# Modular Arithmetic and Elliptic Curves

# Point Counting

- $y^2 = x^3 + ax + b$
  - This curve contains infinitely many points in the real numbers
- $y^2 \equiv x^3 + ax + b \pmod{p}$
  - This curve restricts the possible points to integers from 0 to p-1
- The points on the curve are integer pairs

# Modular Arithmetic

- Division Algorithm
  - $a = bn + r$
  - For a given a and n, b and r exist and are unique
  - Then r is the remainder
- Modular notation
  - $a = bn + r \Leftrightarrow a \equiv r (\mathrm{mod}\, b)$
  - So only the remainder of a number when divided by b is of concern

# An Example (mod 5)

Addition

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | 3 |

Multiplication

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 |
| **2** | 0 | 2 | 4 | 1 | 3 |
| **3** | 0 | 3 | 1 | 4 | 2 |
| **4** | 0 | 4 | 3 | 2 | 1 |

- Addition
  - Zero is the identity
  - Every number has an inverse
- Multiplication
  - One is the identity
  - Inverses exist
  - Zero is a product only when zero is a multiplier
- Note: 5 is prime

$$N_{a,b} = |\{(x,y) \in F_p \times F_p : y^2 = x^3 + ax + b\}|$$

$$F_p = \{0, 1, 2, \ldots, p-1\}$$

# For example, consider a = 1, b =2.

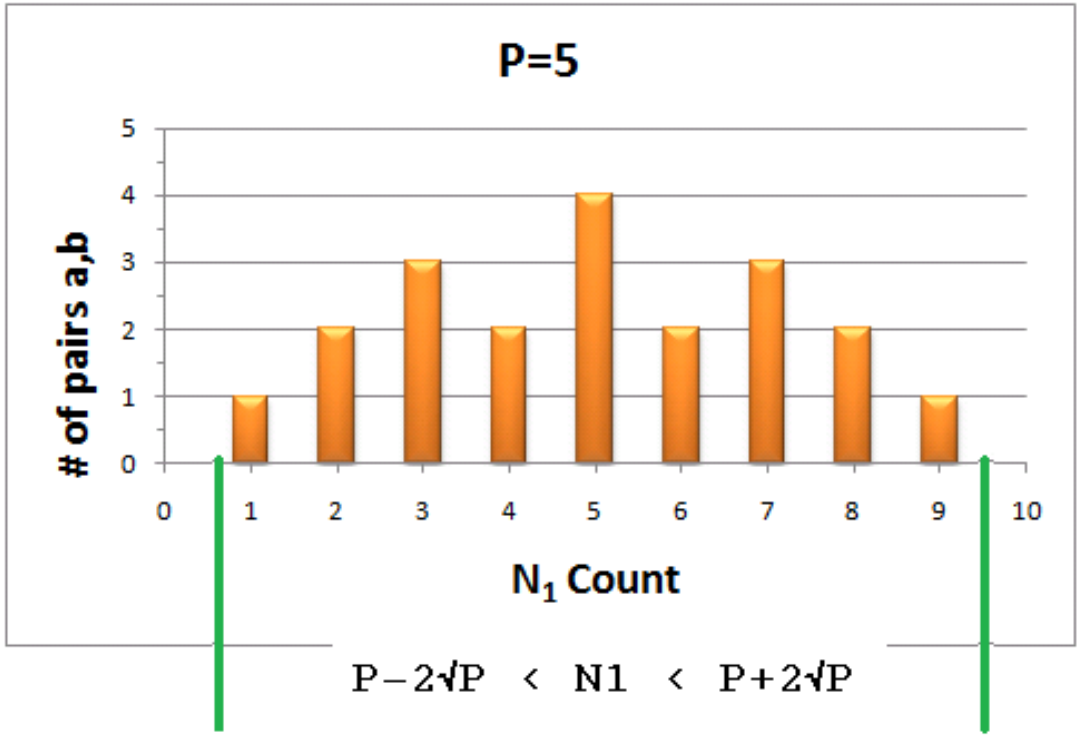
$$y^2 = x^3 + x + 2$$

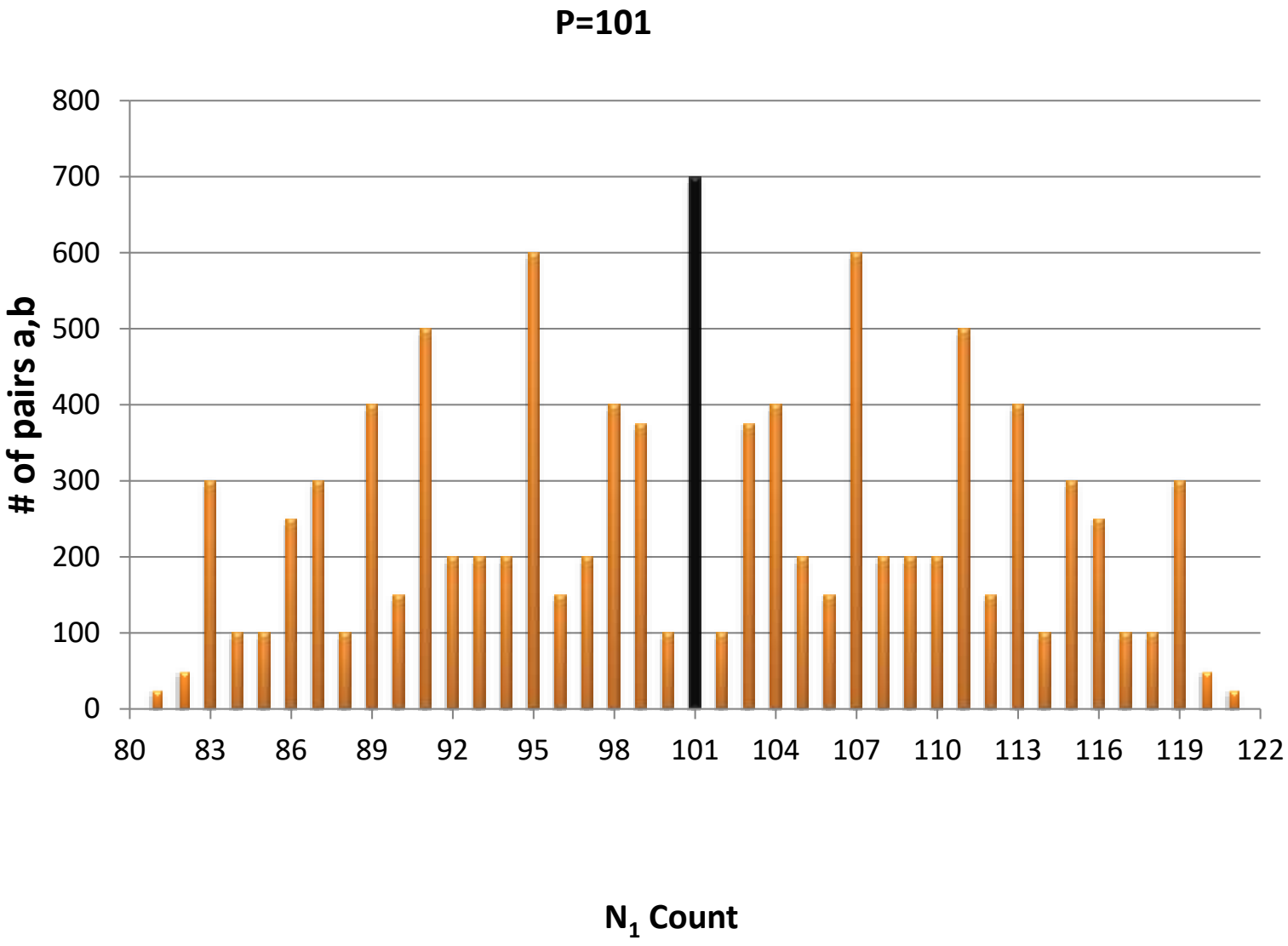
| x | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^3$ | 0 | 1 | 8 | 27 | 64 |
| $x^3$ mod 5 | 0 | 1 | 3 | 2 | 4 |

