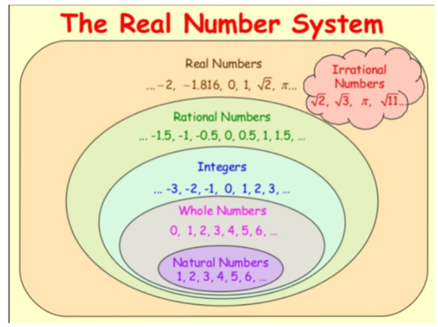
Number Theory Chapter 4.1-4.4

4.1 Divisibility

Divison



Integer

$a | b$ iff $\exists c : \boxed{ac = b}$ ($a, b, \in \mathbb{Z}$, $c \in \mathbb{Z}^+$)

a divides b — Some Value of c

$3 | 15$ $\quad$ $3c = 15$

$c = 5 \in \mathbb{Z}^+$

Since that # goes in evenly.

Another Example: $3 | 22$ $\quad$ $3c = 22$

$c = \frac{22}{3} \notin \mathbb{Z}^+$

Not an Integer

Properties of Divisibility

$a | b \quad ac = b$

$a t = c$

$\boxed{\text{a) if } a | b \text{ and } a | c \text{, then } a | (b+c)}$ ← "a divides into both"

Example: $3 | 15$ $\quad$ $3 | 6$ $\quad$ $3 | (15+6)$ or $3 | 21$ ✓ Shown its true

Start Proof: There exist two integers s and t such that

$b = as$ and $c = at$ from defin. of divisibility.

$b + c = \underbrace{as + at}_{\text{Equivelent}} = a(s+t)$

$b + c = a(s+t)$

$\therefore a | (b+c)$ ← Proof

Properties of Divisibility

$\boxed{\text{b.) iff } a|b \text{ then } a|bc \text{ for all } c \in \mathbb{Z}}$

$3|15 \quad 3|30 \quad 3|45 \quad 3|60$

$\quad\quad\quad 15\cdot 2 \quad 15\cdot 3 \quad 15\cdot 4 \quad$ ~ if $b = 15$, $c = \mathbb{Z}$

If $a|b$ then $b = at$ for some $t \in \mathbb{Z}$

$bc = (at)c = a(tc)$

$bc = a(tc)$ ← Regroup Associated Property

$\therefore a|bc$ by defin. of divisibility

$\boxed{\text{C.) If } a|b \text{ and } b|c \text{, then } a|c}$

$3|6$ and $6|18$, then $3|18$ ✓

Since $a|b$ then $b = at$ for some $t \in \mathbb{Z}$

Since $b|c$ then $c = bs$ for some $s \in \mathbb{Z}$.

Then by substitution:

Then $c = (at)s$, or $c = a(ts)$

$\therefore a|c$

Division Algorithm:

$d \mid a \quad a = dq$

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. $\exists! \, q, r : a = dq + r$.

there exist a q and r

divisor

quotient

remainder

Example:

$4 \mid 21 \qquad 21 = 4q + r$

$$\begin{array}{r} 5 \text{ R}1 \\ 4 \overline{)21} \\ -20 \\ \hline 1 \end{array}$$

$21 = 4(5) + \underline{\underline{1}} \quad 0 \le r < d \quad$ Important

Examples:

Give the quotient and remainder for each.

a) $7 \mid 18$

d a

$a = dq + r$

$18 = 7(2) + 4 \qquad 0 \le r < 7$

Notation:

quotient:

$q = a \text{ div } d$

remainder:

$r = a \text{ mod } d$

$2 = 18 \text{ div } 7$

$4 = 18 \text{ mod } 7$

If we took 18 divided by 7 our remainder would be 4

b.) $10 \mid -112 \qquad -112 = 10(-11) + -2 \quad \not\longrightarrow \quad 0 \le r < 10$

- negative two is not b/w 0 and 10!

$\boxed{-112 = 10(-12) + 8}$

Correct Way to Write

$a = dq + r$

quotient:

$-12 = -112 \text{ div } 10$

remainder:

$8 = -112 \text{ mod } 10$

c) $14 \mid 0 \qquad 0 = 14(0) + 0$

$a = dq + r$

quotient:

$0 = 0 \text{ div } 14$

remainder:

$0 = 0 \text{ mod } 14$

Modular Arithmetic

If $a,b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff $m \mid a-b$.

