Properties of Numbers:

**Division**

**Divisibility**

We say $m$ divides $n$ or $n$ is divisible by $m$ if

$n = m \cdot k$, for some $k \in \mathbb{Z}$

$m$ is a **divisor** or **factor** of $m$ and $m$ is **divisible** by $m$.

We call $mk = n$ a **decomposition** or **factorization** of $m$.

Clearly: $k$ is also a divisor of $m$ and is uniquely determined by $m$.

Divisors occur in pairs $(m, k)$.
**Square Number**

\[ n \text{ is a square number if and only if divisors of } n \text{ are } (m, m) \]

\[ n = m \cdot m \]

\[ m = m^2 \]

**Fact**

If \((m, k)\) is a divisor of \(n\), so is \((-m, -k)\) - associated divisor

**Proof**

\[ m = m \cdot k, \text{ so } n = (-m)(-k) = mk \]

**Remark:**

Each number has an obvious decomposition

\[ c = 1 \cdot c = (-1)(-c) \]

\[ \text{i.e. FACT 1a} \]

\(-m, k \) ± 1 together with \(±c\)

are trivial divisors of \(c\)

\((1, c) \quad (-1, -c)\)
FACT 2

If \( m | n \) and \( m | m \), then \( m, n \) are associated i.e.
\[ m = \pm n \]

Proof

\( m | n \) i.e. \( n = mk_1 \) \( k_1, k_2 \in \mathbb{Z} \)
\( m | m \) i.e. \( m = mk_2 \)
so \( m = mk_1k_2 \) i.e. \( k_1 = k_2 = 1 \) and \( m = n \)
or \( k_1 = k_2 = -1 \), and \( m = -n \).

FACT 3

If \( m | n_1 \) and \( m | n_2 \)
THEN \( m | (n_1 \pm n_2) \)

\( m | n_1 \) i.e. \( n_1 = mk_1 \)
\( m | n_2 \) i.e. \( n_2 = mk_2 \), hence
\( (n_1 \pm n_2) = m(k_1 \pm k_2) \) i.e.
\( m | (n_1 \pm n_2) \)
FACT 9

If $m|n$ and $n|k$, then $m|k$.

Proof:

$m|n \Rightarrow n = mk_1$ \rightarrow $k = mk_1k_2 = m|k$.

$m|k = k = mk_2$

In most questions regarding divisors we assume that $m > 0$ and that one only considers positive divisors $(m, k)$.

We look first at positive factorizations and then we work out others.

The book definition is $n, m \in \mathbb{Z}$

$m|m$ iff $m > 0$ and $n = mk$, for some $k \in \mathbb{Z}$

Consider only positive $m$, i.e. divisor $(m, k) > 0, k \in \mathbb{Z}$
**Definition**

**Proper Divisors of m**: all positive divisors, including 1 that are less than m.

**Fact 5**

If \((m, k)\) is a divisor of \(m\) then the factors \(m, k\) can't be both \(> \sqrt{m}\) \(> \sqrt{m}\).

**Proof:**

Assume \(m, k > \sqrt{m}\) and \(k > \sqrt{m}\) then \(m, k > \sqrt{m} \cdot \sqrt{m} = m\) contradiction with \(m = mk\).

Re-write Fact 5

If \((m, k)\) is a divisor of \(m\) then \(m \leq \sqrt{m}\) or \(k \leq \sqrt{m}\).
Problem:

Find all positive divisors of $m = 60$

By fact 5, the number of divisors $m \leq \sqrt{m} = \sqrt{60} \quad i.e.$

$m < 8$ \quad m \leq \sqrt{60} < \sqrt{64} = 8$

Six pairs of divisors

$(1, 60) \quad (3, 20) \quad (5, 12) \quad (2, 30) \quad (4, 15) \quad (6, 10)$

$m = 1, 2, 3, 4, 5, 6$
DIVISION AND REMINDERS

Let \( b \neq 0 \), and \( b \in \mathbb{Z} \).
Any \( a \in \mathbb{Z} \) is either a multiple of \( b \) or fall between two consecutive multiples \( qb \) and \( (q+1)b \) of \( b \).

WE WRITE IT

\[
\begin{align*}
a &= qb + r \\
r &= 0, 1, 2, \ldots, \lfloor b \rfloor - 1
\end{align*}
\]

\( r \) is called the least positive remainder or simply \( \text{THE REMINDER} \) of \( a \) by division with \( b \).

\( q \) is the incomplete quotient or simply \( \text{THE QUOTIENT} \) of \( a \) by division with \( b \).

\[321 = 4 \times 74 + 25, \quad 48 = (-2) \cdot (-17) + 2\]
DIVISION and REMAINders

\[ b \neq 0, \ a, b \in \mathbb{Z} \]

\[ a = q \cdot b + r \quad 0 \leq r < |b| \]

\( q \) - quotient of \( a \) by division with \( b \)

\( r \) - reminder of \( a \) by division with \( b \)

**Note:** Given \( a, b \in \mathbb{Z} \), \( q \) and \( r \) are uniquely determined and each integer \( a \in \mathbb{Z} \) can be written as

\[ a = q \cdot b + r , \ 0 \leq r < |b| \]

In particular any \( m \in \mathbb{Z} \)

\[ m = 2q \quad \text{or} \quad m = 2q + 1 \]

**Even** \( \text{Odd} \)

**Thm:** The square of \( m \in \mathbb{Z} \) is either divisible by 4, or leaves the remainder 1 when divided by 4

**Proof**

\[ n = 2q, \ n^2 = (2q)^2 = 4q^2; \quad n^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 \]
DIVISION and REMAINDERS

\[ \boxed{\text{if } a \div b = q \text{, then } a = bq + r} \]

we can write it as

\[ \frac{a}{b} = q + \frac{r}{b} \quad \text{where } 0 \leq \frac{r}{b} < 1 \]

