$f: \mathbb{Z} \to \mathbb{N}$

$f(x) = |x| + 3$

$f(1) = |1| + 3 = 4$

$f(-1) = |-1| + 3 = 4$

$f(1) = f(-1)$

but $1 \neq -1$ $\therefore$ f is not one-one.

---

f is onto iff range(f) = $\mathbb{N}$

But range(f) = $[3, \infty)$

and $[3, \infty) \neq \mathbb{N}$

Hence, f is not onto.

To show that A is countable

find a bijective function $f: \mathbb{N} \to A$.

To show that A is uncountable.

we need to show that there does not exist any bijective function between A and $\mathbb{N}$.

Proposition :- Any open interval in $\mathbb{R}$ is uncountable.

i.e $(0,1)$ is uncountable.

$\mathbb{R}$ is uncountable

0.00001 ← 1
0.000095 ↔ 2
0.00003 ↔ 3

$f: (0,1)$

$f(ab) = f(a)f(b)$

The concept of cardinality is an equivalence relation

$A \sim A$ $\quad |A| = |A|$

If $A \sim B$ then $B \sim A$ $\quad$ If $|A| = |B|$ then $|B| = |A|$

If $A \sim B$ and $B \sim C$ then $A \sim C$

$|A| = |B|$ $\quad |B| = |C|$

$\Rightarrow |A| = |C|$

$\Rightarrow A \sim C$

Proposition :- A subset of a countable set is countable.

$|A| = |B|$

$|B| = |\mathbb{R}|$

$\mathbb{Z}$ is countable

$\mathbb{Z}^-$ is also countable as it is a subset of $\mathbb{Z}$ which is countable.

$A = \left\{ \frac{m}{n} \,\middle|\, m,n \in \mathbb{Z},\ m<100,\ n>20 \right\}$

Is A countable?

Ans: As $A \subseteq \mathbb{Q}$ and $\mathbb{Q}$ is countable, hence A is countable.

3(c) $\mathbb{N}\times\mathbb{N}$ and $A = \{ a+bi \in \mathbb{C} \mid a,b \in \mathbb{N} \}$

$f: \mathbb{N}\times\mathbb{N} \to A$

$f(a,b) = a+bi$ Canonical mapping

One-one: Let $f(a,b) = f(c,d)$, $a,b,c,d \in \mathbb{N}$

$a+bi = c+di$

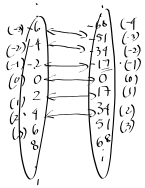
$\Rightarrow a=c$ and $b=d$.

$\therefore (a,b) = (c,d)$

Onto: Let $a+bi \in A$. $a,b \in \mathbb{N}$

then $f(a,b) = a+bi$

and $(a,b) \in \mathbb{N}\times\mathbb{N}$



3(b) $f: 2\mathbb{Z} \to 17\mathbb{Z}$

$f(n) = 17\,\frac{n}{2}$

One-one:

Let $f(n_1) = f(n_2)$

$\Rightarrow \frac{17n_1}{2} = \frac{17n_2}{2}$

$\Rightarrow n_1 = n_2$

Onto:

Let $y \in 17\mathbb{Z}$.

$\Rightarrow y = \frac{17n}{2}$ for some $n \in 2\mathbb{Z}$.

$\Rightarrow \frac{2y}{17} = n$

$\Rightarrow 2\left(\frac{y}{17}\right) = n$

$\Rightarrow$ As $y \in 17\mathbb{Z}$

hence $\frac{y}{17} \in \mathbb{Z}$.

$\therefore f\left(\frac{2y}{17}\right) = y$.

$a, b \in \mathbb{Z}$ $b \neq 0$

$\boxed{a = bq + r \quad 0 \leq r \leq |b|}$

$a = 20 \quad b = 7$

$20 = 2 \cdot 7 + 6$

$20 = 1 \cdot 7 + 13$

$a = -47$

$b = -8$

$-47 = 6 \cdot -8 + 1$

If an integer n is divided by another integer m, then, the possible remainders are $0, 1, 2, 3, \ldots, m-1$

This means, any integer n is one of these form

$mk, mk+1, mk+2, \ldots, mk+(m-1)$

for some integer k.

