580828275935650626254401}{112983858512463619737216684496448000} \right]$$

$$8, \left[\frac{-38588308319846692331485009382883}{6433437028050748454240723606641}, \frac{6056228937102241081991642356775948265805217721}{16317911804506723620780282462635842443354311689} \right]$$

$$9, \left[\frac{339623358722762426094451563298394625625}{19652221475511578582811254387824437604}, \frac{-5869544619324614780595892276791057797695461715964593892675}{87119921378299734860754326833913445245577177202786392808} \right]$$

$$10, \left[\frac{-2512776550703017851462002707141301981572730067}{24693804285487612458809956902508606206944615209}, \frac{7425979074210113673657917982788245778472213771855848368670943739722447}{3880449202583286201483684978743391154828721407443504941067779207054677} \right]$$

```
[ On conjecture donc que P est d'ordre infini
```

Question 5

```
> appartmodp:=proc(E,P,p);
if P=Origine then return(true);fi;
if P[2]^2 mod p = P[1]^3+E[1]*P[1]+E[2] mod p then
return(true) else return(false);fi;
end;
> sommelmodp:=proc(E,P,Q,p) local alpha,x3,y3;
alpha:=(Q[2]-P[2])/(Q[1]-P[1]) mod p;
x3:=alpha^2-P[1]-Q[1] mod p;
y3:=-P[2]+alpha*(P[1]-x3) mod p;
return([x3,y3]);end;
> somme2modp:=proc(E,P,p) local alpha,x3,y3;
alpha:=(3*P[1]^2+E[1])/(2*P[2]) mod p;
x3:=alpha^2-2*P[1] mod p;
y3:=-P[2]+alpha*(P[1]-x3) mod p;
return([x3,y3]);end;
> sommemodp:=proc(E,P,Q,p) local alpha, x3,y3;
if deltaE(E) mod p = 0 then error("ceci n'est pas une courbe
elliptique")
else
if (P=0 or appartmodp(E,P,p)=true)
and (Q=0 or appartmodp(E,Q,p)=true)
then
if P<>0 and Q<>0 then
if P[1]<>Q[1] then return(sommelmodp(E,P,Q,p));
elif P[2]=Q[2] and Q[2]<> 0 then
return(somme2modp(E,P,p));
else return(0)
fi;
elif P=0 then return(Q);
```

```

else return(P);
fi;
else error("l'un des points au moins n'est pas sur la
courbe");
fi;
fi;
end:
> ordremodp:=proc(E,P,p) local n,Q;
if not(appartmodp(E,P,p)) then error("le point n'est pas sur
la courbe")
else n:=1; Q:=P;
while Q<>0 do
n:=n+1; Q:=sommemodp(E,Q,P,p); od;
return(n);
fi;
end:
> pointsmodp:=proc(E,p) local N, L, i, fx, x, y, o;
L:=[[0,1]];N:=1;
for i from 0 to p-1 do
fx:=subs(x=i,x^3+E[1]*x+E[2]) mod p;
if fx=0 then L:=[op(L),[[i,0],2]]; N:=N+1
else y:=numtheory[msqrt](fx,p);
if y<>FAIL then o:=ordremodp(E,[i,y],p);
L:=[op(L),[[i,y],o],[[i,-y],o]]; N:=N+2;
fi;
fi;
od;
return([N,L]);
end:
> E:=[-36,0]: pointsmodp(E,5);
[8, [[0, 1], [[0, 0], 2], [[1, 0], 2], [[2, 1], 4], [[2, -1], 4], [[3, 2], 4], [[3, -2], 4], [[4, 0], 2]]]
Il n'y a pas d'élément d'ordre 8 mais des éléments d'ordre 4, donc E(F_5) est isomorphe à
Z/4Z x Z/2Z

```

Question 6

```

> candidatasy:=proc(E) local L,r,i,d;
L:=ifactors(4*E[1]^3+27*E[2]^2); r:=1;
for d in L[2] do r:=r*d[1]^iquo(d[2],2);od;
return([0,op(numtheory[divisors](r))]);
end:
> trouverx:=proc(E,y) local x,sol,L,d;
sol:={solve(y^2=x^3+E[1]*x+E[2],x)};
L:=[]; for d in sol do if type(d,integer) then L:=[op(L),d];
fi; od;
return(L);
end:

