1. Calculate the following numbers.

   (a) $98 + 96 + 94 + 92 + 90 \bmod 100$

   Solution: We can calculate it directly as $470 \bmod 100 = 70$, or using the rules of modular arithmetic,

$$98 + 96 + 94 + 92 + 90 \equiv -2 - 4 - 6 - 8 - 10 \equiv -(2 + 4 + 6 + 8 + 10) \equiv -30 \equiv 70 \pmod{100}.$$

   (b) $17 \cdot 23 - 2 \cdot 3 \bmod 17$

   Solution: $17 \cdot 23 - 2 \cdot 3 \bmod 17 \equiv 0 \cdot 6 - 2 \cdot 3 \pmod{17} \equiv (-6) \pmod{17} \equiv 11 \pmod{17}$.

   (c) $9^{-1} \bmod 23$

   Solution: We first calculate $9^{-1} \bmod 23$ using the extended GCD algorithm:

$$\begin{aligned} E(23,9) &= E(9,5) & 23 &= 2 \cdot 9 + 5 \\ &= E(5,4) & 9 &= 5 + 4 \\ &= E(4,1) & 5 &= 4 + 1 \\ &= E(1,0). \end{aligned}$$

   so we can write 1 as the following combination of 23 and 9:

$$1 = 5 - 4 = 5 - (9 - 5) = -9 + 2 \cdot 5 = -9 + 2 \cdot (23 - 2 \cdot 9) = 2 \cdot 23 - 5 \cdot 9$$

   It follows that $9^{-1} \equiv -5 \pmod{23} \equiv 18 \pmod{23}$.

   (d) $95 \cdot 41^{-1} \bmod 97$. (97 is a prime number.)

   Solution: We first calculate $41^{-1} \bmod 97$ using the extended GCD algorithm:

$$\begin{aligned} E(97,41) &= E(41,15) & 97 &= 2 \cdot 41 + 15 \\ &= E(15,11) & 41 &= 2 \cdot 15 + 11 \\ &= E(11,4) & 15 &= 11 + 4 \\ &= E(4,3) & 11 &= 2 \cdot 4 + 3 \\ &= E(3,1) & 4 &= 3 + 1 \\ &= E(1,0) & 3 &= 3 \cdot 1 + 0 \end{aligned}$$

   Now we use the equations in reverse to express 1 as a combination of 97 and 41:

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \cdot 4) \\ &= -11 + 3 \cdot 4 \\ &= -11 + 3 \cdot (15 - 11) \\ &= 3 \cdot 15 - 4 \cdot 11 \\ &= 3 \cdot 15 - 4 \cdot (41 - 2 \cdot 15) \\ &= -4 \cdot 41 + 11 \cdot 15 \\ &= -4 \cdot 41 + 11 \cdot (97 - 2 \cdot 41) \\ &= 11 \cdot 97 - 26 \cdot 41 \end{aligned}$$

   It follows that $41^{-1} \equiv -26 \pmod{97}$. Therefore

$$95 \cdot 41^{-1} \equiv 95 \cdot (-26) \equiv (-2) \cdot (-26) \equiv 52 \pmod{97}.$$

2. Calculate the following numbers using the suggested method:

   (a) 2^9 mod 11 using iterated multiplication.

   Solution: $2^9 \equiv 4\cdot 2^7 \equiv 8\cdot 2^6 \equiv 16\cdot 2^5 \equiv 5\cdot 2^5 \equiv 10\cdot 2^4 \equiv 20\cdot 2^3 \equiv 9\cdot 2^3 \equiv 18\cdot 2^2 \equiv 7\cdot 2^2 \equiv 14\cdot 2 \equiv 3\cdot 2 \equiv 6 \pmod{11}$.

   (b) 2^{81} mod 11 using fast exponentiation (the *Power* algorithm from Lecture 5).

   Solution: $2^{81} \equiv 2\cdot 2^{80} \equiv 2\cdot 4^{40} \equiv 2\cdot 16^{20} \equiv 2\cdot 5^{20} \equiv 2\cdot 25^{10} \equiv 2\cdot 3^{10} \equiv 2\cdot 9^5 \equiv 2\cdot 9\cdot 9^4 \equiv 2\cdot 9\cdot 81^2 \equiv 2\cdot 9\cdot 4^2 \equiv 2\cdot 9\cdot 16 \equiv 2\cdot 9\cdot 5 \equiv 90 \equiv 2 \pmod{11}$.

   (c) $2^{2^{81}}$ mod 11 using Fermat's Little Theorem (Theorem 5 from Lecture 5).

