Foundations of Discrete Mathematics

Chapter 4

By Dr. Dalia M. Gil, Ph.D.

The Binary Relation $\leq$

The binary relation $\leq$ is

- Reflexive: $a \leq a$ for all $a \in R$,
- Antisymmetric: if $a \leq b$ and $b \leq a$, $b \in R$, then $a = b$, and
- Transitive: if $a \leq b$ and $b \leq c$,

  for $a, b, c \in R$, then $a \leq c$.

Properties of + and .

Let a, b, and c be real numbers.

1. (closure) $a + b$ and ab are both real numbers.
2. (commutative) $a + b = b + a$ and $ab = ba$.
3. (associativity) $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

Properties of + and .

4. (identities) a + 0 = a and a . 1 = a.

5. (distributivity) a(b + c) = ab + ac and (a + b)c = ac + bc.

6. (additive inverse) a + (-a) = 0.

7. (multiplicative inverse) a(1/a) = 1 if a ≠ 0.

Properties of + and .

8. $a \leq b$ implies $a + c \leq b + c$

9. $a \leq b$ and $c \geq 0$ implies $ac \leq bc$

10. $a \leq b$ and $c \leq 0$ implies $ac \geq bc$

Well-Ordering Principle

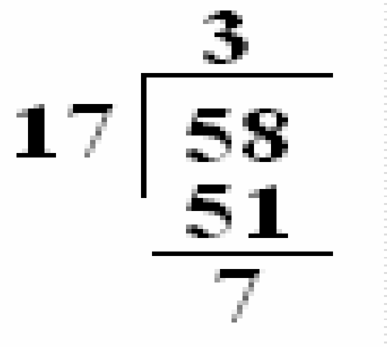
Any nonempty set of natural numbers has a smallest element.

4.1.3 Theorem

Given natural numbers a and b, there are unique nonnegative integers q and r, with $0 \leq r < b$, such that $a = qb + r$.

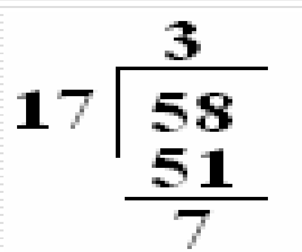
$a = 58$ $q = 3$

$b = 17$ $r = 7$



4.1.4 Definition

- If a and b are natural numbers and $a = qb + r$ for nonnegative integers q and r with $0 \le r < b$,
- q ← the quotient,
  r ← reminder when a is divided by b.



the quotient $q = 3$

the remainder $r = 7$

The Division Algorithm

- Let a, b $\in$ Z, b $\neq$ 0. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = qb + r$

a	b	q	r
-58	-17	4	7

$$q = \lceil -58/-17 \rceil = \lceil 3.41 \rceil = 4$$

a < 0 and b < 0

↑ q = The ceiling = 4

The Division Algorithm

- Let $a, b \in Z$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = qb + r$

a	b	q	r
-58	17	-4	10

$$q = \lfloor -58/17 \rfloor = \lfloor -3.41... \rfloor = -4$$

a < 0 and b > 0

↑ q = The floor = -4

The Division Algorithm

- Let a, b $\in$ Z, b $\neq$ 0. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that a = qb + r

a	b	q	r
58	-17	-3	7

$$q = \lfloor -58/17 \rfloor = \lceil -3.41 \rceil = -3$$

a > 0 and b < 0

↑ q = The ceiling = -3

The Division Algorithm

- Let a, b $\in$ Z, b $\neq$ 0. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = qb + r$

a	b	q	r
58	17	3	10

$$q = \lfloor -58/17 \rfloor = \lfloor 3.4 \rfloor = 3$$

a > 0 and b > 0

↑ q = The floor = 3

4.1.6 Proposition

Let a, b $\in$ Z, with $0 \leq r < |b|$ then

- $q = \lfloor a/b \rfloor$ if $b > 0$ ← the floor
- $q = \lceil a/b \rceil$ if $b < 0$ ← the ceiling

Let a = -1027 and b = 38

$$b > 0 \rightarrow \lfloor a/b \rfloor = \lfloor -1027/38 \rfloor$$

$$= \lfloor -27.026... \rfloor = -28 = q$$

$$a = bq + r \rightarrow r = a - bq$$

$$r = -1027 - (38)(-28)$$

$$= -1027 + 1064$$

$$= 37$$

Number System

- Number system is a convention for representing quantities.

