HW11

(In Hoffstein book) 7.16, 7.22 ( (a)(b) by hand (c) (d) use Sage)

7.16. A lattice L of dimension n = 251 has determinant det(L) ≈ 2^2251.58. With no further information, approximately how large would you expect the shortest nonzero vector to be?

According the Gaussian Heuristic, we know that expected shortest length is

. And using python, the shortest nonzero vector v= 1922.9618674339863

Python Code:

import math

math.sqrt(251/(2\*math.pi\*math.e))\*(2\*\*2251.58/251))

Result:

1922.9618674339863

7.22. Compute (by hand!) the polynomial convolution product c = a \* b using the given value of N.

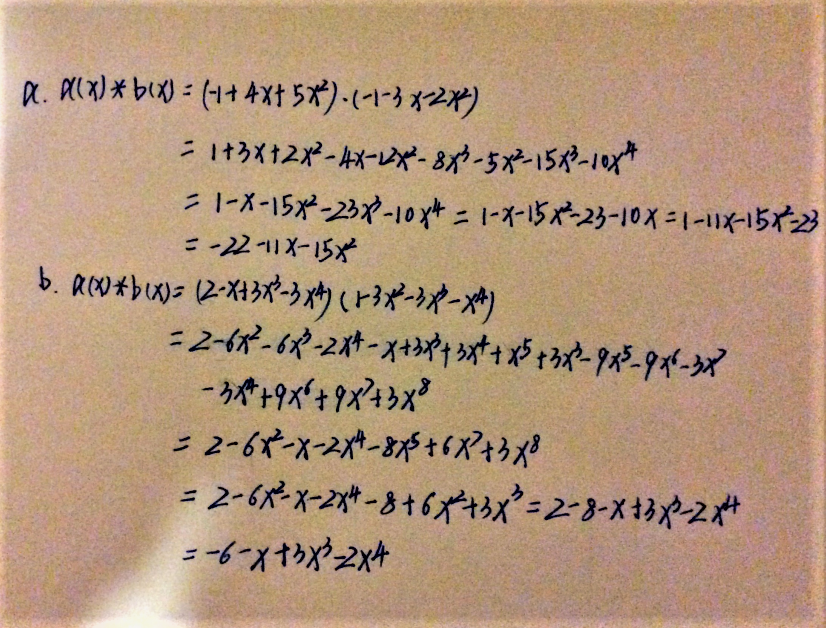
(a) N = 3, a(x) = −1 + 4x + 5x2, b(x) = −1 − 3x − 2x2;

(b) N = 5, a(x) = 2 − x + 3x3 − 3x4, b(x) = 1 − 3x2 − 3x3 − x4;

(c) N = 6, a(x) = x + x2 + x3, b(x) = 1 + x + x5;

(d) N = 10, a(x) = x + x2 + x3 + x4 + x6 + x7 + x9, b(x) = x2 + x3 + x6 + x8.

(a)(b) by hand:



(c)(d)

SageMath Code:

#HW11 7.22 (c)(d)

#(c)

R.<y>=ZZ[]

Rc.<x>=QuotientRing(R,y^6-1)

ac=x+x^2+x^3

bc=1+x+x^5

print '(c): na(x)\*b(x)='+str(ac\*bc)

#(d)

R.<y>=ZZ[]

Rd.<x>=QuotientRing(R,y^10-1)

ad=x+x^2+x^3+x^4+x^6+x^7+x^9

bd=x^2+x^3+x^6+x^8

print '(d): na(x)\*b(x)='+str(ad\*bd)

Result:

(c): a(x)\*b(x)=x^4 + 2\*x^3 + 3\*x^2 + 2\*x + 1

(d): a(x)\*b(x)=4\*x^9 + 2\*x^8 + 3\*x^7 + 2\*x^6 + 4\*x^5 + 3\*x^4 + 2\*x^3 + 3\*x^2 + 2\*x + 3