# Exploring Divisors

Discrete Mathematics 27100 Winter 2022

January 24, 2022

## 1 Divisibility and Divisors

**Definition 1.1** (Divisibility). *We say that $n$ is divisible by $a$ (which we write as $a \mid n$) if $\exists b \in \mathbb{Z}(ab = n)$. If so, we say that $a$ is a divisor of $n$ and $n$ is a multiple of $a$. If $n$ is not divisible by $a$ then we write that $a \nmid n$.*

**Remark 1.2.** *Note that by this definition, $0|0$. While Rosen and many other textbook authors make a special exception to say that $0$ is not divisible by $0$, following Professor Babai, we do not do so. However, it is important to note that $\frac{0}{0}$ is still undefined because there isn't a unique $b$ such that $0 * b = 0$.*

**Definition 1.3.** *Given $n \in \mathbb{Z}$, we define $Div(n) = \{a \in \mathbb{Z} : a|n\}$ to be the set of divisors of $n$.*

**Example 1.4.** $Div(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

**Example 1.5.** $Div(0) = \mathbb{Z}$

## 2 Positive Divisors of one Number

### 2.1 Finding divisors via the prime factorization of $n$

Q: How do we find the positive divisors of a natural number $n$? For example, what are the positive divisors of $36$?

A: We can first find the *prime factorization* of $n$ and then use this to find the positive divisors of $n$.

**Example 2.1.** *The prime factorization of $36$ is $36 = 2^2 \cdot 3^2$ and the positive divisors of $36$ are*

$$Div(36) \cap \mathbb{N} = \{2^a 3^b : a, b \in \mathbb{Z}, 0 \le a \le 2, 0 \le b \le 2\} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

*The positive divisors of $36$ can be represented visually as follows:*

| | $\times 1$ | $\times 2$ | $\times 4$ |
|---|---|---|---|
| $\times 1$ | 1 | 2 | 4 |
| $\times 3$ | 3 | 6 | 12 |
| $\times 9$ | 9 | 18 | 36 |

To write down the general pattern, let's go through each of these steps more carefully. We start with the definition of a prime number.

**Definition 2.2.** *We say that a natural number $p$ is a prime number if $p > 1$ and $Div(p) \cap \mathbb{N} = \{1, p\}$. Equivalently, a natural number $p$ is a prime number if $p > 1$ and $\forall d \in [2, p-1] \cap \mathbb{N}$, $d \nmid p$ (the only positive divisors of $p$ are $1$ and $p$).*

We now need the fact that every natural number has a unique prime factorization. While this fact is intuitive from our experience with numbers, it should not be taken for granted! This fact is actually the Fundamental Theorem of Arithmetic which we will prove in a few lectures.

**Theorem 2.3** (The Fundamental Theorem of Arithmetic)**.** *For all natural numbers $n$, there exists a unique prime factorization of $n$. More precisely, letting $p_1, p_2, p_3, \dots$ be the sequence of primes in ascending order, there exists a unique sequence $c_1, c_2, c_3, \dots$ of non-negative integers such that:*

1. *Only finitely many $c_i$ are nonzero.*
2. $n = \prod_{i=1}^{\infty} p_i^{c_i}$

**Remark 2.4.** *The Fundamental Theorem of Arithmetic can be stated as follows wihout using an infinite sequence or an infinite product:*

*For all $n \in \mathbb{N}$, there exists a unique $k \in \mathbb{N} \cup \{0\}$, primes $p_1, p_2, \dots, p_k$, and natural numbers $c_1, \dots, c_k$ such that*

1. $p_1 < p_2 < \dots < p_{k-1} < p_k$ *(the primes are listed in increasing order)*
2. $n = \prod_{i=1}^{k} p_i^{c_i}$

*We state the Fundamental Theorem of Arithmetic using an infinite sequence and an infinite product in order to avoid having to keep track of which primes divide each number.*

Using the Fundamental Theorem of Arithmetic, we can now write down the set of positive divisors of $n$ explicitly.

