

**Integer Factorization**

**Chinese Remainder Theorem**

- Reading:** Reminders for Two Modules  
10 min
- Reading:** Chinese Remainder Theorem  
10 min
- Quiz:** Reminders  
4 questions
- Quiz:** Chinese Remainder Theorem: Code  
1 question

**Modular Exponentiation**

---

**Reminders**

**Grade received 100%**      **Latest Submission 100%**      **To pass 75% or higher**      **Go to next item**

**Review Learning Objectives**

- If  $n \equiv 5 \pmod{9}$ , what can be  $n \pmod{3}$ ? 1 / 1 point

☐ 1
 ☒ **Submit your assignment**
Due Jan 15, 11:59 PM IST

☐ 0, 1 or 2

---

**Correct**      **Receive grade**      **Your grade 100%**      **View Feedback**  
To Pass 75% or higher We keep your highest score

3 divides 9, so remainder modulo 9 defines remainder modulo 3, and  $5 \pmod{3} = 2$ .

      

- If  $n \equiv 1 \pmod{6}$ , what can be  $n \pmod{5}$ ? 1 / 1 point

☐ 1
 ☐ 1, 2 or 3.
 ☒ 0, 1, 2, 3 or 4

**Correct**  
 Correct! 5 and 6 are coprime, so the remainders modulo 5 and 6 are independent. In particular,  
 $25 \equiv 1 \pmod{6}, 25 \equiv 0 \pmod{5},$   
 $1 \equiv 1 \pmod{6}, 1 \equiv 1 \pmod{5},$   
 $37 \equiv 1 \pmod{6}, 37 \equiv 2 \pmod{5},$   
 $13 \equiv 1 \pmod{6}, 13 \equiv 3 \pmod{5},$   
 $19 \equiv 1 \pmod{6}, 19 \equiv 4 \pmod{5}.$
- If  $n \equiv 2 \pmod{10}$ , then what can be  $n \pmod{6}$ ? 1 / 1 point

☒ 0, 2 or 4
 ☐ 0, 1, 2, 3, 4 or 5.
 ☐ 2
 ☐ 1, 2 or 4

**Correct**  
 Correct! If  $n \equiv 2 \pmod{10}$ , then 2 divides  $n$ , so  $n$  is even, and  $n \pmod{6}$  can only be even. Also,  
 $12 \equiv 2 \pmod{10}, 12 \equiv 0 \pmod{6},$   
 $32 \equiv 2 \pmod{10}, 32 \equiv 2 \pmod{6},$   
 $22 \equiv 2 \pmod{10}, 22 \equiv 4 \pmod{6}.$
- What is the smallest positive integer  $n$  such that  $n \equiv 3 \pmod{11}$  and  $n \equiv 7 \pmod{17}$ ? 1 / 1 point

☒ 58
 ☐ 24
 ☐ 25
 ☐ 619

**Correct**  
 Correct! You could find this number either by trying all numbers with remainder 7 modulo 17 starting from 7, 24, 41, ... and computing their remainders modulo 11 until you find 58. Alternatively, you could use the algorithm from the lecture. First use Extended Euclid's Algorithm to find out that  $1 = 14 \cdot 11 - 9 \cdot 17$ . Then compute  $n = 14 \cdot 11 \cdot 7 - 9 \cdot 17 \cdot 3 = 619$ , then compute  $619 \pmod{11 \cdot 17} = 619 \pmod{187} = 58$ .