2020-06-08-212246.sagews

Author	**Alvaro Lozano-Robledo**
Date	**2020-06-09T14:09:32**
Project	**ef1d5fd2-b423-4b56-bc95-ad5dffd6c0e5**
Location	**2020-06-08-212246.sagews**
Original file	**2020-06-08-212246.sagews**

```
# GCD
GCD(3,6)
xgcd(3,7)
```

```
3

(1, -2, 1)
```

```
1 == -2*3 + 1*7
```

```
True
```

```
# Modular Arithmetic
Mod(16,7)
R = Integers(7)
R(16)
```

```
2

2
```

```
# CRT
crt(1,2,5,7)
```

```
16
```

```
Mod(16,5)
Mod(16,7)
```

```
1

2
```

```
# Some arithmetic functions
euler_phi(100)
```

```
40
```

```
# Euler's theorem!
```

```
Mod(3^40,100)
```

```
1
```

```
# Sigma arithmetic function
sigma(10,2)
```

```
130
```

```
#check it
1^2+2^2+5^2+10^2
```

```
130
```

```
# Primes
P = Primes()
P
P[0]
P[2]
```

```
Set of all prime numbers: 2, 3, 5, 7, ...

2

5
```

```

```