$0, 1, 2$

$n = 3k+0$

$n = 3k+1$

$n = 3k+2$

$a \in \mathbb{Z} \qquad a^2 = \begin{cases} 3k \\ 3k+1 \end{cases}$ for some integer k

a is one of the forms $3k$, $3k+1$, or $3k+2$ for some integer k.

Case 1 $a = 3k$

$a^2 = (3k)^2 = 9k^2 = 3(3k^2) = 3m$ for some $m \in \mathbb{Z}$

Case 2 $a = 3k+1$

$a^2 = (3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k) + 1$

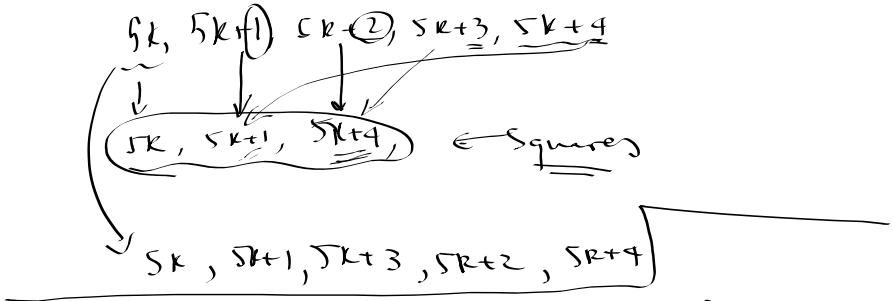
$= 3m+1$ for some $m \in \mathbb{Z}$

Case 3 $a = 3k+2$

$a^2 = (3k+2)^2 = 9k^2+12k+4 = 9k^2+12k+3+1$

$= 3(3k^2+4k+1)+1$

$= 3m+1$ for some $m \in \mathbb{Z}$.



Divisibility and the Euclidean Algorithm.

3 divides 6. $n = 3k$ $n = 3k+1$

Definition:- An integer a is divisible by a non-zero integer b iff there exists an integer k, such that

$$a = bk$$

Notation:-

b divides $a \iff b \mid a$

b does not divide $a \iff b \nmid a$

$5 \mid 10$ $\quad 5 \nmid 13$

b divides $a \iff a$ is a multiple of b

$\iff b$ is a factor of a.

Is divisibility an equivalence relation?

Q aRb iff $a|b$, $a,b \in \mathbb{Z}$

Reflexive $a|a \Rightarrow a = a \cdot 1$
Hence aRa

Symmetric $5|10$ but $10 \nmid 5$
Hence R is not symmetric

Transitive Let $a|b$ and $b|c$
$\Rightarrow b = ak$ $c = bm$
for some $k \in \mathbb{Z}$ $m \in \mathbb{Z}$.
$\Rightarrow c = a(km)$
as $km \in \mathbb{Z}$
hence $a|c$
So R is transitive

Anti-symmetric Let $a|b$ and $b|a$
$5|-5$ and $-5|5$
but $5 \neq -5$
Hence R is not anti-symmetric

Proposition :- Let $a|b$ and $a|c$. Then
$a|(bx \pm cy)$ for any integers x, y.