```

Si tous les itérés de P ont des coordonnées entières, on peut leur appliquer le lemme : il n'y en a donc qu'un nombre fini.
Ainsi un point d'ordre infini est tel que pour n assez grand nP a une des coordonnées qui n'est plus entière.
On peut se limiter à aller jusqu'à n=12 à cause du théorème de Mazur.

```

> ordre:=proc(E,P) local n,Q;

```

```

if not(appart(E,P)) then error("le point n'est pas sur la
courbe")
else n:=1; Q:=P;
while type(Q[1],integer) and type(Q[2],integer) and n<12
and Q<>0 do
n:=n+1; Q:=somme(E,Q,P); od;
if Q=0 then return(n) else return(infinity);
fi;
fi;
end:
> ordre(E,[-3,9]); ordre(E,[6,0]); ordre(E,0);
∞
2
1

```

[Ainsi P est bien d'ordre infini

Question 7

```

> NagellLutz:=proc(E) local Ly,ctors,tors,x,y,t,N,o;
if 4*E[1]^3+27*E[2]^2=0 then error("ceci n'est pas une courbe
elliptique")
else ctors:=[]; Ly:=candidatsy(E);
for y in Ly do for x in trouverx(E,y) do
ctors:=[op(ctors),[x,y]]; od; od;
tors:=[[0,1]]; N:=1;
for t in ctors do
if t[2]=0 then tors:=[op(tors),[t,2]]; N:=N+1;
else o:=ordre(E,t);
if o<>infinity then
tors:=[op(tors),[t,o],[[t[1],-t[2]],o]]; N:=N+2;
fi;
fi;
od;
return([N,op(tors)]);
fi;
end:
> NagellLutz(E);

```

[4, [0, 1], [[-6, 0], 2], [[0, 0], 2], [[6, 0], 2]]

[Donc E(Q)_tors est isomorphe au groupe de Klein Z/2Z x Z/2Z

Question 8

```

> E:=[0,3]; NagellLutz(E);
E := [0, 3]
[1, [0, 1]]

```

[Donc E(Q)tors={O}. Seconde méthode utilisant la réduction :

```

> ifactor(27*3); pointsmodp(E,5); pointsmodp(E,7);
(3)^4
[6, [[0, 1], [[1, 2], 6], [[1, -2], 6], [[2, 1], 3], [[2, -1], 3], [[3, 0], 2]]]
[13, [[0, 1], [[1, 2], 13], [[1, -2], 13], [[2, 2], 13], [[2, -2], 13], [[3, 3], 13], [[3, -3], 13],
[[4, 2], 13], [[4, -2], 13], [[5, 3], 13], [[5, -3], 13], [[6, 3], 13], [[6, -3], 13]]]

