**COEN 350: Network Security**

**ASSIGNMENT 4**

**Shweta Kharat**

**Date: 08/27/2019**

**Blum, Blum, and Shub Pseudorandom Bit Generator**

**Code (Java):**

**import** java.util.ArrayList;

**import** java.util.Arrays;

**import** java.util.Collections;

**import** java.util.HashSet;

**import** java.util.List;

**public** **class** PseudoRandomBitGenerator {

**public** **static** **void** main(String[] args) {

// **TODO** Auto-generated method stub

*BBSPseudoRandomBitGenerator*(3, 7);

*BBSPseudoRandomBitGenerator*(7, 11);

*BBSPseudoRandomBitGenerator*(19, 23);

}

**public** **static** **int** EuclideanAlgo(**int** a, **int** b){

**int** temp = 0;

**while**(b != 0){

temp = b;

b = a % b;

a = temp;

}

**return** a;

}

**public** **static** **void** BBSPseudoRandomBitGenerator(**int** p, **int** q){

System.***out***.println("Given p = "+p+" q = "+q);

**int** n = p \* q;

**int** l = n-1;

**int** size = (n-1) / 2;

**int** [] s = **new** **int**[size];

**int** s1 = 1, i = 0;

**while**(s1 <= size){

**int** t1 = *EuclideanAlgo*(s1,p);

**int** t2 = *EuclideanAlgo*(s1,q);

**if**(t1 == 1 && t2 == 1){

s[i] = s1;

i++;

}

s1++;

}

System.***out***.print("S = ");

**for**(**int** j = 0; j < i; j++){

System.***out***.print(s[j] + " ");

}

**int** [] x0 = **new** **int**[size];

**int** itr = 0;

**for**(**int** j = 0; j < i; j++){

**int** temp = 1;

**int** t3 = (s[j] \* s[j]) % n;

**if**(j>0){

**for**(**int** k = 0; k < j; k++){

**if**(x0[k] == t3){

temp = 0;

}

}

}

**if**(temp == 1){

x0[itr] = t3;

itr++;

}

}

**int** len = 0;

**int** [] x0t = **new** **int**[itr];

**for**(**int** li = 0; li<size; li++){

**if**(x0[li] != 0){

x0t[len] = x0[li];

len++;

}

}

Arrays.*sort*(x0t);

System.***out***.print("\nx0 = ");

**for**(**int** m = 0; m<x0t.length; m++){

System.***out***.print(x0t[m] + " ");

}

System.***out***.println("\n");

List<Integer> [] cycles = **new** List[x0t.length];

List<Integer> [] bi = **new** List[x0t.length];

**for**(**int** ii=0; ii<x0t.length; ii++){

cycles[ii] = **new** ArrayList();

bi[ii] = **new** ArrayList();

**int** []x = **new** **int**[x0t.length];

x[0] = x0t[ii];

bi[ii].add(x0t[ii]%2);

**for**(**int** ij=1;ij<x0t.length;ij++){

x[ij] = (x[ij - 1] \* x[ij - 1]) % n;

bi[ii].add(x[ij]%2);

}

**int** k=0;

**for**(**int** il=1; il<x.length; il++){

**if**(x[0] == x[il]){

k = il;

**break**;

}

}

**if**(k==0)k=1;

System.***out***.print("Integers in cycle for x0= "+x0t[ii]);

System.***out***.print("\tT=" + k +"\n");

**for**(**int** ik=0;ik<k;ik++){

System.***out***.print(x[ik]+" ");

cycles[ii].add(x[ik]);

}

System.***out***.print("\nBits Bi= " );

**if**(k>20){

k = 20;

}

**for**(**int** ikk=0;ikk<k;ikk++){

System.***out***.print(bi[ii].get(ikk)+" ");

}

System.***out***.println("\n");

}

**boolean** []flag = **new** **boolean**[x0t.length];

**for**(**int** zz=0; zz<x0t.length; zz++){

flag[zz] = **false**;

Collections.*sort*(cycles[zz]);

