9.1 - The Division Algorithm

Tuesday, July 11, 2023 12:47 PM

EXERCISE 9.1.1: Integer divisibility.

Indicate whether each expression is true or false.

(a) 8 | 40 True, $x \mid y$ iff $x \neq 0$ ≠8 & $\exists k(y=kx)$ b/c for $k=5$, $40=(5)(8)$.

(b) 7 | 50 False, $\nexists k(y=kx)$ ∴ $7 \nmid 50$.

EXERCISE 9.1.2: Positive divisors.

List all the positive divisors of each number.

(a) 24 $\{1, 2, 3, 4, 6, 8, 12, 24\}$

(b) -36 $\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

(a) 1×24

2×12

3×8

4×6

(b) -1×36 $\quad$ 1×-36

-2×18 $\quad$ 2×-18

-3×12 $\quad$ 3×-12

-4×9 $\quad$ 4×-9

-6×6 $\quad$ 6×-6

EXERCISE 9.1.3: Computing div and mod.

Compute the value of the following expressions:

(a) 344 mod 5 4

(b) 344 div 5 68

(c) (-344) mod 5 1

(d) (-344) div 5 -69

9.2 - Modular arithmetic

Tuesday, July 11, 2023 12:53 PM

EXERCISE 9.2.1: Computing using modular arithmetic.

Compute the value of the following expressions:

(a) $46^{30} \bmod 9$

(b) $38^{7} \bmod 3$

(c) $[72 \cdot (-65) + 211] \bmod 7$

(a) $46^{30} \bmod 9$

$= [(46 \bmod 9)^{30}] \bmod 90$

$= (1)^{30} \bmod 90$

$= 1 \bmod 90$

$= 1$

(b) $38^{7} \bmod 3$

$= [(38 \bmod 3)^{7}] \bmod 3$

$= (2)^{7} \bmod 3$

$= 128 \bmod 3$

$= 2$

(c) $[72 \cdot (-65) + 211] \bmod 7$

$= [(72 \bmod 7)(-65 \bmod 7) + (211 \bmod 7)] \bmod 7$

$= [(2)(5) + 1] \bmod 7$

$= [10 + 1] \bmod 7$

$= 11 \bmod 7$

$= 4$

EXERCISE | 9.2.3: Computing exponents mod m.

Compute each quantity below using the methods outlined in this section. Show your steps, and remember that you should not use a calculator.

(a) $46^{10} \bmod 7$

$46^{10} \bmod 7$

$= [(46 \bmod 10)^{10}] \bmod 7$

$= [(4)^{10}] \bmod 7$

we know: $4^1 = 4$
$4^2 = 16$
$4^3 = 64$

$= [(4)^3 (4)^3 (4)^3 (4)^1] \bmod 7$

$= [(4^3 \bmod 7)(4^3 \bmod 7)(4^3 \bmod 7)(4^1 \bmod 7)] \bmod 7$

$= [(64 \bmod 7)(64 \bmod 7)(64 \bmod 7)(4 \bmod 7)] \bmod 7$

$= [(64 \bmod 7)(64 \bmod 7)(64 \bmod 7)(4 \bmod 7)] \bmod 7$

$= [(1)(1)(1)(4)] \bmod 7$

$= 4 \bmod 7$

$= 4$

EXERCISE 9.2.5: Congruence mod m.

(a) Group the following numbers according to congruence mod 11. That is, put two numbers in the same group if they are equivalent mod 11.
{−57, 17, 108, 0, −110, −93, 1111, 130, 232}

Number	Mod 11
-57	9
17	6
108	9
0	0
-110	0
-93	6
1111	0
130	9
232	1

$\{0, -110, 1111\}, \{232\}, \{17, -93\}, \{-57, 108, 130\}$

9.3 - Prime factorizations

Tuesday, July 11, 2023 3:15 PM

Theorem 9.3.2: GCD and LCM from prime factorizations.