Remainders

$\frac{4}{4} \to 0$

$\frac{5}{4} \to 1$

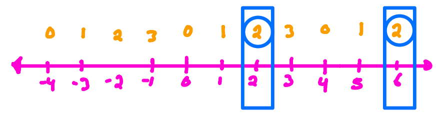
$\frac{6}{4} \to 2$

$\frac{-4}{4} \to 3$

Mod 4 = { 0, 1, 2, 3 }

possible remainders

pattern



a) Determine if $\boxed{2 \equiv 6} \pmod{4}$

Question Asked → is 2 <u>congruent</u> to 6 in mod 4?

Both on two

If I take $\frac{2}{4}$ or $\frac{6}{4}$ my <u>remainder is 2</u>, which is exactly the same, so yes, they're <u>Equivalent.</u>

- Can do it w/o number line by seeing if the <u>difference</u> <u>b/w</u> the <u>two Values is divisible by 4</u>

$2 \equiv 6 \pmod{4}$ $\quad 4 \mid (2-6)$

$4 \mid (-4)$ ✓ yes is congruent

b) Determine if $24 \equiv 14 \pmod{6}$

$6 \mid (24-14)$

$6 \mid 10$ ✗

Not Equivalent

Let $a, b, \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ iff $\boxed{a \bmod m = b \bmod m}$

^if the remanderr are equal to one another then they're congruent

Determine if $2 \equiv 6 \pmod{4}$

$4 | 2 = 4(0) + 2$

$2 \bmod 4 = 6 \bmod 4$

$2 = 2 \bmod 4$

$4 | 6 = 4(1) + 2$

$2 = 6 \bmod 4$

Determine if $24 \equiv 14 \pmod{6}$

$6 | 24 = 6(4) + 0$

$24 \bmod 6 \neq 14 \bmod 6$

$\underline{0} = 24 \bmod 6$

$6 | 14 = 6(2) + 2$

$\underline{2} = 14 \bmod 6$

Thereom:

$a \equiv b \pmod m$

P The Integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$ q

Assuming → Let $a \equiv b \pmod m$

Then $m \mid (a-b)$ by defin of congruence

Then $a-b = km$ for some $k \in \mathbb{Z}$, by defin of divisibility.

By addition of b, then $a = b + km$.

Proved in both directions

Assume $a = b + km$.

Then $a - b = km$ by subtraction.

Then $m \mid (a-b)$, so $a \equiv b \pmod m$.

Thereom

Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $\boxed{a + c \equiv b + d \pmod m}$ and $\boxed{ac \equiv bd \pmod m}$.

Assume $a \equiv b \pmod m$. Then $a = b + km$ for some $k \in \mathbb{Z}$.

Assume also, $c \equiv d \pmod m$. Then $c = d + lm$ for some $l \in \mathbb{Z}$.

$a + c = (b + km) + (d + lm) = (b+d) + (km + lm) = (b+d) + m(k+l)$

$a + c = (b+d) + m(k+l)$ so $(a+c) - (b+d) = m(k+l)$ so

$m \mid (a+c) - (b+d)$ so $a + c \equiv b + d \pmod m$.

$ac = (b + km)(d + lm) = bd + blm + kdm + klm^2 = bd + m(bl + kd + klm)$

So $ac - bd = m(bl + kd + klm)$ so $m \mid ac - bd$ so $ac \equiv bd \pmod m$

Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

Find $7 + 11 \pmod 5$ and $7 \cdot 11 \pmod 5$

$7 + 11 \pmod 5$ and $7 \cdot 11 \pmod 5$

$7 + 11 = 18 \equiv 3 \pmod 5$

Congruent to

$7 \cdot 11 = 77 \equiv 2 \pmod 5$

$7 \cdot 11 = 2 \cdot 1 = 2 \pmod 5$

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7 + 11 = 2 + 1 = 3 \pmod 5$

Arithmetic modulo m

- We can define operations on $\mathbb{Z}_m$, the set of non-negative integers less than m, $\{0, 1, 2, \ldots, m-1\}$.