}

**for**(**int** z=0; z<x0t.length-1; z++){

**for**(**int** y=z+1; y<x0t.length; y++){

**if**(cycles[z].equals(cycles[y])){

flag[y] = **true**;

//System.out.println(y+" ");

}

}

}

System.***out***.println("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*");

System.***out***.println("Unique cycles are ");

System.***out***.print("\*");

**for** (**int** iw = 0; iw < x0t.length; iw++) {

**if**(flag[iw] == **false**){

**for** (**int** jw = 0; jw < cycles[iw].size(); jw++) {

System.***out***.print(" "+ cycles[iw].get(jw) + " ");

}

System.***out***.print("\n\* ");

}

}

System.***out***.println("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*");

System.***out***.println("\n");

}

}

**Output:**

Given p = 3 q = 7

S = 1 2 4 5 8 10

x0 = 1 4 16

Integers in cycle for x0= 1 T=1

1

Bits Bi= 1

Integers in cycle for x0= 4 T=2

4 16

Bits Bi= 0 0

Integers in cycle for x0= 16 T=2

16 4

Bits Bi= 0 0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Unique cycles are

\* 1

\* 4 16

\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Given p = 7 q = 11

S = 1 2 3 4 5 6 8 9 10 12 13 15 16 17 18 19 20 23 24 25 26 27 29 30 31 32 34 36 37 38

x0 = 1 4 9 15 16 23 25 36 37 53 58 60 64 67 71

Integers in cycle for x0= 1 T=1

1

Bits Bi= 1

Integers in cycle for x0= 4 T=4

4 16 25 9

Bits Bi= 0 0 1 1

Integers in cycle for x0= 9 T=4

9 4 16 25

Bits Bi= 1 0 0 1

Integers in cycle for x0= 15 T=4

15 71 36 64

Bits Bi= 1 1 0 0

Integers in cycle for x0= 16 T=4

16 25 9 4

Bits Bi= 0 1 1 0

Integers in cycle for x0= 23 T=2

23 67

Bits Bi= 1 1

Integers in cycle for x0= 25 T=4

25 9 4 16

Bits Bi= 1 1 0 0

Integers in cycle for x0= 36 T=4

36 64 15 71

Bits Bi= 0 0 1 1

Integers in cycle for x0= 37 T=4

37 60 58 53

Bits Bi= 1 0 0 1

Integers in cycle for x0= 53 T=4

53 37 60 58

Bits Bi= 1 1 0 0

Integers in cycle for x0= 58 T=4

58 53 37 60

Bits Bi= 0 1 1 0

Integers in cycle for x0= 60 T=4

60 58 53 37

Bits Bi= 0 0 1 1

Integers in cycle for x0= 64 T=4

64 15 71 36

Bits Bi= 0 1 1 0

Integers in cycle for x0= 67 T=2

67 23

Bits Bi= 1 1

Integers in cycle for x0= 71 T=4

71 36 64 15

Bits Bi= 1 0 0 1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Unique cycles are

\* 1

\* 4 9 16 25

\* 15 36 64 71

\* 23 67

\* 37 53 58 60

\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Given p = 19 q = 23

S = 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 20 21 22 24 25 26 27 28 29 30 31 32 33 34 35 36 37 39 40 41 42 43 44 45 47 48 49 50 51 52 53 54 55 56 58 59 60 61 62 63 64 65 66 67 68 70 71 72 73 74 75 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 93 94 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 134 135 136 137 139 140 141 142 143 144 145 146 147 148 149 150 151 153 154 155 156 157 158 159 160 162 163 164 165 166 167 168 169 170 172 173 174 175 176 177 178 179 180 181 182 183 185 186 187 188 189 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 208 210 211 212 213 214 215 216 217 218

x0 = 1 4 6 9 16 24 25 26 35 36 39 47 49 54 55 58 62 64 73 77 81 82 85 87 93 96 100 101 104 118 119 121 123 131 139 140 142 144 150 156 163 169 177 187 188 196 197 210 213 215 216 220 225 232 233 234 239 248 254 256 271 277 282 289 292 294 301 302 305 308 311 315 324 328 330 334 340 346 347 348 349 351 353 358 370 372 377 381 384 386 397 400 403 404 415 416 422 423 427

