Divisors, prime numbers

Application of discrete models

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

1 Division with remainder

There are four fundamental operations ($+$, $-$, $\cdot$, $/$), but only three of them work completely within the set of integers, because division does not always produce an integer, e.g. $2/3 \notin \mathbb{Z}$.

Therefore, we need another operation: **division with remainder** (also known as **Euclidean division**), which always stays within $\mathbb{Z}$ (for nonzero divisors). It is based on the following theorem:

Theorem 1.1 (Division theorem)**.** *If $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exist unique $q, r \in \mathbb{Z}$ for which $a = qb + r$ and $0 \leq r < |b|$.*

Definition 1.2. In the above theorem, q is the **quotient** of a and b (notation: $a \operatorname{div} b$), and r is the **remainder** (notation: $a \bmod b$). Calculating q and r is called **division with remainder**.

Example. If $a = 36$ and $b = 10$, then the quotient is $q = 3$, and the remainder is $r = 6$, because $36 = 3 \cdot 10 + 6$ and $0 \leq 6 < 10$. We can also write that $36 \operatorname{div} 10 = 3$ and $36 \bmod 10 = 6$.

Example. If $a = -36$ and $b = 10$, then $q = -4$ and $r = 4$. (But not $q = -3$ and $r = -6$, because the theorem requires r to be nonnegative.)

In Sage, the quotient operation is denoted by a double slash (`//`), and the remainder is denoted by a percent sign (`%`):

```
sage: 36 // 10
3
sage: 36 % 10
6
```

The two results can also be calculated at once (more efficiently than separately):

```
sage: divmod(36, 10)
(3, 6)
```

Attention: avoid regular division (`/`) for integers, because the type of the result is not `Integer`, but `Rational`, even if the result is mathematically an integer. This can lead to problems, so it's better to always use division with remainder (`//`), which gives an `Integer`. For example:

```
sage: 36 / 10
18/5                # not an integer
sage: 30 / 10
3                   # looks like an integer...
```

```
sage: type(30 / 10)
<class 'sage.rings.rational.Rational'>  # but its type is not Integer!
sage: type(30 // 10)
<class 'sage.rings.integer.Integer'>    # now it's Integer
sage: # The type is important, e.g. "prime" is meaningless for rational numbers:
sage: (30 / 10).is_prime()
False
sage: (30 // 10).is_prime()
True
```

2 Divisors

Definition 2.1. $a \in \mathbb{Z}$ is **divisible** by $b \in \mathbb{Z}$ if $\exists c \in \mathbb{Z} : a = bc$. Notation: $b \mid a$. Notation of the negation: $b \nmid a$. It is also said that b is a **divisor** of a, b **divides** a, or a is a **multiple** of b.

Example. 6 is divisible by 2 (2 is a divisor of 6), because $6 = 2 \cdot 3$.

(Note: even though it is called "divisibility", it is defined in terms of 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.)

Notice that by the above definition, 0 is divisible by 0 (this convention will be useful later), so it is not true that "a is divisible by b if a/b is an integer". This is only true under the assumption that $b \neq 0$. A similar statement is true for division with remainder:

Theorem 2.2 (relation of divisibility to division and division with remainder)**.**
If $a, b \in \mathbb{Z}$ and $\boldsymbol{b \neq 0}$, then:

1. $b \mid a \iff a/b \in \mathbb{Z}$;
2. $b \mid a \iff a \bmod b = 0$.

Theorem 2.3 (properties of divisibility)**.**

1. *reflexivity:* $\forall a \in \mathbb{Z} : a \mid a$ *(every number divides itself);*
2. $\forall a \in \mathbb{Z} : a \mid 0$ *(every number divides* 0*);*
3. $\forall a \in \mathbb{Z} : 1 \mid a$ *(*1 *divides every number);*
4. $\forall a \in \mathbb{Z} : 0 \mid a \iff a = 0$ *(*0 *divides only* 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 it 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 2.4. $b \in \mathbb{N}$ is a **proper divisor** of $a \in \mathbb{N}$ if it is a divisor, and $b \neq a$.

Definition 2.5. The **trivial divisors** of $a \in \mathbb{Z}$ are 1, -1, a and $-a$.

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 $2, 3$.

In Sage, we can use the following divisibility-related operations:

```
sage: 5.divides(10)
True
sage: 5.divides(12)
False
sage: 0.divides(0)
True
sage: divisors(12)   # list of positive divisors
[1, 2, 3, 4, 6, 12]
sage: # Using division with remainder (for nonzero divisor):
sage: 10 % 5 == 0
True
sage: 12 % 5 == 0
False
sage: 0 % 0 == 0
[...]
ZeroDivisionError: Integer modulo by zero
```

Another related notion:

Definition 2.6. 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. not only the equals, but also the negatives are associates.