   Solution: Fermat's little theorem says that $2^{11} \equiv 2 \pmod{11}$, so $2^{10} \equiv 1 \pmod{11}$. Therefore $2^{2^{81}} \equiv 2^{2^{81} \bmod 10} \pmod{11}$: If 2^{81} is represented as $10q + r$ then $2^{2^{81}} \equiv (2^{10})^q \cdot 2^r \equiv 2^r \pmod{11}$.
   We can calculate 2^{81} mod 10 using fast exponentiation: $2^{81} \equiv 2\cdot 2^{80} \equiv 2\cdot 4^{40} \equiv 2\cdot 16^{20} \equiv 2\cdot 6^{20} \equiv 2\cdot 36^{10} \equiv 2\cdot 6^{10} \equiv 2\cdot 36^5 \equiv 2\cdot 6^5 \equiv 2\cdot 6\cdot 6^4 \equiv 2\cdot 6\cdot 36^2 \equiv 2\cdot 6\cdot 6^2 \equiv 2\cdot 6\cdot 36 \equiv 2\cdot 6\cdot 6 \equiv 72 \equiv 2 \pmod{10}$.
   Therefore $2^{2^{81}} \equiv 2^2 \equiv 4 \pmod{11}$.

3. Calculate the following numbers.

   (a) x and y that solve $5x + 7y \equiv 17 \pmod{19}$ and $4x + 11y \equiv 13 \pmod{19}$.

   Solution: To get rid of x we multiply the first equation by 4, multiply the second equations by 5 and subtract to obtain $(7\cdot 4 - 11\cdot 5)y \equiv 17\cdot 4 - 13\cdot 5 \pmod{19}$. We simplify

$$\begin{aligned} 7\cdot 4 - 11\cdot 5 &= 28 - 55 = -27 \equiv 11 && \pmod{19}, \\ 17\cdot 4 - 13\cdot 5 &\equiv -2\cdot 4 + 6\cdot 5 = 22 \equiv 3 && \pmod{19}. \end{aligned}$$

   To solve $11y \equiv 3 \pmod{19}$ we need the multiplicative inverse of 11:

$$\begin{aligned} E(19,11) &= E(11,8) && 19 = 11 + 8 \\ &= E(8,3) && 11 = 8 + 3 \\ &= E(3,2) && 8 = 2\cdot 3 + 2 \\ &= E(2,1) && 3 = 2 + 1 \\ &= E(1,0), \end{aligned}$$

   from where

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2\cdot 3) = -8 + 3\cdot 3 \\ &= -8 + 3\cdot(11 - 8) = 3\cdot 11 - 4\cdot 8 \\ &= 3\cdot 11 - 4\cdot(19 - 11) = -4\cdot 19 + 7\cdot 11 \end{aligned}$$

   so $11^{-1} \bmod 19 = 7$. Therefore $y \equiv 7\cdot 3 = 21 \equiv 2 \pmod{19}$. Plugging into the first equation we get that $5x \equiv 17 - 7\cdot 2 = 3 \pmod{19}$, from where $x = 3\cdot 5^{-1} \bmod 19$. Now

$$\begin{aligned} E(19,5) &= E(5,4) && 19 = 3\cdot 5 + 4 \\ &= E(4,1) && 5 = 4 + 1 \\ &= E(1,0) \end{aligned}$$

   so $1 = 5 - 4 = 5 - (19 - 3\cdot 5) = -19 + 4\cdot 5$, and $5^{-1} \equiv 4 \pmod{19}$. The solution is $x = 12, y = 2$.

   (b) $1^1 + 2^2 + \cdots + 99^{99}$ mod 3.

   Solution: We can reduce

$$1^1 + 2^2 + 3^3 + 4^4 + 5^5 + \cdots + 99^{99} \equiv 1^1 + (-1)^2 + 0^3 + 1^4 + (-1)^5 + 0^6 + \cdots + 0^{99} \pmod{3}$$

This expression has 33 values of the form 0^n all of which equal zero and 33 values of the form 1^n all of which equal one so their sum modulo 3 is congruent to zero. What remains is

$$(-1)^2 + (-1)^5 + \cdots + (-1)^{98} \pmod 3$$

Since the powers of -1 alternate between even and odd, this expression is congruent to

$$1 + (-1) + 1 + (-1) + \cdots + 1 \pmod 3$$

which evaluates to 1 modulo 3.

(c) $1^{-1} + 2^{-1} + \cdots + 96^{-1} \bmod 97$.

Solution: As each number between 1 and 96 has a unique multiplicative inverse modulo 97, each of the numbers $1^{-1}, 2^{-1}, \ldots, 96^{-1}$ occurs exactly once in the list $1, 2, \ldots, 96$, so

$$1^{-1} + 2^{-1} + \cdots + 96^{-1} \equiv 1 + 2 + \cdots + 96 = \frac{96 \cdot 97}{2} = 48 \cdot 97 \equiv 49 \cdot 0 = 0 \pmod{97}.$$

(d) **(Optional)** $42! \bmod 43$ (*Hint:* Pair up each number with its inverse. You can try $6! \bmod 7$ first.)

