Math 251, Mon 16-Nov-2020 -- Mon 16-Nov-2020
Discrete Mathematics
Fall 2020

$a \mid b \to a \mid (bc)$

$a \mid b$ means $\exists\, k \in \mathbb{Z}$ so that $ak = b$. But then

$a \cdot \underline{kc} = bc$?

$a \mid b$ and $b \mid c$ then $\exists\, k_1, k_2 \in \mathbb{Z}$ w/ $ak_1 = b$ and $bk_2 = c$

So $a\, \underline{k_1 k_2} = c$?

Monday, November 16th 2020

Wk 12, Mo

Topic:: Modular arithmetic
Read:: Rosen 4.1
HW[[WW ModularArithmetic due Tues.

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

$$\begin{array}{r|l} & 7 \\ 3 & 21 \\ 2 & 42 \\ 2 & 84 \\ 2 & 168 \end{array}$$

$15 = 2^0 \cdot 3^1 \cdot 5^1$

$24 = 2^3 \cdot 3^1 \cdot 5^0$

$120 = 2^3 \cdot 3^1 \cdot 5 = \mathrm{lcm}(5, 24)$

$\frac{8}{15} + \frac{7}{24} = \frac{\quad}{120}$

want common denom — multiple of both 15 and 24

$168 = 2^3 \cdot 3^1 \cdot 7^1$

$= 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 31^0$

$155 = 5 \cdot 31 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 31^1$

$\gcd(155, 168) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 31^0 = 1$

$\mathrm{lcm}(155, 168) = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 31^1$

$13 \mid 52$ since $4 \in \mathbb{Z}$ and $(13)(4) = 52$

Divisors and multiples

$13 \nmid 49$

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 $a \nmid b$.

Recall that the Fundamental Theorem of Arithmetic, which we proved using strong induction, says 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

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

Which among the following appear to be true claims? T or F ?

F • Let $n, d \in \mathbb{Z}^+$, and $A = \{a \in \mathbb{Z}^+ : (a \leqslant n) \wedge (d \mid a)\}$. Then $|A| = \lceil n/d \rceil$. Fixed (made True) if $\lfloor n/d \rfloor$

A gives all pos. multiples of d not exceeding n

Ex. $n = 55$, $d = 4$

$A = \{4, 8, 12, 16, \ldots 52\}$

• $\forall a \in \mathbb{Z}^+, \forall b \in \mathbb{Z}^+, \forall c \in \mathbb{Z}^+,$
- F ○ $(a \mid b) \rightarrow a \leqslant \sqrt{b}$. $8 \mid 16$ but $8 > \sqrt{16}$
- T ○ $(a \mid b) \wedge (b \mid c) \rightarrow a \mid c$.
- T ○ $(a \mid b) \wedge (a \mid c) \rightarrow a \mid (b + c)$.
- F ○ $a \mid (bc) \rightarrow (a \mid b) \vee (a \mid c)$. $6 \mid 18 = 2 \cdot 9$ but $6 \nmid 2$ and $6 \nmid 9$
- T ○ $(a \mid b) \rightarrow a \mid (bc)$.
- T ○ $(a \mid b) \wedge (a \mid c) \rightarrow \forall m, n \in \mathbb{Z}, a \mid (mb + nc)$.

$a \mid b \Rightarrow k_1 \in \mathbb{Z}$ so that $ak_1 = b$

$a \mid c \Rightarrow k_2 \in \mathbb{Z}$ " " $ak_2 = c$

$a(mk_1 + nk_2) = mb + nc$

Theorem 1 (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

$$a = dq + r.$$

$7 \text{ r. } 2$

$5 \overline{)\,37}$

35

2

$-59 \% 5 = 1$

Note that

$-59 = (-12)(5) + \boxed{1}$

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

Not the same

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

Is $17 \equiv 3 \pmod 5$? No, since $5 \nmid (17-3)$

$17 \equiv 3 \pmod 7$? Yes, $7 \mid (17-3)$

Modular congruence

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 2: The following are equivalent: = i.e., if any one of these is true, then all three are.

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

$a \% m$

$17 \equiv 3 \pmod 7$
$36 \equiv 29 \pmod 7$ $\Big\} \overset{?}{\Longrightarrow}$ $17+36 \equiv 3+29 \pmod 7$

Theorem 3: 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 $2^{8888} \mod 5$.

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 $f(n) = n \mod m$ 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

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

are equivalent, belonging to the class with representative 3. There are just 5 classes when $m = 5$ into which all integers fall, and the five elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ act as their representatives:

$$\begin{array}{rl}
\ldots, -10, -5, -0, 5, 10, \ldots & \text{represented by} \quad 0 \\
\ldots, -9, -4, 1, 6, 11, \ldots & \text{represented by} \quad 1 \\
\ldots, -8, -3, 2, 7, 12, \ldots & \text{represented by} \quad 2 \\
\ldots, -7, -2, 3, 8, 13, \ldots & \text{represented by} \quad 3 \\
\ldots, -6, -1, 4, 9, 14, \ldots & \text{represented by} \quad 4
\end{array}$$

We make $\mathbb{Z}_m$ into something more than just a set of objects by giving it addition and multiplication as follows:

$$a \cdot_m b = ab \mod m, \qquad \text{and} \qquad a +_m b = a + b \mod m.$$

Write out addition and multiplication tables for $\mathbb{Z}_5$. Use it to solve the congruence equation $4x + 3 \equiv 2 \pmod 5$.