Why are associates interesting? If two numbers are associates, then they behave in exactly the same way regarding divisibility, e.g. $2 \mid 6 \implies 2 \mid -6,\ -2 \mid 6,\ -2 \mid -6$. Therefore, we can usually deal with only one of each associate pair, e.g. we can deal with only $\mathbb{N}$ instead of the whole $\mathbb{Z}$.

(Note: it is still not clear 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.)

Associatedness is an equivalence relation, i.e. it is reflexive, symmetric and transitive.

We have seen in the above list of properties that divisibility is antisymmetric in $\mathbb{N}$, and therefore it is also a partial order (= reflexive + antisymmetric + transitive). But why was it stated specifically for $\mathbb{N}$? By comparing the definitions of associatedness 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 $\mathbb{N}$, divisibility as a partial order usually "orders" numbers 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" according to the divisibility as a partial order, because every integer divides 0.)

3 Prime numbers

Definition 3.1. $n \in \mathbb{N}$ 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).

Example. The first few prime numbers are: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \ldots$.

Definition 3.2. $n \in \mathbb{N}$ 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.

Sage has several prime-related functions:

```
sage: is_prime(7)          # or: 7.is_prime()
True
sage: next_prime(1000)
1009
sage: previous_prime(1000)
997
sage: nth_prime(4)         # fourth prime number
7
sage: primes_first_n(4)    # the first 4 prime numbers
[2, 3, 5, 7]
sage: prime_range(20)      # like range(), but for prime numbers
[2, 3, 5, 7, 11, 13, 17, 19]
sage: prime_range(10, 20)
[11, 13, 17, 19]
sage: random_prime(1000)   # random prime number between 2 and 1000
193
sage: random_prime(1000, lbound=500)   # between 500 and 1000
613
```

Now consider the following question: what digits can prime numbers end with? With the exception of $p = 2$, prime numbers can only end with odd numbers, otherwise they would be divisible by 2. Similarly, except for $p = 5$, prime numbers cannot end with 5, or they would be divisible by 5. So the possible last decimal digits of the prime numbers $p \geq 7$ are: 1, 3, 7 and 9.

Definition 3.3. 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**.

Example. The first few twin prime pairs: $(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), \ldots$.

3.1 Trial division

How can we determine whether a given $n \in \mathbb{N}$ is a prime number – without using Sage functions? The simplest method is *trial division*, i.e. to check all possible numbers whether they divide n.

But what are the "possible numbers"? Since 1 and n are always divisors, and there are no divisors above n, the simplest method is to check all numbers from 2 to $n-1$ whether they divide n. But for large n, this method takes a very long time. Can we do better?

First, we don't need to go as far as $n-1$, we can stop after $n/2$ (more precisely $\lfloor n/2 \rfloor$), because a proper divisor cannot be greater than that. This already halves the running time.

But it is even better to stop at $\sqrt{n}$. This works because each divisor k has a pair, n/k, so that if $k > \sqrt{n}$, then $n/k < \sqrt{n}$, i.e. we have already found n/k before k. E.g. for $n = 100$, we can stop after 10, because even though 20 is a bigger divisor, we have already found $100/20 = 5$. (Note: the square root calculation can be avoided by turning $k \leq \sqrt{n}$ into its square: $k^2 \leq n$.)

So the algorithm of trial division can be done like this:

Is-prime(n):
- **Input:** $n \in \mathbb{N}$
- **if** $n < 2$ **then** $\rightarrow$ *not prime*
- **for** $k := 2, 3, \ldots$ **while** $k^2 \leq n$ **do**
  - **if** $k \mid n$ **then**
    - $\rightarrow$ *not prime*
- $\rightarrow$ *prime*

This can be implemented in Sage as follows:

```
def isprime (n):    # note: is_prime() (with underscore) is a built-in function
    if n < 2: return False
    k = 2
    while k*k <= n:
        if n % k == 0:
            return False
        k += 1
    return True
```

We can improve this algorithm further. For example, we can step by two: after checking that 2 doesn't divide n, we only need to check the odd numbers. This logic can be carried further by first checking 2 and 3, and then stepping by 6 ($= 2 \cdot 3$), checking only numbers of the form $6k + 1$ and $6k + 5$, because the others are divisible by either 2 or 3.

3.2 Prime factorization

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

Theorem 3.4 (Fundamental theorem of arithmetic)**.** *All integers greater than* 1 *can be written* ***uniquely*** *as a product of prime numbers, up to the order of the factors.*

Example. $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

Definition 3.5. The product in the above theorem is called the **prime factorization** of the number.

The word "uniquely" is crucial to 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. $30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3$, as these two factorizations are still "essentially" 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. requiring that they are listed in increasing order. Then, for brevity, we can write adjacent identical prime factors as powers. Then we get the following representation:

Definition 3.6. The **canonical representation** of an integer $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, where $p_1 < p_2 < \ldots < p_m$ are prime numbers, and k_i's are positive integers. It is also called the **standard form** of n.

Example. The canonical representation of 360 is $2^3 \cdot 3^2 \cdot 5$.