```

```

[ Card E(Q)tors divise 6 et 13, donc est égal à 1.
> E:=[1,0]; NagellLutz(E);
      E := [1, 0]
      [2, [0, 1], [[0, 0], 2]]
[ Donc E(Q)tors est isomorphe à Z/2Z. Seconde méthode :
> ifactor(4); pointsmotp(E,3); pointsmotp(E,5);
      (2)2
      [4, [[0, 1], [[0, 0], 2], [[2, 1], 4], [[2, -1], 4]]]
      [4, [[0, 1], [[0, 0], 2], [[2, 0], 2], [[3, 0], 2]]]
[ Donc Card E(Q)tors divise 4. Cette information sur le cardinal ne suffit pas à trancher entre
Z/2Z et Z/4Z (Z/2Z x Z/2Z n'est pas possible car il n'y a qu'un seul point d'ordre 2 : (0,0) ; ces
points se trouvent en résolvant y=0 et non par Nagell-Lutz, évidemment).
On regarde donc plus précisément : E(F3) est isomorphe à Z/4Z et E(F5) à Z/2Z x Z/2Z.
Comme E(Q)tors s'identifie à un sous-groupe de ces deux groupes, c'est Z/2Z.
> E:=[-43,166]; NagellLutz(E);
      E := [-43, 166]
      [7, [0, 1], [[3, 8], 7], [[3, -8], 7], [[-5, 16], 7], [[-5, -16], 7], [[11, 32], 7], [[11, -32], 7]]
[ Donc E(Q)tors est isomorphe à Z/7Z. Seconde méthode :
> ifactor(4*(-43)^3+27*166^2); for i from 3 to 12 do if
isprime(i) then print(i,pointsmotp(E,i)); fi; od;
      (2)15 (13)
      3, [7, [[0, 1], [[0, 1], 7], [[0, -1], 7], [[1, 1], 7], [[1, -1], 7], [[2, 1], 7], [[2, -1], 7]]]
      5, [7, [[0, 1], [[0, 1], 7], [[0, -1], 7], [[1, 2], 7], [[1, -2], 7], [[3, 2], 7], [[3, -2], 7]]]
      7, [7, [[0, 1], [[2, 2], 7], [[2, -2], 7], [[3, 1], 7], [[3, -1], 7], [[4, 3], 7], [[4, -3], 7]]]
      11, [14, [[0, 1], [[0, 1], 7], [[0, -1], 7], [[1, 5], 14], [[1, -5], 14], [[2, 0], 2], [[3, 3], 7],
      [[3, -3], 7], [[4, 5], 14], [[4, -5], 14], [[6, 5], 7], [[6, -5], 7], [[8, 2], 14], [[8, -2], 14]]]
[ Donc E(Q)tors est un sous-groupe de Z/7Z, mais le théorème de réduction ne peut nous en
dire plus, quel que soit le p choisi : pour trancher entre {O} et Z/7Z, il faut exhiber un point
rationnel non trivial.

```

Question 9

Le cardinal détermine le groupe, sauf pour Z/2Z x Z/2Z et Z/4Z, Z/2Z x Z/4Z et Z/8Z, Z/2Z x Z/6Z et Z/12Z. On regarde alors le nombre de points d'ordre 2 ou la présence d'un générateur d'ordre maximal.

l'équation sera présenté sous la forme : $y^2+ay+bx=$ polynome en x de degre 3

```

> transf:=proc(eq) local F,a,b,c;
F:=-lhs(eq)+rhs(eq); a:=coeff(F,y);
if a>0 then F:=expand(subs(y=y+a/2,F)); fi;
b:=coeff(coeff(F,x),y);
if b>0 then F:=expand(subs(y=y+b*x/2,F)); fi;
c:=coeff(F,x^2);
if c>0 then F:=expand(subs(x=x-c/3,F)); fi;
return(y^2=sort(subs(y^2=0,F)));
end:
> x:='x': y:='y': eq:=transf(y^2+7*x*y=x^3+16*x); ifactor(864);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);

```

```

      eq := y^2 = x^3 - 1633/48 x + 61201/864
      (2)5 (3)3
      eq := y^2 = x^3 - 44091 x + 3304854
> NagellLutz([-44091, 3304854]);
[8, [0, 1], [[147, 0], 2], [[75, 648], 8], [[75, -648], 8], [[-141, 2592], 8], [[-141, -2592], 8],
[[291, 3888], 4], [[291, -3888], 4]]
[ Il s'agit de Z/8Z
> eq:=transf(y^2+x*y-5*y=x^3-5*x^2);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq := y^2 = x^3 - 481/48 x - 4879/864
      eq := y^2 = x^3 - 12987 x - 263466
> NagellLutz([-12987, -263466]);
[8, [0, 1], [[-102, 0], 2], [[-21, 0], 2], [[123, 0], 2], [[-57, 540], 4], [[-57, -540], 4],
[[303, 4860], 4], [[303, -4860], 4]]
[ Il s'agit de Z/2 X Z/4Z
> eq:=transf(y^2-y=x^3-x^2); ifactor(108);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq := y^2 = x^3 - 1/3 x + 19/108
      (2)2 (3)3
      eq := y^2 = x^3 - 432 x + 8208
> NagellLutz([-432, 8208]);
[5, [0, 1], [[-12, 108], 5], [[-12, -108], 5], [[24, 108], 5], [[24, -108], 5]]
[ Z/5Z
> eq:=transf(y^2+x*y+y=x^3-x^2-14*x+29); ifactor(32);
eq:=2^6*subs(x=x/2^2,y=y/2^3,eq);
      eq := y^2 = x^3 - 219/16 x + 827/32
      (2)5
      eq := y^2 = x^3 - 219 x + 1654
> NagellLutz([-219, 1654]);
[9, [0, 1], [[11, 24], 9], [[11, -24], 9], [[3, 32], 3], [[3, -32], 3], [[-13, 48], 9], [[-13, -48], 9],
[[35, 192], 9], [[35, -192], 9]]
[ Z/9Z
> eq:=transf(y^2+x*y=x^3-45*x+81);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq := y^2 = x^3 - 2161/48 x + 73225/864
      eq := y^2 = x^3 - 58347 x + 3954150
> NagellLutz([-58347, 3954150]);
[10, [0, 1], [[75, 0], 2], [[219, 1296], 5], [[219, -1296], 5], [[3, 1944], 10], [[3, -1944], 10],

