Divisors, prime numbers

Number theory

Application of discrete models

Number theory deals mainly with integers ($\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$), and sometimes with its subset, the natural numbers ($\mathbb{N} = \{0, 1, 2, \ldots\}$).

1 Divisors

Definition 1.1. $a \in \mathbb{Z}$ is a *divisor* of $b \in \mathbb{Z}$ if $\exists c \in \mathbb{Z} : b = ac$. Notation: $a \mid b$. Notation of negation: $a \nmid b$. We also say that a *divides* b, b is *divisible* by a, or b is a multiple of a.

For example 2 is a divisor of 6, because $6 = 2 \cdot 3$.

(Note: although it is called "divisor", we define it using multiplication, not division. This is because multiplication is a simpler operation, and also because it allows us to remain completely inside $\mathbb{Z}$. This will make it possible to extend divisibility to other structures which may not have division at all. Also note that by the above definition, 0 is a divisor of 0. Therefore, naive "definitions" like "a is a divisor of b if b/a is an integer" would not be equivalent to the actual definition.)

Some properties of divisibility:

1. reflexivity: $\forall a \in \mathbb{Z} : a \mid a$ (each number divides itself);
2. $\forall a \in \mathbb{Z} : a \mid 0$ (each number divides 0);
3. $\forall a \in \mathbb{Z} : 1 \mid a$ (1 divides each number);
4. $\forall a \in \mathbb{Z} : 0 \mid a \iff a = 0$ (only 0 divides 0);
5. transitivity: $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ b \mid c \implies a \mid c$;
6. antisymmetry in $\mathbb{N}$: $\forall a, b \in \mathbb{N} : a \mid b \ \wedge \ b \mid a \implies a = b$;
7. $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ a \mid c \implies a \mid b + c$ (if a divides both terms, then it also divides the sum);
8. $\forall a, b, c \in \mathbb{Z} : a \mid b \ \wedge \ a \mid c \implies a \mid b - c$;
9. $\forall a, b, c, d \in \mathbb{Z} : a \mid b \ \wedge \ c \mid d \implies ac \mid bd$;
10. $\forall a, b \in \mathbb{N}^+ : a \mid b \implies a \leq b$.

Related notions:

Definition 1.2. $a \in \mathbb{N}$ is a *proper divisor* of $b \in \mathbb{N}$ if it is a divisor, and $a \neq b$.

Definition 1.3. The *trivial divisors* of $b \in \mathbb{Z}$ are 1, -1, b and $-b$.

For example in $\mathbb{N}$, the divisors of 6 are $1, 2, 3, 6$; the proper divisors are $1, 2, 3$; and the nontrivial divisors are $2, 3$.

We have seen that the divisibility relation is antisymmetric in $\mathbb{N}$, so it is also a partial order (= reflexive + antisymmetric + transitive). Is it true in $\mathbb{Z}$ too? First, introduce another notion:

Definition 1.4. a and b are *associates* if $a \mid b$ and $b \mid a$.

In $\mathbb{N}$, only the equal numbers are associates. In $\mathbb{Z}$ however, a and b are associates if and only if $a = b$ or $a = -b$, i.e. it is not only the equals, but also the negatives.

By comparing the definitions of associates and antisymmetry, we can see that the divisibility relation is antisymmetric (and hence a partial order) if and only if the equal numbers are the only associates, so it is true in $\mathbb{N}$, but not in $\mathbb{Z}$.
(Note that in $\mathbb{N}$, the divisibility as a partial order usually "orders" the elements in the same way as the natural order ($\leq$) – see the last property above –, but not always: the exception is 0, which is the smallest element of $\mathbb{N}$, but it is the "largest" by the divisibility as a partial order, because every integer divides 0.)
Why are associates interesting? If two numbers are associates, then they behave in exactly the same way regarding divisibility. For example, $2 \mid 6$ implies $2 \mid -6$, $-2 \mid 6$ and $-2 \mid -6$. Therefore, it is usually sufficient to deal with only one of each associate pair, e.g. we can deal with only $\mathbb{N}$ instead of the whole $\mathbb{Z}$.
(Note: we still don't see why the name "associate" is necessary, instead of just calling them "numbers with the same magnitude". But later, when we generalize divisibility to other structures, associates will be a separate concept, independent from sign and magnitude.)
Here are the most important operations of Sage regarding division and divisors:

`a / b`	division (with fractional result)	`36 / 10 == 18/5`
`a // b`	quotient of integer division	`36 // 10 == 3`
`a % b`	remainder of integer division	`36 % 10 == 6`
`a.quo_rem(b)`	quotient and remainder in a tuple	`36.quo_rem(10) == (3, 6)`
`a.divides(b)`	does a divide b?	`5.divides(10) == True`
`divisors(a)`	list of positive divisors of a	`divisors(12) == [1,2,3,4,6,12]`