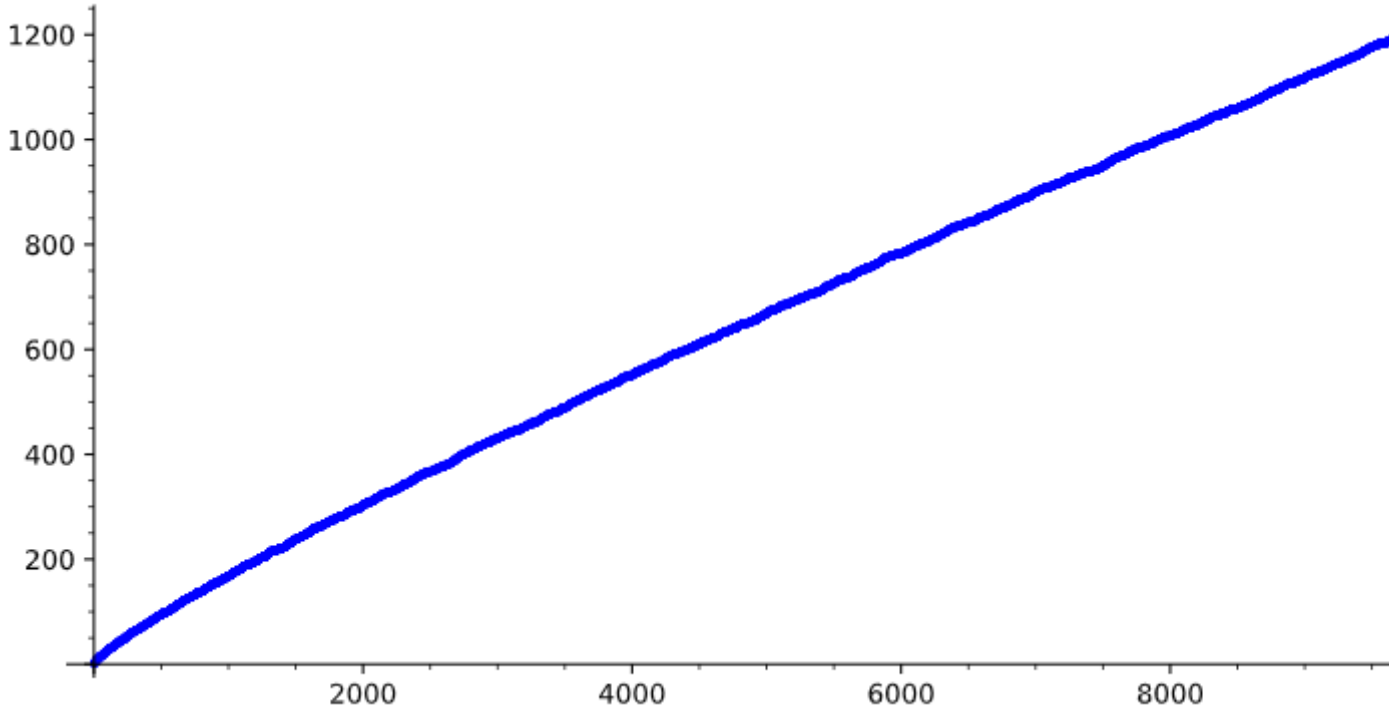
```
# Sieves!
L = [i for i in range(2,100) if (GCD(i,30*7) == 1)]
L
```

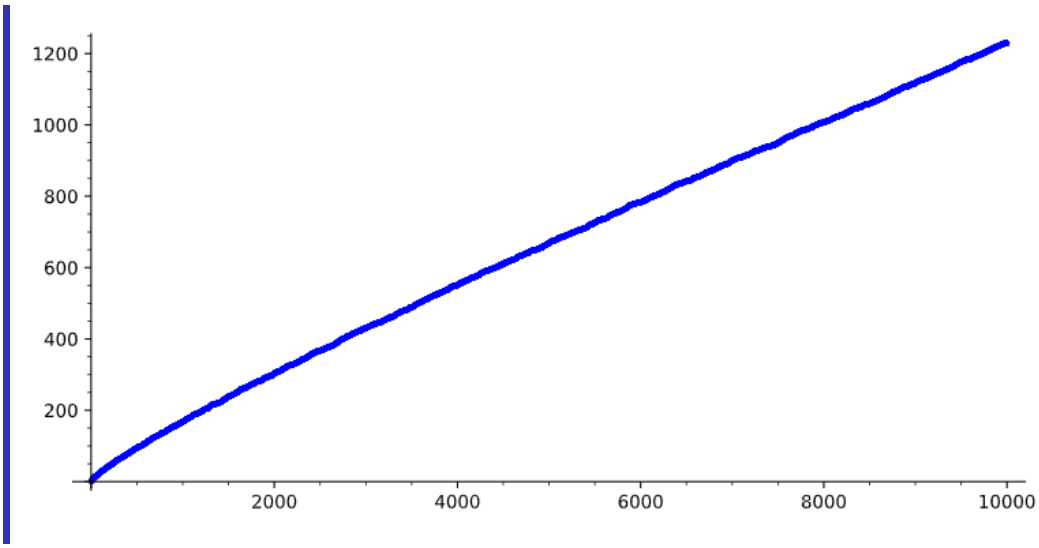
```
[11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]
```

```
# prime counting function
prime_pi(500000)
```

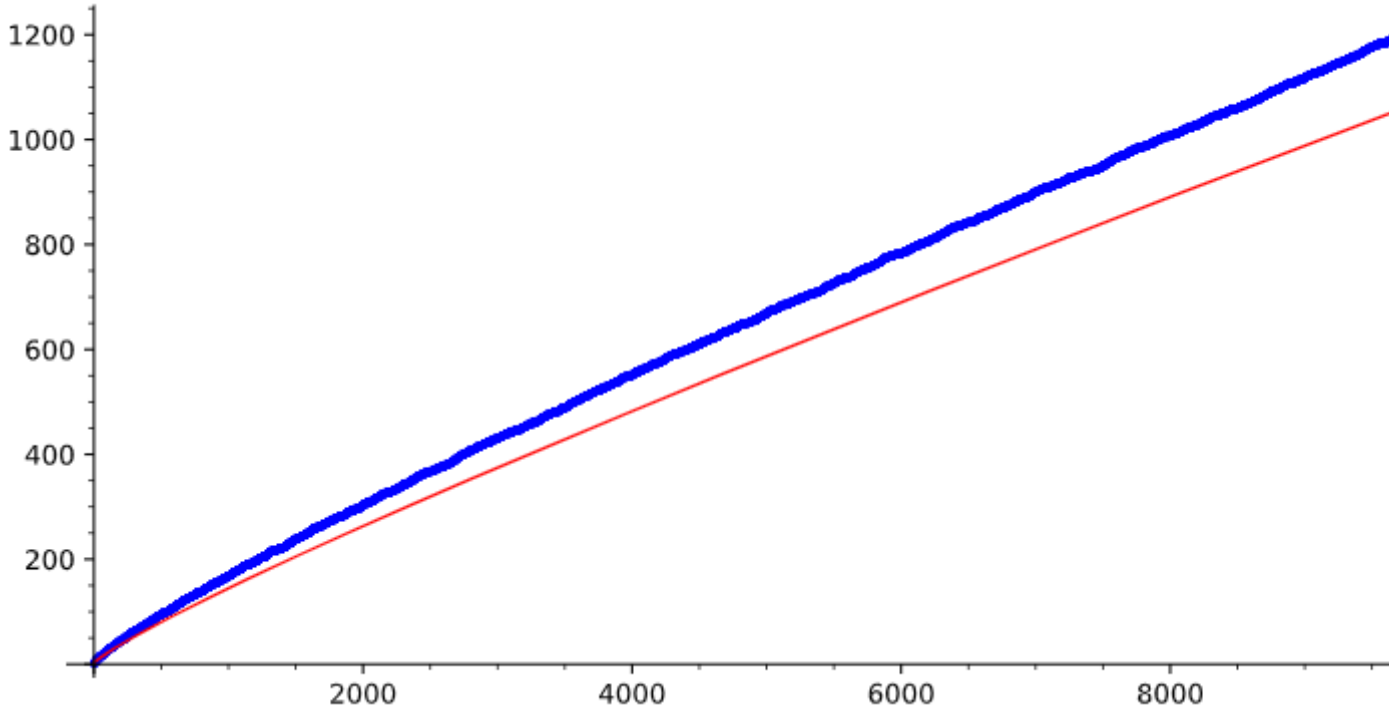
```
41538
```

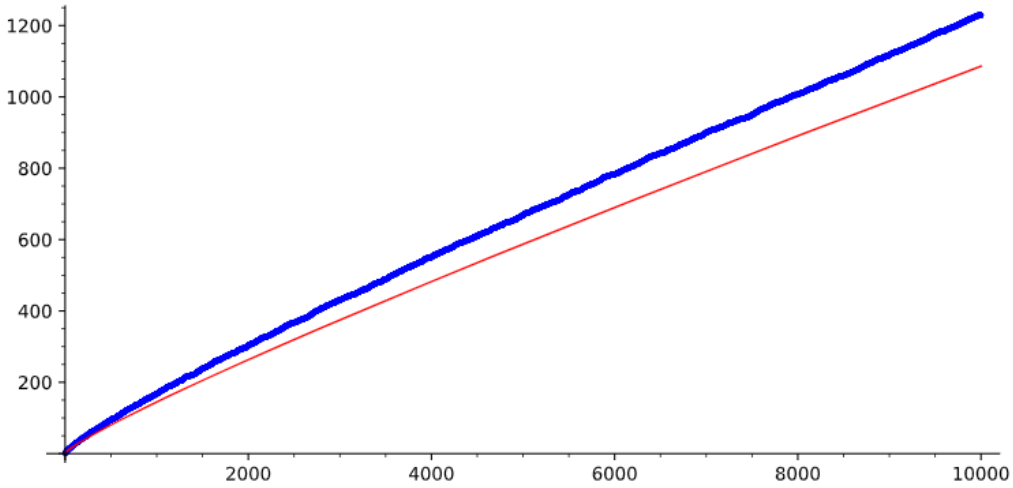
```
#ignore

plot(point([(i,prime_pi(i)) for i in range(2,10000)]))
```



