

Number Theory Chapter 4.1-4.3

Section 4.1

Divisibility

Division

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

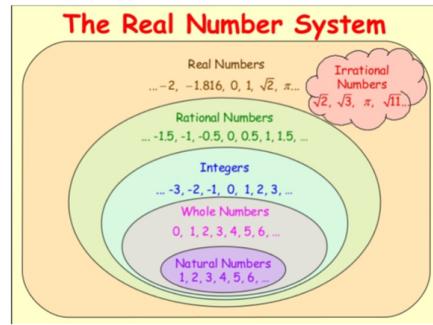
\downarrow \downarrow

a divides b Some Value of c

$$3|15 \quad 3c = 15 \quad c = 5 \in \mathbb{Z}^+$$

\downarrow

Since that # goes in evenly.



Another Example: $3|22$ $3c = 22$
 $c = \frac{22}{3} \notin \mathbb{Z}^+$
 \uparrow Not an Integer

DEFINITION 1

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b , and that b is a *multiple* of a . The notation $a | b$ denotes that a divides b . We write $a \nmid b$ when a does not divide b .

Properties of Divisibility

$$a|b \quad ac = b$$

$$at = c$$

a) if $a|b$ and $a|c$, then $a|(b+c)$

\nwarrow "a divides into both"

Example: $3|15$ $3|6$ $3|(15+6)$ or $3|21 \checkmark$ shown it's true

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

$$\begin{aligned} b &= as \quad \text{and} \quad c = at \quad \text{from defini. of divisibility.} \\ \downarrow & \quad \downarrow \\ b+c &= \underline{\underline{as + at}} = a(s+t) \\ &\quad \quad \quad \text{Equivalent} \end{aligned}$$

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

$$\therefore a|(b+c) \quad \leftarrow \text{Proof}$$

COROLLARY 1

If a, b , and c are integers, where $a \neq 0$, such that $a | b$ and $a | c$, then $a | mb + nc$ whenever m and n are integers.

Properties of Divisibility

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

$$\begin{array}{r} 3|15 \\ 15=2 \end{array} \quad \begin{array}{r} 3|30 \\ 15=3 \end{array} \quad \begin{array}{r} 3|45 \\ 15=4 \end{array} \quad \begin{array}{r} 3|60 \\ 15=5 \end{array}$$

~ if $b=15$, $c=\mathbb{Z}$

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

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

$$bc = a(tc) \quad \leftarrow \begin{array}{l} \text{Regroup} \\ \text{Associated Property} \end{array}$$

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

c.) If $a|b$ and $b|c$, then $a|c$

$$3|6 \text{ and } 6|18, \text{ then } 3|18 \quad \checkmark$$

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:

$$\downarrow \quad \text{Then } c = (at)s, \text{ or } c = a(ts)$$

$\therefore a|c$

Division Algorithm:

THEOREM 2

THE DIVISION ALGORITHM Let a be an integer and d a positive integer. Then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.

$d | a \quad a = dq$
 Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. $\exists! q, r : a = dq + r$ remainder
 then exist q and r divisor quotient

Example:

$$4 | 21 \quad 21 = 4q + r$$

$$\begin{array}{r} 5 \\ 4 \overline{)21} \\ -20 \\ \hline 1 \end{array} \quad 21 = 4(5) + 1 \quad 0 \leq r < d \quad \text{Important}$$

Example:

Give the quotient and remainder for each.

a) $7 | 18 \quad a = dq + r$
 $d \wedge \quad 18 = 7(2) + 4 \quad 0 \leq r < 7$

Notation: quotient: $q = a \text{ div } d$ remainder: $r = a \bmod d$

$$2 = 18 \text{ div } 7 \quad 4 = 18 \bmod 7$$

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

b) $10 | -112 \quad -112 = 10(-11) + -2 \quad \text{---} \rightarrow 0 \leq r < 10 \quad \text{negative two is not b/w 0 and 10?}$
 $-112 = 10(-12) + 8$

Correct Way to Write

quotient: $-12 = -112 \text{ div } 10$ remainder: $8 = -112 \bmod 10$

c) $14 | 0 \quad 0 = 14(0) + 0$

$a = dq + r$

quotient:

$$0 = 0 \text{ div } 14$$

remainder:

$$0 = 0 \bmod 14$$

Modular Arithmetic

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



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

Asked: Is 2 congruent to 6 in mod 4?