Solution: Let's try $6! \bmod 7$ first. We can calculate

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot (-3) \cdot (-2) \cdot (-1) \equiv -(2 \cdot 3)^2 \equiv -1^2 = -1 \equiv 6 \pmod 7.$$

How can we explain this answer? Let's list the multiplicative inverses of all nonzero remainders mod 7:

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

Only 1 and 6 are their own inverse. The inverse of every other number is different from itself. In the product $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ we can now group every number apart from 1 and 6 with its inverse to conclude that

$$6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 = 6 \pmod 7.$$

We can apply the same strategy to calculate $42! \bmod 43$. In the product $1 \cdot 2 \cdots 42$, after pairing up every number with its ineverse modulo 43, what remains is the product of the numbers that are their own inverses. Which are these numbers? If $x \equiv x^{-1} \pmod{43}$ and we multiply both sides by x we obtain that $x^2 \equiv 1$, so $x^2 - 1 \equiv 0$, so $(x-1)(x+1) \equiv 0 \pmod{43}$. Therefore 43 must divide $(x-1)(x+1)$. As 43 is a prime number it must divide $x - 1$ *or* $x + 1$. It follows that $x \equiv 1$ or $x \equiv -1$ modulo 43, so 1 and $-1 \equiv 42$ are the only two numbers that are their own inverses. We conclude that $42! \equiv 1 \cdot 42 = 42 \pmod{43}$.

4. You will investigate the "baby RSA" encryption from Lecture 5. Recall that the public encryption key e and "secret" decryption key d are chosen so that $ed \equiv 1 \pmod{n-1}$ for prime modulus n.

(a) Assume $n = 29$ and $d = 11$. Show how to choose e to enable decryption.

Solution: e should satisfy the decryption equation $ed \equiv 1 \pmod{n-1}$, which in this case says $11e \equiv 1 \pmod{28}$. So e must be a multiplicative inverse of 11 modulo 28, if one exists. We can try to find one using extended Euclid's algorithm:

$$\begin{aligned} E(28, 11) &= E(11, 6) & \qquad 28 &= 2 \cdot 11 + 6 \\ &= E(6, 5) & 11 &= 6 + 5 \\ &= E(5, 1) & 6 &= 5 + 1 \\ &= E(1, 0), \end{aligned}$$

from where $1 = 6 - 5 = 6 - (11 - 6) = -11 + 2 \cdot 6 = -11 + 2 \cdot (28 - 2 \cdot 11) = 2 \cdot 28 - 5 \cdot 11$. We can choose $e \equiv -5 \equiv 23 \pmod{28}$.

(b) Calculate the encryption $c = m^e \bmod n$ of the message $m = 10$ and the encryption key e from part (a). Then calculate the decryption $c^d \bmod n$.

Solution: Using fast exponentiation (and replacements of big numbers by their additive inverses to keep the calculation manageable) we obtain

$$\begin{aligned} c = m^e = 10^{23} = 10 \cdot 10^{22} &\equiv 10 \cdot 100^{11} \\ &\equiv 10 \cdot 13^{11} = 10 \cdot 13 \cdot 13^{10} = 10 \cdot 13 \cdot 169^5 \equiv 10 \cdot 13 \cdot 24^5 \\ &\equiv 10 \cdot 13 \cdot (-5)^5 = 10 \cdot 13 \cdot (-5) \cdot (-5)^4 = 10 \cdot 13 \cdot (-5) \cdot 25^2 \\ &\equiv 10 \cdot 13 \cdot (-5) \cdot (-4)^2 \equiv 10 \cdot 13 \cdot (-5) \cdot 16 \equiv 11 \qquad \pmod{29}. \end{aligned}$$

To decrypt Bob calculates

$$c^d = 11^{11} = 11 \cdot 11^{10} \equiv 11 \cdot 121^5 \equiv 11 \cdot 5^5 = 11 \cdot 5 \cdot 5^4 = 11 \cdot 5 \cdot 25^2 \equiv 11 \cdot 5 \cdot (-4)^2 = 11 \cdot 5 \cdot 16 \equiv 10 \pmod{29}.$$

As expected, c^d recovers the message m.

(c) Now suppose Eve observes the ciphertext $c = 33$ that Alice sent to Bob using modulus $n = 37$ and encryption key $e = 7$. How can Eve recover the message m without knowing d?

Solution: Eve can determine Bob's secret key by solving the equation $ed \equiv 1 \pmod{n-1}$, namely $7d \equiv 1 \pmod{36}$. She runs extended GCD to find

$$\begin{aligned} E(36,7) &= E(7,1) \qquad && 36 = 5 \cdot 7 + 1 \\ &= E(1,0), \end{aligned}$$

so $1 = 36 - 5 \cdot 7$ and $d \equiv -5 \equiv 31 \pmod{36}$. Eve can now decrypt c by calculating

$$\begin{aligned} c^d = 33^{31} &\equiv (-4)^{31} \equiv (-4) \cdot 16^{15} \equiv (-4) \cdot 16 \cdot 16^{14} \\ &\equiv (-4) \cdot 16 \cdot 256^7 \equiv (-4) \cdot 16 \cdot (-3)^7 \equiv (-4) \cdot 16 \cdot (-3) \cdot (-3)^6 \\ &\equiv (-4) \cdot 16 \cdot (-3) \cdot 9^3 \equiv (-4) \cdot 16 \cdot (-3) \cdot 9 \cdot 81 \\ &\equiv 4 \cdot 16 \cdot 3 \cdot 9 \cdot 7 \equiv 8 \qquad \pmod{37}. \end{aligned}$$