

1. Calculate the following numbers.
 - (a) $1 - 4 + 7 - 11 \pmod{6}$
 - (b) $11 \cdot 13 - 4 \cdot 5 \pmod{17}$
 - (c) $4 \cdot 9^{-1} \pmod{23}$
2. Calculate the following numbers using the suggested method:
 - (a) $2^9 \pmod{11}$ using iterated multiplication.
 - (b) $2^{81} \pmod{11}$ using fast exponentiation (the *Power* algorithm from Lecture 5).
 - (c) $2^{2^{81}} \pmod{11}$ using Fermat's Little Theorem (Theorem 5 from Lecture 5).
3. Calculate the following numbers.
 - (a) x and y that solve $5x + 7y \equiv 17 \pmod{19}$ and $4x + 11y \equiv 13 \pmod{19}$.
 - (b) $1^1 + 2^2 + \dots + 99^{99} \pmod{3}$.
 - (c) **(Optional)** $42! \pmod{43}$ (*Hint*: Pair up each number with its inverse. You can try $6! \pmod{7}$ first.)
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.
 - (b) Calculate the encryption $c = m^e \pmod{n}$ of the message $m = 10$ and the encryption key e from part (a). Then calculate the decryption $c^d \pmod{n}$.
 - (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 ?