Integers in cycle for x0= 1 T=1

1

Bits Bi= 1

Integers in cycle for x0= 4 T=30

4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416

Bits Bi= 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1

Integers in cycle for x0= 6 T=30

6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81

Bits Bi= 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0

Integers in cycle for x0= 9 T=30

9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187

Bits Bi= 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1

Integers in cycle for x0= 16 T=30

16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4

Bits Bi= 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0

Integers in cycle for x0= 24 T=6

24 139 93 346 415 47

Bits Bi= 0 1 1 0 1 1

Integers in cycle for x0= 25 T=30

25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271

Bits Bi= 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0

Integers in cycle for x0= 26 T=10

26 239 311 144 197 353 64 163 349 315

Bits Bi= 0 1 1 0 1 1 0 1 1 1

Integers in cycle for x0= 35 T=30

35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308

Bits Bi= 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1

Integers in cycle for x0= 36 T=30

36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6

Bits Bi= 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1

Integers in cycle for x0= 39 T=10

39 210 400 58 305 381 77 248 324 96

Bits Bi= 1 0 0 0 1 1 1 0 0 0

Integers in cycle for x0= 47 T=6

47 24 139 93 346 415

Bits Bi= 1 0 1 1 0 1

Integers in cycle for x0= 49 T=10

49 216 334 121 220 330 87 140 372 292

Bits Bi= 1 0 0 1 0 0 1 0 0 0

Integers in cycle for x0= 54 T=30

54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289

Bits Bi= 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1

Integers in cycle for x0= 55 T=30

55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348

Bits Bi= 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0

Integers in cycle for x0= 58 T=10

58 305 381 77 248 324 96 39 210 400

Bits Bi= 0 1 1 1 0 0 0 1 0 0

Integers in cycle for x0= 62 T=30

62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142

Bits Bi= 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0

Integers in cycle for x0= 64 T=10

64 163 349 315 26 239 311 144 197 353

Bits Bi= 0 1 1 1 0 1 1 0 1 1

Integers in cycle for x0= 73 T=30

73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232

Bits Bi= 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0

Integers in cycle for x0= 77 T=10

77 248 324 96 39 210 400 58 305 381

Bits Bi= 1 0 0 0 1 0 0 0 1 1

Integers in cycle for x0= 81 T=30

81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9

Bits Bi= 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1

Integers in cycle for x0= 82 T=30

82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328

Bits Bi= 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1

Integers in cycle for x0= 85 T=30

85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73

Bits Bi= 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1

Integers in cycle for x0= 87 T=10

87 140 372 292 49 216 334 121 220 330

Bits Bi= 1 0 0 0 1 0 0 1 0 0

Integers in cycle for x0= 93 T=6

93 346 415 47 24 139

Bits Bi= 1 0 1 1 0 1

Integers in cycle for x0= 96 T=10

96 39 210 400 58 305 381 77 248 324

Bits Bi= 0 1 0 0 0 1 1 1 0 0

Integers in cycle for x0= 100 T=30

100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427

Bits Bi= 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0

Integers in cycle for x0= 101 T=30

101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233

Bits Bi= 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0

Integers in cycle for x0= 104 T=30

104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377

Bits Bi= 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1

Integers in cycle for x0= 118 T=30

118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131

Bits Bi= 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0

Integers in cycle for x0= 119 T=30

119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370

Bits Bi= 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1

Integers in cycle for x0= 121 T=10

121 220 330 87 140 372 292 49 216 334

Bits Bi= 1 0 0 1 0 0 0 1 0 0

Integers in cycle for x0= 123 T=30

123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358

Bits Bi= 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0

Integers in cycle for x0= 131 T=30

131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234

Bits Bi= 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0

Integers in cycle for x0= 139 T=6

139 93 346 415 47 24

Bits Bi= 1 1 0 1 1 0

Integers in cycle for x0= 140 T=10

140 372 292 49 216 334 121 220 330 87

