# Test 2

Sam Grayson

May 26, 2015

1. $p \in \mathbb{P} \land q \in \mathbb{P} \to p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

   **Proof:** $p^{q-1} \equiv 1 \pmod{q}$ and $q^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. $q^{p-1} \equiv 0 \pmod{q}$ and $p^{q-1} \equiv 0 \pmod{p}$ (since always $a|a^i$). Then $p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \pmod{q}$ and $p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \pmod{q}$. By Theorem 4.21, $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. ■

2. Let $i \in \mathbb{Z}$ where $\gcd(\operatorname{ord}(a), i) = 1$. Then $\operatorname{ord}(a^i) = \operatorname{ord}(a)$.

   **Proof:** $(a^{\operatorname{ord}(a)})^i \equiv 1 \equiv (a^i)^{\operatorname{ord}(a)}$, so $\operatorname{ord}(a^i) | \operatorname{ord}(a)$. In a similar way, $(a^i)^{\operatorname{ord}(a^i)} \equiv 1 \equiv a^{i \cdot \operatorname{ord}(a^i)}$, so $\operatorname{ord}(a) | (i \operatorname{ord}(a^i))$. But by Theorem 1.39, since $\gcd(\operatorname{ord}(a^i), i) = 1$, $\operatorname{ord}(a) | \operatorname{ord}(a^i)$. Together with $\operatorname{ord}(a^i) | \operatorname{ord}(a)$, this proves that $\operatorname{ord}(a^i) = \operatorname{ord}(a)$. ■

3. Let $\gcd(a, m) = 1$ for $a, m \in \mathbb{Z}$. $\operatorname{ord}(a) | \phi(m)$. (All orders and congruences are taken mod $m$.)

   **Proof:** $a^{\phi(m)} \equiv 1$ by Theorem 4.32 (Euler's Theorem). $\operatorname{ord}(a) | \phi(m)$ by Theorem 4.10. ■

4. $\phi(pq) = \phi(p)\phi(q)$. This is not necessarily true when $p = q$.

   **Counter example:** Consider the case where $p = 5$ and $q = 5$.

   $\phi(5) = 4 \quad \{1, 2, 3, 4, \cancel{5}\}$
   $\phi(25) = 20 \quad \{1, 2, 3, 4, \cancel{5}, 6, 7, 8, 9, \cancel{10}, 11, 12, 13, 14, \cancel{15}, 16, 17, 18, 19, \cancel{20}, 21, 22, 23, 24, \cancel{25}\}$
   $\phi(5) \cdot \phi(5) = 4 \cdot 4 = 16 \neq \phi(25)$

5.

6. **Code:**

```python
def gcd(a1, b1):
    # Returns the greatest common multiple
    # WLOG a > b > 0
    a = max(abs(a1), abs(b1))
    b = min(abs(a1), abs(b1))
        # find the remainder upon division
    q, r = division(a, b)
    if r == 0:
        return b
    else:
        return gcd(b, r)

```

```python
def coprime(a, b):
    # Returns True if a and b are coprime
    return gcd(a, b) == 1

def phi(n):
    count = 0
    for i in range(1, n+1): # 1 ≤ i < n+1
        if coprime(i, n):
            count = count + 1
    return count

for x in range(10000):
    if phi(x) == 24:
        print(x)
```

**Output:**

$\phi(x) = 24 \leftrightarrow x \in \{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}$

7. I really enjoyed your course. This was a highlight of my A-day schedule.