Addition (denoted $+_m$): $a +_m b = (a+b) \bmod m$

Multiplication (denoted $\cdot_m$): $a \cdot_m b = (a \cdot b) \bmod m$

Example:

Find $4 +_3 5$ and $4 \cdot_3 5$

$4 + 5 = 9 \equiv 0 \pmod 3$

3 goes into 9 evenly

$4 \cdot 5 = 20 \equiv 2 \pmod 3$

4.2 Decimal Expansions from Binary, Octal and Hexadecimal

Let $b \in \mathbb{Z}$ and $b > 1$. Then if $n \in \mathbb{Z}^+$ it can be expressed uniquely in the form:

$$\boxed{n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0}$$

dec. $b = 10$
Binary $b = 2$
Oct $= 8$
hex $b = 16$

Where k is a non-negative integer, $a_0, a_1, \dots a_k$ are non-negative integers less than b, and $a_k \neq 0$.

Write the decimal expression of $10,456$.
base 10
10^4 10^0

$$\boxed{10,456 = 1 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 6 \cdot 10^0}$$

Binary to Decimal Expansion

What is the decimal expansion that has $(1011\ 1101)_2$ as its binary expansion?
7 6 5 4 3 2 1 0

$$(1011\ 1101)_2 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$= 1 \cdot 128 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 1$$

$$= 128 + 32 + 16 + 8 + 4 + 1$$

$$\boxed{= 189}$$

Octal to Decimal Expansion

What is the decimal expansion of the number with an octal expansion of $(4072)_8$?
exp. 3 2 1 0

$$(4072)_8 = 4 \cdot 8^3 + 0 \cdot 8^2 + 7 \cdot 8^1 + 2$$

$$= 4 \cdot 512 + 0 \cdot 64 + 7 \cdot 8 + 2$$

$$= 2048 + 0 + 56 + 2$$

$$\boxed{= (2106)_{10}} \quad \text{or} \quad 2106$$

Hexadecimal to decimal Expansion

What is the decimal expansion of the number with a hexadecimal expansion of $(\overset{4}{2}\overset{3}{A}\overset{2}{E}\overset{1}{0}\overset{0}{B})_{16}$?

Values for Hexadecimal Expansion → A = 10 B = 11 C = 12 D = 13 E = 14 F = 15

0 1 2 3 4 5 6 7 8 9 A B C D E F

$$(2AE0B)_{16} = 2\cdot 16^4 + 10\cdot 16^3 + 14\cdot 16^2 + 0\cdot 16 + 11$$

$$= 131072 + 40960 + 3584 + 0 + 11$$

$$\boxed{= (175,627)_{10}} \quad \text{or} \quad 175627$$

Binary, Octal and Hexadecimal Expansions from Decimal

Finding an Octal Expansion

Find the Octal expansion of $(12543)_{10}$ intrested in the remainder

8 $\boxed{\text{mod } 8}$

To solve these problems → Division Algorithm: $a = dq + r$

$12543 = 8\,\underline{1567} + 7 \cdot 8^0$

quotient

$1567 = 8(195) + 7 \cdot 8^1$

$195 = 8(24) + 3 \cdot 8^2$

$24 = 8(3) + 0 \cdot 8^3$

$3 = \underline{\underline{8(0)}} + 3 \cdot 8^4$

Done Since quotient is 0

$\boxed{(30377)_8}$

Finding a hexadecimal Expansion

Find the hexadecimal (16) expansion of $(19472)_{10}$

A = 10 B = 11 C = 12 D = 13 E = 14 F = 15

$(19,472)_{10} = 16 \cdot 1217 + 0$

$1217 = 16 \cdot \underline{76} + 1$

$76 = 16 \cdot \underline{4} + 12$

$4 = 16 \cdot \underline{0} + 4$

Will replace with C from above

4 12 1 0

$\boxed{(4C10)_{16}}$

Finding a Binary Expansion:

Find the binary $^{(2)}$ expansion of 141.

$$141 = 2 \cdot \underline{70} + 1$$

$$70 = 2 \cdot \underline{35} + 0$$

$$35 = 2 \cdot \underline{17} + 1$$

$$17 = 2 \cdot \underline{8} + 1$$

$$8 = 2 \cdot \underline{4} + 0$$

$$4 = 2 \cdot \underline{2} + 0$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 2 \cdot 0 + 1$$

