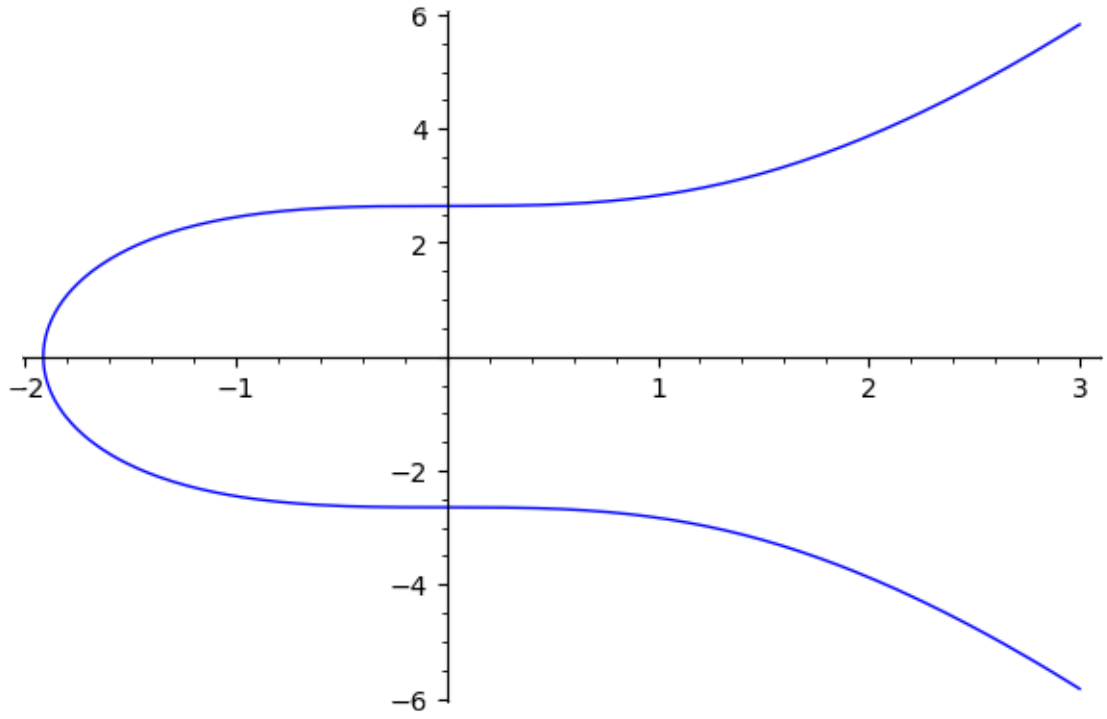
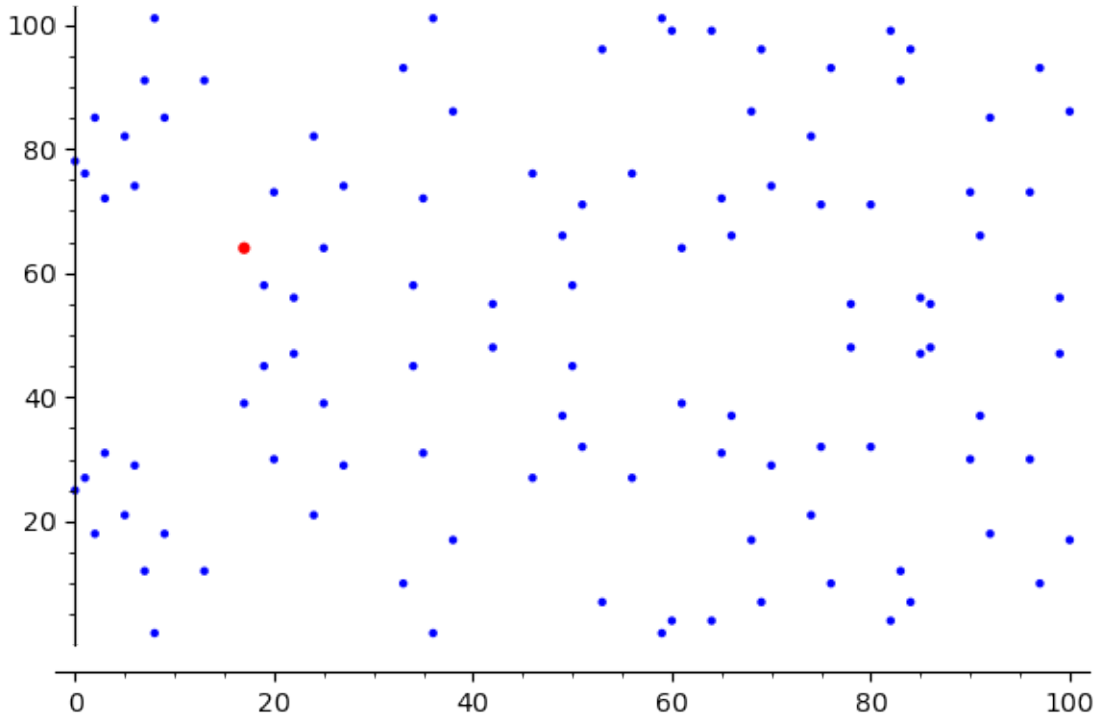
courbe E =>  Elliptic Curve defined by y^2 = x^3 + 7 over Rational Field

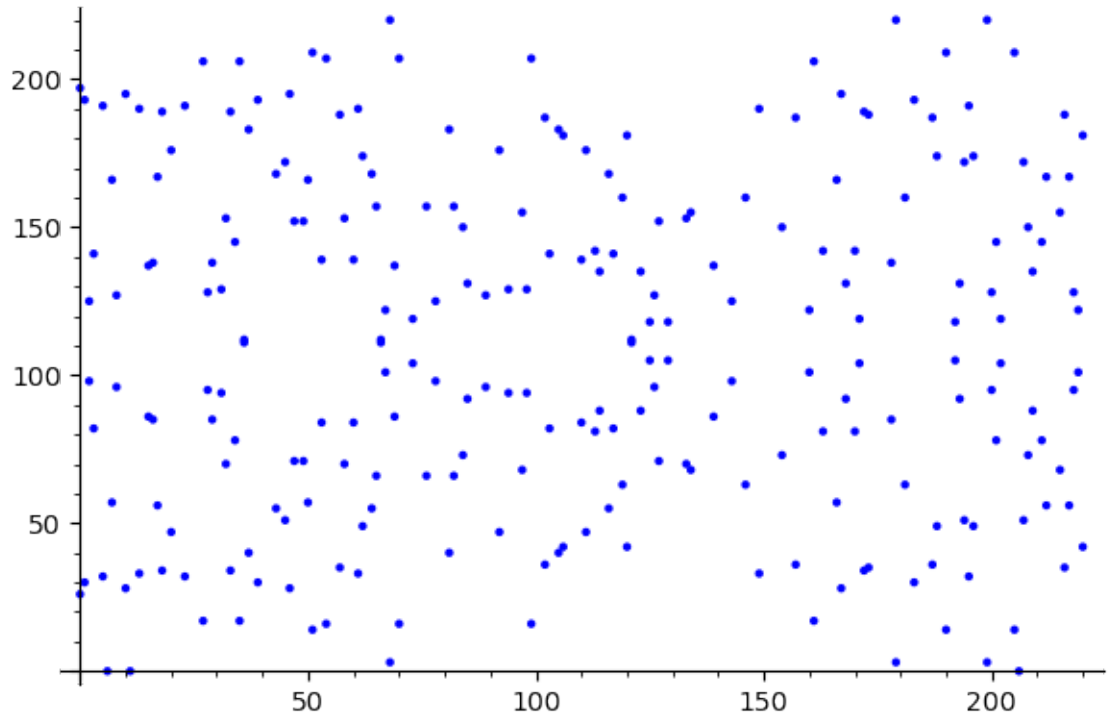



Domaine F103
n= 103
79
79
a = 17  b = 64  sur la courbe ?