Proof :- $a|b \Rightarrow b = ak$, $k \in \mathbb{Z}$
$a|c \Rightarrow c = am$, $m \in \mathbb{Z}$

$bx + cy = akx + amy$
$= a(kx + my)$
integer
$\Rightarrow a|(bx+cy)$

Greatest Common Divisor (GCD)

$\{8, 16, 32\}$

Definition :- Let a and b be integers not both of which are 0. A positive integer g is the greatest common divisor (g.c.d) of a and b, denoted by $gcd(a,b)$, iff,

1. $g|a$ and $g|b$
2. If $h|a$ and $h|b$, then $h \leq g$

Examples

$gcd(8,16) = 8$
$gcd(9,12) = 3$
$gcd(9,17) = 1$

Definition :- Two integers a and b are said to be relatively prime iff $gcd(a,b) = 1$

$f(x) = \frac{1}{1-x} + 8 \qquad (1,2) \to (9,\infty)$

$f\left(\frac{3}{7}\right) = \frac{1}{1-\frac{3}{7}} + 8$

$= \frac{1}{\frac{4}{7}} + 8$

$= \frac{7}{4} + 8 = \frac{39}{4}$

$f(x) = \frac{9}{2-x}$

$\frac{9}{2-x} = y$

$\frac{9}{y} = 2-x$

$x = 2 - \frac{9}{y}$

$9 < y < \infty$

$\frac{1}{9} > \frac{1}{y} > 0$

$1 > \frac{9}{y} > 0$

$-1 < -\frac{9}{y} < 0$

$1 < 2 - \frac{9}{y} < 2$

$1 < x < 2$

$a^2 + b^2 = c^2$

$5^2 = 3^2 + 4^2$

$c^3 = a^3 + b^3 \qquad c^4 = a^4 + b^4$

---

7 Millenium Problems

(1) 6 left

$\cong$

$P = NP$

Euclidean Algorithm

Used to find the gcd of two integers.

Repeated use of the division algorithm

$a = bq + r, \quad 0 \le r < |b|$

gcd (451, 44)

$451 = 10(44) + 11$

$44 = 4(11) + 0 \leftarrow$ Stop when the remainder is 0.

gcd

gcd (630, 196)

$630 = 3(196) + 42$

$196 = 4(42) + 28$

$42 = 1(28) + 14$

$28 = 2(14) + 0$

gcd

$\therefore$ gcd (630, 196) = 14

gcd (−630, 196)

$-630 = (196)$

Theorem:- If d is the greatest common divisor of two integers a and b, then there exists integers m and n such that

$$ma + nb = d$$

How to find m and n?

Extended Euclidean Algorithm

$\gcd(630, 196) = 14$

$630 = 3(196) + 42$

$196 = 4(42) + 28$

$42 = 1(28) + 14$

$28 = 2(14) + 0$

$14 = 42 - 1(28)$

$14 = 42 - 1(196 - 4(42))$

$= 42 - 196 + 4(42)$

$= 5(42) - 196$

$14 = 5(630 - 3(196)) - 196$

$14 = 5(630) - 15(196) - 196$

$14 = 5(630) - 16(196)$

3150

196 | 16 | 9
3136 | (14)

$3150 - 3136$

$= 14$

Q Show that 17,369 and 5472 are relatively prime

Then Find integers m and n such that

$17{,}369m + 5472n = 1$.

$17369 = 3(5472) + 953$

$5472 = 5(953) + 707$

$953 = 1(707) + 246$

$707 = 2(246) + 215$

707
492
215

$246 = 1(215) + 31$

$215 = 6(31) + 29$

$31 = 1(29) + 2$

$29 = 14(2) + 1$

$2 = 2(1) + 0$

$\gcd(17369, 5472) = 1$.

$1 = 29 - 14(2)$

$= 29 - 14(31 - 29)$

$= 29 - 14(31) + 14(29)$

$= 15(29) - 14(31)$

$= 15(215 - 6(31)) - 14(31)$

$= 15(215) - 90(31) - 14(31)$

$= 15(215) - 104(31)$

$= 15(215) - 104(246 - 215)$

$= 119(215) - 104(246)$

Least Common Multiple

a is a multiple of b if there exists an integer c such that

$$a = bc$$

Definition - If a and b are non-zero integers, we say that l is the least common multiple (lcm) of a and b, written as $l = \text{lcm}(a,b)$, iff l is a positive integer satisfying.

