1. **Repeated Squaring** Compute $3^{383} \pmod 7$. (Via repeated squaring!)

   Solution: Here we go...
   Divide 383 repeatedly by 2, flooring every time. We get the sequence

   $$383, 191, 95, 47, 23, 11, 5, 2, 1.$$

   So, to compute 3^{383}, we compute:

   $$\begin{aligned}
   3^1 \bmod 7 &\equiv 3 \\
   3^2 \bmod 7 &\equiv 2 \\
   3^5 \bmod 7 &\equiv (3^2)^2 \times 3 \equiv 2^2 \times 3 \equiv 12 \equiv 5 \\
   3^{11} \bmod 7 &\equiv 5 \times 5 \times 3 \equiv 4 \times 3 \equiv 5 \\
   3^{23} \bmod 7 &\equiv 5 \times 5 \times 3 \equiv 5 \\
   3^{47} \bmod 7 &\equiv \ldots \equiv 5 \\
   3^{95} \bmod 7 &\equiv \ldots \equiv 5 \\
   3^{191} \bmod 7 &\equiv \ldots \equiv 5 \\
   3^{383} \bmod 7 &\equiv \ldots \equiv 5
   \end{aligned}$$

2. **Modular Potpourri**

   (a) Evaluate $4^{96} \pmod 5$

   Solution: One way: $4 \equiv -1 \pmod 5$, and $(-1)^{96} \equiv 1$
   Another: $4^2 \equiv 1 \pmod 5$, so $4^{96} = (4^2)^{48} \equiv 1 \pmod 5$.
   Mention that it is **invalid** to "apply the mod to the exponent": $4^{96} \not\equiv 4^1 \pmod 5$

   (b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod 6$.

   Solution: Impossible, consider both mod 2 (why is it valid to do so?)

   (c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$

   Solution: False, consider $x \equiv 8$.

3. **Just a Little Proof**

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

Solution: Because $\gcd(a, pq) = 1$, we have that a does not divide p and a does not divide q. By Fermat's Little Theorem,

$$a^{(p-1)(q-1)+1} = (a^{(p-1)})^{(q-1)} \cdot a \equiv (1)^{q-1} \cdot a \equiv a \pmod{p}.$$

Similarly, by Fermat's Little Theorem, we have

$$a^{(p-1)(q-1)+1} = (a^{(q-1)})^{(p-1)} \cdot a \equiv (1)^{p-1} \cdot a \equiv a \pmod{q}.$$

Now, we want to use this information to conclude that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. We will first take a detour and show a more general result (you could write this out separately as a lemma if you want).

Consider the system of congruences

$$x \equiv a \pmod{p}$$
$$x \equiv a \pmod{q}.$$

Let's run the CRT symbolically. First off, since p and q are relatively prime, we know there exist integers g, h such that

$$g \cdot p + h \cdot q = 1.$$

We could find these via Euclid's algorithm. By the CRT, the solution to our system of congruences will be

$$x \equiv a \cdot y_1 \cdot q + a \cdot y_2 \cdot p \pmod{pq}.$$

To solve for y_1 and y_2, we must find y_1 such that

$$x_1 \cdot p + y_1 \cdot q = 1$$

and y_2 such that

$$x_2 \cdot q + y_2 \cdot p = 1.$$

This is easy since we already know $g \cdot p + h \cdot q = 1$: the answers are $y_1 = h$ and $y_2 = g$. Finally we can plug in to the solution to get

$$x \equiv a \cdot h \cdot q + a \cdot g \cdot p \equiv a(h \cdot q + g \cdot p) \equiv a(1) \equiv a \pmod{pq}.$$

Therefore by the CRT we know that the set of solutions that satisfy both $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ is exactly the set of solutions that satisfy $x \equiv a \pmod{pq}$.

So since $a^{(p-1)(q-1)+1} \equiv a \pmod{p}$ and $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$, then by the CRT we know that $a^{(p-1)(q-1)+1}$ satisfies $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

4. **Euler's totient function**

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \le i \le n, \texttt{gcd}(n, i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m, n such that $\texttt{gcd}(m, n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

Solution:

Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.
So, $\phi(p) = p-1$.

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

Solution:

The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.
Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.
The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.
The total number of positive integers less than or equal to p^k is, obviously, p^k.
So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod p$?
(Hint: use Fermat's Little Theorem.)

Solution:

From Fermat's Little Theorem, and part 1,
$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod p$

(d) Let b be a number whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.
Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1, 2, \ldots, k\}, \ a^{\phi(b)} \equiv 1 \pmod{p_i}$$

Solution: From the property of the totient function and part 3:

$$\phi(b) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k})$$
$$= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k})$$
$$= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1)$$

This shows that, for every p_i, which is a prime factor of b, we can write $\phi(b) = c \cdot (p_i - 1)$, where c is some constant. Since a and b are relatively prime, a is also relatively prime with p_i. From Fermat's Little Theorem:
$a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$
Since we picked p_i arbitrarily from the set of prime factors of b, this holds for all such p_i.