Both are two

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

Can do it w/o numberline by seeing if the difference b/w the two values is divisible by 4

$$\begin{array}{l} 2 \equiv 6 \pmod{4} \\ \hline 4 \mid (2-6) \\ 4 \mid (-4) \quad \checkmark \end{array}$$

yes is congruent

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

$$6 \mid (24-14)$$

$$6 \mid 10 \quad \times$$

Not Equivalent

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

if the remainders 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 $24 \equiv 14 \pmod{6}$

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

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

$$0 = 24 \bmod 6$$

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

$$2 = 14 \bmod 6$$

Theorem:

$$a \equiv b \pmod{m}$$

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

Assuming \rightarrow 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 $a \equiv b \pmod{m}$.

Theorem

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 $ac \equiv bd \pmod{m}$.

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 $l \in \mathbb{Z}$.

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

$$a+c = (b+d) + m(k+l) \text{ so } (a+c) - (b+d) = m(k+l) \text{ so }$$

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

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

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

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 $a \cdot c \equiv b \cdot d \pmod{m}$.

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

$$\begin{array}{l} 7+11 \pmod{5} \text{ and } 7 \cdot 11 \pmod{5} \\ 7+11 = 18 \equiv 3 \pmod{5} \\ \text{Congruent to} \end{array} \quad \left\{ \begin{array}{l} 7 \cdot 11 = 77 \equiv 2 \pmod{5} \\ 7 \cdot 11 = 2 \cdot 1 = 2 \pmod{5} \end{array} \right.$$

$$7 \equiv 2 \pmod{5}$$

$$11 \equiv 1 \pmod{5}$$

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

Arithmetic modulo m

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

Addition (denoted $+_m$): $a +_m b = (a+b) \text{ mod } m$

Multiplication (denoted \cdot_m): $a \cdot_m b = (a \cdot b) \text{ mod } m$

Example:

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

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

2 goes into 9 evenly

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

Decimal Expansions from Binary, Octal and Hexadecimal

Section 4.2

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

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

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

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 $\frac{10}{10^3} \cdot \frac{456}{10^0}$ base 10.

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

Binary to Decimal Expansion

What is the decimal expansion that has $(10111101)_2$ as its binary expansion?

$$\begin{aligned}
 (10111101)_2 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\
 &= 1 \cdot 128 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 1 \\
 &= 128 + 32 + 16 + 8 + 4 + 1 \\
 &= 189
 \end{aligned}$$

Octal to Decimal Expansion

What is the decimal expansion of the number with an octal expansion of $(4072)_8$?

$$\begin{aligned}
 (4072)_8 &= 4 \cdot 8^3 + 0 \cdot 8^2 + 7 \cdot 8^1 + 2 \\
 &= 4 \cdot 512 + 0 \cdot 64 + 7 \cdot 8 + 2 \\
 &= 2048 + 0 + 56 + 2 \\
 &= (2106)_{10} \quad \text{or } 2106
 \end{aligned}$$

Hexadecimal to decimal Expansion

What is the decimal expansion of the number with a hexadecimal expansion of $(2AE0B)_{16}$?

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

Hexadecimal
Expansion

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

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

$$= 131672 + 40960 + 3584 + 0 + 11$$

$$= (175627)_{10} \quad \text{or } 175627$$

Binary, Octal and Hexadecimal Expansion from Decimal

Section 4.2

Finding an Octal Expansion

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

interested in the remainder

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

$$\begin{aligned}
 12543 &= 8 \underline{1567} + 7 \cdot 8^0 \\
 \text{quotient} \quad | & \\
 1567 &= 8(195) + 7 \cdot 8^1 \\
 | & \\
 195 &= 8(24) + 3 \cdot 8^2 \\
 | & \\
 24 &= 8(3) + 0 \cdot 8^3 \\
 | & \\
 3 &= \underline{8(0)} + 3 \cdot 8^4 \\
 | & \\
 \text{Done. Since quotient is } 0 &
 \end{aligned}$$

$(30377)_8$

Finding a hexadecimal Expansion

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

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

$$\begin{aligned}
 (19472)_{10} &= 16 \cdot 1217 + 0 \\
 | & \\
 1217 &= 16 \cdot \underline{76} + 1 \\
 | & \\
 76 &= 16 \cdot \underline{4} + 12 \\
 | & \\
 4 &= 16 \cdot \underline{0} + 4
 \end{aligned}$$