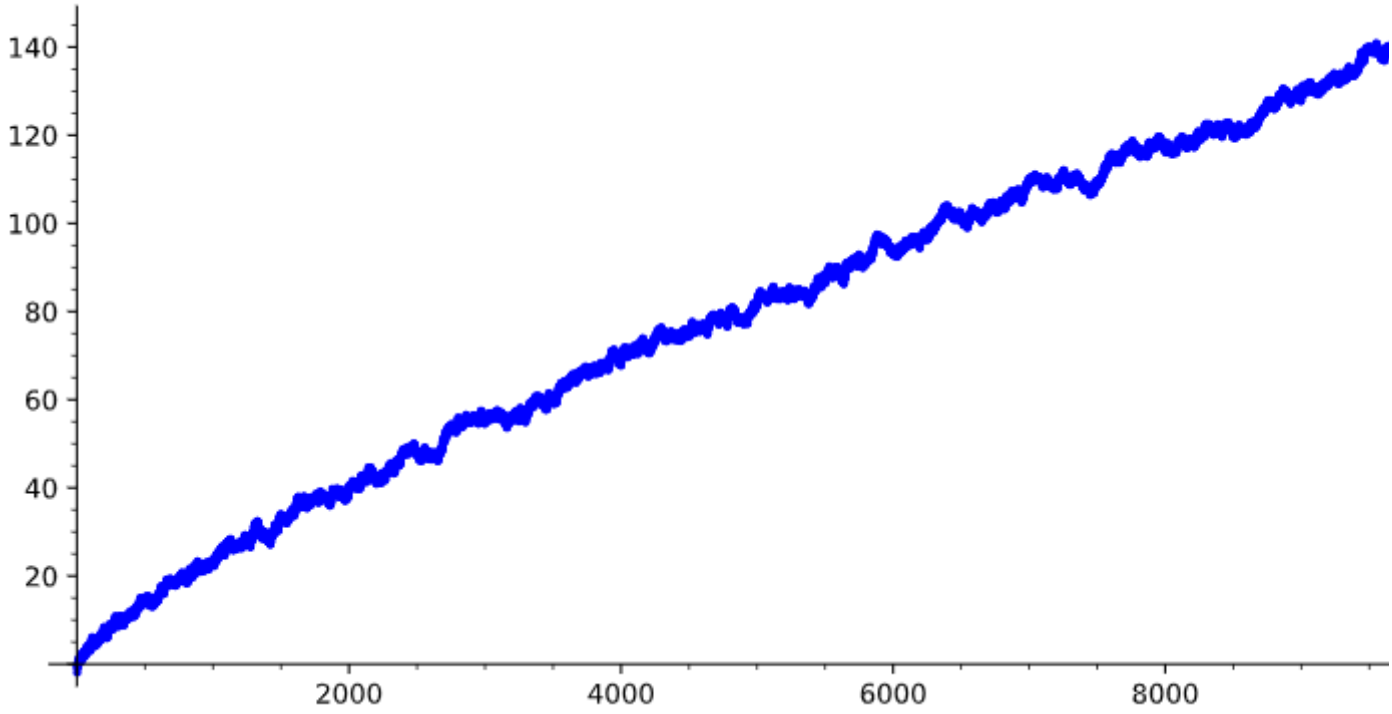


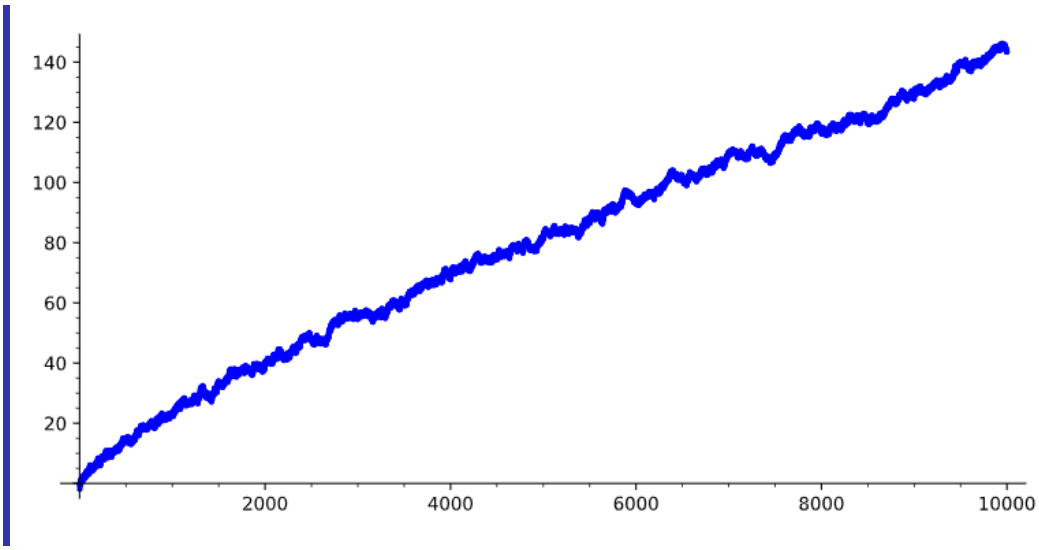

```
34 plot(point([(i,prime_pi(i)) for i in range(2,10000)])) + plot(x/log(x),(1,10000),rgbcolor=(1,0,0
```



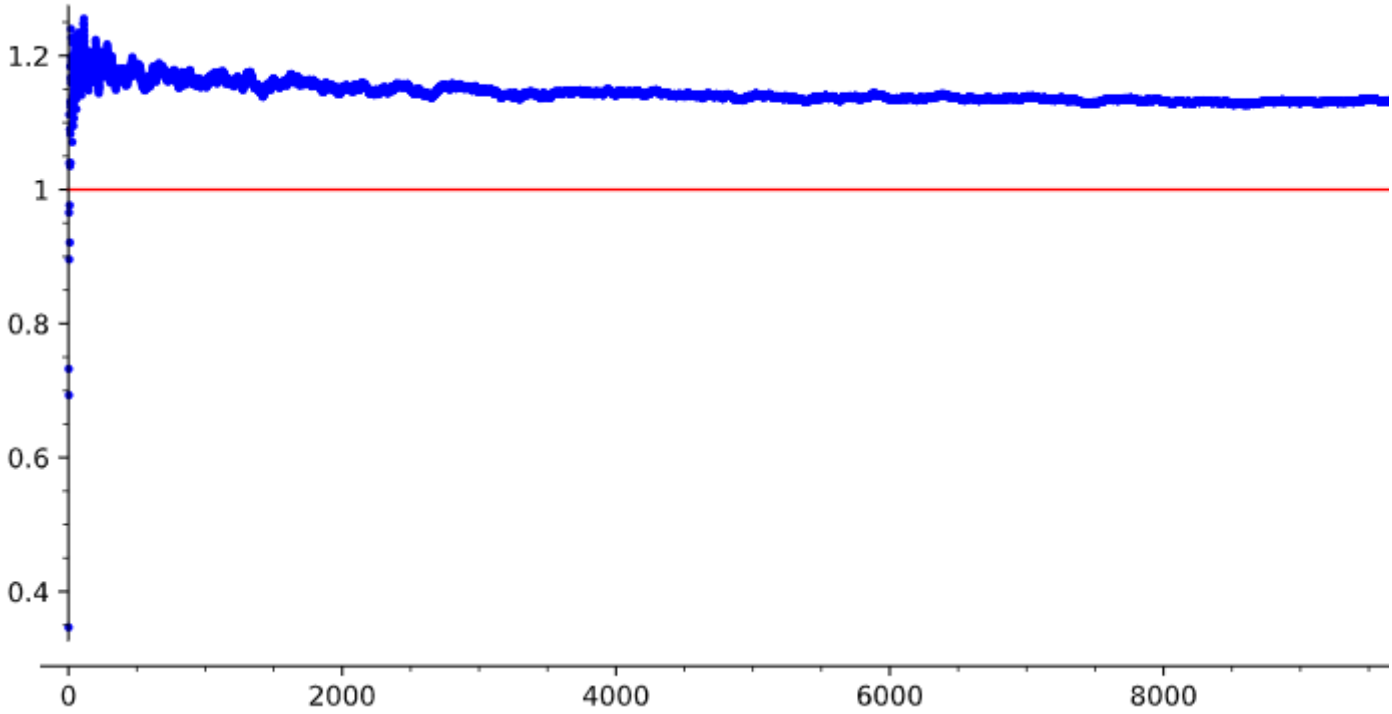


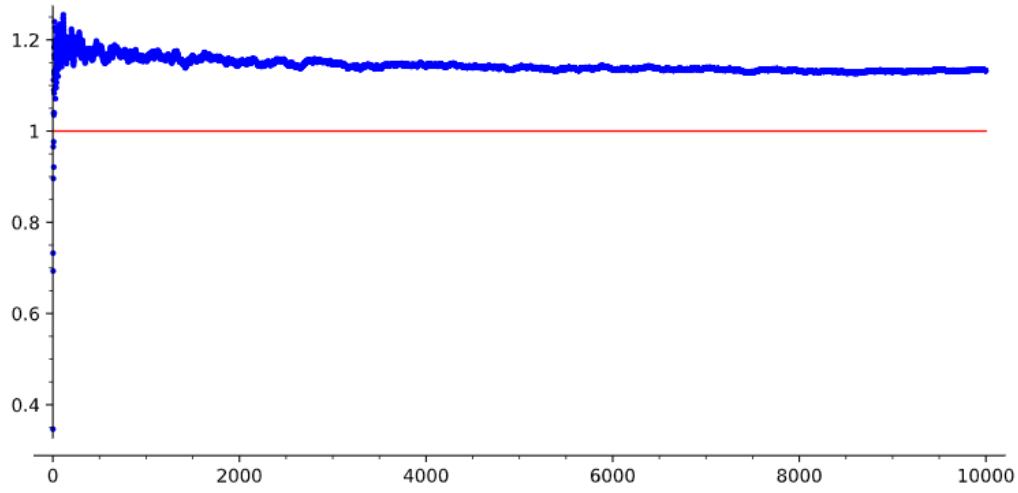

```
35 plot(point([(i,prime_pi(i)-i/log(i)) for i in range(2,10000)]))
```






```
36 plot(point([(i,(prime_pi(i))/(i/log(i))) for i in range(2,10000)]))+plot(1,(1,10000),rgbcolor=(1
```






```
37 # How to write a function
38 def IsSophie(p):
39     if p.is_prime() != True:
40         print "Oh come on! This number is not even prime!"
41     elif (2*p+1).is_prime():
42             print p, " is a Sophie Germain prime :) because ", 2*p+1, " is also prime. Well done
43 IsSophie(6)
```

```
Oh come on! This number is not even prime!
```

```
44 IsSophie(3)
```

```
3  is a Sophie Germain prime :) because  7  is also prime. Well done.