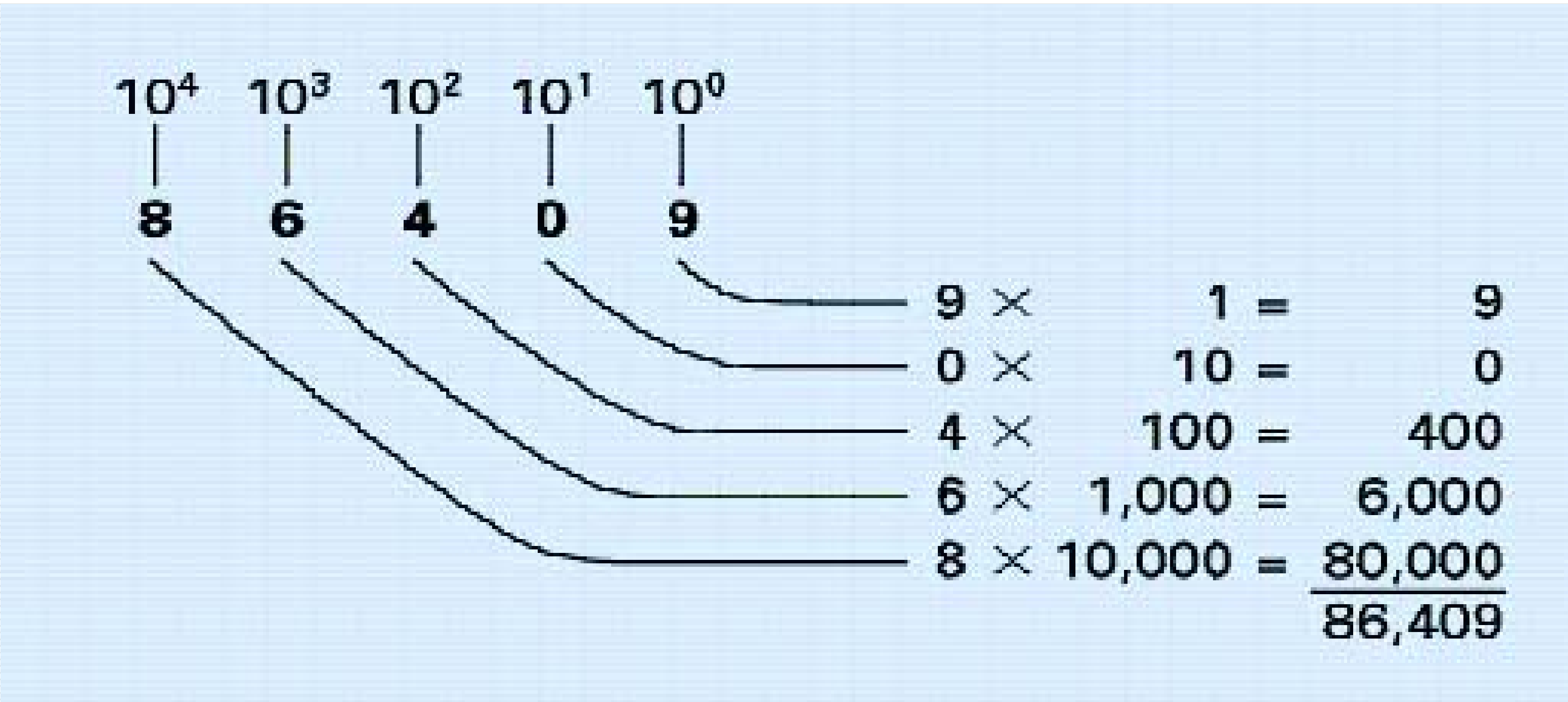
- There are several number systems.

Number Systems

- Decimal number System.
- Binary Number System.
- Octal Number System.
- Hexadecimal Number System.

Decimal Number System

The decimal number representation (10 digits from 0 to 9).



$(8x10^4) + (6x10^3) + (4x10^2) + (0x10^1) + (9x10^0) = 86{,}409$

(positional notation)

Decimal, Octal, Hexadecimal and Binary Equivalents

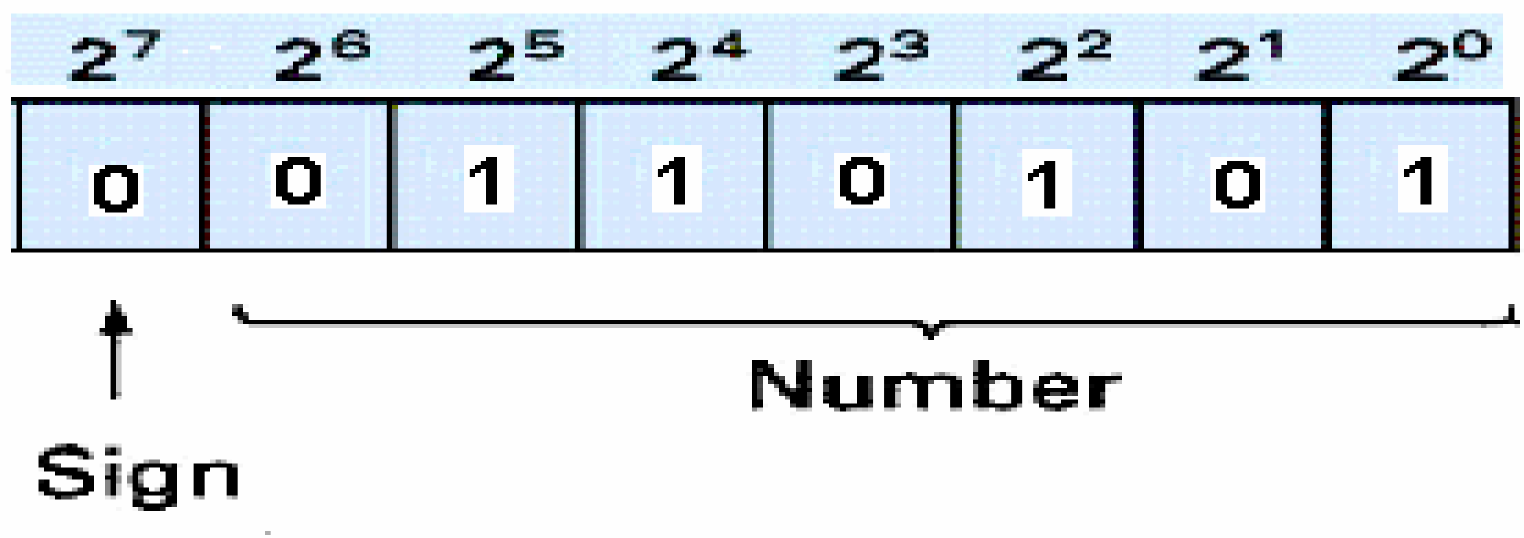
Decimal	Octal	Hexadecimal	Binary
0	0_8	0	0000
1	1	1	0001
2	2	2	0010
3	3	3	0011
4	4	4	0100
5	5	5	0101
6	6	6	0110
7	7	7	0111

