CIS 3362 Homework #5c Solutions

1) For each prime in between 20 and 1000, pick a random a and b and create the corresponding elliptic curve. For each elliptic curve, calculate the number of points on that curve, including the point O. Make a graph of your data with the x-axis being the prime number and the y-axis being the number of points. Answer the following questions:

a) What pattern(s) do you see in this graph?

b) What points were the “biggest outliers”?

c) What, if any, conclusions do you think can be drawn about the relationship between the prime p and the corresponding number of points on the elliptic curve.

Solution
The code used to create the data is in ectest.c. The corresponding chart is contained in the spreadsheet Hmk5c.xlsx in the tab Question1. Here is the chart corresponding to the data generated:

![Chart](chart.png)

a) The only consistent pattern is that the dots cluster around the line y = x, indicating that the claim the textbook makes, that the number of points on an elliptic curve is roughly equal to the prime being used is likely to be correct. The “band” created around the line seems to be widening (there’s more fluctuation around primes in the 900s than the 500s) in absolute terms, but as p grows large, it’s possible that band is relatively narrow. But, this data is in too narrow a range to draw any conclusions.
b) The biggest outliers were \( p = 797 \) and \( p = 821 \) with 748 and 873 points, respectively. I don’t think there’s anything important about these primes. Rather, it just so happened for the \( a \) and \( b \) (I don’t have that charted) that I picked for these two primes, I got an abnormally low and high number of points.

c) As previously mentioned the only conclusion is that the number of points is “close to” the value of the prime used for the curve.

2) This time, pick five different primes in between 500 and 1000. For each prime, generate 100 valid pairs of \( a \) and \( b \) to generate an elliptic curve. For each curve you generate, determine the number of points on it. Grouping your data by each prime, collect the following statistics about the number of points:

1. average
2. standard deviation
3. minimum
4. maximum
5. mode

a) What pattern(s) do you see in this data?

b) What, if any, conclusions can you draw about the variation of points in an elliptic curve when the prime number chosen is fixed?

Solution
The code used to create the data is in ectest2.c. The corresponding chart is contained in the spreadsheet Hmk5c.xlsx in the tab Question2. Here is the chart corresponding to the data generated:

<table>
<thead>
<tr>
<th>prime</th>
<th>599</th>
<th>641</th>
<th>757</th>
<th>829</th>
<th>997</th>
</tr>
</thead>
<tbody>
<tr>
<td>average</td>
<td>604.23</td>
<td>643.12</td>
<td>758.03</td>
<td>830.47</td>
<td>994.15</td>
</tr>
<tr>
<td>stdev</td>
<td>22.13086</td>
<td>24.53622</td>
<td>28.91138</td>
<td>29.69422</td>
<td>32.31204</td>
</tr>
<tr>
<td>min</td>
<td>556</td>
<td>600</td>
<td>708</td>
<td>778</td>
<td>938</td>
</tr>
<tr>
<td>max</td>
<td>642</td>
<td>690</td>
<td>812</td>
<td>884</td>
<td>1060</td>
</tr>
<tr>
<td>mode</td>
<td>624</td>
<td>636</td>
<td>732</td>
<td>844</td>
<td>970</td>
</tr>
</tbody>
</table>

a) The average values are very close to the value of the prime in each case and show less variation than individual cases of choosing \( a \) and \( b \), once we average over the choice of many \( a \)’s and \( b \)’s. The range for each prime we see is consistent with the range we saw in question 1, indicating that the low and high values in question 1 were simply a matter of luck based on the \( a \) and \( b \) picked for that particular instance. The mode’s however, aren’t necessary very close to the primes themselves and appear to be largely random.

b) Very little except that as we pick more and more curves with the same \( p \), the average number of points each curve generates seems to tend closer and closer to \( p \) itself.