Let x and y be two positive integers with prime factorizations expressed using a common set of primes as:

$$x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$
$$y = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$$

The p_i's are all distinct prime numbers. The exponents α_i's and β_i's are non-negative integers.

Then:

- x divides y if and only if $\alpha_i \leq \beta_i$ for all $1 \leq i \leq r$
- $\gcd(x, y) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$
- $\operatorname{lcm}(x, y) = p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_r^{\max\{\alpha_r,\beta_r\}}$

Feedback?

EXERCISE | 9.3.2: Computing using prime factorizations.

Some numbers and their prime factorizations are given below.

- $140 = 2^2 \cdot 5 \cdot 7$
- $175 = 5^2 \cdot 7$
- $532 = 2^2 \cdot 7 \cdot 19$
- $648 = 2^3 \cdot 3^4$
- $1078 = 2 \cdot 7^2 \cdot 11$
- $1083 = 3 \cdot 19^2$
- $15435 = 3^2 \cdot 5 \cdot 7^3$
- $25480 = 2^3 \cdot 5 \cdot 7^2 \cdot 13$

Use these prime factorizations to compute the following quantities.

(a) gcd(532, 15435)

(b) gcd(648, 1083)

(c) lcm(532, 1083)

(a) gcd(532, 15435)

Prime factorizations:

$532 = 2^2 \cdot 7^1 \cdot 19^1 = \underline{2^2} \cdot \underline{3^0} \cdot \underline{5^0} \cdot \underline{7^1} \cdot \underline{19^1}$

$15435 = 3^2 \cdot 5^1 \cdot 7^3 = \underline{2^0} \cdot \underline{3^2} \cdot \underline{5^1} \cdot \underline{7^3} \cdot \underline{19^0}$

- smaller base exponent

· smaller base exponent

· larger base exponent

$\therefore \gcd(532, 15435)$

$= 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 19^0$

$= (1)(1)(1)(7)(1)$

$= 7$

(b) $\gcd(648, 1083)$

Prime factorizations:

$648 = 2^3 \cdot 3^4 = 2^3 \cdot 3^4 \cdot 19^0$

$1083 = 3^1 \cdot 19^2 = 2^0 \cdot 3^1 \cdot 19^2$

· smaller base exponent

· larger base exponent

$\therefore \gcd(648, 1083)$

$= 2^0 \cdot 3^1 \cdot 19^0$

$= (1)(3)(1)$

$= 3$

(c) $\operatorname{lcm}(532, 1083)$

Prime factorizations:

$532 = 2^2 \cdot 7^1 \cdot 19^1 = 2^2 \cdot 3^0 \cdot 7^1 \cdot 19^1$

$1083 = 3^1 \cdot 19^2 = 2^0 \cdot 3^1 \cdot 7^0 \cdot 19^2$

· smaller base exponent

· larger base exponent

$\therefore \ \mathrm{lcm}(532, 1083)$

$= 2^2 \cdot 3^1 \cdot 7^1 \cdot 19^2$

$= (4)(3)(7)(361)$

$= 30324$

9.8 - Introduction to cryptography

Thursday, July 20, 2023 9:11 AM

EXERCISE 9.8.6: Deducing the key from a single (plaintext, ciphertext) pair.

(a) Suppose Alice and Bob use the simple encryption scheme in which c = (m + k) mod N and m = (c − k) mod N. Suppose that Eve knows that N = 4657. Suppose that she also manages to learn that the message m corresponding to c = 1322 is 3411. Can she infer the value for k? What is k? Give your answer as a number mod N. That is, your answer would be a number in the range 0, ..., N-1.

Feedback?

Eve

$N = 4657$

$c = 1322$

$m = 3411$

Alice

$c = (m + k) \bmod N$

$c = m + k - N$

$1322 = 3411 + k - 4657$

$k = 2568$

Bob

$m = (c - k) \bmod N$

$m = c - k + N$

$3411 = 1322 - k + 4657$

$k = 2568$

yes, Eve can infer the value of k.

$k = 2568 \pmod N$, $N = 4657$ in this case.