MATH 181: QUIZ 10
With a solution

Name: Anton Bernshteyn

Problem 1. (4 pts.) You are planning to use the RSA with \( N = 51 = 3 \cdot 17 \). For the given pairs of numbers, determine if they form a valid public/private key pair.

(a) \( e = 2, \ d = 17 \).

We have
\[
 p = 3 \quad \text{and} \quad q = 17,
\]
so
\[
 (p - 1) \cdot (q - 1) = 2 \cdot 16 = 32.
\]
Now,
\[
 e \cdot d = 2 \cdot 17 = 34 = 2 \pmod{32},
\]
so this is not a valid public/private key pair.

(b) \( e = 5, \ d = 13 \).

We have
\[
 e \cdot d = 5 \cdot 13 = 65 = 1 \pmod{32},
\]
so this is a valid public/private key pair.

Problem 2. (6 pts.) In a galaxy far, far away, a presidential election is being held. Each voter casts a ballot with their list of preferences. The table below shows all the ballots cast:

<table>
<thead>
<tr>
<th></th>
<th>40%</th>
<th>20%</th>
<th>35%</th>
<th>5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top choice</td>
<td>Darth Vader</td>
<td>Han Solo</td>
<td>Princess Leia</td>
<td>Jar Jar Binks</td>
</tr>
<tr>
<td>Second choice</td>
<td>Han Solo</td>
<td>Princess Leia</td>
<td>Han Solo</td>
<td>Han Solo</td>
</tr>
<tr>
<td>Third choice</td>
<td>Princess Leia</td>
<td>Darth Vader</td>
<td>Darth Vader</td>
<td>Princess Leia</td>
</tr>
<tr>
<td>Fourth choice</td>
<td>Jar Jar Binks</td>
<td>Jar Jar Binks</td>
<td>Jar Jar Binks</td>
<td>Darth Vader</td>
</tr>
</tbody>
</table>

(a) Which candidate is selected as the winner by the plurality vote? Darth Vader

(b) Which candidate is selected as the winner by the Condorcet method? Han Solo

(c) Which candidate is selected as the winner by the instant-runoff voting? Princess Leia