

Chapter 4 section 1-2 cont'd

Chapter 4 section 1-2 cont'd

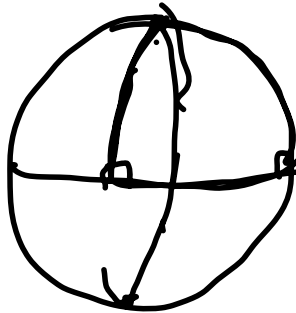
Axioms

POSTULATE = AXIOM

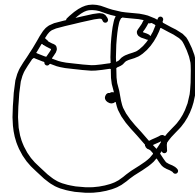
Our book does not mention axioms but it should. Axioms are statements that are asserted to be true for purposes of constructing a theory. For example:

Axiom: Given a line L , and a point P not on L , there is exactly one line through P parallel to L .

Axiom: An empty set exists.



Parallel
Postulate



Axioms in this course

- ▶ Existence of integers, natural numbers, rational numbers, and real numbers.
- ▶ Properties of addition, multiplication such as commutative and associative laws, including closure.
- ▶ Properties of $>$ and $<$

The Division Algorithm

The Division Algorithm: Given $\underline{a}, \underline{b} \in \mathbb{Z}$ with $b > 0$, there are unique integers $\underline{q}$ and $\underline{r}$ with $0 \leq \underline{r} < \underline{b}$ so that $\underline{a} = \underline{bq} + \underline{r}$.

$$a = 31 \quad b = 9$$

$$31 = 99 + 5$$

$$0 \leq r < 9$$

$$j=3 \quad n=4$$

$$0 \leq y < 9$$

$$31 = 3 \cdot 9 + 4$$

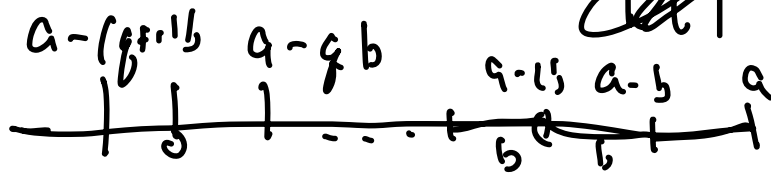
$$f = 0 \quad r = 31$$

$$31 \approx 9g + r$$

$$r > 9$$

31 = 985

$$2 \cdot 31 = 9(9 + 1) + (5 - 9)$$



Proof: Consider the set
of integers $\{a - qb : q \in \mathbb{Z}\}$

, $a - 5b, a - 4b, a - 3b, \dots, a, a + b, a + 2b, \dots$
 $\{31 - q : q \in \mathbb{Z}\}$

$-14, -5, 4, 13, 22, 31, 40, \dots$ and such

Let $\mathbb{N}_0 = \{0, 1, 2, \dots\}$

Any non empty subset of $\mathbb{N}_0$ has a
smallest element.

$$A = \{a - bq \mid q \in \mathbb{Z}, a - bq \geq 0\}$$

Not empty.

has smallest element r

$0 \leq r < b$ because if $r \geq b$

$$\text{then } a - b(q+1) = a - bq - b = r - b < 0$$

So r isn't smallest. $0 \leq r < b$.

$$a = bq + r$$

The Fundamental Theorem of Arithmetic

Theorem: Every natural number greater than one is a product of prime numbers, and this factorization into primes is unique up to rearranging the terms.

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

$$75 = 3 \cdot 5 \cdot 5$$

$$101 = 101 \text{ is prime}$$

$$a + b\sqrt{-5} \quad a, b \in \mathbb{Z}$$

"numbers"

$$6 + 0 \cdot \sqrt{-5} = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

F.T. of Algebra.

Some fundamental definitions: divisibility

Definition: Suppose a and b are integers. We say that a **divides** b , written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a divisor of b and that b is a multiple of a .

$3|b$ because

$$b = qa + \underline{\underline{0}}$$

if $\exists c \in \mathbb{Z}$ such that $b = ac$.

$\exists c$ s.t. $b = 3 \cdot c$?

2 does not divide 7

$\exists c \in \mathbb{Z}$ where $7 = 2c$ $q = 3$
 $r = 1$

NO

$$7 = 2 \cdot 3 + \hat{1}$$

$$0 \leq 1 < 2$$

GCD and LCM

Definition: The greatest common divisor of integers a and b , written $\gcd(a, b)$, is the largest integer that divides both a and b .

Definition: The least common multiple of integers a and b , written $\text{lcm}(a, b)$, is the smallest integer that is a multiple of both a and b .

$$\gcd(52, 64) = 4$$

$$\textcircled{1} \quad 4 \mid 52$$

$$q = 13, r = 0$$

$$\text{and } 4 \mid 64$$

$$q = 16, r = 0$$

$$\textcircled{2} \quad \text{or suppose}$$

$$52 = 4 \cdot 13$$

$$64 = 4 \cdot 16$$

$$52 = 2 \cdot 2 \cdot 13$$

$$64 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$

$$\text{or } d = 2^a \cdot 13^b$$

$$\begin{aligned} a &= 2 \\ b &= 0 \end{aligned}$$

$$52 = 2^2 \cdot 13$$

$$64 = 2^6$$

$$\text{lcm} = 2^6 \cdot 13$$

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

Factor: 32816

Given N

test each prime $p \leq \sqrt{N}$
divide out what you find.

~~Factor N~~

$\sqrt{N}$ divisions

10^{12} divisions per second

100 digit # 10^{100}

$\sqrt{N} \sim 10^{50}$

10^{50} divisions

$10^{50} / 10^{12} \text{ div/sec}$

$\sim 10^{38} \text{ seconds}$