Math 251, Mon 16-Nov-2020 -- Mon 16-Nov-2020
Discrete Mathematics
Fall 2020

Monday, November 16th 2020

Wk 12, Mo

Topic:: Modular arithmetic
Read:: Rosen 4.1
HW[[WW ModularArithmetic due Tues.

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

$$\begin{array}{r|l} & 19 \\ 7 & 133 \\ 2 & 266 \\ 2 & 532 \\ 2 & 1064 \end{array}$$

$$1064 = \underline{2^3 \cdot 7^1 \cdot 19^1}$$

$$= 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 \cdot 17^0 \cdot 19^1$$

Can write $19 \mid 1064$

$13 \nmid 1064$

$$36 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 11^0$$
$$55 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 11^1$$

$$\gcd(36, 55) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 11^0$$
$$= 1$$

relatively prime

 Ch. 4 Rosen

Divisors and multiples

$2 \mid 12$

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 $a \nmid b$.

$5 \nmid 12$

Recall that the Fundamental Theorem of Arithmetic, which we proved using strong induction, says every positive integer $a \geqslant 2$ is either prime or the product of primes:

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

$\frac{8}{15} + \frac{7}{24}$

common denom?

$= \text{lcm}(15, 24)$

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

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

$15 = 2^0 \cdot 3^1 \cdot 5^1$

$24 = 2^3 \cdot 3^1 \cdot 5^0$

$\text{lcm} = 2^3 \cdot 3^1 \cdot 5^1$

$= 12$

Which among the following appear to be true claims?

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

  Count number of multiples of $d \leq n$. Answer?

  Fixed by writing $\left\lfloor \frac{n}{d} \right\rfloor$

- $\forall a \in \mathbb{Z}^+, \forall b \in \mathbb{Z}^+, \forall c \in \mathbb{Z}^+,$
  - F ◦ $(a \mid b) \to a \leqslant \sqrt{b}$.
  - T ◦ $(a \mid b) \wedge (b \mid c) \to a \mid c$. $\exists k_1, k_2 \in \mathbb{Z}$ so $ak_1 = b$ and $bk_2 = c$. So $k_1 k_2 a = c$
  - T ◦ $(a \mid b) \wedge (a \mid c) \to a \mid (b + c)$.
  - F ◦ $a \mid (bc) \to (a \mid b) \vee (a \mid c)$. $6 \mid 18 = 3 \cdot 9$
  - T ◦ $(a \mid b) \to a \mid (bc)$. $\exists k \in \mathbb{Z}$ such that $ak = b$ So $(kc)a = bc$
  - T ◦ $(a \mid b) \wedge (a \mid c) \to \forall m, n \in \mathbb{Z}, a \mid (mb + nc)$.

$a \mid 0$ trivially since $a \cdot 0 = 0$.

Theorem 1 (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

$$a = dq + r.$$

$-59 \% 5 = 1$

$-59 = (-12)(5) + 1$

$5 \overline{)17}$ 3 r. 2

$17 = 3 \cdot 5 + 2$

remainder

$0 \leq 2 < 5$

Note that

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

not equal.

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

Is $17 \equiv 3 \pmod 5$? No, since $5 \nmid (17-3)$

$17 \equiv 3 \pmod 7$? Yes, since $7 \mid (17-3)$

Modular congruence

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 2: The following are equivalent: (If you know one is true, you know all 3 are).

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

Theorem 3: 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 $2^{8888} \mod 5$.

Note: The theorem above does *not* say that $ac \equiv bc$ (mod $()m$) 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 $f(n) = n \mod m$ 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

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

are equivalent, belonging to the class with representative 3. There are just 5 classes when $m = 5$ into which all integers fall, and the five elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ act as their representatives:

$$\begin{aligned}
\ldots, -10, -5, -0, 5, 10, \ldots &\quad \text{represented by} \quad 0 \\
\ldots, -9, -4, 1, 6, 11, \ldots &\quad \text{represented by} \quad 1 \\
\ldots, -8, -3, 2, 7, 12, \ldots &\quad \text{represented by} \quad 2 \\
\ldots, -7, -2, 3, 8, 13, \ldots &\quad \text{represented by} \quad 3 \\
\ldots, -6, -1, 4, 9, 14, \ldots &\quad \text{represented by} \quad 4
\end{aligned}$$

We make $\mathbb{Z}_m$ into something more than just a set of objects by giving it addition and multiplication as follows:

$$a \cdot_m b = ab \mod m, \qquad \text{and} \qquad a +_m b = a + b \mod m.$$

Write out addition and multiplication tables for $\mathbb{Z}_5$. Use it to solve the congruence equation $4x + 3 \equiv 2 \pmod{5}$.

$(37)(63) - 58^4 \mod 11 = \left((37)(63) \mod 11 - 58^4 \mod 11 \right) \mod 11$

$= (37 \mod 11)(63 \mod 11) \mod 11 - (58 \mod 11)(58 \mod 11)^3 \mod 11$