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: We know that a is not a divsible by p and a is not divisible by q since $\gcd(a, pq) = 1$.We subtract a from both sides to get

$$a^{(p-1)(q-1)+1} - a \equiv 0 \mod pq$$
$$a(a^{(p-1)(q-1)} - 1) \equiv 0 \mod pq$$

Since p, q are primes, we just need to show that the left hand side is divisible by both p and q. Since a is not divisible by p, we can use Fermat's Little Theorem to state that $a^{p-1} \equiv 1 \mod p$.

$$a((a^{(p-1)})^{q-1} - 1) \mod p$$
$$a(1^{q-1} - 1) \mod p$$
$$0 \mod p$$

Thus $a(a^{(p-1)(q-1)} - 1)$ is divisible by p. We can apply the same reasoning to show that the expression is divisible by q. Therefore we have proved our claim that $a^{(p-1)(q-1)+1} \equiv a \mod pq$.

Alternative Proof:
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. **RSA Warm-Up**

   Consider an RSA scheme modulus $N = pq$, where p and q are prime numbers larger than 3.

   (a) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

   Solution: Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

   (b) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

   Solution: $N = p \cdot q = 85$ and $e = 3$ are displayed publically. Make sure to point out that in practice, p and q should be much larger 512-bit numbers. We are only choosing small numbers here to allow manual computation.

   (c) What is the private key?

   Solution: We must have $ed = 3d \equiv 1 \mod 64$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $gcd(x,y) = 1 = ax + by$, and $a = 1, b = -21$.

   (d) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

   Solution: We have $E(x) = x^3 \mod 85$. $100^3 \equiv 65 \mod 85$, so $E(x) = 65$.

   (e) Alice receives the message $y = 24$ back from Bob. What equation would she use to decrypt the message?

   Solution: We have $D(y) = y^{43} \mod 85$. $24^{43} \equiv 14 \mod 85$, so $D(y) = 14$.