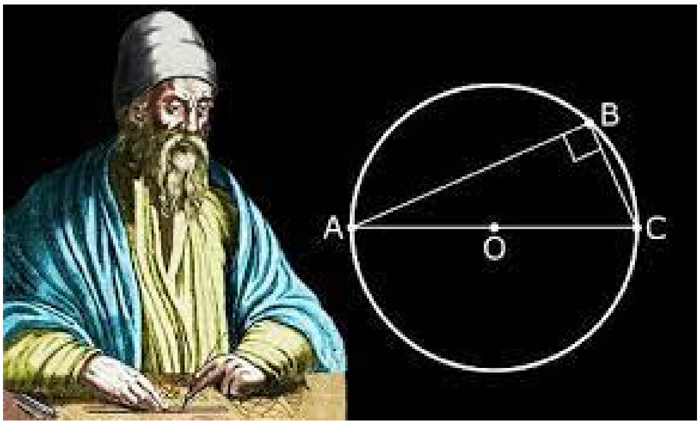
MATH CIRCLE TTU

Number Theory

Congruences



Congruences

Two integers a and b are congruent modulo c,

$$a \equiv b \pmod{c} \qquad \Longleftrightarrow \qquad a = n \times c + b\,,$$

if the remainder of dividing a by c and the remainder of dividing b by c is the same.

Example. 25 is congruent with 4 modulo 7, that is, $25 \equiv 4 \pmod{7}$.

(i) What is the remainder of dividing 25 by 7?

(ii) What is the remainder of dividing 4 by 7?

(iii) Clearly, $25 = 3 \times 7 + 4$.

Problem 1.

(i) Is $22 \equiv -1040 \pmod{18}$?

(ii) Is $416 \equiv 3 \pmod{7}$?

Greatest Common Divisor

Problem 2.

(i) What is the greatest common divisor of 4 and 12?

(ii) What is the greatest common divisor of 8 and 12?

(iii) What is the greatest common divisor of 7 and 18?

Extended Euclidean Algorithm

The greatest common divisor of a and b, $\gcd(a, b)$, can be written as

$$\gcd(a, b) = n \times a + m \times b\,.$$

Example. We work with 8 and 14 and we follow these steps:

1. We divide the largest number 14 by the other one 8 and we get 1 and remainder 6, that is,
$$14 = 1 \times 8 + 6\,.$$
2. Now, we divide 8 by 6 and get 1 and remainder 2, so
$$8 = 1 \times 6 + 2\,.$$
3. If we divide 6 by 2 the remainder is 0. (We repeat previous steps until we get remainder 0).
4. The last nonzero remainder is the greatest common divisor. In our case, $\gcd(8, 14) = 2$.
5. Moreover, going backwards and using above equations,
$$2 = 8 - 1 \times 6 = 8 - 1 \times (14 - 1 \times 8) = 2 \times 8 + (-1) \times 14\,.$$

Problem 3. Apply the extended Euclidean algorithm for 7 and 18.

Easy Problem

Problem 4. A store sells boxes of donuts at \$7 each and pizzas at \$18 each. If in one day they have sold 25 items in total and received \$208, how many pizzas and boxes of donuts were sold?

Even Easier Problem

Problem 5. A store sells boxes of donuts at \$7 each and pizzas at \$18 each. If in one day they have received \$208, how many pizzas and boxes of donuts were sold? Is that the only solution?