

## NHÓM 1 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 499$ ;  $m = 6337$ ;  $n = 6337$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 2705$ ;  $n = 6577$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 281$ ;  $m = 764$ ;  $n = 6967$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 2863$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 27$ ;  $m = 2201$ ;  $n = 5400$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 101$ ;  $k = 76$ ;  $n = 49913$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 11$ ;  $m_2 = 13$ ;  $m_3 = 17$ ;  $a_1 = 6$ ;  $a_2 = 2$ ;  $a_3 = 4$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 11$ ;  $n = 293$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 3$ ;  $b = 8$ ;  $n = 19$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 83$ ;  $b = 17$ ;  $x = 354$ ;  $y = 314$ ;  $n = 241$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 2 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 419$ ;  $m = 6217$ ;  $n = 6217$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 2656$ ;  $n = 5741$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 479$ ;  $m = 822$ ;  $n = 6803$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 4346$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 29$ ;  $m = 3196$ ;  $n = 300$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 199$ ;  $k = 54$ ;  $n = 43381$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 13$ ;  $m_2 = 17$ ;  $m_3 = 19$ ;  $a_1 = 6$ ;  $a_2 = 8$ ;  $a_3 = 14$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 11$ ;  $n = 331$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 5$ ;  $b = 7$ ;  $n = 17$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 71$ ;  $b = 11$ ;  $x = 419$ ;  $y = 369$ ;  $n = 181$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

### NHÓM 3 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 397$ ;  $m = 6329$ ;  $n = 6329$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 1885$ ;  $n = 6563$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 439$ ;  $m = 760$ ;  $n = 6269$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 3992$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 23$ ;  $m = 3885$ ;  $n = 395$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 227$ ;  $k = 80$ ;  $n = 60421$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 17$ ;  $m_2 = 19$ ;  $m_3 = 11$ ;  $a_1 = 5$ ;  $a_2 = 16$ ;  $a_3 = 3$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 5$ ;  $n = 463$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 3$ ;  $b = 5$ ;  $n = 19$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 37$ ;  $b = 97$ ;  $x = 581$ ;  $y = 364$ ;  $n = 127$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

#### NHÓM 4 BÀI TẬP

1. **TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 239$ ;  $m = 6653$ ;  $n = 6653$   
Tìm Output:  $b =$
2. **TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 1974$ ;  $n = 7841$   
Tìm Output:  $x =$
3. **SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 311$ ;  $m = 821$ ;  $n = 6311$   
Tìm Output:  $b =$
4. **TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 3312$   
Tìm Output:  $\phi(n) =$
5. **SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 38$ ;  $m = 2934$ ;  $n = 220$   
Tìm Output:  $b =$
6. **SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 241$ ;  $k = 59$ ;  $n = 63307$   
Tìm Output:  $b =$
7. **SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 19$ ;  $m_2 = 11$ ;  $m_3 = 13$ ;  $a_1 = 5$ ;  $a_2 = 5$ ;  $a_3 = 6$ ;  
Tìm Output:  $x =$
8. **KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 5$ ;  $n = 263$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
9. **TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 2$ ;  $b = 7$ ;  $n = 11$   
Tìm Output:  $k =$
10. **TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 31$ ;  $b = 67$ ;  $x = 375$ ;  $y = 539$ ;  $n = 211$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 5 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 311$ ;  $m = 6719$ ;  $n = 6719$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 2451$ ;  $n = 6547$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 433$ ;  $m = 797$ ;  $n = 6353$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 3606$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 36$ ;  $m = 2445$ ;  $n = 282$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 157$ ;  $k = 67$ ;  $n = 18073$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 11$ ;  $m_2 = 13$ ;  $m_3 = 17$ ;  $a_1 = 9$ ;  $a_2 = 8$ ;  $a_3 = 8$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 5$ ;  $n = 281$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 6$ ;  $b = 7$ ;  $n = 13$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 89$ ;  $b = 41$ ;  $x = 514$ ;  $y = 615$ ;  $n = 149$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 6 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 347$ ;  $m = 6829$ ;  $n = 6829$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 2084$ ;  $n = 6113$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 499$ ;  $m = 891$ ;  $n = 6353$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 4432$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 23$ ;  $m = 3304$ ;  $n = 274$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 163$ ;  $k = 79$ ;  $n = 70151$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 13$ ;  $m_2 = 17$ ;  $m_3 = 19$ ;  $a_1 = 9$ ;  $a_2 = 5$ ;  $a_3 = 4$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 5$ ;  $n = 257$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 5$ ;  $b = 6$ ;  $n = 17$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 53$ ;  $b = 83$ ;  $x = 574$ ;  $y = 494$ ;  $n = 331$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 7 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 317$ ;  $m = 6221$ ;  $n = 6221$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 1125$ ;  $n = 3739$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 433$ ;  $m = 843$ ;  $n = 6899$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 4533$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 36$ ;  $m = 3918$ ;  $n = 287$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 179$ ;  $k = 53$ ;  $n = 41477$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 17$ ;  $m_2 = 19$ ;  $m_3 = 11$ ;  $a_1 = 16$ ;  $a_2 = 18$ ;  $a_3 = 7$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 7$ ;  $n = 449$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 3$ ;  $b = 6$ ;  $n = 19$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 71$ ;  $b = 83$ ;  $x = 596$ ;  $y = 375$ ;  $n = 239$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 8 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 277$ ;  $m = 6863$ ;  $n = 6863$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 3331$ ;  $n = 6551$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 241$ ;  $m = 850$ ;  $n = 6737$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 2856$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 26$ ;  $m = 3369$ ;  $n = 363$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 191$ ;  $k = 58$ ;  $n = 79663$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 19$ ;  $m_2 = 11$ ;  $m_3 = 13$ ;  $a_1 = 8$ ;  $a_2 = 2$ ;  $a_3 = 8$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 3$ ;  $n = 353$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 2$ ;  $b = 7$ ;  $n = 11$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 53$ ;  $b = 31$ ;  $x = 336$ ;  $y = 585$ ;  $n = 293$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$



