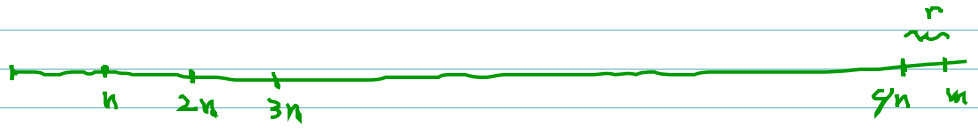
MTH 354 9-25-17

§5.1 Division in Integers

Division algorithm

Theorem 1: If $n, m \in \mathbb{Z}$ with $n > 0$, we can write $m = qn + r$ uniquely for some integers q and r with $0 \leq r < n$



$m = qn + r$ (q ↙, r ↙)

Ex: $n = 3$, $m = 16$. $16 = 3(5) + 1$

$n = 10$, $m = 3$, $3 = 10(0) + 3$

note: If in Theorem 1, $r = 0$, such that $m = qn$, Then we write $n \mid m$ (n divides m). If $m \neq qn$ (n does not divide m), then $n \nmid m$.

(In es, if $m = qn$, then $m \bmod n = 0$.)

notation: $n \mid m \Leftrightarrow m = qn$ ← divisor (factor)

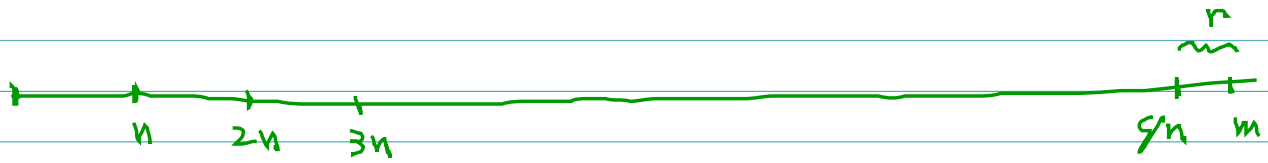
dividend (multiple) ↑ quotient

MTH 354 9-25-17

§ 5.1 Division in Integers

Division algorithm

Theorem 1: If $n, m \in \mathbb{Z}$ with $n > 0$, we can write $m = qn + r$ uniquely for some integers q and r with $0 \leq r < n$



$m = qn + r$

Ex: $n = 3$, $m = 16$. $16 = 3(5) + 1$ ($q = 5$, $r = 1$)

$n = 10$, $m = 3$, $3 = 10(0) + 3$

note: If in Theorem 1, $r = 0$, such that $m = qn$, Then we write $n \mid m$ (n divides m). If $m \neq qn$ (n does not divide m), then $n \nmid m$.

(In cs, if $m = qn$, then $m \bmod n = 0$.)

notation: $n \mid m \iff m = qn$ ← divisor (factor)

dividend (multiple) ↑ quotient

Theorem 2: Let a, b, and c be integers ($a, b, c \in \mathbb{Z}$)

a) If $a \mid b$ and $a \mid c$, then $a \mid b+c$
b) If $a \mid b$ and $a \mid c$, where $b > c$, then $a \mid b-c$
c) If $a \mid b$ or $a \mid c$, then $a \mid bc$
d) If $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity)
e) If $a \mid b$, then $a \mid bq$ for any $q \in \mathbb{Z}$.

Pf (c) Assume $a \mid b$ or $a \mid c$. Since $a \mid b$, we have $b = aq_1$ for some $q_1 \in \mathbb{Z}$. Since $a \mid c$, we have $c = aq_2$ for some $q_2 \in \mathbb{Z}$.
We need to show $a \mid bc$, i.e., $bc = a \cdot q$ for some $q \in \mathbb{Z}$.

Case 1: Suppose $a \mid b$, i.e. $b = aq_1$. Then
$bc = aq_1c = a(q_1c)$ where $q_1c \in \mathbb{Z}$ (closure of integers under multi)
Hence $a \mid bc$.

Case 2: Suppose $a \mid c$, i.e., $c = aq_2$. Then multiplying both sides of the equality by b, we get

$bc = aq_2b = a(q_2b)$ where $q_2b \in \mathbb{Z}$ (by closure of $\mathbb{Z}$ under).

* ∎

Defn: A positive integer p is called prime if the only positive integers that divide p are p and 1.

Q: How do we decide if N is a prime?
one method:
If $N = 2$, then N is prime otherwise
divide N by every integer from 2 to $N-1$.
If none of these is a divisor of N, then N is a prime.

A more efficient algo

If $x = mk$, i.e. x is not a prime number, then either m or $k \leq \sqrt{N}$. (otherwise $mk > N$)

Thus if N is not a prime, then it has a divisor k such that $1 < k \leq \sqrt{N}$. Therefore, we only need to examine numbers in that range. Furthermore if N has any even number as divisor, it must have 2 as a divisor. Hence after checking for divisibility by 2, we can skip all even integers

Algorithm: (5.1.18) Test if $N > 1$ is a prime

1. If $N = 2$, then N is prime
2. check if $N \mid 2$. If so N is not a prime, otherwise proceed to the next step
3. Compute $K = \lfloor \sqrt{N} \rfloor$
4. check whether $D \mid N$ where D is any odd integer between 1 and K, i.e. $1 < D \leq K$

#4)

Ex. $N = 637$

1. $637 \neq 2$ ✓
2. $2 \nmid 637$ ✓
3. $K = \lfloor \sqrt{637} \rfloor = 25$
4. $3 \nmid 637$, $5 \nmid 637$, $7 \mid 637$ terminate

output D - 7