Divisibility and Modular Arithmetic

Definitions

1. Let $a, b \in \mathbb{Z}$ and $a \neq 0$. We say "a divides b" if there is $c \in \mathbb{Z}$ such that $b = ac$. We write $a \mid b$. If a does not divide b, then we write $a \nmid b$. (By definition, any nonzero integer divides 0.)

2. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. We say "a is congruent to b modulo m" if $m \mid a - b$. We write this as $a \equiv b \mod m$ or $a \equiv b \pmod{m}$. If a is not congruent to b, we write $a \not\equiv b \mod m$.

Exercises

1. If $a \mid bc$, is it the case that $a \mid b$ or $a \mid c$? What about $a \mid b + c$?

2. Let $m > 1$ be an integer. What is the cardinality of the set $\{x \mod m \mid x \in \mathbb{Z}\}$?

3. Is it true that $x \equiv y \pmod{m} \iff ax \equiv ay \pmod{m}$ for any integers $a, x, y \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$? If not, is either implication true (remember a biconditional is equivalent to two implications)?

4. Compute $5^{23001} \mod 6$. Compute $80^{40} \mod 21$.

Bases

Definitions

1. The *base b-representation* of an integer $m \in \mathbb{Z}$ is the unique representation of m in the form: $\sum_{i=0}^{k} a_i b^i$ where $k, a_i \in \mathbb{Z}_{\geq 0}$, $a_i < b$, and $a_k \neq 0$.

2. There are some special names for particular b. If $b = 2$, we call it binary; if $b = 10$, we call it decimal, and if $b = 16$, we call it hexadecimal.

Exercises

1. Express 74 in base 2. Express 27 in base 9.

2. Convert the binary number 10101 to base 4. Do the same for base 8. Can you guess a pattern?

Primes

Definitions

1. A positive integer greater than 1 is *prime* if its only factors are 1 and itself. Otherwise, if it has more factors, we call it *composite*.

2. A *prime factorization* of a positive integer n is a representation of n as a product of prime numbers.

3. The *Fundamental Theorem of Arithmetic* says that every positive integer greater than 1 has a unique prime factorization, up to reordering (i.e. $12 = 2^2 * 3 = 3 * 2^2$).

Exercises

1. Consider the theorem: Let $a, b \in \mathbb{Z}$ and let d be the largest integer dividing both a and b (we call d the *greatest common divisor* of a and b, and we write $d = \gcd(a, b)$). Then there are $x, y \in \mathbb{Z}$ such that $xa + yb = d$.

   Use this to prove the statement: Let p be a prime number. If $p \mid ab$ and $p \nmid a$ for $a, b \in \mathbb{Z}$, then $p \mid b$. Fill in the blanks in the proof below.

   Proof: Since $p \nmid a$, then $\gcd(p, a) =$ _____. Then we can use the supplied theorem to get integers x, y such that $xp + ya =$ _____. Now multiply both sides by b to get the equation $xpb + yab =$ _____. By assumption, $p \mid ab$, and $p \mid p$, so $p \mid (xpb + yab)$. Therefore p also divides the right hand side. Therefore, $p \mid$ _____, completing the proof.

2. The statement we proved above is equivalent to the following statement: Let p be a prime number. If $p \mid ab$, then $p \mid a$ or $p \mid b$. Can you see why? In English, this says that if a prime number divides a product of two numbers, then it must divide one of those numbers.