Decimal, Octal, Hexadecimal and Binary Equivalents

Decimal	Octal	Hexadecimal	Binary
8	10	8	1000
9	11	9	1001
10	12	10 (A)	1010
11	13	11 (B)	1011
12	14	12 (C)	1100
13	15	13 (D)	1101
14	16	14 (E)	1110
15	17	15 (F)	1111

Binary Number System

10101101 ← binary number representation of the decimal 173



$(1 \times 2^7) + (1 \times 2^5) + (1 \times 2^2) + (1 \times 2^1) + (1 \times 2^0) = 173$

(positional notation)

Converting a Binary Number to Decimal

110101 ← binary number representation

$$1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$1 \times 32 + 1 \times 16 + 0 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1$$

$$32 + 16 + 0 + 4 + 0 + 1 = \underline{53}$$

Converting an Octal Number to Binary

Octal		Binary
0_8	→	000_2
1_8	→	001_2
2_8	→	010_2
3_8	→	011_2
4_8	→	100_2
5_8	→	101_2
6_8	→	110_2
7_8	→	111_2

$653_8 \rightarrow \underline{110}\ \underline{101}\ \underline{011}_2$

Octal		Binary
6_8	→	110_2
5_8	→	101_2
3_8	→	011_2

Hexadecimal Number System

Dec.	Hexadecimal		Binary
5	5_{16}	→	0101_2
6	6_{16}	→	0110_2
7	7_{16}	→	0111_2
8	8_{16}	→	1000_2
9	9_{16}	→	1001_2
10	10_{16} (A)	→	1010_2
11	11_{16}	→	1011_2
12	12_{16}	→	1100_2
13	13_{16} (D)	→	1101_2
14	14_{16}	→	1110_2
15	15_{16} (F)	→	1111_2

HexaDec		Binary
F	→	1111_2
A	→	1010_2
D	→	1101_2
5	→	0101_2

$FAD5_{16}$ =

$1111\ 1010\ 1101\ 0101_2$

Converting an Octal Number to Decimal

7614 ← octal number

$$7 \times 8^3 + 6 \times 8^2 + 1 \times 8^1 + 4 \times 8^0$$

$$7 \times 512 + 6 \times 64 + 1 \times 8 + 4 \times 1$$

3584+ 384 + 8 + 4 = <u>3980</u> ←decimal number

Converting Hexadecimal Number to Decimal

AD3B ← hexadecimal number

$$A \times 16^3 + D \times 16^2 + 3 \times 16^1 + B \times 16^0$$

$$10 \times 16^3 + 13 \times 16^2 + 3 \times 16^1 + 11 \times 16^0$$

$$10 \times 4096 + 13 \times 256 + 3 \times 16 + 11 \times 1$$

40960+ 3328 + 48 + 11 = <u>44347</u> ←decimal number

Converting Decimal Number to Binary

57 ← decimal number

1. **Write the positional values from right to left until we reach a column whose positional value is less than the decimal number.**

Position value as a power	2^5	2^4	2^3	2^2	2^1	2^0
Position value	32	16	8	4	2	1

32 < 57

Converting Decimal Number to Binary

Position value as a power 2^5 2^4 2^3 2^2 2^1 2^0

Position value 32 16 8 4 2 1

32 < 57

2. Divide this positional value 32 into 57. The result 1 is written in the column with value 32.

	32	16	8	4	2	1
Position value	**32**	**16**	**8**	**4**	**2**	**1**
	1					

Converting Decimal Number to Binary (cont.)

3. The remainder 25. This value is greater than the following position value 16.

4. Divide this positional value 16 into 25. The result 1 is written in the column with value 16.

Position value	**32**	**16**	**8**	**4**	**2**	**1**
	1	**1**				

Converting Decimal Number to Binary (cont.)

5. The remainder 9. This value is greater than the following position value 8.

6. Divide this positional value 8 into 9. The result 1 is written in the column with value 8.

Position value	**32**	**16**	**8**	**4**	**2**	**1**
	1	**1**	**1**			

Converting Decimal Number to Binary (cont.)

7. **The remainder 1. This value is equal to the position value 1.**

8. **The result 1 is written in the column with value 1, and zero in the columns 2 and 4**

Position value	**32**	**16**	**8**	**4**	**2**	**1**
	1	**1**	**1**	**0**	**0**	**1**

Converting Decimal Number to Binary

Verify the results **1 1 1 0 0 1** $_2$

$$1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$1 \times 32 + 1 \times 16 + 1 \times 8 + 0 \times 4 + 0 \times 2 + 1 \times 1$$

$$32 + 16 + 8 + 0 + 1 = 57$$

Converting Decimal Number to Octal

103 ← decimal number

1. Write the positional values from right to left until we reach a column whose positional value is less than the decimal number.