```

```
45 # CURVES OVER FINITE FIELDS
```

```
A.<x,y> = AffineSpace(GF(5),2)
C = Curve([x^2-y^2-1],A)
C
```

```
Affine Plane Curve over Finite Field of size 5 defined by x^2 - y^2 - 1
```

```
# points over F_5
C.count_points(1)
```

```
[4]
```

```
# over F_5 and F_25
C.count_points(2)
```

```
[4, 24]
```

```
C.rational_points()
```

```
[(0, 2), (0, 3), (1, 0), (4, 0)]
```

```
C.is_smooth()
```

```
True
```

```
C.projective_closure()
```

```
Projective Plane Curve over Finite Field of size 5 defined by -x0^2 + x1^2 - x2^2
```

```
P.<X,Y,Z> = ProjectiveSpace(GF(5),2)
C = Curve([X^2-Y^2-Z^2],P)
C
```

```
Projective Plane Curve over Finite Field of size 5 defined by X^2 - Y^2 - Z^2
```

```
C.count_points(1)
```

```
[6]
```

```
C.rational_points()
```

```
[(0 : 2 : 1), (0 : 3 : 1), (1 : 0 : 1), (1 : 1 : 0), (4 : 0 : 1), (4 : 1 : 0)]
```

```
# Elliptic curves over finite fields
# http://sage-doc.sis.uta.fi/reference/curves/sage/schemes/elliptic_curves/ell_finite_field.htm
E = EllipticCurve([GF(5)(1),2,3,4,6])
E
```

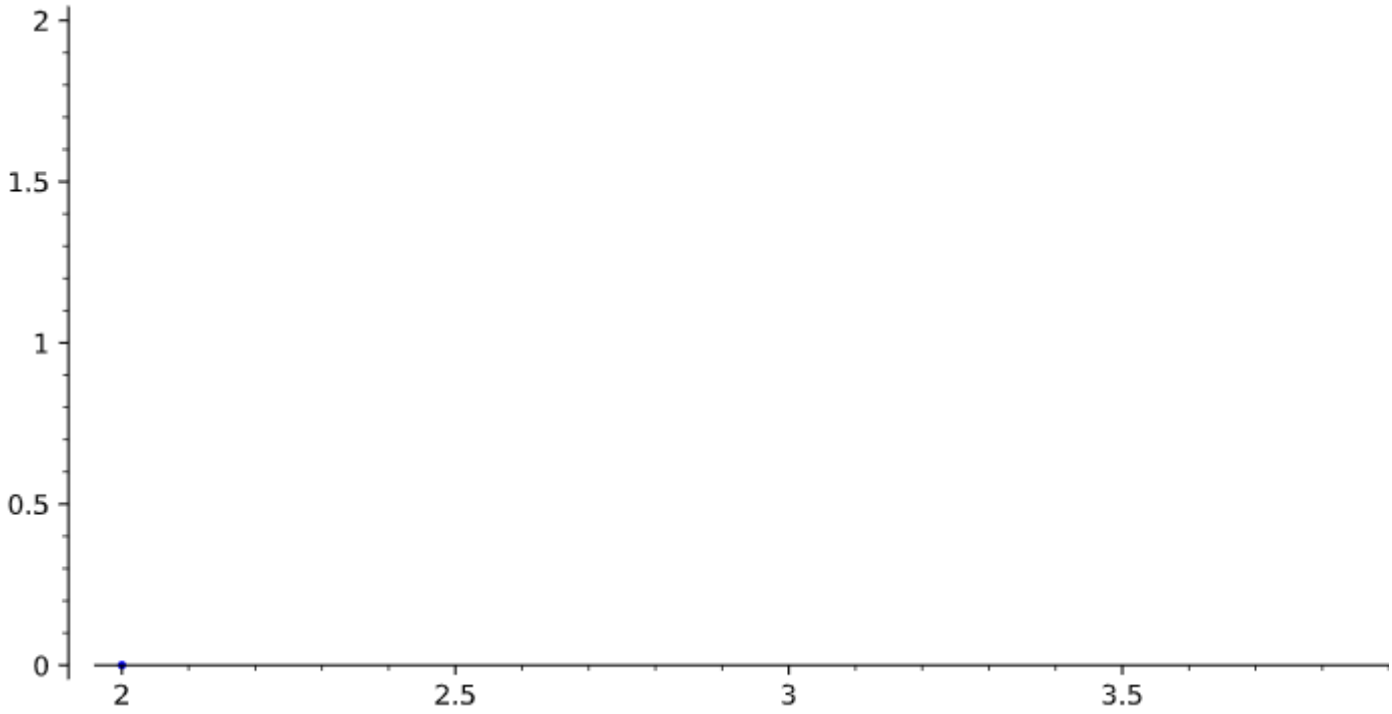
```
Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 1 over Finite Field of size 5
```

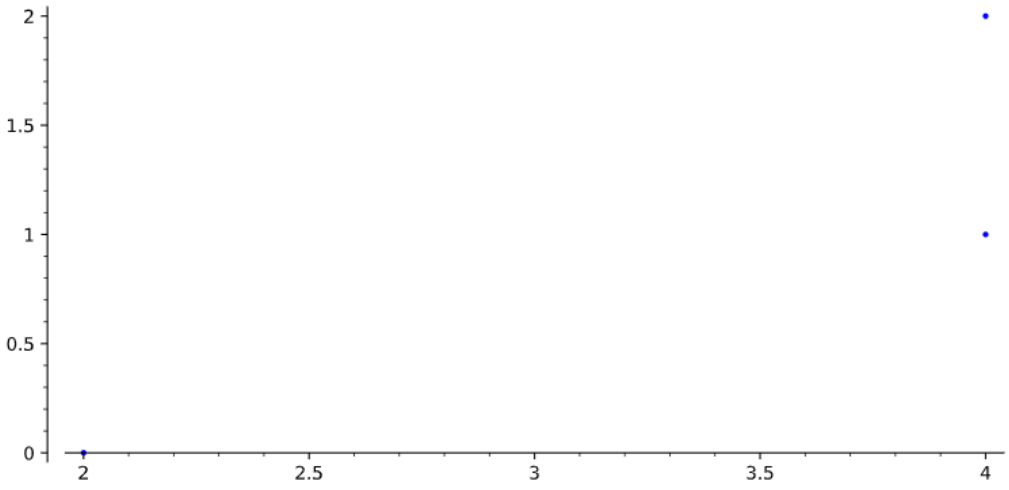
```
E = EllipticCurve(GF(5),[1,2,3,4,6])
```

```
66 E
```

```
Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 1 over Finite Field of size 5
```

```
67 plot(E)
```






```
68 E.count_points()
```

```
4
```

```
69 E.rational_points()
70 E.points()
```

```
[(0 : 1 : 0), (2 : 0 : 1), (4 : 1 : 1), (4 : 2 : 1)]
```

```
[(0 : 1 : 0), (2 : 0 : 1), (4 : 1 : 1), (4 : 2 : 1)]
```

```
71 E.abelian_group()
```

```
Additive abelian group isomorphic to Z/4 embedded in Abelian group of points on Elliptic Curve
defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 1 over Finite Field of size 5
```

```
72 P = E.abelian_group().gens()[0]
73 P
```

```
(4 : 1 : 1)
```

```
74 P+P
75 3*P
```

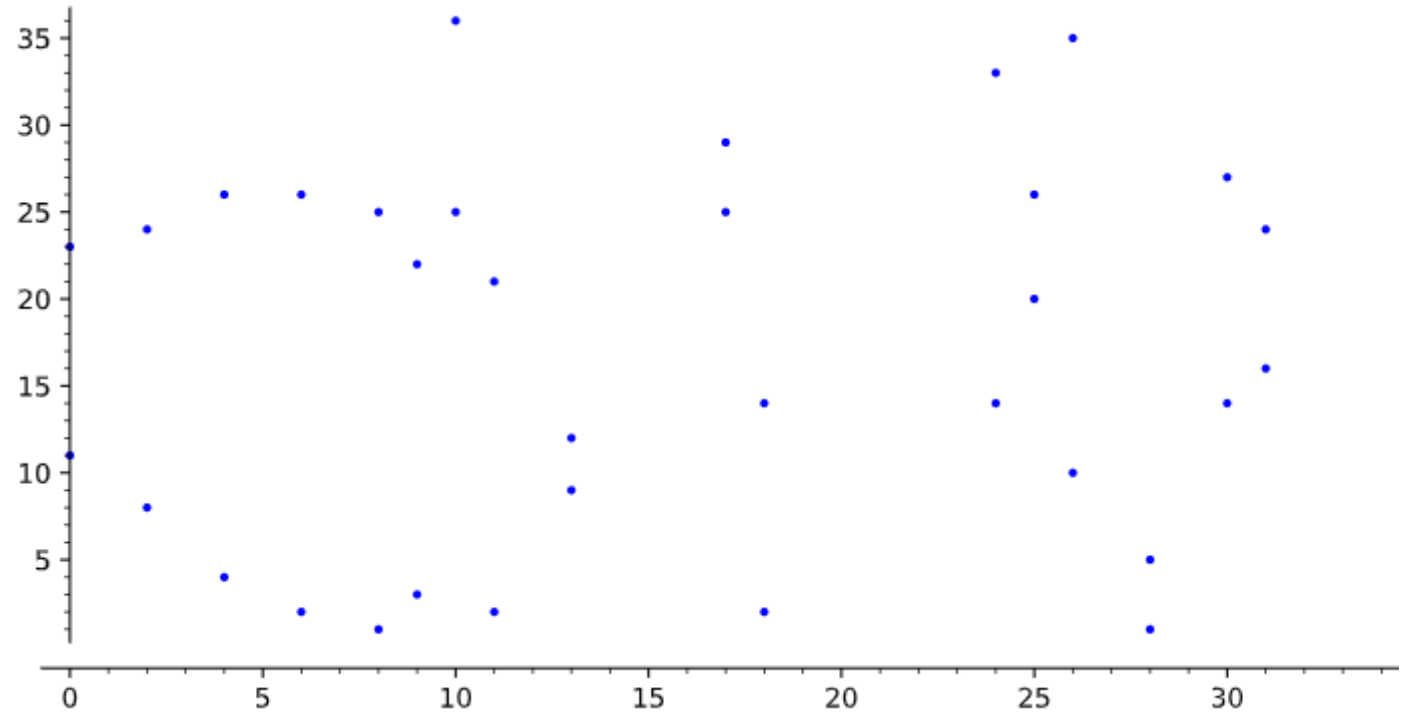
```
(2 : 0 : 1)
```

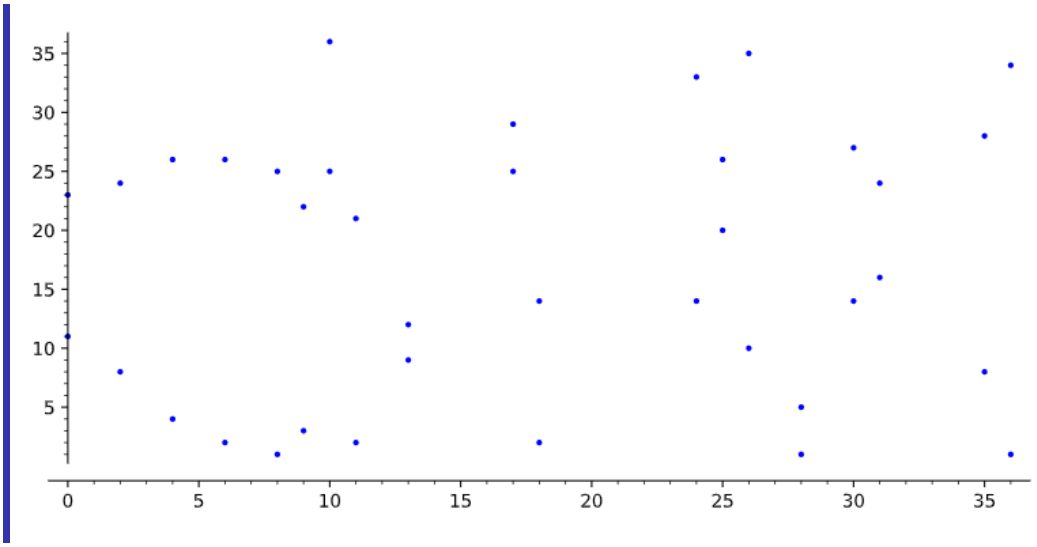
```
(4 : 2 : 1)
```

```
76 E = EllipticCurve(GF(37),[1,2,3,4,6])
77 E.abelian_group()
```

```
Additive abelian group isomorphic to Z/39 embedded in Abelian group of points on Elliptic Curve
defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 6 over Finite Field of size 37
```

```
78 E.plot()
```






```
79 E.frobenius()
```

```
phi
```

```
80 E.frobenius().minpoly()
```

```
x^2 + x + 37
```

```
81 E.trace_of_frobenius()
```

```
-1
```

```
82 E.is_supersingular()
```

```
False
```

```
83 I=E.isogenies_prime_degree()
84 I
```

```