As discussed above, the canonical representation is unique.

The fundamental theorem of arithmetic demonstrates why the prime numbers are so important: they are the "building blocks" of positive integers, i.e. every integer greater than 1 can be split into the product of those. (The prime numbers are not exceptions: they can be written as a product of *one* prime number, namely themselves, e.g. $13 = 13$.)

The theorem also explains 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 prime factorization of a number can be calculated by `factor()`:

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

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

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

Note: for very large numbers, calculating the prime factorization is an extremely difficult task. So difficult in fact that certain cryptographic systems (such as 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.

3.3 Sieve of Eratosthenes

How can we find all prime numbers up to a given n?

The naive solution would be to apply trial division (see above) to each number individually. But this is very inefficient, because it involves a lot of redundant work (for example, if a number turned out to be 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 multiples 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~~

This algorithm can be improved in a couple of ways:

1. We only need to check the prime numbers up to $\sqrt{n}$, because the multiples of greater primes were already crossed out by smaller primes. (So in the above example, it was indeed enough

to 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 algorithm works as follows:

Sieve of Eratosthenes(n):

Input: $n \in \mathbb{N}^+$
Output: P, a list of boolean values (*true*/*false*) from 0 to n, where $P[i]$ indicates whether i is prime.
Initialize P to all *true*, except $P[0] = P[1] = false$.
for $i := 2, 3, \ldots$ **while** $i^2 \leq n$ **do**
  if $P[i]$ **then**
    for $j := i^2, i^2 + i, i^2 + 2i, \ldots$ **while** $j \leq n$ **do**
      $P[j] := false$

(Note: although P only needs to start from 2, but for simplicity, we started it from 0 to make it easier to implement in Sage.)

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

4 Divisor-related functions

Let's see some more functions related to divisors. For example:

Definition 4.1. Let $\boldsymbol{\tau(n)}$ be the number of positive divisors of $n \in \mathbb{N}^+$. (τ is pronounced "tau".)

Example. $\tau(6) = 4$, because $n = 6$ has 4 positive divisors: 1, 2, 3 and 6.

The first few values of τ (Sage calls it `number_of_divisors()`):

```
sage: matrix([[n, number_of_divisors(n)] for n in range(1, 26)]).transpose()
[ 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25]
[ 1  2  2  3  2  4  2  4  3  4  2  6  2  4  4  5  2  6  2  6  4  4  2  8  3]
```

The value of $\tau(n)$ clearly separates 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 use the definition, i.e. to simply count the divisors of n. But if we know the prime factorization of n, we have a better solution:

Theorem 4.2 (calculation of τ)**.** *If the canonical representation of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, then*

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_m + 1).$$

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

(Proof: any divisor of n has the same or less prime factors as n, on the same or less power than in n. Therefore, the divisors can be written as $p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}$ with the same p_i's as in n, and with exponents $0 \leq l_i \leq k_i$. To count how many such divisors exist, take the number of possible ways each l_i can be chosen, which is k_i+1 (since they are between 0 and k_i), and multiply them, i.e. $(k_1+1)(k_2+1)\cdots(k_m+1)$. But how do we know that all of these divisors are different? From the fundamental theorem of arithmetic, which states that the prime factorization is unique.)

Here is another interesting arithmetic function:

Definition 4.3. Let $\boldsymbol{\sigma(n)}$ be the sum of positive divisors of $n \in \mathbb{N}^+$. (σ is pronounced "sigma".)

Example. $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

The first few values of σ:

```
sage: matrix([[n, sigma(n)] for n in range(1, 26)]).transpose()
[ 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25]
[ 1  3  4  7  6 12  8 15 13 18 12 28 14 24 24 31 18 39 20 42 32 36 24 60 31]
```

This function can also be calculated from the prime factorization:

Theorem 4.4 (calculation of σ). *If the canonical representation of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, then*

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_m^{k_m+1} - 1}{p_m - 1}.$$

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

Definition 4.5 (Aliquot sum). Let $\boldsymbol{s(n)}$ 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 4.6. $n \in \mathbb{N}^+$ is a **perfect number** if $s(n) = n$.

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

The non-perfect numbers can be categorized into two groups:

Definition 4.7. $n \in \mathbb{N}^+$ is an **abundant number** if $s(n) > n$, or a **deficient number** if $s(n) < n$.

There is a related notion to perfect numbers:

Definition 4.8. $a \in \mathbb{N}^+$ and $b \in \mathbb{N}^+$ are **amicable numbers** if $s(a) = b$ and $s(b) = a$, but $a \neq b$.

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

5 Author

This document was written by Uray M. János, partly using the following sources:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa (Hungarian)

[2] https://en.wikipedia.org/wiki/Euclidean_division

[3] https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic

[4] https://en.wikipedia.org/wiki/Perfect_number

Errors and suggestions can be reported here: uray.janos@inf.elte.hu.