Position value as a power	8^3	8^2	8^1	8^0
Position value	**512**	**64**	**8**	**1**

$64 < 103$

Converting Decimal Number to Octal

Position value as a power	**8^3**	**8^2**	**8^1**	**8^0**
Position value	**512**	**64**	**8**	**1**

64 < 103

2. Divide this positional value 64 into 103. The result 1 is written in the column with value 64.

Position value	**64**	**8**	**1**
	1		

Converting Decimal Number to Octal (cont.)

3. **The remainder 39. This value is greater than the following position value 8.**

4. **Divide this positional value 8 into 39. The result 4 is written in the column with value 8.**

Position value	**64**	**8**	**1**
	1	**4**	

Converting Decimal Number to Octal (cont.)

5. The remainder 7. This value is greater than the following position value 1.

6. Divide this positional value 1 into 7. The result 7 is written in the column with value 1.

Position value	64	8	1
	1	4	7

Converting Decimal Number to Octal

Verify the results 147_8

$1 \times 8^2 + 4 \times 8^1 + 7 \times 8^0$

$1 \times 64 + 4 \times 8 + 7 \times 1$

$64 + 32 + 7 = 103$

Converting Decimal Number to Hexadecimal

375 ← decimal number

1. **Write the positional values from right to left until we reach a column whose positional value is less than the decimal number.**

Position value as a power	16^2	16^1	16^0
Position value	**256**	**16**	**1**

256 < 375

Converting Decimal Number to Hexadecimal

Position value as a power	16^2	16^1	16^0
Position value	**256**	**16**	**1**

256 < 375

2. Divide this positional value 256 into 375. The result 1 is written in the column with value 256.

Position value	**256**	**16**	**1**
	1		

Converting Decimal Number to Hexadecimal (cont.)

3. The remainder 119. This value is greater than the following position value 16.

4. Divide this positional value 16 into 119. The result 7 is written in the column with value 16.

Position value	256	16	1
	1	7	

Converting Decimal Number to Hexadecimal (cont.)

5. The remainder 7. This value is greater than the following position value 1.

6. Divide this positional value 1 into 7. The result 7 is written in the column with value 1.

Position value	256	16	1
	1	7	7

Converting Decimal Number to Hexadecimal

Verify the results $\mathbf{1\ 7\ 7}_{16}$

$$1 \times 16^2 + 7 \times 16^1 + 7 \times 16^0$$

$$1 \times 256 + 7 \times 16 + 7 \times 1$$

$$256 + 112 + 7 = 375$$

Two's Complement Notation

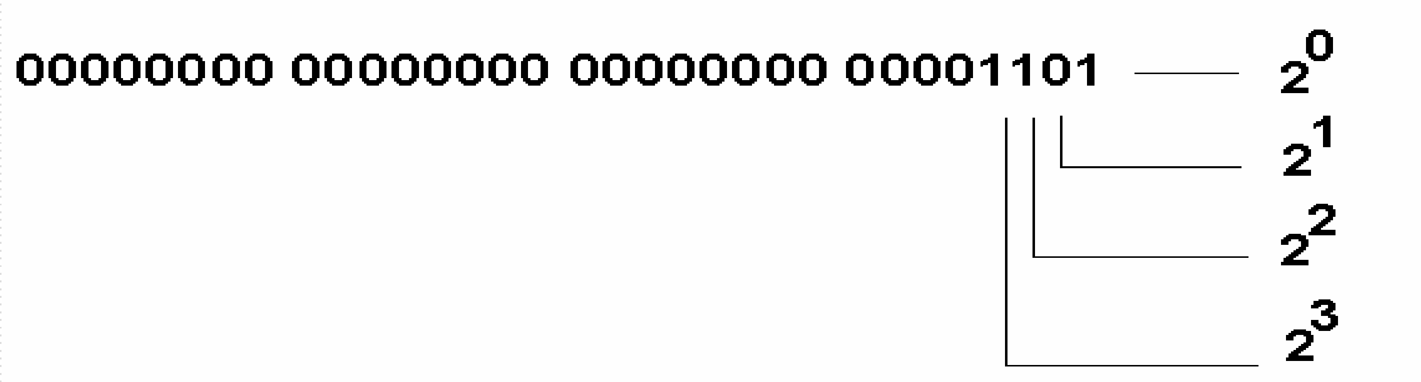
- **How computers represent negative numbers using two's complement notation.**
- **How the two's complement of a binary number is formed.**
- **Why it represents the negative value of the given binary number.**

Two’s Complement Notation

- **Consider a machine with 32-bit integers.**
- **Suppose the integer value 13.**

Two’s Complement Notation

- **Consider a machine with 32-bit integers. Suppose the integer value 13.**
- **The 32-bit representation of value is**



$$1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 13$$

Two’s Complement Notation

- **To form the negative of value we first form its one’s complement--ones become zeros and zeros become ones.**

value :

00000000 00000000 00000000 00001101

one’s complement :

