Modular Arithmetic

Congruence

$a \equiv b \pmod{m}$, a and b are integers and m is a positive integer

a is congruent to b modulo m if m divides a – b or $m \mid a - b$

Is $7 \equiv 5 \pmod{6}$?

6 does not divide 7 - 5 =2
No

Is $18 \equiv 9 \pmod{3}$?

3 divides 18 - 9 =9
Yes

Application of Congruence: Generating pseudorandom numbers

Linear congruence, $x_{n+1} = (ax_n + c) \bmod m$.

$2 \leq a < m$

$0 \leq c < m$

$0 \leq x_0 < m$

the modulus m, multiplier a, increment c, seed x0

Application of Congruence: Generating pseudorandom numbers

Let $m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$

x0 = 3

Application of Congruence: Generating pseudorandom numbers

Let $m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$

x0 = 3
x1 = (7 x0 + 4) mod 9 = (7.3 + 4) mod 9 = 25 mod 9 = 7

Application of Congruence: Generating pseudorandom numbers

Let m = 9, a = 7, c = 4, and x_0 = 3

x0 = 3
x1 = (7 x0 + 4) mod 9 = (7.3 + 4) mod 9 = 25 mod 9 = 7
x2 = (7x1 + 4) mod 9 = (7.7 + 4) mod 9 = 53 mod 9 = 8

Application of Congruence: Generating pseudorandom numbers

Let $m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$

x0 = 3
x1 = (7 x0 + 4) mod 9 = (7.3 + 4) mod 9 = 25 mod 9 = 7
x2 = (7x1 + 4) mod 9 = (7.7 + 4) mod 9 = 53 mod 9 = 8
x3 = (7x2 + 4) mod 9 = (7.8 + 4) mod 9 = 60 mod 9 = 6
x4 = (7x3 + 4) mod 9 = (7.6 + 4) mod 9 = 46 mod 9 = 1
x5 = (7x4 + 4) mod 9 = (7.1 + 4) mod 9 = 11 mod 9 = 2
x6 = (7x5 + 4) mod 9 = (7.2 + 4) mod 9 = 18 mod 9 = 0
x7 = (7x6 + 4) mod 9 = (7.0 + 4) mod 9 = 4 mod 9 = 4
x8 = (7x7 + 4) mod 9 = (7.4 + 4) mod 9 = 32 mod 9 = 5
x9 = (7x8 + 4) mod 9 = (7.5 + 4) mod 9 = 39 mod 9 = 3

x10 = (7x9 + 4) mod 9 = (7.3 + 4) mod 9 = 25 mod 9 = 7

Gcd and lcm

Determine lcm of 10, 14, and 147.

$10 = 2 . 5$

$14 = 2. 7$

$147 = 3. 7^2$

$\text{Lcm } (10, 14, 21) = 2^{\max(1, 1, 0)} \times 3^{\max(0, 0, 1)} \times 5^{\max(1, 0, 0)} \times 7^{\max(0, 1, 2)}$

$= 2^1 \times 3^1 \times 5^2 \times 7^2$

Gcd and lcm

Determine gcd of 10, 14, and 147.

$10 = 2 . 5$

$14 = 2. 7$

$147 = 3. 7^2$

$\text{Gcd } (10, 14, 21) = 2^{\min(1, 1, 0)} \times 3^{\min(0, 0, 1)} \times 5^{\min(1, 0, 0)} \times 7^{\min(0, 1, 2)}$

$= 2^0 \times 3^0 \times 5^0 \times 7^0$