Number Theory Chapter 4.1-4.3

Section 4.1

Divisibility

Divison

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

Integer

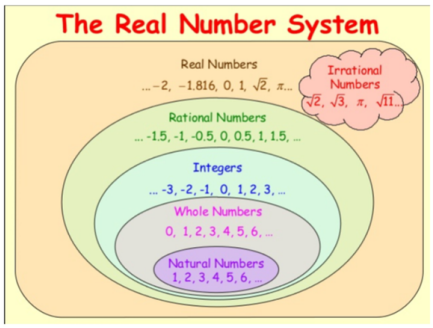
$a|b$: a divides b

$\exists c : ac = b$: 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

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 $a \mid b$ 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 $c|b$ and $a|c$, then $a|(b+c)$

"a divides into both"

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

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

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

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

Equivalent

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

$\therefore a|(b+c)$ ← Proof

COROLLARY 1 If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Properties of Divisibility

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

$3|15$ $3|30$ $3|45$ $3|60$

$15=2$ $15=3$ $15=4$ ~ 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

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

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, quotient, divisor

there exists a q and r

Example:

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

$4\overline{)21}$ 5 R 1, -20, 1

$21 = 4(5) + 1$ ← $0 \leq r < d$ Important

Examples:

Give the quotient and remainder for each.

a) $7|18$ (d a)

$a = dq + r$

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

Notation:

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

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

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

b) $10|-112$ $\quad -112 = 10(-11) + -2$ ~~→~~ $0 \leq r < 10$ · negative two is not b/w 0 and 10!

$-112 = 10(-12) + 8$

$a = dq + r$

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

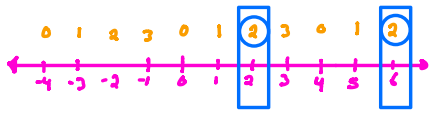
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff $m \mid a-b$.

Remainders
$\frac{-4}{4}$ → 0
$\frac{-3}{4}$ → 1
$\frac{-2}{4}$ → 2
$\frac{-1}{4}$ → 3

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

possible remainders

pattern



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

Question 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 number line by seeing if the difference b/w the two values is divisible by 4

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

$4 \mid (-4)$ ✓ yes is congruent

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

$6 \mid (24-14)$

$6 \mid 10$ X

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 $2 \equiv 6 \pmod{4}$

$2 \bmod 4 = 6 \bmod 4$

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

$2 = 2 \bmod 4$

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

$2 = 6 \bmod 4$

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

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

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

$0 = 24 \bmod 6$

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

$2 = 14 \bmod 6$

Theorem:

$a \equiv b \pmod m$

P — The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$ — 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 $a \equiv b \pmod m$.

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 $l \in \mathbb{Z}$.

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

$a + c = (b+d) + m(k+l)$ 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 $7 \cdot 11 \pmod 5$

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

(18 congruent to 3)

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

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

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

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

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

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

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 $b = 2$
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 (base 10) of $10,456$ (10^4 10^3 10^2 10^1 10^0)

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

Binary to Decimal Expansion

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

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

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

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

$$= 189$$

Octal to Decimal Expansion

What is the decimal expansion of the number with an octal expansion of $(4072)_8$? (8^3 8^2 8^1 8^0)

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

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

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

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

Hexadecimal to decimal Expansion

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

4 3 2 1 0

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

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

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

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

Binary, Octal and Hexadecimal Expansion from Decimal

Section 4.2

Finding an Octal Expansion

Find the Octal (8) expansion of $(12543)_{10}$ mod 8

interested in the remainder

Division Algorithm: $a = dq + r$

To solve these problems

$12543 = 8(1567) + 7 \cdot 8^0$

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

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

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

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

quotient

Done Since quotient is 0

$(30377)_8$

Finding a hexadecimal Expansion

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

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

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

$1217 = 16 \cdot 76 + 1$

$76 = 16 \cdot 4 + 12$

$4 = 16 \cdot 0 + 4$

Will replace with C from chart

4 12 1 0

$(4C10)_{16}$

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

$(1000\ 101)_2$

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:

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

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

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

0011 1110 1011

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

001 111 101 011

(4 2 1 | 4 2 1)