11111111 11111111 11111111 11110010

Two’s Complement Notation

- **To form the two’s complement add one to the one’s complement**

one’s complement :

11111111 11111111 11111111 11110010

two’s complement :

11111111 11111111 11111111 11110011

- **This value represents -13**

Verify the results

two's complement (value –13):

11111111 11111111 11111111 11110011

value (13):

00000000 00000000 00000000 00001101

The addition between both amounts is zero

```
  11111111 11111111 11111111 11110011
+ 00000000 00000000 00000000 00001101
-------------------------------------
  00000000 00000000 00000000 00000000
```

Divisibility

- Given integers ***a*** and ***b*** with **b** ≠ 0, we say that ***b*** is a divisor or a factor of ***a*** and that ***a*** is divisible by ***b*** if and only if ***a* = qb** for some integer q.

- ***b* | *a*** ← ***a*** is divisible by ***b*** ("***b* divides *a***.")

  - $1|n \ \forall$ n integer, n ≠ 0
  - $n|0 \ \forall$ n integer, n ≠ 0

4.2.2 Proposition

- The binary relation R on N defined by (a, b) ∈ R if and only if a | b is a partial order.

  - 3 is a divisor of 18 **or 3|18**
  - -7 is a divisor of 35 **or -7|35**

Note: **a|b "a divides b" or "b is divisible by a."**

Proof of 4.2.2 Proposition

The binary relation R on N defined by $(a, b) \in R$ if and only if $a \mid b$ is a partial order.

Reflexive: For any $a \in N$, $a \mid a$ because

$a = 1 . a$

Note: **a|b "a divides b" or "b is divisible by a."**

Proof of 4.2.2 Proposition

- Antisymmetric: Suppose $a, b \in N$ are such that $a \mid b$ and $b \mid a$.
- Then $b = q_1 a$ for some natural number q_1 and
- $a = q_2 b$ for some natural number q_2.
- Thus, $a = q_2(q_1 a) = (q_1 q_2)a$.

Proof of 4.2.2 Proposition

- Thus, $a = q_2(q_1 a) = (q_1 q_2)a$.
- Since $a \neq 0$, $q_1 q_2 = 1$, and
- since q_1, and q_2 are natural numbers,
- we must have $q_1 = q_2 = 1$; thus, $a = b$.

Proof of 4.2.2 Proposition

- Transitive: if a, b, c $\in$ N are such that a | b and b | c,
- then $b = q_1 a$ and $c = q_2 b$

for some natural numbers q_1 and q_2.

- Thus $c = q_2 b = q_2(q_1 a) = (q_1 q_2)a$,

with $q_1 q_2$ a natural number. So a | c

4.2.3 Proposition

- Suppose a, b, c $\in$ N are such that c | a and c | b, then c |(xa + yb) for any integers x and y.

Proof of 4.2.3 Proposition

- Since c | a , a = q_1c for some integer q_1
- Since c | b, b = q_2c for some integer q_2
- Thus, $xa + yb = xq_1c + yq_2c$

  $= (q_1x + q_2y)c$
- Since $q_1x + q_2y$ is an integer,

  c |(xa + xb), as required.

The Greatest Common Divisor (gcd)

- Let a and b be integers not both of which are 0.

- An integer g is the gcd of a and b if and only if g is <u>the largest common divisor</u> of a and b; that is, if and only if

1. $g \mid a$, $g \mid b$ and
2. If c is any integer such that $c \mid a$ and $c \mid b$, then $c \leq g$.

The Greatest Common Divisor (gcd)

- The gcd of 15 and 6 is 3.
- gcd(-24, 18) = 6
- gcd(756, 210) = 42
- gcd(-756, 210) = 42
- gcd(-756, -210) = 42

4.2.3 Lemma

- If a = qb + r for integers a, b, q, and r, then gcd(a, b) = gcd(b, r).
- If a = b = 0 then a = qb + r , then r = 0
- If b = r = 0 then a = 0
- In either case, the result is true since neither gcd(a,b) nor gcd(b,r) is defined.

Euclidean Algorithm

- Let a and b be natural numbers with $b < a$. To find the gcd of a and b, write

$$a = q_1 b + 1 \text{ with } 0 \le r_1 < b$$

If $r_1 \neq 0$ write $b = q_2 r_1 + r_2$, with $0 \le r_2 < r_1$

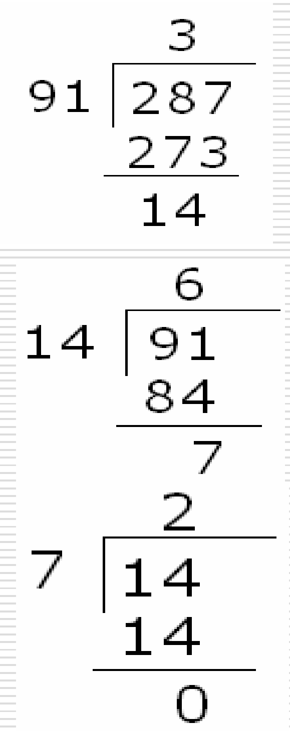
If $r_2 \neq 0$ write $r_1 = q_3 r_2 + r_3$, with $0 \le r_3 < r_2$

If $r_3 \neq 0$ write $r_2 = q_4 r_3 + r_4$, with $0 \le r_4 < r_3$

Continue the process until some remainder $r_{k+1} = 0$. Then the gcd of a and b is r_k, the **last nonzero remainder**.