[Isogeny of degree 3 from Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 6 over
Finite Field of size 37 to Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 33*x + 10 o
Finite Field of size 37, Isogeny of degree 7 from Elliptic Curve defined by y^2 + x*y + 3*y = x^
2*x^2 + 4*x + 6 over Finite Field of size 37 to Elliptic Curve defined by y^2 = x^3 + 33 over Fi
Field of size 37, Isogeny of degree 13 from Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*
+ 4*x + 6 over Finite Field of size 37 to Elliptic Curve defined by y^2 = x^3 + 7*x + 33 over Fi
Field of size 37, Isogeny of degree 13 from Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*
+ 4*x + 6 over Finite Field of size 37 to Elliptic Curve defined by y^2 = x^3 + x + 3 over Finit
Field of size 37, Isogeny of degree 19 from Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*
+ 4*x + 6 over Finite Field of size 37 to Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^
13 over Finite Field of size 37, Isogeny of degree 19 from Elliptic Curve defined by y^2 + x*y +
= x^3 + 2*x^2 + 4*x + 6 over Finite Field of size 37 to Elliptic Curve defined by y^2 + x*y + 3*
x^3 + 2*x^2 + 30*x + 31 over Finite Field of size 37, Isogeny of degree 31 from Elliptic Curve
defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 6 over Finite Field of size 37 to Elliptic Curv
defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 30*x + 17 over Finite Field of size 37, Isogeny of de
31 from Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 4*x + 6 over Finite Field of s
```

```
37 to Elliptic Curve defined by y^2 + x*y + 3*y = x^3 + 2*x^2 + 18*x + 11 over Finite Field of s
37]
```

```
85 [psi.degree() for psi in I]
```

```
[3, 7, 13, 13, 19, 19, 31, 31]
```

```
86 # p-ADICS
87 Z5 = Zp(5,prec=20)
88 a = Z5(1/2)
89 b = Z5(1/3)
90 a
91 b
```

```
3 + 2*5 + 2*5^2 + 2*5^3 + 2*5^4 + 2*5^5 + 2*5^6 + 2*5^7 + 2*5^8 + 2*5^9 + 2*5^10 + 2*5^11 + 2*5^
2*5^13 + 2*5^14 + 2*5^15 + 2*5^16 + 2*5^17 + 2*5^18 + 2*5^19 + O(5^20)
```

```
2 + 3*5 + 5^2 + 3*5^3 + 5^4 + 3*5^5 + 5^6 + 3*5^7 + 5^8 + 3*5^9 + 5^10 + 3*5^11 + 5^12 + 3*5^13
5^14 + 3*5^15 + 5^16 + 3*5^17 + 5^18 + 3*5^19 + O(5^20)
```

```
92 a+b
```

```
5 + 4*5^2 + 4*5^4 + 4*5^6 + 4*5^8 + 4*5^10 + 4*5^12 + 4*5^14 + 4*5^16 + 4*5^18 + O(5^20)
```

```
93 v = Z5.valuation()
94 v(a+b)
```

```
1
```

```
95 P.<x> = PolynomialRing(Z5)
96 f= x^2-2
97 f.roots()
```

```
[]
```

```
98 P.<x> = PolynomialRing(Z5)
99 f= x^2-1
100 f.roots()
```

```
[(4 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + 4*5^9 + 4*5^10 + 4*5^11 + 4*