**FACT**

- \( q \) is the greatest integer such that \( q \leq \frac{a}{b} \)

**SPECIAL NOTATION**

\[ \lfloor q \rfloor = \frac{a}{b} \] (old notation)

**NEW NOTATION** (after K.E. Iverson, 1960)

\[ \lfloor \frac{a}{b} \rfloor = \text{greatest integer such that } \frac{a}{b} \leq \frac{a}{b} \]

**GENERAL DEFINITION**

**FLOOR**

\[ \lfloor x \rfloor = \text{the greatest integer } \geq x \]

**CEILING**

\[ \lceil x \rceil = \text{the least integer } \geq x \]
Division and Remainders

\[ q = \lfloor \frac{a}{b} \rfloor \]

\( q \leq \frac{a}{b} \) (Floor)

is also called

The Greatest Integer Contained in \( \frac{a}{b} \)

Examples

\[ \lfloor \frac{27}{5} \rfloor = 5, \quad \lfloor \frac{5}{3} \rfloor = 1, \quad \lfloor \frac{2}{1} \rfloor = 2, \quad \lfloor \frac{1}{3} \rfloor = -1 \]

\[ \lfloor \frac{1}{3} \rfloor = 0 \]

We extend notation to Real Numbers

\( x = q + y, \quad 0 \leq y < 1, \quad q \in \mathbb{Z} \)

\( x, y \in \mathbb{R} \)

\[ q = \lfloor x \rfloor \]

Examples

\[ \lfloor \pi \rfloor = 3, \quad \lfloor e \rfloor = 2, \quad \lfloor \frac{\pi^2}{2} \rfloor = 4 \]

More of this in Chapter 3.
NUMBER SYSTEMS

Represent:

\[ a = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 \]

where \( a_i \in \{0, 1, \ldots, b-1\} \)

Write

\[ a = (a_n, a_{n-1}, \ldots, a_1, a_0)_b \]

**Question**

1. How to find the representation under base \( b \)?
2. How to pass from one base to the other.

**Observation**

1. \( a_0 \) is the remainder of \( a \) by division by \( b \) and \( a_0 = b(a_n b^n + a_1) + a_0 \)

\[ a = q_1 b + a_0 \]

where \( q_1 = a_m b^{m-1} + \ldots + a_2 b + a_1 \)
\[ a = q_1 b + a_0 \]

\[ q_1 = a_m b^{m-1} + \ldots + a_2 b + a_1 \]

Perform a repeat

\[ q_1 = b q_2 + a_1 \]

\[ q_2 = a_m b^{m-1} + \ldots + a_3 b + a_2 \]

\[ q_2 - \text{is a reminder of } q_2 \]

by division by \( b \)

Repeat to find all \( a, a_2, \ldots, a_n \)!

\[ a_i - \text{is a reminder of } q_i \]

by division by \( b \)

**Example:** Represent \( 1,749 \) in a system with base \( 7 \)

\[ 1,749 = 249 \cdot 7 + 6 \]

\[ 249 = 35 \cdot 7 + 4 \]

\[ 35 = 5 \cdot 7 + 0 \]

\[ 1,749 = (5, 0, 4, 6)_7 \]
EXAMPLE

Represent 19,151 to the base 12

\[ 19,151 = 1,595 \cdot 12 + 11 \]
\[ 1,595 = 132 \cdot 12 + 11 \]
\[ 132 = 11 \cdot 12 + 0 \]

\[ 19,151 = (11, 0, 11, 11)_{12} \]

We evaluate \( a_0, a_1, \ldots, a_n \) from the lowest upward.

Now let's evaluate \( a_n, a_{n-1}, \ldots, a_0 \) downward.

In this case we have to determine the highest power of 12 such that \( 6^m \) is less than \( a \), while the next power \( 6^{m+1} \) exceeds \( a \).
We look for a division of \( a \) by \( b^n \) and

\[
a = a_n b^n + \pi_{n-1}
\]

\[
\pi_{n-1} = a_{n-1} b^{n-1} + \ldots + a_0
\]

We determine \( a_{n-1} \) from \( \pi_{n-1} \)

\[
a_0 = \pi_{n-1}
\]

\[
\pi_{n-2} = a_{n-2} b^{n-2} + \ldots + a_0
\]

\[
\pi_{n-2} = a_{n-2} b^{n-2} + \pi_{n-3}
\]

\[
\pi_{n-2} = a_{n-2} b^{n-2} + \pi_{n-3}
\]

\[
\text{etc.}
\]

**EXAMPLE:** Represent 1,832 in the base 7.

**FIRST:** Calculate powers of 7.

\[
7, 7^2 = 49, 7^3 = 343, 7^4 = 2,401
\]
\[ a = a_n b^n + r_{n-1} \]

\[ r_{n-1} = a_{n-1} b^{n-1} + \ldots + a_0 \]

\[ n = 3 \]

\[ 1,832 = 5 \cdot 7^3 + 117 r_2 \]

\[ 117 = 2 \cdot 7^2 + 19 r_1 \]

\[ 19 = 2 \cdot 7 + 5 r_0 = a_0 \]

\[ a_3 = 5 \]

\[ a_2 = 2 \]

\[ a_1 = 2 \]

\[ a_0 = 5 \]

\[ 1,832 = (5, 2, 2, 5)_7 \]

Why different bases? For example, division becomes simpler:

\[ \frac{1}{3} = 0.3333\ldots \quad \text{(base } 10) \]

\[ \frac{1}{3} = (0, 2)_6 = (0, 4)_{12} \]

Large bases - short representations, but multiplication tables grow!

12 x 12 for base 12

60 x 60 for base 60