Groups of 4

$$\boxed{(1000\ 101)_2}$$

Conversions Between Binary, Octal and Hexadecimal Expansions

Conversions between binary, Octal and hexadecimal

Find the octal ($8 = 2^3$) and hexadecimal (16, 2^4) expansions of:

$$(11\ 1110\ 1011)_2$$

8	4	2	1
2^3	2^2	2^1	2^0

Octal $8 = 2^3$ (4 2 1)

00 11 1110 1011

~ We like things in 3s so we add two zeros at the end

001 111 101 011

1 7 5 3

$\boxed{(1753)_8}$

Hexadecimal

0011 1110 1011

~ Groups of fours
~ Add zeros to make group of 4

0011 1110 1011

3 14 11
E B

$\boxed{(3EB)_{16}}$

A = 10
B = 11
C = 12
D = 13
E = 14
F = 15

Find the binary (2^1) expansion of $(37274)_8$ (2^3)

for octal:

4	2	1
2^2	2^1	2^0

3	7	2	7	4
0 1 1	1 1 1	0 1 0	1 1 1	1 0 0

Group in groups of 4 for final Solution.
- and start from the right side
- Add 0 at end if needed to Group 4 together

$\boxed{(0011\ 1100\ 1011\ 1100)_2}$

Find the hexidecimal Expansion of $(37274)_8$

$$\boxed{\frac{8}{2^3}\ \frac{4}{2^2}\ \frac{2}{2^1}\ \frac{1}{2^0}}$$

0011 1110 1011 1100

3 14 11 12

$\boxed{(3EBC)_{16}}$

A = 10
B = 11
C = 12
D = 13
E = 14
F = 15

Find the binary expansion of $(A8D)_{16}$ Hexadecimal to binary

2^1

$$\boxed{\frac{8}{2^3}\ \frac{4}{2^2}\ \frac{2}{2^1}\ \frac{1}{2^0}}$$

A (10)	8	D (13)
1 0 1 0	1 0 0 0	1 1 0 1

$\boxed{(1010\ 1000\ 1101)_2}$

A = 10
B = 11
C = 12
D = 13
E = 14
F = 15

Find the Octal Expansion of $(A8D)_{16}$

$$\frac{4}{2^2}\ \frac{2}{2^1}\ \frac{1}{2^0}$$

1 0 1 0 1 0 0 0 1 1 0 1

5 2 1 5

$\boxed{(5215)_8}$

Operation on base 'n' numbers

Find the sum and product of $(1011)_2$ and $(011)_2$

$$\begin{array}{r} {\scriptstyle 1\ 1\ \ } \\ 1011 \\ +\ 011 \\ \hline 1110 \end{array} \qquad \begin{array}{r} 1011 \\ \times\ 011 \\ \hline 1011 \\ 10110 \\ 000000 \\ \hline 100001 \end{array}$$

The Sum is:

$$\boxed{(1110)_2}$$

In Binary:

$2 = \underline{1}\ \underline{0}$

$3 = \underline{1}\ \underline{1}$

Should be grouping in fours
- Put zeros in front if needed

$$\boxed{(0010\ 0001)_2}$$

Algorithms for Integer Operations

Pseudocode: Algorithm for Base b Expansions

Procedure: Base b expansion(n, b: positive integers, b > 1)

$q = n$

$k = 0$

While $q \neq 0$

$a_k = q \text{ mod } b$
$q = q \text{ div } b$

$k = k + 1$

return $(a_{k-1}, \ldots, a_1, a_0)$ { $(a_{k-1}, \ldots a_1, a_0)$ is base b expansion of n }

Addition Algorithm - Binary

- To add a and b, first add their right-most bits. This gives:

$$a_0 + b_0 = C_0 \cdot 2 + S_0$$ where S_0 = rightmost bit C_0 = Carry (0 or 1)

Then, add the next pair of bits with the carry, which gives:

$$a_1 + b_1 + C_0 = C_1 \cdot 2 + S_1$$

Continue untill you've added the last bits. At the last stage,

add a_{n-1}, b_{n-1} and C_{n-2} to obtain $C_{n-1} \cdot 2 + S_{n-1}$

$$a + b = (S_n S_{n-1} S_{n-2} S_{n-3} \ldots S_1 S_0)_2$$

Additon Algorithm Example

Add $a = (1011)_2$ and $b = (1110)_2$

$s_0 = a_0 + b_0 = 1 + 0 = 0 \cdot 2 + 1$

$s_1 = a_1 + b_1 = 1 + 1 + 0 = 1 \cdot 2 + 0$

$s_2 = a_2 + b_2 = 0 + 1 + 1 = 1 \cdot 2 + 0$

$s_3 = a_3 + b_3 = 1 + 1 + 1 = 1 \cdot 2 + 1$

$s_4 = c_3 = 1$

$\therefore s = a + b = (11001)_2$

Pseudocode: Addition Algorithm

procedure add (a, b : positive integers)