1. $a \mid l$ and $b \mid l$
2. For any other integer n, if $a \mid n$ and $b \mid n$, then $l \leq n$.

$\text{lcm}(4,8) = 8$

16

Theorem :- Given integers a and b,

$$\gcd(a,b)\,\mathrm{lcm}(a,b) = |ab|$$

From previous days work.

$$\mathrm{lcm}(630,196) = \frac{|630 \times 196|}{\gcd(630,196)}$$

$$= \frac{630 \times 196^{14}}{14}$$

$$= \boxed{8820}$$

$\frac{1}{3} + \frac{1}{5}$ ← $\frac{1}{4} + \frac{1}{8}$

$\frac{3}{8}$ $\frac{2+1}{8}$ $\frac{8+4}{32} = \frac{12}{32} = \frac{3}{8}$

Q Suppose $a, b, x \in \mathbb{Z}$ and $a \mid bx$. If a and b are relatively prime, then show that $a \mid x$.

Ans :- As $\gcd(a,b) = 1$

hence $\exists\ m, n \in \mathbb{Z}$ such that

$$ma + nb = 1$$

$$x(ma + nb) = x$$

$$max + nbx = x$$

As $a \mid bx \Rightarrow bx = ap$ for $p \in \mathbb{Z}$

$$\Rightarrow max + nap = x$$

$$a(mx + np) = x$$

As $mx + np \in \mathbb{Z}$, hence $a \mid x$.

$a \mid b$ $a \mid c$

$a \mid b \pm c$

Theorem :- Given any natural number $n \geq 2$, there exists a prime p that divides n.

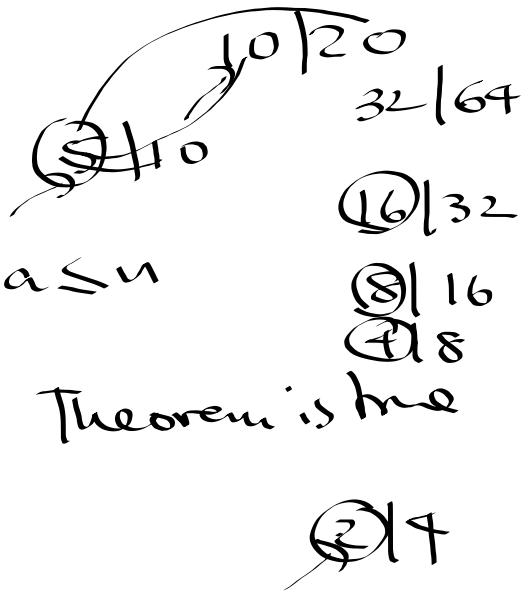
Proof :- Check the book.

(1) n is prime $\Rightarrow n \mid n$

(2) n is composite $\Rightarrow a \mid n$ $\quad a \leq n$

Is a prime? Yes $\Rightarrow$ Theorem is true

Is a composite? Yes.



4.2 Prime Numbers

Definition:- A natural number $n \geq 2$, is a prime number iff the only divisors of n are 1 and n. A number that is not a prime number is called a composite number.

Ex - 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, . . .

(2 — only even prime)

Q Are there infinitely many prime numbers?

A Yes. Archimedes' Proof.

Proof by contradiction

Suppose there are finitely many prime numbers

Let $p_1, p_2, \ldots, p_n$ are all the prime numbers

Let $N = p_1 p_2 p_3 \cdots p_n + 1$

As N is a positive integer, hence by previous theorem, there exist some prime q that divides N.

As $p_1, p_2, \ldots, p_n$ are the only primes, hence $q = p_i$ for some i.

$\therefore p_i \mid N$ and $p_i \mid p_1 p_2 \cdots p_n$

$\Rightarrow p_i \mid (N - p_1 p_2 \cdots p_n)$

$\Rightarrow p_i \mid 1$

Contradiction as $p_i \geq 2$.

$\therefore$ There are infinitely many prime numbers

Sieve of Eratosthenes