```

```

[ [-213, 2592], 10], [[-213, -2592], 10], [[651, 15552], 5], [[651, -15552], 5]]
[ Z/10Z
> eq:=transf(y^2+43*x*y-210*y=x^3-210*x^2);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq:=y^2=x^3-1234801/48*x+1364775049/864
      eq:=y^2=x^3-33339627*x+73697852646
> NagellLutz([-33339627,73697852646]);
[12, [O, 1], [[3531, 0], 2], [[3027, 22680], 12], [[3027, -22680], 12], [[4107, 77760], 3],
[[4107, -77760], 3], [[1515, 163296], 4], [[1515, -163296], 4], [[-4533, 362880], 12],
[[4533, -362880], 12], [[10587, 952560], 6], [[10587, -952560], 6]]
[ Z/12Z
> eq:=transf(y^2+5*x*y-6*y=x^3-3*x^2);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq:=y^2=x^3-889/48*x+24013/864
      eq:=y^2=x^3-24003*x+1296702
> NagellLutz([-24003,1296702]);
[12, [O, 1], [[-177, 0], 2], [[66, 0], 2], [[111, 0], 2], [[39, 648], 6], [[39, -648], 6],
[[147, 972], 3], [[147, -972], 3], [[-69, 1620], 6], [[-69, -1620], 6], [[471, 9720], 6],
[[471, -9720], 6]]
[ Z/2Z x Z/6Z
> eq:=transf(y^2+17*x*y-120*y=x^3-60*x^2);
eq:=6^6*subs(x=x/6^2,y=y/6^3,eq);
      eq:=y^2=x^3-51361/48*x+6826609/864
      eq:=y^2=x^3-1386747*x+368636886
> NagellLutz([-1386747,368636886]);
[16, [O, 1], [[-1293, 0], 2], [[282, 0], 2], [[1011, 0], 2], [[147, 12960], 8], [[147, -12960], 8],
[[1227, 22680], 8], [[1227, -22680], 8], [[-285, 27216], 4], [[-285, -27216], 4],
[[933, 29160], 8], [[933, -29160], 8], [[2307, 97200], 4], [[2307, -97200], 4],
[[8787, 816480], 8], [[8787, -816480], 8]]
[ Z/2Z x Z/8Z
[ Au final, il manque Z/3Z et Z/6Z
> for a from 0 to 10 do for b from 0 to 10 do if
4*a^3+27*b^2<>0 then NL:=NagellLutz([a,b]); if NL[1] in {3,6}
then print(a,b,NL); fi; fi; od; od;
      0, 1, [6, [O, 1], [[-1, 0], 2], [[0, 1], 3], [[0, -1], 3], [[2, 3], 6], [[2, -3], 6]]
      0, 4, [3, [O, 1], [[0, 2], 3], [[0, -2], 3]]
      0, 9, [3, [O, 1], [[0, 3], 3], [[0, -3], 3]]
Résumé :
E(Q)_tors (a,b)
{0} (0,3)
Z/2Z (1,0)
Z/3Z (0,4)

```

```

Z/4Z (1,2)
Z/5Z (-432,8208)
Z/6Z (0,1)
Z/7Z (-43,166)
Z/8Z (-44091,3304854)
Z/9Z (-219,1654)
Z/10Z (-58347,3954150)
Z/12Z (-33339627,73697852646)
Z/2Z x Z/2Z (-1,0)
Z/2Z x Z/4Z (-12987,-263466)
Z/2Z x Z/6Z (-24003,1296702)
Z/2Z x Z/8Z (-1386747,368636886)