{ the binary expansions of a and b are ($a_{n-1}\ a_{n-2} \cdots a_1 a_0$) and ($b_{n-1}\ b_{n-2} \cdots b_1\ b_0$) }

C: = 0

For j: = 0 to n – 1

d: = $\lfloor (a_j + b_j + c)/2 \rfloor$

$s_j = a_j + b_j + c - 2d$

c: = d

S : = C

Return ($s_0, s_1, s_2, \ldots s_n$) { the binary expansions of the sum ($s_n\ s_{n+1} \ldots\ s_1\ s_0$ $)_2$}

Multiplication Algorithm Example

Multiply $a = (101)_2$ and $b = (110_2)$.

procedure multiply (a, b : positive integers)

for $j = 0$ to $n-1$

if $b_j = 1$ then $c_j := a$ shifted j places

else $c_j = 0$

$p := 0$

for $j = 0$ to $n-1$

$p = p + c_j$

return p

4.3 Prime Numbers and Their Properties

Prime and Composite Numbers

If $p \in \mathbb{Z}^+$ and $p > 1$, then p is considered prime if the only factors of p are 1 and p. Otherwise, the number is composite. This means p is composite iff $\exists a \in \mathbb{Z}^+$ such that $a \mid p$ and $1 < a < p$.

Some prime #s: $2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}$

$9 = 3 \cdot 3$ Composite

$23 = 23 \cdot 1$ Prime

$51 = 17 \cdot 3$ Composite

9

3 3

23

Doesn't Breakdown

51

3 17

product of primes

$2 \cdot 1 = 2$

$3 \cdot 1 = 3$

× $4 \cdot 1 = 4$ and $2 \cdot 2 = 4$

$5 \cdot 1 = 5$

× $6 \cdot 1 = 6$ and $2 \cdot 3 = 6$

$7 \cdot 1 = 7$

× $8 \cdot 1 = 8$ and $4 \cdot 2 = 8$

× $9 \cdot 1 = 9$ and $3 \cdot 3 = 9$

The Fundamental Theorem of Arithmetic

Every Positive integer greater than 1 can be written uniquely as a prime or the product of 2 or more primes where primes are written in non-decreasing order.

~ factor tree

Write the Unique prime factorization:

$27 = 3 \cdot 3 \cdot 3 = 3^3$

$200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 2^3 \cdot 5^2$

Trial Division - Theorem and Proof

If n is a positive integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

If n is composite, then by definition we know n has a factor $a \in \mathbb{Z}^+$ such that $1 < a < n$. By definition of a factor, $n = ab$, where $b \in \mathbb{Z}^+$ and $b > 1$. We want to show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof:
If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contridiction. Therefore, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Therefore, n has a positive divisior not exceeding $\sqrt{n}$. This divisor is either prime, or by the fundamental Theorem of Arithmetic has a prime divisor.

Trial Divison Example

Use trial division to determine if 539 is prime

$\sqrt{539} \approx 23.216....$ $\qquad < 23.216$

$\cancel{2}, \cancel{3}, \cancel{5}, 7, 11, 13, 17, 19, 23$

$539 \div \underline{7} = 77$

Composite Number since we found a Value

The Sieve of Erastosthenes

A method for <u>finding all primes</u> <u>not exceeding</u> <u>a certain integer</u> by <u>deleting multiples of 2</u> (except 2), then multiples of 3 (except 3), then 5 (except 5), etc. up to the largest prime, a, such that $a \leq \sqrt{n}$.

$a \leq \sqrt{25} = 5$

~ looking for all prime #'s up to and including 5

Example: Find all primes not exceeding 25.

not prime or composite ~ $\cancel{1}$ 2 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$

Then cross-out all multiplys of 2, 3, 5

13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$

- method leaves all the primes left over

More Fun Facts about Primes

There are an inifinite number of primes.