2 Prime numbers

Definition 2.1. $n \in \mathbb{N}$ is a *prime number* if $n > 1$ and it has only trivial divisors.
In other words: n is a prime number if it has exactly two positive divisors (1 and n).
The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.
Definition 2.2. $n \in \mathbb{N}$ is a *composite number* if $n > 1$ and it is not a prime number.
Note: 1 is neither prime nor composite. The reason behind this will be explained later, after the fundamental theorem of arithmetic.
Prime numbers have a property that could be used as a definition:
Theorem 2.3. *$n \in \mathbb{N}$ is a prime number if and only if $n > 1$ and $\forall a, b \in \mathbb{N} : n \mid ab \implies n \mid a \vee n \mid b$.*
This means that if a prime number divides a product, then it also divides one of its factors (e.g. $5 \mid 7 \cdot 10$, and indeed, $5 \mid 10$), but for composite numbers, this is not true for all products (e.g. $6 \mid 4 \cdot 9$, but $6 \nmid 4$ and $6 \nmid 9$).
(The direction of the theorem that it's not true for composite numbers can be proven easily: then n, by definition, has nontrivial divisors, i.e. $n = ab$ for some $1 < a, b < n$. Then of course $n \mid ab$ is also true, but neither $n \mid a$ nor $n \mid b$ is. The other direction is slightly more difficult, so it is omitted, but it can be proven using the fundamental theorem of arithmetic.)
Some Sage operations related to prime numbers:

`is_prime(n)`	is n a prime number?	`is_prime(7) == True`
`next_prime(n)`	next prime after n	`next_prime(1000) == 1009`
`previous_prime(n)`	previous prime before n	`previous_prime(1000) == 997`
`nth_prime(n)`	n^{th} prime number (from $n = 1$)	`nth_prime(3) == 5`
`primes_first_n(n)`	list of first n primes	`primes_first_n(4) == [2,3,5,7]`

Now let's see how to determine whether a number $n \in \mathbb{N}$ is a prime (without using the above functions).

The simplest method is *trial division*, i.e. to check for all numbers between 2 and $n-1$ if they divide n. This method can be improved in multiple ways:

1. There is no need to go as far as $n-1$, we can stop after $n/2$, because this is the largest possible proper divisor of n. This already halves the running time.
2. An even better limit is to stop after $\sqrt{n}$. This works because for each divisor k, there is another divisor, n/k, and if $k > \sqrt{n}$, then $n/k < \sqrt{n}$, so we have already found n/k before k.
3. We can step by two: if we check that 2 doesn't divide n, then we only need to check the odd numbers.
4. This logic can be improved by first checking 2 and 3, and then stepping by 6 ($= 2 \cdot 3$), checking only the numbers $6k + 1$ and $6k + 5$, because others are divisible by 2 or 3.

2.1 Number of primes

Now examine the question that how many prime numbers there are. First:

Theorem 2.4. *There are infinitely many prime numbers.*

(Proof: assume that there are only finitely many primes, for example $p_1, p_2, p_3, \ldots, p_n$. Then calculate the following number: $p_1 p_2 p_3 \ldots p_n + 1$. It cannot be prime, because it is greater than all assumed prime numbers, but it cannot be composite either, because none of our prime numbers divide it – so we reached a contradiction, meaning that there are really infinitely many prime numbers.)

This answers the question *mathematically* that how many primes there are, but it's still not the full picture. For example, both the natural numbers and the powers of two $(1, 2, 4, 8, 16, \ldots)$ are infinitely many, but the latters are much rarer. To formalize this, we can ask how many numbers of a certain kind (e.g. prime) there are between 1 and n. For example, there are n natural numbers, $\lfloor n/2 \rfloor$ even numbers, and $\lfloor \log_2 n \rfloor + 1$ powers of two (which is very few, e.g. for $n = 1000000$, it's only 20). For prime numbers, this is denoted as follows:

Definition 2.5 (Prime-counting function)**.** Let $\pi(n)$ be the number of prime numbers between 1 and n (inclusive).

For example $\pi(7) = 4$, because there are four prime numbers up to 7: $2, 3, 5, 7$.

The exact value of $\pi(n)$ cannot be expressed by a simple formula, but there is a simple approximation:

Theorem 2.6 (Prime number theorem)**.** $\pi(n) \approx \dfrac{n}{\ln n}$, *more precisely:* $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n/\ln n} = 1$.

In other words, the probability that a number between 1 and n is a prime is ca. $1/\ln n$. For example from 1 to 100, one quarter of the numbers are primes ($\pi(100) = 25$, and $\ln 100 \approx 4{,}6$), and to 1000000, it's ca. one thirteenth ($\ln 1000000 \approx 13{,}8$).