**Corollary 2.5.** *If the prime factorization of $n$ is $n = \prod_{i=1}^{\infty} p_i^{c_i}$ then*

$$Div(n) \cap \mathbb{N} = \left\{ \prod_{i=1}^{\infty} p_i^{a_i} : \forall i \in \mathbb{N}(a_i \in \mathbb{Z} \land 0 \leq a_i \leq c_i) \right\}$$

*Proof.* In order to prove this, we need to prove two things:

1. If $x \in \{\prod_{i=1}^{\infty} p_i^{a_i} : \forall i \in \mathbb{N}(a_i \in \mathbb{Z} \land 0 \leq a_i \leq c_i)\}$ then $x \mid n$. In other words, if the prime factorization of $x$ is $x = \prod_{i=1}^{\infty} p_i^{a_i}$ where $\forall i \in \mathbb{N}(0 \leq a_i \leq c_i)$ then $\exists y \in \mathbb{N}(xy = n)$.
2. If $x \notin \{\prod_{i=1}^{\infty} p_i^{a_i} : \forall i \in \mathbb{N}(a_i \in \mathbb{Z} \land 0 \leq a_i \leq c_i)\}$ then $x \nmid n$. In other words, if the prime factorization of $x$ is $x = \prod_{i=1}^{\infty} p_i^{a_i}$ where $a_j > c_j$ for some $j \in \mathbb{N}$ then for all $y \in \mathbb{N}(xy \neq n)$.

For the first statement, we can take $y = \prod_{i=1}^{\infty} p_i^{c_i - a_i}$. Now

$$xy = \prod_{i=1}^{\infty} p_i^{a_i} p_i^{c_i - a_i} = \prod_{i=1}^{\infty} p_i^{c_i} = n$$

For the second statement, given $y \in \mathbb{N}$, let $y = \prod_{i=1}^{\infty} p_i^{b_i}$ be the prime factorization of $y$. Now

$$xy = \prod_{i=1}^{\infty} p_i^{a_i} p_i^{b_i} = \prod_{i=1}^{\infty} p_i^{a_i + b_i}$$

Since $a_j > c$ and $b_j \geq 0$, $a_j + b_j > c_j$. Since the prime factorization of $n$ is unique and $a_j + b_j \neq c_j$, $xy \neq n$, as needed. ☐

## 2.2 Number of Positive Divisors and Sum of Positive Divisors

Q: How many positive divisors does $n$ have?

**Corollary 2.6.** *If the prime factorization of $n$ is $n = \prod_{i=1}^{\infty} p_i^{c_i}$ then $|Div(n) \cap \mathbb{N}| = \prod_{i=1}^{\infty} (c_i + 1)$.*

*Proof.* Recall that

$$Div(n) \cap \mathbb{N} = \left\{ \prod_{i=1}^{\infty} p_i^{a_i} : \forall i \in \mathbb{N}, a_i \in \mathbb{Z} \text{ and } 0 \leq a_i \leq c_i \right\}$$

Choosing a positive divisor of $n$ is equivalent to choosing a non-negative integer $a_i$ between $0$ and $c_i$ for each $i \in \mathbb{N}$. For each $i \in \mathbb{N}$ there are $c_i + 1$ choices for $a_i$ and all of these choices are independent so the total number of choices is $\prod_{i=1}^{\infty} (c_i + 1)$, as needed. ☐

**Example 2.7.** *If $n = 48$ then the prime factorization of $n$ is $n = 2^4 \cdot 3^1$ so there are $(4+1)(1+1) = 10$ positive divisors of $n$. Indeed, $Div(48) \cap \mathbb{N} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48\}$.*

Q: What is the sum of the positive divisors of $n$?

Answer: If the prime factorization of $n$ is $n = \prod_{i=1}^{\infty} p_i^{c_i}$ then $\sum_{x \in Div(n) \cap \mathbb{N}} x = \prod_{i=1}^{\infty} \left( \sum_{j=0}^{c_i} p_i^j \right)$

**Example 2.8.**
*Q: What is the sum of the positive divisors of $28$?*
*Answer: The prime factorization of $28$ is $2^2 \cdot 7^1$ so the sum of the positive divisors of $28$ is $(1+2+4)(1+7) = 7 \cdot 8 = 56$. Indeed, $Div(28) \cap \mathbb{N} = \{1, 2, 4, 7, 14, 28\}$ and $1+2+4+7+14+28 = 56$*

*Q: What is the sum of the positive divisors of $30$?*
*Answer: The prime factorization of $30$ is $2^1 \cdot 3^1 \cdot 5^1$ so the sum of the positive divisors of $30$ is $(1+2)(1+3)(1+5) = 3 \cdot 4 \cdot 6 = 72$. Indeed, $Div(30) \cap \mathbb{N} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and $1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72$*

## 3 Perfect numbers

**Definition 3.1.** *We say that $n$ is a perfect number if $\sum_{d \in Div(n) \cap \mathbb{N}} d = 2n$. In other words, $n$ is a perfect number if the sum of all of the positive divisors of $n$ except for $n$ is equal to $n$.*

**Example 3.2.** $n = 6$ *is a perfect number because the positive divisors of* $6$ *are* $\{1, 2, 3, 6\}$ *and* $1 + 2 + 3 = 6$.