Euclid proved this in a simple proof thought to be the most beautiful elegant proof in mathematics

Mersene primes are primes in the form $2^p - 1$

The Prime Number Theorem tells us that the ratio of the number of prime nt exceeding x can be approximated by $\frac{x}{\ln x}$

Greatest Common Divisors and Least Common Multiples

GCD - Greatest Common Divisor

The GCD of a and b, where $a, b \in \mathbb{Z}$ and $a, b \neq 0$ is the largest integer d such that $d \mid a$, $d \mid b$ and $\forall e \neq d$, if $e \mid a$ and $e \mid b$, then $e < d$.

Find gcd(16, 32)

16 = 1, 2, 4, 8, 16

32 = 1, 2, 4, 8, 16, 32

$16 = 2^4$ $\quad 2^4$

$32 = 2^5$ $\quad 2^4 \cdot 2$

$GCD = 2^4 = 16$

Find the following gcd's:

gcd(12, 30)

$12 = 2^2 \cdot 3$

$30 = 2 \cdot 3 \cdot 5$

How much they occur in both

$gcd = 2^1 \cdot 3^1 \cdot 5^0 = 6$

gcd(17, 55)

17 = 17

$55 = 5 \cdot 11$

gcd = 1

* Relatively prime

~ don't have any factors in common

gcd(14,237, 21,931) → Euclid Alg.

LCM - Least Common Multiple

The LCM of a and b, where $a, b \in \mathbb{Z}$ and $a, b \neq 0$ is smallest integer m such that $a|m$ and $b|m$, and if $a|n$ and $b|n$, then $m < n$.

Find $\text{lcm}(8,14)$

$8 = 8, 16, 24, 32, 40, 48, 56$

$14 = 14, 28, 42, 56$

$8 = 2^3$

$14 = 2 \cdot 7$

$\text{lcm}(8,14) = 2^3 \cdot 7 = 56$

Find the following lcm's:

$\text{lcm}(5, 25) = 25$

most time each occur

$\text{lcm}(2^2 \cdot 3 \cdot 5,\ 2 \cdot 3^2 \cdot 5^2) = 2^2 \cdot 3^2 \cdot 5^2 = 900$

Another LCM Method

$$LCM(m,n) = \frac{m \cdot n}{gcd(m,n)}$$

Find $lcm(8, 14) = 56$

$8 = 2^3$

$14 = 2 \cdot 7$

$$lcm(8,14) = \frac{8(14)}{2} = \frac{112}{2} = 56$$

The Euclidean Algorithm

Find gcd(544, 212)

Same gcd

$544 = \underline{212}(2) + \underline{120}$ $\quad\quad$ gcd(212, 120)

$212 = 120(1) + \underline{92}$ $\quad\quad$ gcd(120, 92)

$120 = 92(1) + 28$ $\quad\quad$ gcd(92, 28)

$92 = 28(3) + 8$ $\quad\quad$ gcd(28, 8)

$28 = 8(3) + \boxed{4}$ $\quad\quad$ gcd(8, 4) = 4

$8 = 4(2) + \boxed{0}$

When we get to a remainder of 0, were done!

What is the gcd? ~ the last remainder

Euclidean Algorithm

Let $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$. Then

$$\gcd(\underline{a, b}) = \gcd(\underline{q, r})$$

If we can show the common divisors of a,b equal the common divisors of q,r then we will have shown that gcd(a,b) = gcd(q,r).

Section 4.1

If $d|a$ and $d|b$, then $d|(a-qb)$. Therefore, a common divisor of a and b is a common divisor of q,r, as $r = a - bq$. Suppose $d|b$ and $d|r$. Then $d|bq + r = a$.

Therefore any divisor of a,b is a common divisor of q,r

Find gcd(414, 662)

$$662 = 414(\ \ ) + r$$

$$662 = 414(1) + 248$$

$$414 = 248(1) + 166$$

$$248 = 166(1) + 82$$

$$166 = 82(2) + 2$$

$$82 = 2(41) + 0$$

$$\boxed{\gcd(414, 662) = 2}$$

The Greatest Common Divisor as Linear Combinations

Write gcd(662, 414) as a linear combination gcd(662, 414) = 662s + 414t

$$662 = 414(1) + 248 \rightarrow 248 = (1(662) - 1(414))$$

$$414 = 248(1) + 166 \rightarrow 166 = (1(414) - 1(248))$$

$$248 = 166(1) + 82 \rightarrow 82 = (1(248) - 1(166))$$

$$166 = 82(2) + 2 \rightarrow 2 = 1(166) - 2(82)$$

$$\cancel{82 = 2(41) + 0}$$

rewrite in terms of the remainder.