In Sage, $\pi(n)$ is called `prime_pi(n)`. The following code plots $\pi(n)$ and its approximation from 1 to 1000 ($\pi(n)$ is the upper, stepped line):

```
sage: var("n"); plot([n/ln(n), prime_pi], (1, 1000))
```

2.2 Twin primes

Another interesting question about prime numbers is how close they can be to each other. The closest ones are 2 and 3, because all other primes are odd, so their distance must be even. Other than that, the closest primes have a special name:

Definition 2.7. A prime number p is a *twin prime* if $p-2$ or $p+2$ is also a prime number. These two primes are collectively called a *twin prime pair*.

For example, $(3,5)$ and $(17,19)$ are twin prime pairs. There is also a *prime triplet*: $(3,5,7)$, but this is the only one (since one of them must be divisible by 3).

We have seen that there are infinitely many prime numbers. Is it true for twin primes? The answer is: we don't know. Mathematicians haven't yet found an answer to this question. (But the conjecture is that they are infinitely many.)

2.3 Prime factorization

Why are the prime numbers important? This is best explained by the following theorem.

Theorem 2.8 (Fundamental theorem of arithmetic)**.** *All positive integers can be written* ***uniquely*** *as a product of prime numbers, up to the order of the factors.*

For example $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

Definition 2.9. The product in the above theorem is called the *prime factorization* of the number.

The word "uniquely" is crucial in the theorem, i.e. it can't happen that different prime factorizations yield the same number, e.g. $2 \cdot 7 \neq 3 \cdot 5$. But it can happen that the same prime factors are written in a different order, e.g. $30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3$, but these two factorizations are "essentiallly" the same, this is what "up to the order of the factors" means. Complete uniqueness can be achieved by fixing the order of the factors, e.g. by requiring increasing order. For brevity, the same prime factors next to each other can be written as a power. This representation has a name:

Definition 2.10. The *canonical representation* of a positive integer n is $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$, where $p_1 < p_2 < \ldots < p_k$ are prime numbers, and n_i's are positive integers. It is also called the *standard form* of n.

As discussed above, this representation is unique.

For example, the canonical representation of 360 is $2^3 \cdot 3^2 \cdot 5$.

The fundamental theorem of arithmetic shows why the prime numbers are important: they are the "building blocks" of positive integers, i.e. each positive integer can be split into those. (Note: the prime numbers are not exceptions to this rule, since they can be written as a product of *one* prime number, i.e. itself, e.g. $13 = 13$. Neither is 1 excluded, which can be treated as a product of *zero* prime numbers, according to the mathematical convention that the value of an empty product is 1, i.e. $1 = \prod_{i=1}^{0} p_i^{n_i}$, like for example $0! = 1$.)

The theorem also shows why 1 is not defined to be a prime number: because it is not a real "building block", since multiplying by 1 doesn't change the number; if it were a prime number, it would break the uniqueness of the factorization, e.g. $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$ etc.
In Sage, the function `factor()` calculates the prime factorization of a number:

```
sage: factor(360)    # vagy: 360.factor()
2^3 * 3^2 * 5
```

The result of `factor()` is a `Factorization` object, which can behave like a sequence, e.g. it can be iterated through by a `for` loop, where the elements are the (p_i, n_i) pairs:

```
sage: for (p, n) in factor(360):
....:     print(f"prime: {p}, exponent: {n}")
prime: 2, exponent: 3
prime: 3, exponent: 2
prime: 5, exponent: 1
```

Note: for large numbers, prime factorization is a very difficult task. So difficult, that certain cryptographic systems (e.g. RSA, as we'll see later) are based on the assumption that nobody will be able to find the secret prime factors of a huge number.

2.4 Sieve of Eratosthenes

How can we find all prime numbers up to a given n?
The naive solution is to check all numbers individually for whether they are prime. But this is not very efficient, because it does a lot of redundant work (for example if we checked that a number is divisible by 13, then we don't have to check the same for the next 12 numbers).
A better solution is the sieve of Eratosthenes: write down all numbers from 2 to n, and systematically cross out all composite numbers using the already discovered prime numbers. The first prime number is 2, so cross out all other even numbers, because they are composite. The next prime is 3, so cross out all other multiples of 3. 4 is already crossed out, so it is not a prime. The next untouched number is 5, so it is a prime, so cross out all other multiplies of 5, and so on. After doing all this, the remaining numbers are exactly the prime numbers.
For example, here is the first few steps of the sieve for $n = 25$:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~	21	~~22~~	23	~~24~~	25
2	**3**	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	25
2	3	~~4~~	**5**	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~

The algorithm can be improved in a few ways:

1. We can stop the algorithm after reaching $\sqrt{n}$ with the primes, because the multiples of greater primes were already crossed out by smaller primes. (So in the above example, we could indeed stop after 5. For example, the multiples of 7 were already crossed out: 14 was crossed out by 2, and 21 by 3.)
2. For a given prime p, we don't have to start from $2p$, only from p^2. Why? Because all multiples of p between p and p^2 have a smaller prime factor than p, so they were already crossed out. (For example, we didn't have to cross out 15 for 5, as it was already done for 3.)