Example of Euclidean Algorithm

- Find the gcd of 287 and 91.
- 287 = 3 . 91 + 14
- 91 = 6 . 14 + 7
- 14 = 2 . 7 + 0



gcd(287,91) = gcd(14,7) = 7

Example of Euclidean Algorithm

- Find the gcd of 287 and 91.
- 287 = 3 . 91 + 14
- 91 = 6 . 14 + 7
- 14 = 2 . 7 + 0

- The last nonzero remainder is 7, so this is the gcd(287,91).

gcd(287,91) = gcd(14,7) = 7

The Least Common Multiple (lcm)

- If a and b are nonzero integers, ℓ is the least common multiple (lcm) of a and b and write $\ell = \text{lcm}(a, b)$ if and only if ℓ is positive integer satisfying

1. $a \mid \ell$, $b \mid \ell$ and,
2. If m is any positive integer such that $a \mid m$ and $b \mid m$, then $\ell \leq m$.

The Least Common Multiple (lcm)

- The lcm of 4 and 14 is 28.
- lcm(-6, 21) = 42
- lcm(-5, -25) = 25
- The lcm is always positive (by definition).

gcd(a, b)lmc(a, b) = |ab|

The Least Common Multiple (lcm)

gcd(a, b) . lmc(a, b) = |ab|

- gcd(6, 21) . lmc(6, 21) = |6.21|
- 3. lcm(6, 21) = 6(21)
- lcm(6, 21) = 6(21) / 3
- lcm(6, 21) = 6(21) / 3 = 42

The Least Common Multiple (lcm)

gcd(a, b) . lmc(a, b) = |ab|

gcd(630, -196) = 14

14 . lcm(630, -196) = 630(196)

lcm(630, -196) = 123480 / 14

lcm(630, -196) = <u>8820</u>

Prime Numbers

A natural number $p \geq 2$ is called prime if and only if natural numbers that divide p are p and 1.

A natural number $n > 1$ that is no prime is called composite.

Thus, $n > 1$ is composite if $n = ab$, where a and b are natural numbers with $1 < a, b < n$.

Prime Numbers

- Given any natural number $n > 1$, there exists a prime p such that $p \mid n$.
- There are infinitely many primes.
- If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

The Sieve of Eratosthenes

- List all integers from 2 to n.
- Circle 2 and then cross out all multiples of 2 in the list.
- Circle 3, the first number not yet crossed out or circled, and cross out all multiples of 3.

The Sieve of Eratosthenes

- Circle 5, the first number not yet crossed out or circled, and cross out all multiples of 5.
- Circle 7 and then cross out all multiples of 7 in the list.
- At the general stage, circle the first number that is neither crossed out nor circled and cross out all its multiples.

The Sieve of Eratosthenes

- Continue until all numbers less than or equal to $\sqrt{n}$ have been circled or crossed out.
- When the process is finished, those integers not crossed out are the primes not exceeding n.

The Sieve of Eratosthenes

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

List all integers from 2 to n.

The Sieve of Eratosthenes

(2)	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11
~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~	21
~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~	31
~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~	41
~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~	51
~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~	61
~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~	71
~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~	81
~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~	91
~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~	

Circle 2 and then cross out all multiples of 2 in the list.

The Sieve of Eratosthenes

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

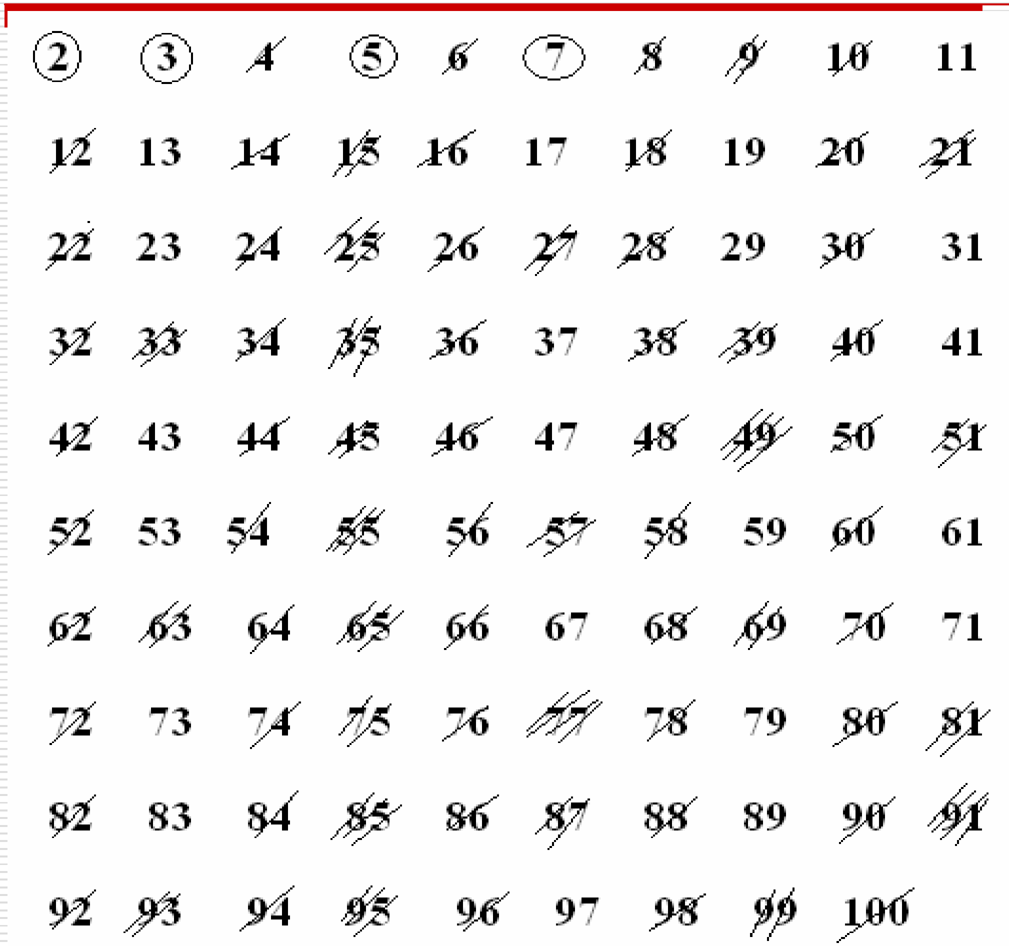
Circle 3, the first number not yet crossed out or circled, and cross out all multiples of 3.