```

Question 10

```

> L:=[]:
for a from 1 to 10 do
for b from 1 to a do
if igcd(a,b)=1 and type(a*b,even) then L:=[op(L),
(a^2-b^2)*a*b];
fi;
od;
od;
sort(L);
[6, 30, 60, 84, 180, 210, 210, 330, 504, 546, 630, 840, 924, 990, 1224, 1320, 1386, 1560,
1710, 2340, 2730, 3570]

```

Question 11

```

[ > x:=Z^2/4: y:=(X^2-Y^2)*Z/8: n:=X*Y/2:
[ > Eq:=y^2-(x^3-n^2*x):
[ > algsubs(Z^2=X^2+Y^2,normal(Eq,expanded));
0
[ Réciproquement :
[ > n:='n': x:='x': y:='y': X:=(n^2-x^2)/y: Y:=-2*n*x/y:
Z:=(n^2+x^2)/y:
[ Si x>0, alors x^2<n^2 et l'on remplace X par -X et Y par -Y
[ > algsubs(y^2=x^3-n^2*x,X^2+Y^2-Z^2);
0
[ > algsubs(y^2=x^3-n^2*x,normal(X*Y/2-n));
0
[ Noter que le triplet est bien défini et composé de nombres non nuls car (x,y) n'est pas d'ordre
2
[ > for n in L do NagellLutz([-n^2,0]); od;
      [4, [O, 1], [[-6, 0], 2], [[0, 0], 2], [[6, 0], 2]]
      [4, [O, 1], [[-30, 0], 2], [[0, 0], 2], [[30, 0], 2]]
      [4, [O, 1], [[-60, 0], 2], [[0, 0], 2], [[60, 0], 2]]
      [4, [O, 1], [[-84, 0], 2], [[0, 0], 2], [[84, 0], 2]]
      [4, [O, 1], [[-210, 0], 2], [[0, 0], 2], [[210, 0], 2]]

```

[4, [0, 1], [[-180, 0], 2], [[0, 0], 2], [[180, 0], 2]]

[4, [0, 1], [[-210, 0], 2], [[0, 0], 2], [[210, 0], 2]]

Warning, computation interrupted

On conjecture qu'il en est de meme pour tous les nombres congruents.

Question 12

```
> for a from 1 to 10 do
  for b from 1 to a do
    if igcd(a,b)=1 and type(a*b,even) and (a^2-b^2)*a*b=30
    then print(a,b);
    fi;
  od;
od ;
```

```
> a:=3: b:=2: X:=a^2-b^2: Y:=2*a*b: Z:=a^2+b^2: x:=Z^2/4;
y:=(X^2-Y^2)*Z/8; n:=X*Y/2;
```

$$x := \frac{169}{4}$$

$$y := \frac{-1547}{8}$$

$$n := 30$$

```
> ordre([-30^2,0],[x,y]);
```

∞

```
> x:=41^2/7^2: y:=720*41/7^3: ordre([-31^2,0],[x,y]);
```

∞

```
> X:=- (31^2-x^2)/y: Y:=2*31*x/y: Z:=(31^2+x^2)/y:
A:=sort([X,Y,Z]); X*Y/2;
```

$$A := \left[\frac{32881958232480}{6452866086721}, \frac{6452866086721}{530354165040}, \frac{45143858820005902416051841}{3422304405537848186433840} \right]$$

```
> P:=[x,y]; Q:=somme([-31^2,0],P,P);
```

$$P := \left[\frac{1681}{49}, \frac{29520}{343} \right]$$

$$Q := \left[\frac{6587235366721}{42700089600}, \frac{-16561674436400736481}{8823546514944000} \right]$$

```
> x:=Q[1]: y:=-Q[2]: X:=- (31^2-x^2)/y: Y:=2*31*x/y:
Z:=(31^2+x^2)/y: B:=sort([X,Y,Z]); X*Y/2;
```

$$B := \left[\frac{32881958232480}{6452866086721}, \frac{6452866086721}{530354165040}, \frac{45143858820005902416051841}{3422304405537848186433840} \right]$$

31