Q: Can we find other perfect numbers?

A: As we saw above, $28 = 2^2 \cdot 7$ is a perfect number because $(1+2+4)(7+1) = 56 = 2 \cdot 28$. Similarly, $496 = 2^4 \cdot 31$ is a perfect number because $(1+2+4+8+16)(31+1) = 31 \cdot 32 = 2 \cdot (16 \cdot 31) = 2 \cdot 496$.

Indeed, there is a pattern here. The following theorem is well-known:

**Theorem 3.3.** *If $n$ is an even perfect number then $n$ has the form $2^{k-1}(2^k - 1)$ where $p = 2^k - 1$ is prime. Note: Primes of the form $p = 2^k - 1$ are called Mersenne primes.*

Challenge: Can you prove this theorem (or at least see why it is true)?

**Remark 3.4.** *It is also well-known that $2^k - 1$ can only be prime if $k$ is prime. Can you see why?*

Open problem: Are there any odd perfect numbers?

## 4 The greatest common divisor

Q: What is $Div(n) \cap Div(m)$? For example, what is $Div(60) \cap Div(105)$?

A: If we write out the divisors of $60$ and $105$ we see that

1. $Div(60) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$
2. $Div(105) = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 15, \pm 21, \pm 35, \pm 105\}$

so $Div(60) \cap Div(105) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$. Observe that $Div(60) \cap Div(105) = Div(15)$. As the reader has likely guessed, this is not a coincidence.

**Definition 4.1.** *Given $x, y \in \mathbb{Z}$ such that $x \neq 0$ or $y \neq 0$, we define the greatest common divisor of $x$ and $y$ (which we write as $gcd(x, y)$) to be $gcd(x, y) = max\{d : d \in Div(x) \cap Div(y)\}$*

**Example 4.2.** $gcd(60, 105) = 15$

**Theorem 4.3.** *For all $x, y \in \mathbb{N}$, letting $x = \prod_{i=1}^{\infty} p_i^{a_i}$ and $y = \prod_{i=1}^{\infty} p_i^{b_i}$ be the prime factorizations of $x$ and $y$,*

1. $Div(x) \cap Div(y) = \{\pm \prod_{i=1}^{\infty} p_i^{c_i} : \forall i \in \mathbb{N}(c_i \in \mathbb{Z} \wedge 0 \leq c_i \leq min\{a_i, b_i\})\}$
2. $gcd(x, y) = \prod_{i=1}^{\infty} p_i^{min\{a_i, b_i\}}$

*Proof.* By Corollary 2.5

$$Div(x) = \left\{ \pm \prod_{i=1}^{\infty} p_i^{c_i} : \forall i \in \mathbb{N}(c_i \in \mathbb{Z} \wedge 0 \leq c_i \leq a_i) \right\}$$

and

$$Div(y) = \left\{ \pm \prod_{i=1}^{\infty} p_i^{c_i} : \forall i \in \mathbb{N}(c_i \in \mathbb{Z} \wedge 0 \leq c_i \leq b_i) \right\}$$

Looking at which elements are in both $Div(x)$ and $Div(y)$, we see that

$$Div(x) \cap Div(y) = \left\{ \pm \prod_{i=1}^{\infty} p_i^{c_i} : \forall i \in \mathbb{N}(c_i \in \mathbb{Z} \wedge 0 \leq c_i \leq min\{a_i, b_i\}) \right\}$$

The largest element of $Div(x) \cap Div(y)$ is $\prod_{i=1}^{\infty} p_i^{min\{a_i, b_i\}}$ so $gcd(x, y) = \prod_{i=1}^{\infty} p_i^{min\{a_i, b_i\}}$. □

**Example 4.4.** *The prime factorization of* $60$ *is* $60 = 2^2 \cdot 3^1 \cdot 5^1$ *and the prime factorization of* $105$ *is* $3^1 \cdot 5^1 \cdot 7^1$ *so* $gcd(60, 105) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15$.

**Corollary 4.5.** *For all* $x, y \in \mathbb{N}$, $Div(x) \cap Div(y) = Div(gcd(x, y))$

**Remark 4.6.** *Professor Babai defines a greatest common divisor of* $x$ *and* $y$ *to be an integer* $d$ *such that* $Div(x) \cap Div(y) = Div(d)$ *and defines* $gcd(x, y) = |d|$ *where* $d$ *is a greatest common divisor of* $x$ *and* $y$. *With this definition, we have* $gcd(0, 0) = 0$, *which is elegant. However, since the definitions only differ on* $gcd(0, 0)$, *we will stick to the more direct defintion that* $gcd(x, y)$ *is the largest element in* $Div(x) \cap Div(y)$