So the steps of the sieve of Eratosthenes are as follows:

1. Create a list from 2 to n, containing only boolean `True` values.
2. For each i from 2 while $i^2 \leq n$:
   - If the i^{th} element of the list is `True`, then:
     - For each j from i^2 up to n, stepping by i (i.e. $j = i^2,\ i^2 + i,\ i^2 + 2i,\ \ldots$):
       - Set the j^{th} element of the list to `False`.
3. The indices of the remaining `True` elements in the list are the prime numbers.

Warning: pay attention to the indexing, as Sage starts the list from 0, but the algorithm starts it from 2. To match them, either subtract 2 from each index, or start the list from 0, and set the 0^{th} and 1^{st} elements immediately to `False`.

It can be proven that the sieve takes approximately $n \log \log n$ steps, which is much better than individual trial division for each number, which would take $n\sqrt{n}$ steps.

3 Divisor-related functions

Let's see a few more interesting notions about divisors. For example:

Definition 3.1. Let $\tau(n)$ be the number of positive divisors of $n \in \mathbb{N}^+$.

For example, $n = 6$ has 4 positive divisors: 1, 2, 3 and 6, therefore $\tau(6) = 4$.

The first few values of this function:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6	2	6

The value of $\tau(n)$ clearly distinguishes between prime numbers, composite numbers and 1:

- $\tau(1) = 1$,
- $\tau(n) = 2$ if n is prime, and
- $\tau(n) \geq 3$ if n is composite.

How can we calculate $\tau(n)$? The most trivial but least effective method is to simply count the divisors of n. But if we know the prime factorization of n, we have a much better solution:

Theorem 3.2. *If the canonical representation of n is $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, then $\tau(n) = (n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$.*

For example $360 = 2^3 \cdot 3^2 \cdot 5$, so $\tau(360) = (3 + 1)(2 + 1)(1 + 1) = 24$.

(Proof: any m divisor of n can have only the same prime factors than n, and they can appear only at most as many times as in n. Therefore, we can write $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where p_i's are the same prime factors, and $0 \leq m_i \leq n_i$ for each m_i. To count how many such m exists, take the number of possible ways each m_i can be chosen, which is $n_i + 1$ (since they are between 0 and n_i), and multiply them, i.e. $(n_1+1)(n_2+1)\cdots(n_k+1)$. But how do we know that all these possibilities really give different divisors? From the fundamental theorem of arithmetic, which states that the prime factorization is unique.)

Note: most values of $\tau(n)$ are even. Why is that so? Because the divisors usually come in pairs: if $k \mid n$, then $\frac{n}{k} \mid n$. The only exception is if the pair of k is k itself, i.e. $k = \frac{n}{k}$, which can be rearranged as $k^2 = n$. Therefore:

Theorem 3.3. *$\tau(n)$ is odd if and only if n is a square number.*

Here is another interesting arithmetic function:

Definition 3.4. Let $\sigma(n)$ be the sum of positive divisors of $n \in \mathbb{N}^+$.

For example for $n = 6$, $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

The first few values of this function:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20	42

The value can also be calculated from the prime factorization:

Theorem 3.5. *If the canonical representation of n is $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, then* $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{n_i+1} - 1}{p_i - 1}$.

In Sage, $\sigma(n)$ is called `sigma(n)`, and $\tau(n)$ is called `number_of_divisors(n)`.

Sometimes a variant of $\sigma(n)$ is used, where n itself is excluded from the divisors:

Definition 3.6 (Aliquot sum)**.** Let $s(n)$ be the sum of proper divisors of $n \in \mathbb{N}^+$.

In other words: $s(n) := \sigma(n) - n$.

This function is used to define certain interesting properties of numbers:

Definition 3.7. $n \in \mathbb{N}^+$ is a *perfect number* if $s(n) = n$.

For example, 6 is a perfect number, because $s(6) = 1 + 2 + 3 = 6$.

(Note: we don't know whether there are infinitely many perfect numbers.)

Definition 3.8. $a \in \mathbb{N}^+$ and $b \in \mathbb{N}^+$ are *amicable numbers* if $s(a) = b$ and $s(b) = a$.

For example, 220 and 284 are amicable numbers, because $s(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$ and $s(284) = 1 + 2 + 4 + 71 + 142 = 220$.

4 Author

These lecture notes were written by Uray M. János, partially using Nagy Ádám's notes in Hungarian:
https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
Please report errors and suggestions here: uray.janos@inf.elte.hu.