The Sieve of Eratosthenes

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

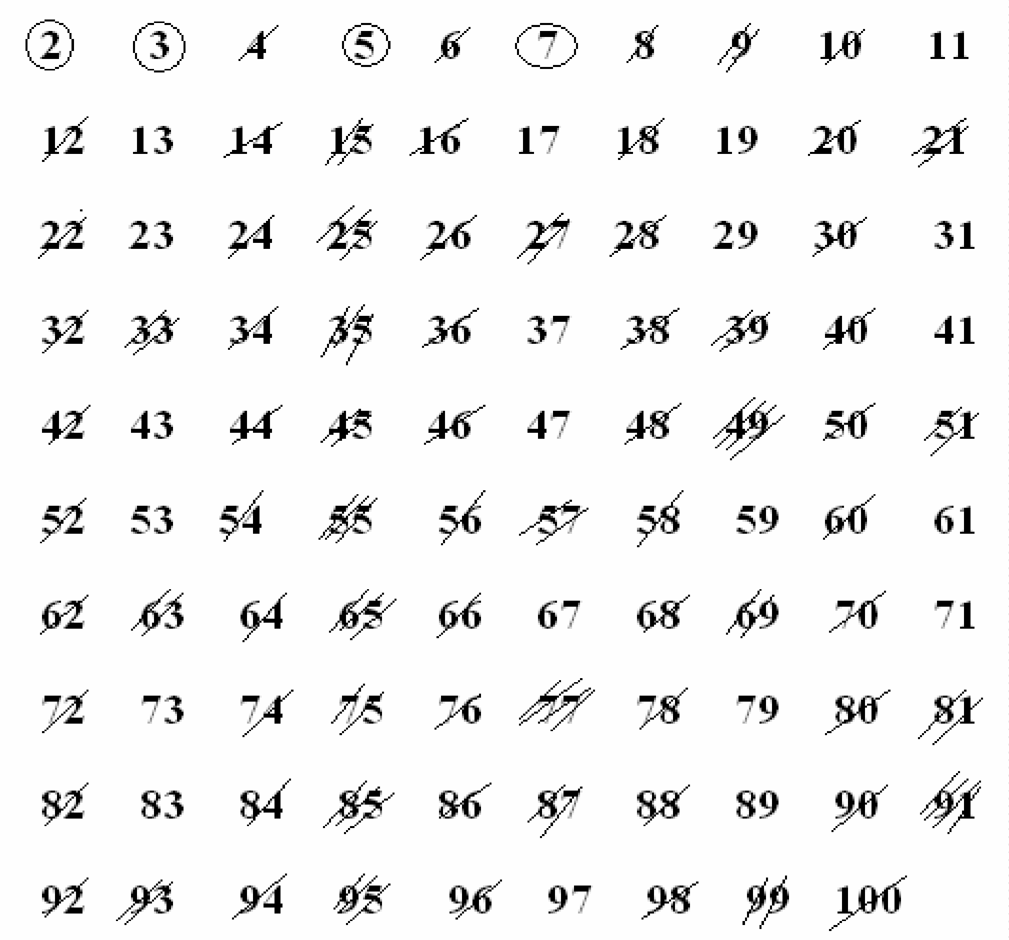
Circle 5, the first number not yet crossed out or circled, and cross out all multiples of 5.

The Sieve of Eratosthenes



Circle 7, the first number not yet crossed out or circled, and cross out all multiples of 7.

The Sieve of Eratosthenes



The primes less than 100 are those not crossed out.

The Sieve of Eratosthenes

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

The primes less than 100 are those not crossed out.