## NHÓM 9 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 449$ ;  $m = 6763$ ;  $n = 6763$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 3122$ ;  $n = 3593$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 373$ ;  $m = 851$ ;  $n = 6211$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 3353$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 34$ ;  $m = 2249$ ;  $n = 374$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 113$ ;  $k = 58$ ;  $n = 37259$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 11$ ;  $m_2 = 13$ ;  $m_3 = 17$ ;  $a_1 = 6$ ;  $a_2 = 11$ ;  $a_3 = 12$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 3$ ;  $n = 239$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 6$ ;  $b = 5$ ;  $n = 13$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 43$ ;  $b = 53$ ;  $x = 308$ ;  $y = 455$ ;  $n = 179$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$

## NHÓM 10 BÀI TẬP

- TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$  BẰNG CÁCH HẠ BẬC LŨY THỪA**  
Input:  $a = 443$ ;  $m = 6373$ ;  $n = 6373$   
Tìm Output:  $b =$
- TÌM NGHỊCH ĐẢO  $x = a^{-1} \bmod n$  THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG**  
Input:  $a = 1392$ ;  $n = 5639$   
Tìm Output:  $x =$
- SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 467$ ;  $m = 971$ ;  $n = 6607$   
Tìm Output:  $b =$
- TÍNH GIÁ TRỊ HÀM EULER  $\phi(n)$ .**  
Input:  $n = 2905$   
Tìm Output:  $\phi(n) =$
- SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO  $b = a^m \bmod n$**   
Input:  $a = 24$ ;  $m = 3919$ ;  $n = 200$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo  $b = a^k \bmod n$**   
Input:  $a = 103$ ;  $k = 61$ ;  $n = 50209$   
Tìm Output:  $b =$
- SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$
  
Input:  $m_1 = 13$ ;  $m_2 = 17$ ;  $m_3 = 19$ ;  $a_1 = 7$ ;  $a_2 = 15$ ;  $a_3 = 11$ ;  
Tìm Output:  $x =$
- KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**  
Input:  $a = 3$ ;  $n = 311$   
Tìm Output:  $a$  có là căn nguyên thủy của  $n$  không?
- TÌM LOGARITHM RỜI RẠC CỦA SỐ  $b$  VỚI CƠ SỐ  $a \pmod n$ ,  $k = \log_a b \pmod n$ .**  
Input:  $a = 5$ ;  $b = 7$ ;  $n = 17$   
Tìm Output:  $k =$
- TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN**  
$$\begin{aligned} A1 &= (a^x + b^y) \bmod n \\ A2 &= (a^x - b^y) \bmod n \\ A3 &= (a^x * b^y) \bmod n \\ A4 &= (b^y)^{-1} \bmod n \\ A5 &= (a^x / b^y) \bmod n \end{aligned}$$
  
Input:  $a = 73$ ;  $b = 67$ ;  $x = 498$ ;  $y = 582$ ;  $n = 269$   
Tìm Output:  $A1 =$  ;  $A2 =$  ;  $A3 =$  ;  $A4 =$  ;  $A5 = ?$