

Integer Factorization

Chinese Remainder Theorem

✓

Reading: Remainers for Two Modules

10 min

✓

Reading: Chinese Remainder Theorem

10 min

✓

Quiz: Remainers

4 questions

📄

Quiz: Chinese Remainder Theorem: Code

1 question

Modular Exponentiation

🎉 Congratulations! You passed!

Grade received 100%

Latest Submission: 100% (100%)

To pass 80% or higher

Go to next item

Chinese Remainder Theorem: Code

Review Learning Objectives

1. Implement the algorithm to construct the number from the Chinese Remainder Theorem.

1 / 1 point

Submit your assignment

Push to grade

Try again

You need to implement the function *ChineseRemainderTheorem*( $n_1, r_1, n_2, r_2$ ) which takes two coprime numbers  $n_1$  and  $n_2$  and the respective remainders  $0 \leq r_1 < n_1$  and  $0 \leq r_2 < n_2$ , and must return the number  $x$  such that  $0 \leq x < n_1 n_2$ ,  $x \equiv r_1 \pmod{n_1}$  and  $x \equiv r_2 \pmod{n_2}$ .

You have access to the function *ExtendedEuclid*( $a, b$ ) which returns pair of numbers ( $x, y$ ) such that  $ax + by = \text{gcd}(a, b)$ .

Implement the function explained in the lectures.

1def ChineseRemainderTheorem(n1, r1, n2, r2):

2 # Your code here

3 return (n1\*r2 + n2\*r1) % (n1\*n2)

4

5 #ChineseRemainderTheorem(11, 3, 17, 7)

Run

Reset

No Output

👍 Correct

Good job!

Your grade

100%

View Feedback

We keep your highest score