Esther, Bobae, Ngozi, Ben, Matt, Antonio

Math 251, Mon 15-Nov-2021 -- Mon 15-Nov-2021

Discrete Mathematics

Fall 2021

Monday, November 15th 2021

Wk 12, Mo

Topic:: Modular arithmetic

Read:: Rosen 4.1

~~HW[[WW ModularArithmetic due Tues.~~

This chapter: investigate number theory---integers, primes, congruences, etc.

Encryption RSA

Divisors and multiples

Definition 1: Let a, b be integers. We say a **divides** b, or $a \mid b$, precisely when there exists an integer c so that $ac = b$. When the negation of $a \mid b$ holds—that is, when no integer c exists so that $ac = b$—we write $a \nmid b$.

$11 \mid 77$ $\qquad$ $4 \nmid 15$

$-3 \mid 24$

Remarks:

Divisors of 12

$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$

- When $a \mid b$, integers, we say a is a **divisor** of b.
- The set of divisors of b lie between $(-b)$ and b.
- The set of **common divisors** to integers b and c looks like $D = \{a \in \mathbb{Z} : (a \mid b) \wedge (a \mid c)\}$. Among the common divisors, D has a largest element, called the **greatest common divisor**, or $\gcd(b, c)$.
- The set of **common multiples** of integers b and c looks like $M = \{m \in \mathbb{Z} : (b \mid m) \wedge (c \mid m)\}$. Among the common multiples, M has a smallest positive element, called the **least common multiple**, or $\operatorname{lcm}(b, c)$.

Call m a multiple of b if $b \mid m$

Example 1:

Find the gcd and lcm of 21560 and 8190.

$$21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11 = 2^3 \cdot 3^0 \cdot 5 \cdot 7^2 \cdot 11^1 \cdot 13^0$$

$$8190 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot 13^1$$

$5 \,)\, 21560 = 4312$, $2 \,)\, 4312 = 2156$, $2 \,)\, 2156 = 1078$, $2 \,)\, 1078 = 539$, $7 \,)\, 539 = 77$, $7 \,)\, 77 = 11$

$5 \,)\, 8190 = 1638$, $2 \,)\, 1638 = 819$, $3 \,)\, 819 = 273$, $3 \,)\, 273 = 91$, $7 \,)\, 91 = 13$

Every prime appearing in one or other factorization

$$\gcd(21560, 8190) = 2^1 \cdot 3^0 \cdot 5 \cdot 7 \cdot 11^0 \cdot 13^0 = 2 \cdot 5 \cdot 7 = 70$$

$$\operatorname{lcm}(21560, 8190) = 2^3 3^2 5^1 7^2 11^1 13^1 = 2522520$$

■

Theorem 1 (Fundamental Theorem of Arithmetic): Every positive integer $a \geqslant 2$ is either prime or the product of primes:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

If a, b are positive integers with prime factorizations

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad \text{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

(where, as needed, some α_j, β_j may be zero), then among all common divisors d of a and b (i.e, numbers which satisfy $(d \mid a) \wedge (d \mid b)$), the **greatest common divisor** is

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}.$$

Likewise, among all common multiples m of a and b (i.e., numbers which satisfy $a \mid m$ and $b \mid m$), the **least common multiple** is

$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}.$$

Note: $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Which among the following appear to be true claims?

- False Let $n, d \in \mathbb{Z}^+$, and $A = \{a \in \mathbb{Z}^+ : (a \leqslant n) \wedge (d \mid a)\}$. Then $|A| = \lceil n/d \rceil$. Counterexample: $n = 50$, $d = 11$

- $\forall a \in \mathbb{Z}^+, \forall b \in \mathbb{Z}^+, \forall c \in \mathbb{Z}^+,$
  - False $(a \mid b) \to a \leqslant \sqrt{b}$.
  - True $(a \mid b) \wedge (b \mid c) \to a \mid c$. some integers k, l exist so that $ak = b$ and $bl = c$. Thus, $a(kl) = c$.
  - True $(a \mid b) \wedge (a \mid c) \to a \mid (b + c)$. Some integers k, l exist so that $ak = b$, $al = c$. Thus, $a(k+l) = b + c$.
  - False $a \mid (bc) \to (a \mid b) \vee (a \mid c)$. Counterexample: $a = 6$, $b = 3$, $c = 4$
  - True $(a \mid b) \to a \mid (bc)$.
  - True $(a \mid b) \wedge (a \mid c) \to \forall m, n \in \mathbb{Z}, a \mid (mb + nc)$.

Theorem 2 (Division Algorithm): Let a be an integer and d a positive integer. There exist unique integers q, r with $0 \leqslant r < d$ such that

$$a = dq + r.$$

Note that

- The remainder r is the output of the mod function: $r = a \bmod d$.

  means the remainder between 0 and d (not included) when a is divided by d.

- If, at the end of a calculation, you intend to perform the mod function, it can be inserted at various additive/multiplicative points along the way:

$$\begin{aligned}
(37)(63) - 58^4 \bmod 11 &= (37 \bmod 11)(63 \bmod 11) - (58 \bmod 11)^4 \bmod 11 \\
&= (4)(8) \bmod 11 - (3)^4 \bmod 11 \\
&= 32 \bmod 11 - 81 \bmod 11 \\
&= 10 - 4 \ = \ 6.
\end{aligned}$$

It doesn't work reliably in exponents, however:

$$\begin{aligned}
6^{17} \bmod 13 &= 6 \cdot (6^2 \bmod 13)^8 \bmod 13 \ = \ 6 \cdot 10^8 \bmod 13 \\
&= 6 \cdot (10000 \bmod 13)^2 \bmod 13 \ = \ 6 \cdot 3^2 \bmod 13 \ = \ 2,
\end{aligned}$$

but

$$6^{17 \bmod 13} \bmod 13 = 6^4 \bmod 13 = 9.$$

True / False

1. $17 \equiv 5 \pmod 7$ F

4. $17 \equiv 5 \pmod{12}$ T

2. $17 \equiv 5 \pmod 3$ T

Modular congruence

3. $17 \equiv 5 \pmod 4$ T

Definition 2: Let $a, b \in \mathbb{Z}$ and $m \geqslant 2$ be an integer. We say that a **and** b **are congruent modulo** m, abbreviating this as $a \equiv b \pmod m$, precisely when $m \mid (a - b)$.

Theorem 3: The following are equivalent:

1. $a \equiv b \pmod m$
2. $a \bmod m = b \bmod m$
3. $\exists k \in \mathbb{Z}$ such that $a = b + km$

Since $36 \bmod 11 = 3$ and $80 \bmod 11 = 3$ then $36 \equiv 80 \pmod{11}$

Theorem 4: If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

Note: It is this theorem which justifies the insertion of mod functions in additive/multiplicative operations above.

Example: Find $2^{8888} \bmod 5$.

Note: The theorem above does *not* say that $ac \equiv bc \pmod{()m}$ allows you to conclude $a \equiv b \pmod m$.

Equivalence classes modulo m; $\mathbb{Z}_m$

If you pick a modulus m, the Division Algorithm ensures that the range of the mod function $f \colon \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n \bmod m$ is $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. That is, all integers a are equivalent to some element in $\mathbb{Z}_m$ modulo m. For instance, relative to modulus $m = 5$ all the numbers

$$\ldots, -7, -2, 3, 8, 13, \ldots$$