1 7 5 3

$(1753)_8$

Hexadecimal

0011 1110 1011

~ Groups of fours

~ Add zeros to make group of 4

0011 1110 1011

3 14 11

E B

$(3EB)_{16}$

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:

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

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

$(0011\ 1100\ 1011\ 1100)_2$

Find the hexidecimal Expansion of $(37279)_8$

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

0011 1110 1011 1100

3 14 11 12

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

$(3EBC)_{16}$

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

2^1

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

A (10) | 8 | D (13)

1010 | 1000 | 1101

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

$(1010\ 1000\ 1101)_2$

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

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

101 010 001 101

5 2 1 5

$(5215)_8$

Operation on base 'n' numbers

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

```
  1 1
  1 0 1 1
+   0 1 1
-------
1 1 1 0
```

The Sum is:

$(1110)_2$

```
    1 0 1 1
  x   0 1 1
  -------
    1 0 1 1
  1 0 1 1 0
0 0 0 0 0 0
-----------
1 0 0 0 0 1
```

In Binary:

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

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

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

$(0010\ 0001)_2$

Algorithms for Integer Operations

Section 4.2

Pseudocode: Algorithm for Base b Expansions

```
procedure base b expansion(n, b : positive integers, b > 1)
q := n
k := 0
while q ≠ 0
    a_k := q mod b
    q := q div b
    k := k + 1
return (a_{k-1}, ..., a_1, a_0) {(a_{k-1}, ..., 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

$a_0 + b_0 = c_0 \cdot 2 + s_0$ $\quad s_0$ = rightmost bit $\quad c_0$ = 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 until you've added the last bits. At the last stage, add a_{n-1}, b_{n-1} and c_{n-2} to obtain $c_{n-1} \cdot 2 + s_{n-1}$

$$a + b = (s_n s_{n-1} s_{n-2} s_{n-3} \cdots s_1 s_0)_2$$

Addition 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, $s = a + b = (1\,1001)_2$

Pseudocode: Addition Algorithm

```
procedure add (a, b: positive integers)
{the binary expansions of a and b are (a_{n-1} a_{n-2} ... a_1 a_0)_2 and (b_{n-1} b_{n-2} ... b_1 b_0)_2}
c := 0
for j := 0 to n-1
    d := ⌊(a_j + b_j + c)/2⌋
    s_j := a_j + b_j + c - 2d
    c := d
s_n := c
return (s_0 s_1 s_2 ... s_n) {the binary expansion of the sum (s_n s_{n-1} ... s_1 s_0)_2}
```

Multiplication Algorithm Example

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

Pseudocode - Multiplication Algorithm

```
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 {p is the value of ab}
```

Pseudocode - Computing div and mod

