Divisibility In The Integers

Recall: the integers $\mathbb{Z}$ consist of all elements of $\mathbb{N}$ along with 0 and the negatives of elements of $\mathbb{N}$.

Facts About the Integers

1) Just like S_n, $\exists$ a binary operation $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, i.e., the sum of any two integers is an integer.

2) The element 0 functions like e for S_n, in that $n + 0 = 0 + n = n \quad \forall\, n \in \mathbb{Z}$.

3) Much like inverses in S_n,

$n+(-n) = (-n)+n = 0$,

so every $n \in \mathbb{Z}$ has an additive inverse.

4) Addition is associative.

But unlike S_n...

5) $\exists$ a second binary operation

$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

6) Multiplication on $\mathbb{Z}$ is associative

7) $\forall\ k, m, n \in \mathbb{Z}$,

$$k \cdot (m+n) = k \cdot m + k \cdot n$$

$$(k+m) \cdot n = k \cdot n + m \cdot n$$

With properties 1) - 7), $\mathbb{Z}$ is an example of a ring.

We have more properties...

8) Addition and multiplication are commutative: $\forall\ n, m \in \mathbb{Z}$, $n+m = m+n$ and $n \cdot m = m \cdot n$

9) $\exists$ an identity element for multiplication, namely, the number 1: $1 \cdot n = n \cdot 1 = n$ $\forall\ n \in \mathbb{Z}$.

Note: Multiplicative inverses for elements of $\mathbb{Z}$ are almost never in $\mathbb{Z}$.

Definition: (divisibility) Let $m, n \in \mathbb{Z}$.

We say that m **divides** n, written "$m | n$", if $\exists\, q \in \mathbb{Z}$ (the **quotient** when dividing n by m) such that

$$\boxed{n = m \cdot q}$$

Proposition: (elementary divisibility results)

Let $m, n, k, a, b \in \mathbb{Z}$.

1) If $a \cdot b = 1$, then either $a = b = 1$ or $a = b = -1$.

2) If $a | b$ and $b | a$, then $a = \pm b$.

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

4) If $n \mid m$ and $n \mid k$, then if an element in $\mathbb{Z}$ has the form $am + bk$, then n divides this element.

proof: Note that, $\forall\ m \in \mathbb{Z}$,

$$0 \cdot m = (0+0) \cdot m$$

$$0 \cdot m = 0 \cdot m + 0 \cdot m.$$

Subtracting $0 \cdot m$ from both sides, we obtain that

$$0 \cdot m = 0.$$

Therefore, neither a nor b can be zero. If we consider the case where both a and and b are positive, then

$$1 = a \cdot b \geq \max\{a, b\} \geq 1$$

$$\Rightarrow \quad a = 1 = b.$$

Similarly,

$$1 = a \cdot b \Rightarrow |a\,b| = 1$$

So $|a| \cdot |b| = 1 \Rightarrow |a| = |b| = 1$.

Therefore either

$a = b = 1$ or $a = b = -1$.

2) If $a \mid b$, then $\exists\, s \in \mathbb{Z}$,

$b = as$, and if $b \mid a$,

$\exists\, t \in \mathbb{Z}$ with $a = bt$.

Then substituting,

$b = a \cdot s = (bt)s$, and

subtracting,

$b - (bt) \cdot s = 0$

Factoring out b,

$$b(1-ts)=0.$$

Therefore, either

$$b=0$$

or

$$1-ts=0.$$

If $b=0$, then

$$a=b\cdot t=0\cdot t=0.$$

If $1-ts=0$, then

$t=\pm 1$, so

either $a = b$ or $a = -b$.

3) If $m \mid n$ and $n \mid k$,

then $\exists$ integers s, t with

$n = s \cdot m$ and $k = t \cdot n$.

But then substituting,

$$k = t \cdot (s \cdot m) = (t \cdot s) \cdot m$$

$\Rightarrow m \mid k$.

4) If $n | m$ and $n | k$,

then $\exists$ $s, t \in \mathbb{Z}$,

$m = sn$ and $k = tn$.

We want to show that

n divides $am + bk$

for any $a, b \in \mathbb{Z}$.

But

$$am + bk = a(sn) + b(tn)$$

$$= (as)n + (bt)n$$

$$= (as + bt)n$$

Since $as+bt \in \mathbb{Z}$, we have that $n \mid (am+bk)$.

$\square$

Definition: (prime / composite) Let $p \in \mathbb{N}$. We say p is **prime** if whenever $p = m \cdot n$ with $m, n \in \mathbb{N}$, either $m = 1$ and $n = p$ or $n = 1$ and $m = p$. An element $k \in \mathbb{N}$ is called **composite** if k is not prime.

Proposition: (1/2 of the Fundamental Theorem of Arithmetic)

If $n \in \mathbb{N}$, $n > 1$,

then n is either prime or a product of primes.

proof: We proceed via induction.

If $n = 2$, then n is prime!

Now let $n > 2$ and suppose the result is true for all $k \in \mathbb{N}$, $2 \leq k < n$.

(Imagine $21{,}538{,}621{,}979 = n$)

Then either n is prime, in which case we are done, or n is composite. If n is composite,

$n = mt$ with $1 < m < n$ and $1 < t < n$. Using our inductive hypothesis, both m and t may be expressed as a product of prime numbers. Therefore, n may be expressed as a product of prime numbers.

$\square$