Bits Bi= 0 0 0 1 0 0 1 0 0 1

Integers in cycle for x0= 142 T=30

142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301

Bits Bi= 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1

Integers in cycle for x0= 144 T=10

144 197 353 64 163 349 315 26 239 311

Bits Bi= 0 1 1 0 1 1 1 0 1 1

Integers in cycle for x0= 150 T=30

150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101

Bits Bi= 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0

Integers in cycle for x0= 156 T=30

156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169

Bits Bi= 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0

Integers in cycle for x0= 163 T=10

163 349 315 26 239 311 144 197 353 64

Bits Bi= 1 1 1 0 1 1 0 1 1 0

Integers in cycle for x0= 169 T=30

169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82

Bits Bi= 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1

Integers in cycle for x0= 177 T=30

177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119

Bits Bi= 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0

Integers in cycle for x0= 187 T=30

187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384

Bits Bi= 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1

Integers in cycle for x0= 188 T=30

188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25

Bits Bi= 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0

Integers in cycle for x0= 196 T=30

196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423

Bits Bi= 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1

Integers in cycle for x0= 197 T=10

197 353 64 163 349 315 26 239 311 144

Bits Bi= 1 1 0 1 1 1 0 1 1 0

Integers in cycle for x0= 210 T=10

210 400 58 305 381 77 248 324 96 39

Bits Bi= 0 0 0 1 1 1 0 0 0 1

Integers in cycle for x0= 213 T=30

213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150

Bits Bi= 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1

Integers in cycle for x0= 215 T=30

215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404

Bits Bi= 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0

Integers in cycle for x0= 216 T=10

216 334 121 220 330 87 140 372 292 49

Bits Bi= 0 0 1 0 0 1 0 0 0 1

Integers in cycle for x0= 220 T=10

220 330 87 140 372 292 49 216 334 121

Bits Bi= 0 0 1 0 0 0 1 0 0 1

Integers in cycle for x0= 225 T=30

225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422

Bits Bi= 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1

Integers in cycle for x0= 232 T=30

232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340

Bits Bi= 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1

Integers in cycle for x0= 233 T=30

233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85

Bits Bi= 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1

Integers in cycle for x0= 234 T=30

234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347

Bits Bi= 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0

Integers in cycle for x0= 239 T=10

239 311 144 197 353 64 163 349 315 26

Bits Bi= 1 1 0 1 1 0 1 1 1 0

Integers in cycle for x0= 248 T=10

248 324 96 39 210 400 58 305 381 77

Bits Bi= 0 0 0 1 0 0 0 1 1 1

Integers in cycle for x0= 254 T=2

254 277

Bits Bi= 0 1

Integers in cycle for x0= 256 T=30

256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16

Bits Bi= 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0

Integers in cycle for x0= 271 T=30

271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123

Bits Bi= 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1

Integers in cycle for x0= 277 T=2

277 254

Bits Bi= 1 0

Integers in cycle for x0= 282 T=30

282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403

Bits Bi= 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0

Integers in cycle for x0= 289 T=30

289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397

Bits Bi= 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0

Integers in cycle for x0= 292 T=10

292 49 216 334 121 220 330 87 140 372

Bits Bi= 0 1 0 0 1 0 0 1 0 0

Integers in cycle for x0= 294 T=30

294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54

Bits Bi= 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0

Integers in cycle for x0= 301 T=30

301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156

Bits Bi= 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0

Integers in cycle for x0= 302 T=30

302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177

Bits Bi= 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0

Integers in cycle for x0= 305 T=10

305 381 77 248 324 96 39 210 400 58

Bits Bi= 1 1 1 0 0 0 1 0 0 0

Integers in cycle for x0= 308 T=30

308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302

Bits Bi= 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1

