

2. Number Theory

Divisibility

An integer a is *divisible* by the integer b , written

$$b \mid a$$

if there exists some integer c , such that $a = bc$. Other ways to say this is that b *divides* a , or that b is a factor, or *divisor* of a . Divisibility is a binary relation (see Chapter 4) defined over \mathbb{Z} .

Basic properties

Every number divides itself, since $a = a \cdot 1$ for all a . We just let $c = 1$. This also means that 1 divides every integer, in which case we set $c = a$. If a divides b , and b divides c , then there are integers d and e , such that $b = ad$ and $c = be$. We then have $c = be = (ad)e = a(de)$, which means that a divides c . So if $a \mid b$ and $b \mid c$, then $a \mid c$. This property of a relation, known as *transitivity*, is discussed more in Chapter 4. Every number is also a divisor of zero, since $0 = a \cdot 0$.

Common Divisors and the GCD function

If a number a divides both b and c , then a is a *common divisor* of b and c . A number d is the *greatest common divisor*, or gcd, of b and c , when

- d is a common divisor of b and c , and
- if e is a common divisor of b and c , then e divides d .

That is, the gcd is the unique common divisor of two numbers which is divisible by any common divisor of those two numbers. For example, the divisors of 42 are $\{1, 2, 3, 6, 7, 14, 21, 42\}$ and the divisors of 24 are $\{1, 2, 3, 4, 6, 8, 12, 24\}$. The common divisors of 42 and 24 are the elements in the intersection of these two sets, viz., $\{1, 2, 3, 6\}$. Every element of this set is a divisor of 6. So the gcd of 42 and 24 is 6.

Prime numbers and coprimality

A number $p \geq 2$ whose only divisors are 1 and p itself is called a *prime* number.

Two integers whose gcd is equal to 1 are called *coprime*, or relatively prime.

For any given sequence of numbers $\{a_1, a_2, \dots, a_n\}$ we can find a number q that is relatively prime to every number a_i in the sequence.

First note that if $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.

then $b = ax$ and $c = ay$, so $b - c = ax - ay = a(x - y)$

Common Multiples and the LCM function

Euclidean Division

Basis Representation Theorem

Congruence and Modular Arithmetic

Euler's Totient Function

Euler's totient function, usually written as $\varphi(n)$, counts the number of positive integers up to n that are coprime (relatively prime) to n .

$$\varphi(n) = |\{k \in \mathbb{N} : \gcd(k, n) = 1\}|$$

| n | $\{k : \gcd(k, n) = 1\}$ | $\varphi(n)$ |
|-----|-------------------------------------|--------------|
| 1 | $\{1\}$ | 1 |
| 2 | $\{1\}$ | 1 |
| 3 | $\{1, 2\}$ | 2 |
| 4 | $\{1, 3\}$ | 2 |
| 5 | $\{1, 2, 3, 4\}$ | 4 |
| 6 | $\{1, 5\}$ | 2 |
| 7 | $\{1, 2, 3, 4, 5, 6\}$ | 6 |
| 8 | $\{1, 3, 5, 7\}$ | 4 |
| 9 | $\{1, 2, 4, 5, 7, 8\}$ | 6 |
| 10 | $\{1, 3, 7, 9\}$ | 4 |
| 11 | $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ | 10 |
| 12 | $\{1, 5, 7, 11\}$ | 4 |

Fermat's Little Theorem

$$a^p \equiv a \pmod{p}$$

for every prime number p and integer a .

Chinese Remainder Theorem