1. Using RSA with public key $(34, 3)$,

   (a) encrypt ***MATH***,

   (b) decrypt the message:

   10 9 16 | 25 23 27 18 23 10.

---

2. (a) Prove that if $n > 4$ is composite then

   $$(n-1)! \equiv 0 \mod n.$$

   (b) Compute $2^{322} \mod 323$ and conclude from Fermat's little theorem that 323 is not prime.

---

3. Find rules of divisibility of an integer by 5, 9 and 11, and prove each of those rules using modular arithmetic.

---

4. Suppose m and n are relatively prime positive integers

   (a) Show that if some a integer $m \mid a$ and $n \mid a$ then $m \cdot n \mid a$.

   (b) Show that the map Ψ defined by

   $$\begin{array}{ccc} \mathbb{Z}^*_{m \cdot n} & \xrightarrow{\Psi} & \mathbb{Z}^*_m \times \mathbb{Z}^*_n \\ [a]_{m \cdot n} & \hookrightarrow & ([a]_m, [a]_n) \end{array}$$

   is a bijection.

   (c) Conclude from (b) that Euler's φ function is multiplicative, i.e.,

   $$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

---

5. Let φ be Euler's function.

   (a) Show that if a and $m > 1$ are relatively prime positive integers, then the inverse of a modulo m is $a^{\varphi(m)-1}$.

   (b) Use (a) to find

   (i) the inverse of 4 modulo 9,

   (ii) the inverse of 5 modulo 8.