INSTRUCTIONS:

- Do all work on these sheets.
- Show all work.
- No books, calculators, or other electronic devices.
- Answers do not necessarily need to be simplified.

<table>
<thead>
<tr>
<th>Question</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>

1. (a) (2 points) State Fermat’s little theorem.

**Solution:** If \( p \) is a prime and \( a \) is a positive integer such that \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \).

(b) (6 points) Use Fermat’s little theorem to compute \( 3^{221} \pmod{23} \).

**Solution:** Since \( 221 = 10 \cdot 22 + 1 \) and by Fermat’s theorem \( 3^{22} \equiv 1 \pmod{23} \), we have \( 3^{221} \equiv (3^{22})^{10} \cdot 3 \equiv 3 \pmod{23} \).

2. (6 points) Suppose that \( p \) and \( q \) are distinct odd primes, that \( a \) is an integer, and that \( \gcd(a, pq) = 1 \). Prove that \( a^{(p-1)(q-1)+1} \equiv a \pmod{pq} \).

**Solution:** Since \( \gcd(a, pq) = 1 \), we have \( p \nmid a \). Then, by Fermat’s theorem, \( a^{p-1}(a-1)^{+1} \equiv 1^{(q-1)} \cdot a \equiv a \pmod{p} \).

Similarly, Since \( \gcd(a, pq) = 1 \), we have \( q \nmid a \). Then, by Fermat’s theorem, \( a^{q-1}(q-1)^{+1} \equiv 1^{(p-1)} \cdot a \equiv a \pmod{q} \).

Then, by the Chinese Remainder Theorem, we have \( a^{(p-1)(q-1)+1} \equiv a \pmod{pq} \).

3. Use Wilson’s theorem to do this problem.

(a) (2 points) State Wilson’s theorem.

**Solution:** If \( p \) is a prime, then \( (p - 1)! \equiv -1 \pmod{p} \).

(b) (6 points) Compute

\[
7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 32 \pmod{11}
\]

Briefly explain your answer.
Solution: 7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 32 \text{ is equivalent modulo 11 to } 7 \cdot 8 \cdot 9 \cdot 4 \cdot 5 \cdot 6 \cdot 1 \cdot 2 \cdot 3 \cdot 10 \equiv 10! \text{ (mod 11)}. \nBut by Wilson’s theorem 10! \equiv -1 \text{ (mod 11)}. \nTherefore, 7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 32 \equiv -1 \text{ (mod 11)}.

(c) (6 points) Compute 13! \cdot 5! \text{ (mod 19)}. 
Show your work.

Solution: By Wilson’s theorem,
\[-1 \equiv (19 - 1)! \equiv 18! \equiv 13! \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \text{ (mod 19)} \n\equiv 13! \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \text{ (mod 19)} \n\equiv -(13!5!) \text{ (mod 19)}. \nTherefore, 13!5! \equiv 1 \text{ (mod 19)}.

4. Let \( n \) be a positive integer. Let \( \tau(n) \) denote the number of positive divisors of \( n \), and let \( \sigma(n) \) denote the sum of the positive divisors of \( n \), as usual.

(a) (6 points) Compute the value of \( \tau(2^5 \cdot 5^3 \cdot 11) \).

Solution: \( \tau(2^5 \cdot 5^3 \cdot 11) = (5+1)(3+1)(1+1) = 48 \)

(b) (6 points) Compute the value of \( \sigma(2^5 \cdot 5^3 \cdot 11) \).

Solution:
\[
\sigma(2^5 \cdot 5^3 \cdot 11) = \frac{2^{5+1}}{2-1} \cdot \frac{5^{3+1}}{5-1} \cdot \frac{11^{1+1}}{11-1}.
\]