+ 4*5^13 + 4*5^14 + 4*5^15 + 4*5^16 + 4*5^17 + 4*5^18 + 4*5^19 + O(5^20), 1), (1 + O(5^20), 1)]
```

```
101 Z7 = Zp(7,20)
102 P.<x> = PolynomialRing(Z7)
103 f= x^2-2
104 f.roots()
```

```
[(3 + 7 + 2*7^2 + 6*7^3 + 7^4 + 2*7^5 + 7^6 + 2*7^7 + 4*7^8 + 6*7^9 + 6*7^10 + 2*7^11 + 7^12 + 7
+ 2*7^15 + 7^16 + 7^17 + 4*7^18 + 6*7^19 + O(7^20), 1), (4 + 5*7 + 4*7^2 + 5*7^4 + 4*7^5 + 5*7^6
4*7^7 + 2*7^8 + 4*7^11 + 5*7^12 + 5*7^13 + 6*7^14 + 4*7^15 + 5*7^16 + 5*7^17 + 2*7^18 + O(7^20),
```

```
105 P.<x> = PolynomialRing(Z5)
```

```
f= x^4-1
f.roots()
```

```
[(4 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + 4*5^9 + 4*5^10 + 4*5^11 + 4*
+ 4*5^13 + 4*5^14 + 4*5^15 + 4*5^16 + 4*5^17 + 4*5^18 + 4*5^19 + O(5^20), 1), (2 + 5 + 2*5^2 + 
3*5^4 + 4*5^5 + 2*5^6 + 3*5^7 + 3*5^9 + 2*5^10 + 2*5^11 + 4*5^13 + 5^14 + 3*5^15 + 2*5^16 + 4*5
4*5^19 + O(5^20), 1), (3 + 3*5 + 2*5^2 + 3*5^3 + 5^4 + 2*5^6 + 5^7 + 4*5^8 + 5^9 + 2*5^10 + 2*5
4*5^12 + 3*5^14 + 5^15 + 2*5^16 + 4*5^18 + O(5^20), 1), (1 + O(5^20), 1)]
```

```
P.<x> = PolynomialRing(Z5)
f= x^2-5
f.roots()
```

```
[]
```

```
Z7 = Zp(7,20)
P.<x> = PolynomialRing(Z7)
f= x^6-1
f.roots()
```

```
[(6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 + 6*7^9 + 6*7^10 + 6*7^11 + 6*
+ 6*7^13 + 6*7^14 + 6*7^15 + 6*7^16 + 6*7^17 + 6*7^18 + 6*7^19 + O(7^20), 1), (5 + 2*7 + 3*7^3 +
6*7^4 + 4*7^5 + 4*7^7 + 2*7^8 + 3*7^9 + 2*7^10 + 2*7^11 + 7^12 + 4*7^13 + 5*7^14 + 4*7^15 + 5*7^
2*7^17 + 5*7^19 + O(7^20), 1), (4 + 2*7 + 3*7^3 + 6*7^4 + 4*7^5 + 4*7^7 + 2*7^8 + 3*7^9 + 2*7^10
2*7^11 + 7^12 + 4*7^13 + 5*7^14 + 4*7^15 + 5*7^16 + 2*7^17 + 5*7^19 + O(7^20), 1), (3 + 4*7 + 6*
+ 3*7^3 + 2*7^5 + 6*7^6 + 2*7^7 + 4*7^8 + 3*7^9 + 4*7^10 + 4*7^11 + 5*7^12 + 2*7^13 + 7^14 + 2*7
+ 7^16 + 4*7^17 + 6*7^18 + 7^19 + O(7^20), 1), (2 + 4*7 + 6*7^2 + 3*7^3 + 2*7^5 + 6*7^6 + 2*7^7
4*7^8 + 3*7^9 + 4*7^10 + 4*7^11 + 5*7^12 + 2*7^13 + 7^14 + 2*7^15 + 7^16 + 4*7^17 + 6*7^18 + 7^1
O(7^20), 1), (1 + O(7^20), 1)]
```

```
C.<c> = CyclotomicField(125)
G = C.galois_group()
G
```

```
Galois group of Cyclotomic Field of order 125 and degree 100
```

```
G.is_cyclic()
G.order()
g = G.gens()[0]
g
```

```
True
```

```
100
```

```
(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35
```

```
H = G.subgroup([g])
```

```
H.fixed_field()
```

```
(Number Field in c0 with defining polynomial x with c0 = 0, Ring morphism:
  From: Number Field in c0 with defining polynomial x with c0 = 0
  To:   Cyclotomic Field of order 125 and degree 100
  Defn: 0 |--> 0)
```

```
K = H.fixed_field()[0]
K.degree()
```

```
1
```

```
H = G.subgroup([g^2])