```
procedure division algorithm (a: integer, d: positive integer)
  q := 0
  r := |a|
while r ≥ d
  r := r - d
  q := q + 1
if a < 0 and r > 0 then
  r := d - r
  q := -(q + 1)
```

Modular Exponentiation Algorithm

To find $b^n \bmod m$ for large values of b, n and m:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0$$

$$b^n = b^{(a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0)}$$

$$b^n = b^{a_{k-1}b^{k-1}} \cdot b^{a_{k-2}b^{k-2}} \cdot \ldots \cdot b^{ab} \cdot b^{a_0}$$

Compute $3^{11} \pmod{10}$

Pseudocode - Modular Exponentiation

procedure modular exponentiation (b: integer, $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$
m: positive integers)

- $x := 1$
- power := b mod m

for $i := 0$ to $k-1$

  if $a_i = 1$ then $x := (x \cdot power) \bmod m$

  $power := (power \cdot power) \bmod m$

return x {x equals $b^n \bmod m$}

Find $3^6 \bmod 5$

x → 1

power → 3 mod 5 = 3

Begin i = 0

Since $a_0 = 0$ nothing is done

power → (3·3) mod 5 = 4

Next let i = 1

Since $a_1 = 1$ x → (1·4) mod 5 = 4

power → (4·4) mod 5 = 1

Next let i = 2

Since $a_1 = 1$ x → (4·1) mod 5 = 4

power → (1·1) mod 6 = 1

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 $a \mid p$ and $1 < a < p$.

$9 = 3 \cdot 3$ Composite

$23 = 23 \cdot 1$ Prime

$51 = 17 \cdot 3$ Composite

Distant Division

product of primes

Some primes: 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~

$2 \cdot 1 = 2$

$3 \cdot 1 = 3$

× $4 \cdot 1 = 4$ 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 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.

$\sqrt{539} \approx 23.216\ldots$ < 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 Erastosthenes

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 $a \leq \sqrt{n}$.

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

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

Example: Find all primes not exceeding 25.

not prime or Composite: ~~1~~ (2) (3) ~~4~~ (5) ~~6~~ (7) ~~8~~ ~~9~~ ~~10~~ (11) ~~12~~

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

(13) ~~14~~ ~~15~~ ~~16~~ (17) ~~18~~ (19) ~~20~~ ~~21~~ ~~22~~ (23) ~~24~~ ~~25~~

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

The Prime Number Theorem tells us that the ratio of the number of primes not exceeding x can be approximated by $\frac{x}{\ln x}$

Greatest Common Divisors and Least Common Multiples

Section 4.3

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 $d|a$, $d|b$ and $\forall e \neq d$, if $e|a$ and $e|b$, then $e < d$.

Find gcd(16,32)

$16 = 1, 2, 4, 8, 16$

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

$16 = 2^4$

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

$GCD = 2^4 = 16$

Find the following gcd's:

gcd(12,30)

$12 = 2^2 \cdot 3$

$30 = 2 \cdot 3 \cdot 5$

How must 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 $lcm(8,14) = 56$

$8 = 2^3$

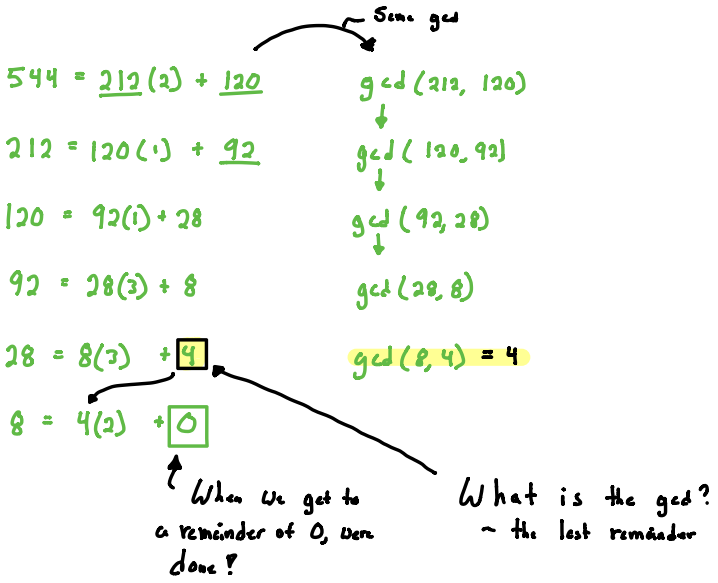
$14 = 2 \cdot 7$

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

The Euclidean Algorithm

Section 4.3

Find gcd(544, 212)



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 $d|(a-qb)$. (→ Section 4.1) 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 $\gcd(662, 414) = 662s + 414t$

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

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

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

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

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

rewrite in terms of the remainder.

Write this in Linear Combination Format

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

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

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

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

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

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

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

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

Solving Linear Congruences Using the Inverse

Section 4.4

-HW # 8 Problems

Linear Congruences

multiplies by the inverse → $\frac{1}{2} \cdot 2x = 4 \cdot \frac{1}{2}$

$\boxed{x = 2}$

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 $a \pmod{m}$

$$\bar{a} \cdot ax \equiv \bar{a} \cdot b \pmod{m}$$

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

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)

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

↑ Congruent

↙ inverse

$\bar{a} = 2$

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!

$37 = 13(2) + 11 \rightarrow 11 = 1(37) - 2(13)$
$13 = 11(1) + 2 \quad\quad 2 = 1(13) - 1(11)$
$11 = 2(5) + \boxed{1} \rightarrow 1 = 1(11) - 5(2)$
$2 = 1(2) + 0$

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

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

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

④ $-17(13x) = -17 \cdot 6 \pmod{37}$

$x = -102 \pmod{37}$

⑤ Solutions:

$+37 \quad +37$

$-102, -65, -28, 9, 46\ldots$

$x = 9 \pmod{37}$