$(4C10)_{16}$

Will replace with C from above

4 12 1 0

Finding a Binary Expansion:

Find the binary expansion of 141 (2)

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

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

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

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

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

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

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

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

Groups of 4

$$(1000\ 101)_2$$

Conversions between Binary, Octal and Hexadecimal Expressions

Conversions between binary, Octal and hexadecimal

Find the octal and hexadecimal expansions of:

$$8 = 2^3 \quad 16 = 2^4$$

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

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

Octal $8 = 2^3$
 $\underline{\quad \quad \quad}$
 $\underline{\quad \quad \quad}$

$$\underline{00}\ 11\ \underline{1110}\ 1011$$

Hexadecimal

$$\underline{00}\ 11\ \underline{1110}\ 1011$$

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

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

$$\begin{array}{ccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ \hline 4 & 3 & 1 & 4 & 1 & 1 & & & & & \end{array}$$

1 7 5 3

$$\boxed{(1753)_8}$$

$$\underline{00}\ 11\ \underline{1110}\ 1011$$

$$\begin{array}{ccc} 3 & 14 & 11 \\ E & B & \end{array}$$

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

$$\begin{array}{l} A = 10 \\ B = 11 \\ C = 12 \\ D = 13 \\ E = 14 \\ F = 15 \end{array}$$

Find the binary expansion of $(37274)_8$

for octal:

$$\begin{array}{c} 4 \\ \hline 2^3 \\ 2^2 \\ 2^1 \\ 2^0 \end{array}$$

$$\begin{array}{ccccc} 3 & | & 7 & | & 2 & | & 7 & | & 4 \\ \hline 0 & 1 & 1 & | & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{array}$$

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 $(37274)_8$

$$\begin{array}{r} 8 \quad 4 \quad 2 \quad 1 \\ \hline 2^3 \quad 2^2 \quad 2^1 \quad 2^0 \end{array}$$

$$0011 \quad 1110 \quad 1011 \quad 1100$$

$$3 \quad 14 \quad 11 \quad 12$$

$$(3EBE)_{16}$$

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

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

Hexadecimal to binary

$$\begin{array}{r} 8 \quad 4 \quad 2 \quad 1 \\ \hline 2^3 \quad 2^2 \quad 2^1 \quad 2^0 \end{array}$$

$$\begin{array}{c|c|c} A^{(10)} & 8 & D^{(13)} \\ \hline 1010 & 1000 & 1101 \end{array}$$

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

$$(1010\ 1000\ 1101)_2$$

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

$$\begin{array}{r} 4 \quad 2 \quad 1 \\ \hline 2^2 \quad 2^1 \quad 2^0 \end{array}$$

$$\begin{array}{cccc} 101 & 010 & 001 & 101 \\ \hline 5 & 2 & 1 & 5 \end{array}$$

$$(5215)_8$$

Operation on base 'n' numbers

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

$$\begin{array}{r}
 & 1 & 1 \\
 + & 1 & 0 & 1 & 1 \\
 \hline
 & 1 & 1 & 1 & 0
 \end{array}$$

$$\begin{array}{r}
 & 1 & 0 & 1 & 1 \\
 \times & 0 & 1 & 1 \\
 \hline
 & 1 & 0 & 1 & 1 & 0 \\
 \hline
 0 & 0 & 0 & 0 & 0 & 0 \\
 \hline
 1 & 0 & 0 & 0 & 0 & 1
 \end{array}$$

The Sum is:

$$(1110)_2$$

In Binary:

$$\begin{array}{r}
 2 = \underline{1} \quad \underline{0} \\
 3 = \underline{1} \quad \underline{1}
 \end{array}$$

Should be grouping in fours
Put zeros in front if needed

$$(0010\ 0001)_2$$

Algorithms for Integer Operations

Prime Numbers and their Properties

Section 4.3

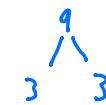
Prime and Composite Numbers

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 $a | p$ and $1 < a < p$.

$$9 = 3 \cdot 3 \quad \text{Composite}$$

$$23 = 23 \cdot 1 \quad \text{Prime}$$

$$51 = 17 \cdot 3 \quad \text{Composite}$$



Some primes: 2, 3, 5, 7, 11, 13

$$2 \cdot 1 = 2$$

$$3 \cdot 1 = 3$$

$$\times 4 \cdot 1 = 4 \text{ and } 2 \cdot 2 = 4$$

$$5 \cdot 1 = 5$$

$$\times 6 \cdot 1 = 6 \text{ and } 2 \cdot 3 = 6$$

$$7 \cdot 1 = 7$$

$$\times 8 \cdot 1 = 8 \text{ and } 4 \cdot 2 = 8$$

$$\times 9 \cdot 1 = 9 \text{ and } 3 \cdot 3 = 9$$

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 contradiction. Therefore, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Therefore, n has a positive divisor not exceeding \sqrt{n} . This divisor is either prime, or by the fundamental Theorem of Arithmetic has a prime divisor.