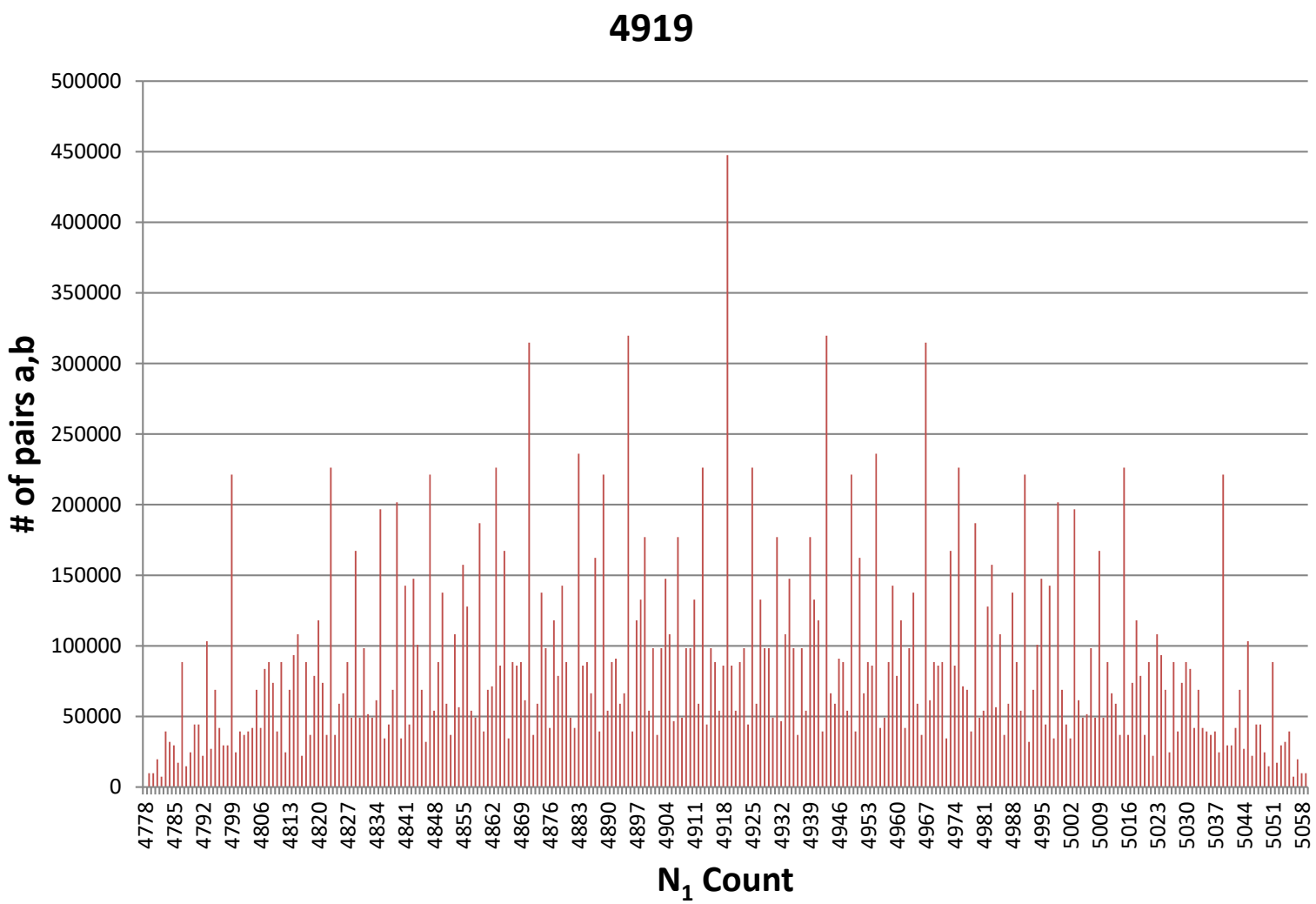
| $x^3 + x + 2$ | 2 | 4 | 12 | 32 | 70 |
|---|---|---|---|---|---|
| mod 5 | 2 | 4 | 2 | 2 | 0 |
| y | | +/- 2 | | | 0 |

| (a,b) | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | ***X*** | 5 | 5 | 5 | 5 |
| 1 | 3 | 8 | 3 | 3 | 8 |
| 2 | 1 | 6 | ***X*** | ***X*** | 6 |
| 3 | 9 | ***X*** | 4 | 4 | ***X*** |
| 4 | 7 | 7 | 2 | 2 | 7 |

| $N_1$ Count | Ordered Pairs a,b that give $N_1$ | $\lvert N_1 \rvert$ |
|---|---|---|
| 0 | | 0 |
| 1 | (2,0) | 1 |
| 2 | (4,2),(4,3) | 2 |
| 3 | (1,0),(1,2),(1,3) | 3 |
| 4 | (3,2),(3,3) | 2 |
| 5 | (0,1),(0,2),(0,3),(0,4) | 4 |
| 6 | (2,1),(2,4) | 2 |
| 7 | (4,0),(4,1),(4,4) | 3 |
| 8 | (1,1),(1,4) | 2 |
| 9 | (3,0) | 1 |
| 10 | | 0 |