K = H.fixed_field()[0]
K.degree()
K
```

```
2

Number Field in c0 with defining polynomial x^2 + 25*x - 625 with c0 = 15.45084971874738?
```

```
H = G.subgroup([g^5])
K = H.fixed_field()[0]
K.degree()
K
```

```
5

Number Field in c0 with defining polynomial x^5 - 250*x^3 + 625*x^2 + 6250*x + 3125 with c0 =
7.812018465429065?
```

```
P.<x> = PolynomialRing(QQ)
K.<k> = NumberField(x^5 - 250*x^3 + 625*x^2 + 6250*x + 3125)
K.is_galois()
K.galois_group().is_cyclic()
```

```
True

True
```

```
# SageMath code for working with number field 5.5.390625.1

# (Note that not all these functions may be available, and some may take a long time to execute.

# Define the number field:
x = polygen(QQ);  K.<a> = NumberField(x^5 - 10*x^3 - 5*x^2 + 10*x - 1)

# Defining polynomial:
K.defining_polynomial()

# Degree over Q:
K.degree()

# Signature:
```

```
K.signature()

# Discriminant:
K.disc()

# Ramified primes:
K.disc().support()

# Integral basis:
K.integral_basis()

# Class group:
K.class_group().invariants()

# Unit group:
UK = K.unit_group()

# Unit rank:
UK.rank()

# Generator for roots of unity:
UK.torsion_generator()

# Fundamental units:
UK.fundamental_units()

# Regulator:
K.regulator()

# Galois group:
K.galois_group(type='pari')

# Frobenius cycle types:
p = 7;  # to obtain a list of $[e_i,f_i]$ for the factorization of the ideal $p\mathcal{O}_K$:
[(e, pr.norm().valuation(p)) for pr,e in K.factor(p)]
```

```
x^5 - 10*x^3 - 5*x^2 + 10*x - 1

5

(5, 0)

390625

[5]

[4/7*a^4 + 2/7*a^3 + 3/7*a^2 + 6/7*a + 1/7, a, a^2, a^3, a^4]

()

4

u0

[2/7*a^4 + 1/7*a^3 - 23/7*a^2 - 18/7*a + 25/7, 1/7*a^4 - 3/7*a^3 - 8/7*a^2 + 19/7*a + 9/7, 2/7*a
1/7*a^3 - 16/7*a^2 - 25/7*a - 10/7, 3/7*a^4 - 2/7*a^3 - 24/7*a^2 - 6/7*a + 6/7]

16.0696118230553
```

```
Galois group PARI group [5, 1, 1, "C(5) = 5"] of degree 5 of the Number Field in a with defining
polynomial x^5 - 10*x^3 - 5*x^2 + 10*x - 1

[(1, 1), (1, 1), (1, 1), (1, 1), (1, 1)]
```

```
P.<x> = PolynomialRing(QQ)
f = cyclotomic_polynomial(16)
C.<c> = NumberField(f)
G = C.galois_group()
gens = G.gens()
len(gens)
```

```
2
```

```
g1 = gens[0]
g2 = gens[1]
g1.order()
g2.order()
```

```
4

2
```

```
H1 = G.subgroup([g1])
H2 = G.subgroup([g1^2,g2])
K1 = H1.fixed_field()[0]
K1
K2 = H2.fixed_field()[0]
K2
H3 = G.subgroup([g1*g2])
K3 = H3.fixed_field()[0]
K3
```

```
Number Field in c0 with defining polynomial x^2 + 16 with c0 = 4*c^4

Number Field in c0 with defining polynomial x^2 - 8 with c0 = -2*c^6 + 2*c^2

Number Field in c0 with defining polynomial x^2 + 8 with c0 = 2*c^6 + 2*c^2
```

```

#
```