True
E =>  Elliptic Curve defined by y^2 = x^3 + 7 over Finite Field of size 103




E points [(0 : 1 : 0), (0 : 25 : 1), (0 : 78 : 1), (1 : 27 : 1), (1 : 76 : 1),
(2 : 18 : 1), (2 : 85 : 1), (3 : 31 : 1), (3 : 72 : 1), (5 : 21 : 1), (5 : 82 :

```
1), (6 : 29 : 1), (6 : 74 : 1), (7 : 12 : 1), (7 : 91 : 1), (8 : 2 : 1), (8 :
101 : 1), (9 : 18 : 1), (9 : 85 : 1), (13 : 12 : 1), (13 : 91 : 1), (17 : 39 :
1), (17 : 64 : 1), (19 : 45 : 1), (19 : 58 : 1), (20 : 30 : 1), (20 : 73 : 1),
(22 : 47 : 1), (22 : 56 : 1), (24 : 21 : 1), (24 : 82 : 1), (25 : 39 : 1), (25 :
64 : 1), (27 : 29 : 1), (27 : 74 : 1), (33 : 10 : 1), (33 : 93 : 1), (34 : 45 :
1), (34 : 58 : 1), (35 : 31 : 1), (35 : 72 : 1), (36 : 2 : 1), (36 : 101 : 1),
(38 : 17 : 1), (38 : 86 : 1), (42 : 48 : 1), (42 : 55 : 1), (46 : 27 : 1), (46 :
76 : 1), (49 : 37 : 1), (49 : 66 : 1), (50 : 45 : 1), (50 : 58 : 1), (51 : 32 :
1), (51 : 71 : 1), (53 : 7 : 1), (53 : 96 : 1), (56 : 27 : 1), (56 : 76 : 1),
(59 : 2 : 1), (59 : 101 : 1), (60 : 4 : 1), (60 : 99 : 1), (61 : 39 : 1), (61 :
64 : 1), (64 : 4 : 1), (64 : 99 : 1), (65 : 31 : 1), (65 : 72 : 1), (66 : 37 :
1), (66 : 66 : 1), (68 : 17 : 1), (68 : 86 : 1), (69 : 7 : 1), (69 : 96 : 1),
(70 : 29 : 1), (70 : 74 : 1), (74 : 21 : 1), (74 : 82 : 1), (75 : 32 : 1), (75 :
71 : 1), (76 : 10 : 1), (76 : 93 : 1), (78 : 48 : 1), (78 : 55 : 1), (80 : 32 :
1), (80 : 71 : 1), (82 : 4 : 1), (82 : 99 : 1), (83 : 12 : 1), (83 : 91 : 1),
(84 : 7 : 1), (84 : 96 : 1), (85 : 47 : 1), (85 : 56 : 1), (86 : 48 : 1), (86 :
55 : 1), (90 : 30 : 1), (90 : 73 : 1), (91 : 37 : 1), (91 : 66 : 1), (92 : 18 :
1), (92 : 85 : 1), (96 : 30 : 1), (96 : 73 : 1), (97 : 10 : 1), (97 : 93 : 1),
(99 : 47 : 1), (99 : 56 : 1), (100 : 17 : 1), (100 : 86 : 1)]
E cardinality  111
facteur  3 * 37
False
Trouve
(17, 64)
True
 Domaine F223
n=  223
E =>   Elliptic Curve defined by y^2 = x^3 + 7 over Finite Field of size 223
```




```
Trouve
(192, 105)
True
Trouve
(17, 56)
True
False
Trouve
(1, 193)
```

```
True
False
```