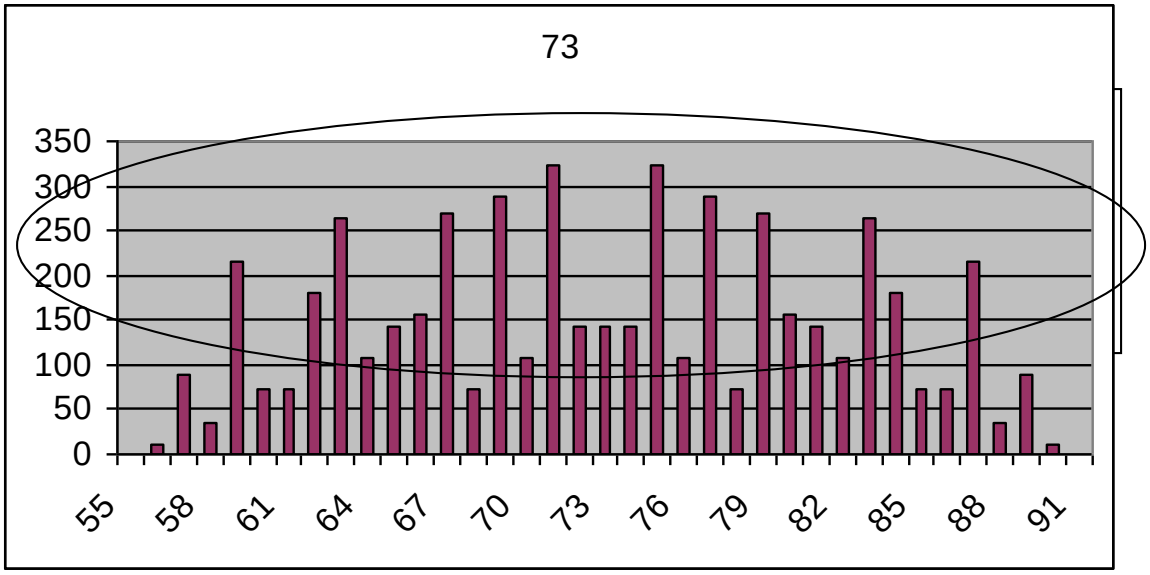

P=101
800
700
600
500
400
300
200
100
0
# of pairs a,b
80
83
86
89
92
95
98
101
104
107
110
113
116
119
122
N1 Count