Congruence

- Let $n > 1$ be a fixed natural number.
- Given integers a and b, a is congruent to be modulo n (or a is congruent to b mod n for short) $a \equiv b \pmod{n}$,
- If and only if $n \mid (a - b)$.
- n is called the modulus of the congruence

Congruence

- $3 \equiv 17 \pmod 7$ because $3 - 17 = -14$ is divisible by 7;
- $-2 \equiv 13 \pmod 3$, because $-2 - 13 = -15$ is divisible by 3;
- $60 \equiv 10 \pmod{25}$, because $60 - 10 = 50$ is divisible by 25;
- $-4 \equiv -49 \pmod 9$, because $-4 + 49 = 45$ is divisible by 9;

Congruence is a binary relation on Z

- Reflexive: $a \equiv a \pmod{n}$ for any integer a. Because $a - a = 0$ is divisible by n.
- Symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. Because if $n \mid (a - b)$ then $n \mid (b - a)$
- Transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$. Because if $n \mid (a - b)$ then $n \mid (b - c)$

The Congruence Class

- The congruence class mod n of an integer a is the set of all integers to which a is congruent mod n. It is denoted $\bar{a}$. Thus

$$\bar{a} = \{ b \in Z \mid a \equiv b \pmod{n} \}$$

Note: Because congruence is symmetric is the same $a \equiv b \pmod{n}$ or $b \equiv a \pmod{n}$

4.4.3 Proposition

- Let a, b, and n be integers with $n > 1$. Then the following statements are equivalent .

- $n \mid (a - b)$
- $a \equiv b \pmod{n}$
- $a \in \overline{b}$
- $b \in \overline{a}$
- $\overline{a} = \overline{b}$

4.4.4 Corollary

- For integers a, b, and n with n > 1,

  $a \equiv b \pmod{n}$ if and only if $\overline{a} = \overline{b}$

- $a \in \overline{b}$
- $b \in \overline{a}$
- $\overline{a} = \overline{b}$

Congruence

- Let n = 5. Since -8 – 17 = -25 is divisible by 5, then $-8 \equiv 17 \pmod{5}$.

- -8 belongs to the congruence class of 17 ($-8 \in \overline{17}$), and $17 \in -\overline{8}$. So $-\overline{8} = \overline{17}$

Congruence

- Find all congruence classes of integers mod 5.

$$\overline{0} = \{b \in Z \mid b \equiv 0 \pmod 5\}$$
$$= \{b \in Z \mid 5 \mid (b - 0)\}$$
$$= \{b \in Z \mid b = 5k \text{ for some integer } k\}$$

Congruence

- Congruence classes of integers mod 5.

$$
\begin{aligned}
\overline{1} &= \{b \in Z \mid b \equiv 1 \pmod 5\} \\
&= \{b \in Z \mid 5 \mid (b - 1)\} \\
&= \{b \in Z \mid b - 1 = 5k \text{ for some integer } k\} \\
&= \{b \in Z \mid b = 5k + 1 \text{ for some integer } k\}
\end{aligned}
$$

Congruence

- Congruence classes of integers mod 5.

$$\overline{2} = \{b \in Z \mid b = 5k + 2 \text{ for some } k \in Z\}$$
$$= 5Z + 2$$

$$\overline{3} = \{b \in Z \mid b = 5k + 3 \text{ for some } k \in Z\}$$
$$= 5Z + 3$$

$$\overline{4} = \{b \in Z \mid b = 5k + 4 \text{ for some } k \in Z\}$$
$$= 5Z + 4$$

4.4.5 Proposition

- Any integer is congruent mod to its remainder upon division by n.
- There are n congruence classes of integers mod n corresponding to each of the n possible remainders.

$\overline{0} = nZ$

$\overline{1} = nZ + 1$

$\overline{2} = nZ + 2$

$\overline{n\text{-}1} = nZ + (n - 1)$

4.4.6 Definition

- If $n > 1$ is a natural number and a is any integer, $a \pmod{n}$ is the remainder r.

  $0 \le r < n$, obtained when a is divided by n.

- $-17 \pmod{5} = 3$
- $28 \pmod{6} = 4$
- $-30 \pmod{9} = 6$
- The integer 29 is 5 mod 6

4.4.6 Definition

- $-17 \pmod 5 = 3$
- $-17/5 = -3.4$
- $5 > 0$, so $\lfloor -17/5 \rfloor = -4$ ← floor
- $-17 = -4(5) + 3 = -20 + 3$ ← remainder

4.4.6 Definition

- $28 \pmod 6 = 6$
- $28/6 = 4.66$
- $6 > 0$, so $\lfloor 28/6 \rfloor = 4$ ← floor
- $28 = 4(6) + 4 = 24 + 4$ ← remainder

4.4.6 Definition

- $-30 \pmod 9 = 4$
- $-30/9 = -3.33$
- $9 > 0$, so $\lfloor -30/9 \rfloor = -4$ ← floor
- $-30 = -4(9) + 6 = -36 + 6$ ← remainder

4.4.6 Definition

- $29 \pmod{6} = 5$
- $29/6 = 4.83$
- $6 > 0$, so $\lfloor 29/6 \rfloor = 4$ ← floor
- $29 = 4(6) + 5 = 24 + 5$ ← remainder

Topics covered

- The Division Algorithm
  - The division algorithm
  - Representing natural numbers in various bases.
- Divisibility and the Euclidean algorithm.
  - gcd
  - Lcm
- Prime numbers
- Congruence

Reference

- “Discrete Mathematics with Graph Theory”, Third Edition, E. Goodaire and Michael Parmenter, Pearson Prentice Hall, 2006. pp 98-146.