Integers in cycle for x0= 311 T=10

311 144 197 353 64 163 349 315 26 239

Bits Bi= 1 0 1 1 0 1 1 1 0 1

Integers in cycle for x0= 315 T=10

315 26 239 311 144 197 353 64 163 349

Bits Bi= 1 0 1 1 0 1 1 0 1 1

Integers in cycle for x0= 324 T=10

324 96 39 210 400 58 305 381 77 248

Bits Bi= 0 0 1 0 0 0 1 1 1 0

Integers in cycle for x0= 328 T=30

328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104

Bits Bi= 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0 1 0

Integers in cycle for x0= 330 T=10

330 87 140 372 292 49 216 334 121 220

Bits Bi= 0 1 0 0 0 1 0 0 1 0

Integers in cycle for x0= 334 T=10

334 121 220 330 87 140 372 292 49 216

Bits Bi= 0 1 0 0 1 0 0 0 1 0

Integers in cycle for x0= 340 T=30

340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215

Bits Bi= 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 0

Integers in cycle for x0= 346 T=6

346 415 47 24 139 93

Bits Bi= 0 1 1 0 1 1

Integers in cycle for x0= 347 T=30

347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294

Bits Bi= 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0

Integers in cycle for x0= 348 T=30

348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62

Bits Bi= 0 1 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1

Integers in cycle for x0= 349 T=10

349 315 26 239 311 144 197 353 64 163

Bits Bi= 1 1 0 1 1 0 1 1 0 1

Integers in cycle for x0= 351 T=30

351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35

Bits Bi= 1 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1

Integers in cycle for x0= 353 T=10

353 64 163 349 315 26 239 311 144 197

Bits Bi= 1 0 1 1 1 0 1 1 0 1

Integers in cycle for x0= 358 T=30

358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213

Bits Bi= 0 1 1 1 0 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1

Integers in cycle for x0= 370 T=30

370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225

Bits Bi= 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0 1 1

Integers in cycle for x0= 372 T=10

372 292 49 216 334 121 220 330 87 140

Bits Bi= 0 0 1 0 0 1 0 0 1 0

Integers in cycle for x0= 377 T=30

377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118

Bits Bi= 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 0

Integers in cycle for x0= 381 T=10

381 77 248 324 96 39 210 400 58 305

Bits Bi= 1 1 0 0 0 1 0 0 0 1

Integers in cycle for x0= 384 T=30

384 187 9 81 6 36 422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188

Bits Bi= 0 1 1 1 0 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1

Integers in cycle for x0= 386 T=30

386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100

Bits Bi= 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1

Integers in cycle for x0= 397 T=30

397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256 423 196

Bits Bi= 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 1

Integers in cycle for x0= 400 T=10

400 58 305 381 77 248 324 96 39 210

Bits Bi= 0 0 1 1 1 0 0 0 1 0

Integers in cycle for x0= 403 T=30

403 282 427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55

Bits Bi= 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1

Integers in cycle for x0= 404 T=30

404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36 422 225 370 119 177 302 308 35 351

Bits Bi= 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 1 1 1 0

Integers in cycle for x0= 415 T=6

415 47 24 139 93 346

Bits Bi= 1 1 0 1 1 0

Integers in cycle for x0= 416 T=30

416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386

Bits Bi= 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0

Integers in cycle for x0= 422 T=30

422 225 370 119 177 302 308 35 351 404 215 340 232 73 85 233 101 150 213 358 123 271 25 188 384 187 9 81 6 36

Bits Bi= 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 1 0

Integers in cycle for x0= 423 T=30

423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282 427 100 386 416 4 16 256

Bits Bi= 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 0 0

Integers in cycle for x0= 427 T=30

427 100 386 416 4 16 256 423 196 397 289 54 294 347 234 131 118 377 104 328 82 169 156 301 142 62 348 55 403 282

Bits Bi= 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 0 0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Unique cycles are

\* 1

\* 4 16 54 55 62 82 100 104 118 131 142 156 169 196 234 256 282 289 294 301 328 347 348 377 386 397 403 416 423 427

\* 6 9 25 35 36 73 81 85 101 119 123 150 177 187 188 213 215 225 232 233 271 302 308 340 351 358 370 384 404 422

\* 24 47 93 139 346 415

\* 26 64 144 163 197 239 311 315 349 353

\* 39 58 77 96 210 248 305 324 381 400

\* 49 87 121 140 216 220 292 330 334 372

\* 254 277

\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*