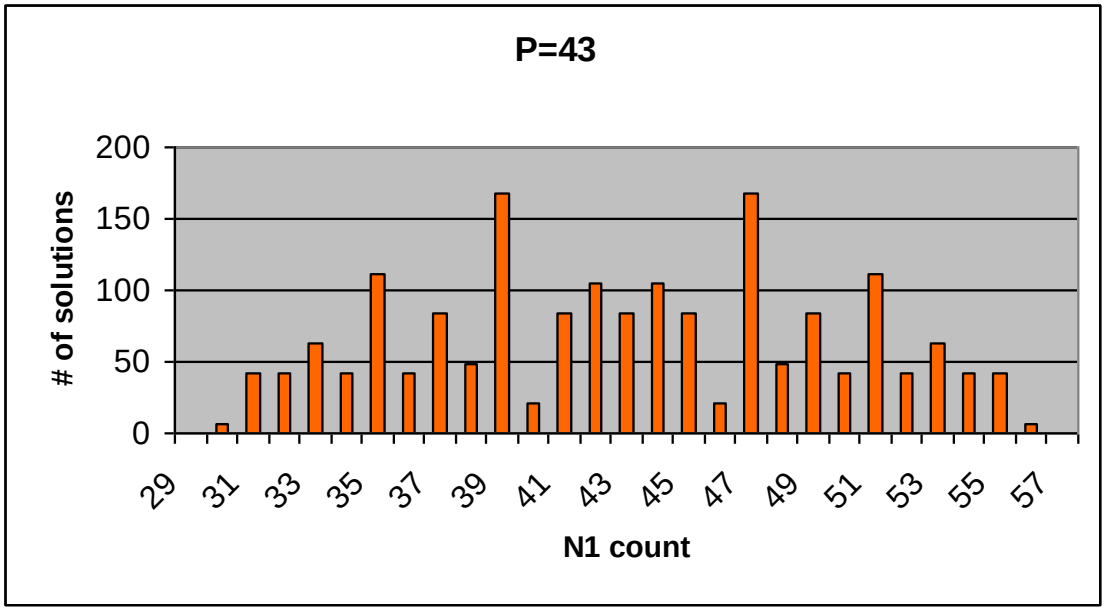

4919
# of pairs a,b
500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
4778
4785
4792
4799
4806
4813
4820
4827
4834
4841
4848
4855
4862
4869
4876
4883
4890
4897
4904
4911
4918
4925
4932
4939
4946
4953
4960
4967
4974
4981
4988
4995
5002
5009
5016
5023
5030
5037
5044
5051
5058
N1 Count

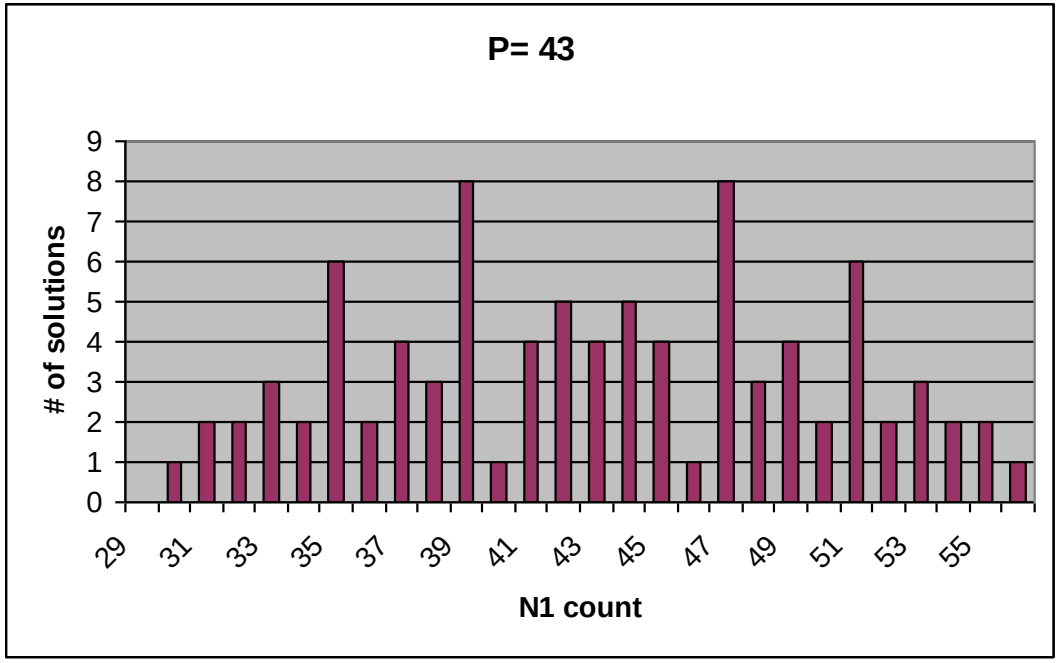
# Future Plans

- Where do the spikes come from?

We know for c a squre in Fp (c^4a,c^6b)=(a',b')




P=43
# of solutions
200
150
100
50
0
29
31
33
35
37
39
41
43
45
47
49
51
53
55
57
N1 count

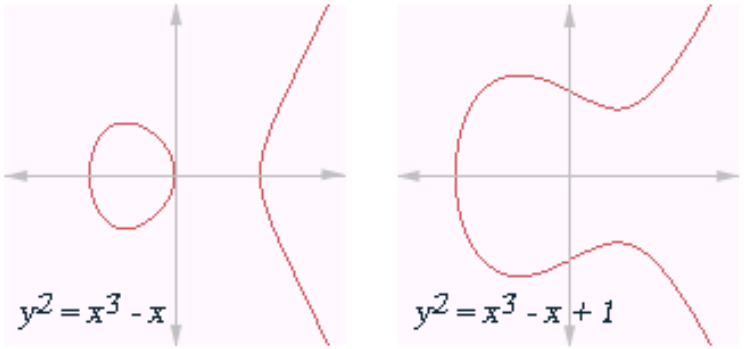

P= 43
# of solutions
9
8
7
6
5
4
3
2
1
0
29
31
33
35
37
39
41
43
45
47
49
51
53
55
N1 count

Special thanks to –

Chris Hall

Siguna Muller

Lynne Ipina




http://schools-wikipedia.org/images/48/4800.png.htm