Write this in Linear Combination Format

$$2 = 1(166) - 2(82) = 1(166) - 2(1(248) - 1(166)) = -2(248) + 3(166)$$

Then simplification

$$-2(248) + 3(1(414) - 1(248)) = 3(414) - 5(248)$$

$$3(414) - 5(1(662) - 1(414)) = \boxed{-5(662) + 8(414)}$$

Write $\gcd(252, 198)$ as a linear combination of 252 and 198.

$$252 = 198(1) + 54 \rightarrow 54 = 1(252) - 1(198)$$

$$198 = 54(3) + 36 \rightarrow 36 = 1(198) - 3(54)$$

$$54 = 36(1) + 18 \rightarrow 18 = 1(54) - 1(36)$$

Ignore $\cancel{36 = 18(2) + 0}$

$$18 = 1(54) - 1\big(1(198) - 3(54)\big) = -1(198) + 4(54)$$

$$-1(198) + 4\big(1(252) - 1(198)\big) = \boxed{4(252) + -5(198)}$$

Bezouts Theorem

$$\gcd(252, 198) = 4\,(252) + -5\,(198)$$

These are called Be'zout Coefficient

If $a, b \in \mathbb{Z}^+$, then $\exists\, s, t \in \mathbb{Z}$ such that

$$\gcd(a,b) = sa + tb.$$

4.4 Solving Linear Congruences using Inverse

Linear Congruences

multiplying by the inverse $\rightarrow$ $\frac{1}{2} \cdot 2x = 4 \cdot \frac{1}{2}$

$\boxed{x = 2}$

A linear congruences in the form $ax \equiv b \pmod{m}$ where $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$ and x is the variable.

To solve a linear congruence, we need to find all x that satisfy the congruence. To eliminate a, we use the inverse of $a \pmod{m}$

$$\bar{a} \cdot a x = \bar{a} \cdot b \pmod{m}$$

$$x = \bar{a} \cdot b \pmod{m}$$

Inverse of $a \pmod{m}$

If a and m are relatively prime integers and $m > 1$, then a unique inverse of $a \pmod{m}$ exists and is denoted $\bar{a}$ with $\bar{a} < m$ and $\boxed{a \cdot \bar{a} \equiv 1 \pmod{m}}$

Ex. Find $\bar{a}$ when $a = 3$ and $m = 5$. (easy with small #'s)

$$3(2) = \underline{5(1)} + 1 \equiv 1 \pmod{5}$$

Congruent

inverse

$\bar{a} = 2$

Euclidean Algorithm

Using EA and linear Combinations

Finding the solutions of the linear congruence $13x \equiv 6 \pmod{37}$

$$\underset{a}{13}\,\underset{x}{x} \equiv 6 \pmod{37}$$

① $\gcd(37, 13) = 1$ ← have to show they're equal to one, so that they're relatively Prime!

$37 = 13(2) + 11 \longrightarrow 11 = 1(37) - 2(13)$

$13 = 11(1) + 2 \qquad 2 = 1(13) - 1(11)$

$11 = 2(5) + \boxed{1} \longrightarrow 1 = 1(11) - 5(2)$

$2 = 1(2) + 0$

Verified gcd is 1.

② Linear Combination

$1 = 1(11) - 5(1(13) - 1(11)) = -5(13) + 6(11)$

$= -5(13) + 6(1(37) - 2(13)) = \boxed{6(37) + -17(13)}$

③ $1 = \boxed{6(37)} + -17(13)$

$1 \equiv -17(13) \pmod{37}$

$\boxed{\bar{a} = -17}$

④ $-17(13x) \equiv -17 \cdot 6 \pmod{37}$

$x \equiv -102 \pmod{37}$

⑤ Solutions:

$-102 \xrightarrow{+37} -65 \xrightarrow{+37} -28,\ 9,\ 46\ldots$

$x \equiv 9 \pmod{37}$