Trial Division Example

Use trial division to determine if 539 is prime.

$$\sqrt{539} \approx 23.216\dots < 23.216$$

$$2, 3, 5, 7, 11, 13, 17, 19, 23$$

$$539 \div 7 = 77$$

Composite Number Since we found a value

The Sieve of Eratosthenes

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

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

Example: Find all primes not exceeding 25.

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



- Method leaves all the primes left over

More Fun Facts about Primes

There are an infinite number of primes.

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

Mersenne primes are prime in the form $2^p - 1$

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

Greatest Common Divisors and Least Common MultiplesSection 4.3GCD - 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 $d|a$, $d|b$ and $\forall c \neq d$, if $c|a$ and $c|b$, then $c < d$.

Find $\gcd(16, 32)$

$$16 = 1, 2, 4, 8, \textcolor{orange}{16}$$

$$32 = 1, 2, 4, 8, \textcolor{orange}{16}, 32$$

$$16 = 2^4$$

$$32 = 2^5$$

$$\text{GCD} = 2^4 = 16$$

Find the following gcd's:

$$\gcd(12, 30)$$

$$12 = 2^2 \cdot 3$$

$$30 = 2 \cdot 3 \cdot 5$$

↓ ↓ ↓
How many 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

$$\gcd(14, 237, 21, 931) \rightarrow \text{Euclid Alg.}$$

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 $m \leq n$.

$$\text{Find } \text{lcm}(8, 14) \quad 8 = 8, 16, 24, 32, 40, 48, 56$$

$$14 = 14, 28, 42, 56$$

$$8 = 2^3$$

$$14 = 2 \cdot 7$$

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

Find the following lcm's:

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

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

Another LCM Method

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

Find $\text{lcm}(8, 14) = 56$

$8 = 2^3$
 $14 = 2 \cdot 7$

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

The Euclidean Algorithm

Section 4.3

Find $\gcd(544, 212)$

$$\begin{array}{rcl}
 544 & = & 212(2) + 120 \\
 212 & = & 120(1) + 92 \\
 120 & = & 92(1) + 28 \\
 92 & = & 28(3) + 8 \\
 28 & = & 8(3) + 4 \\
 8 & = & 4(2) + 0
 \end{array}$$

Since \gcd
 \downarrow
 $\gcd(212, 120)$
 \downarrow
 $\gcd(120, 92)$
 \downarrow
 $\gcd(92, 28)$
 \downarrow
 $\gcd(28, 8)$
 \downarrow
 $\gcd(8, 4) = 4$

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

What is the \gcd ?
 ~ the last remainder

Euclidean Algorithm

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

$$\gcd(a, b) = \gcd(q, r)$$

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

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 $r = a - qb$. 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 $\gcd(414, 662)$

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

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

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

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

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

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

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

The Greatest Common Divisor as Linear Combinations

Write $\gcd(662, 414)$ as a linear combination $\gcd(662, 414) = \underline{662s + 414t}$

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

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

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

$$166 = 82(2) + 0 \rightarrow 0 = 1(166) - 2(82)$$

$$\underline{82} = 2(414) + 0$$

rewrite in terms of
the remainder.

Write this in Linear Combination Format

$$2 \cdot 1(166) - 2(82) = 1(\underline{166}) - 2(1(248) - 1(166)) = -2(248) + 3(166)$$

$$\underline{-2(248)} + 3(1(414) - 1(248)) = 3(414) - 5(248)$$

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

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

$$36 = 18(2) + 0$$

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

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

Bézout's Theorem

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

These are called Bézout Coefficients

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

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

Solving Linear Congruences Using the Inverse

Section 4.4

Linear Congruences

A linear congruence is 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 $a \pmod{m}$.

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 $\bar{a} \leq m$ and $a \cdot \bar{a} \equiv 1 \pmod{m}$.

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

Using EA and linear Combinations

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