Gør tanke til handling

VIA University College

Division

Divisors

All the numbers that go into a given number are called the number's **divisors.**

We use the symbol | to write that one number goes into another number, i.e. that it is a divisor of that number.

Examples:

The divisors of 12 are 1, 2, 3, 4, 6 and 12: $1|12$, $2|12$, $3|12$, $4|12$, $6|12$, $12|12$.

The divisors of 13 are 1 and 13: $1|13$, $13|13$.

Primes

<u>Definition:</u>

A number is a **prime** if its only divisors are 1 and the number itself.

Example: 5 is prime, because its only divisors are 1 and 5.

9 is not prime, because 3 is one of its divisors.

Prime factorization

The fundamental theorem of arithmetic:

"Every positive integer can be written in a unique way as a product of primes"

This product is called the number's **prime factorization.**

For example, we can write the number 45 as $45 = \underbrace{5 \cdot 3 \cdot 3}_{\text{Prime factorization of 45.}}$.

Remainders

If you try to divide a number, a, by another number, b, which is **not** one of $a's$ divisors, you are left with a non-zero **remainder.**

Ex: Let's try to divide 30 by 12.

12 goes into 30 two whole times, so there is a remainder of 6:

$$30 = 2 \cdot 12 + 6$$

The division “algorithm”

NOTE: it is not an algorithm!!

Given integers a and b, we can always find a ”quotient” q and a ”remainder” $rem(a,b)$ such that

$$a = q \cdot b + rem(a,b),$$

where $0 \leq rem(a,b) < b$.

Example:

If $a = 14$ and $b = 5$, then the equation becomes

$$14 = 2 \cdot 5 + 4,$$

so $q = 2$ and $rem(14,5) = 4$.

The greatest common divisor

The largest number that is a divisor of two integers a and b is called the **greatest common divisor** of a and b: $\gcd(a, b)$.

We can find $\gcd(a, b)$ by using the **Euclidean algorithm**.

<u>Example</u>

Find the greatest common divisor of 10 and 25 – that is, find $\gcd(10,25)$:

The divisors of 10 are 1, 2, 5 and 10.

The divisors of 25 are 1, 5, 25.

→ The greatest (i.e. largest) divisors they have in common is 5, so

$$\gcd(10,25) = 5$$

The Euclidean algorithm

We can use remainders to find the $\gcd$ between two numbers by using the **Euclidean algorithm**:

$$\boxed{\gcd(a,b) = \gcd(b, rem(a,b))}$$

Example: Find the greatest common divisor between 93 and 62:

$$\begin{aligned} &\gcd(93,62) && = \gcd(62, rem(93,62)) \\ = &\gcd(62,31) && = \gcd\big(31, rem(62,31)\big) \\ = &\gcd(31,0) && = 31 \end{aligned}$$

Reading from the first to the last line, we see that $\gcd(93,62) = 31$

Gør tanke til handling

VIA University College

The Extended Eulclidean Algorithm

Bézout's theorem

"It is always possible to find integers s and t such that

$$\gcd(a, b) = s \cdot a + t \cdot b."$$

Linear combination of a and b.

Example:

$\gcd(55,14) = 1$. In this case, $s = -1$ and $t = 4$, since
$1 = (-1) \cdot 55 + 4 \cdot 14$.

In general, we can find s and t using **the extended Euclidean algorithm.**

The Extended Euclidean Algorithm

$$\gcd(78,21) = \gcd\big(21, rem(78,21)\big)$$

$$15 = 1\cdot 78 - 3\cdot 21$$

$$= \gcd(21,15) = \gcd(15, rem(21,15))$$

$$\begin{aligned} 6 &= 1\cdot 21 - 1\cdot 15 \\ &= 1\cdot 21 - 1\cdot(1\cdot 78 - 3\cdot 21) \\ &= -1\cdot 78 + 4\cdot 21 \end{aligned}$$

$$= \gcd(15,6) = \gcd\big(6, rem(15,6)\big)$$

$$\begin{aligned} 3 &= 1\cdot 15 - 2\cdot 6 \\ &= 1\cdot(1\cdot 78 - 3\cdot 21) - 2\cdot(-1\cdot 78 + 4\cdot 21) \\ &= 3\cdot 78 - 11\cdot 21 \end{aligned}$$

$$= \gcd(6,3) = \gcd(3, rem(6,3))$$

$$= \gcd(3,0) = 3$$

$$\downarrow$$

$$\boxed{\gcd(78,21) = 3 = 3\cdot 78 - 11\cdot 21}$$

Relatively prime numbers

If two numbers have a greatest common divisor of 1, they are called **relatively prime:**

<u>Definition:</u>

Two integers a and b are called **relatively prime** if $\gcd(a, b) = 1$.

For example,

- 3 and 4 are relatively prime because $\gcd(3,4) = 1$.
- 2 and 4 are not relatively prime because $\gcd(2,4) = 2$.

Euler's φ-function

<u>Question:</u>

How many numbers between 1 and 11 are relatively prime to 12?

Lets check each number:

$\gcd(1,12) = 1,\quad \gcd(\cancel{2},12) = 2,\quad \gcd(\cancel{3},12) = 3,\quad \gcd(\cancel{4},12) = 4,$
$\gcd(5,12) = 1,\quad \gcd(\cancel{6},12) = 6,\quad \gcd(7,12) = 1,\quad \gcd(\cancel{8},12) = 4,$
$\gcd(\cancel{9},12) = 3,\quad \gcd(\cancel{10},12) = 2,\quad \gcd(11,12) = 1$

This number is denoted by "**Euler's phi-function**", $\varphi(12)$. That is $\varphi(12) = 4$.

In general: **The number of numbers between 1 and $n - 1$ that are relatively prime to n is denoted by $\varphi(n)$.**

How to calculate $\varphi(n)$

Instead of counting, there are some useful rules for how to calculate $\varphi(n)$:

1. If n is a prime, then $\varphi(n) = n - 1$.
2. If m and n are relatively prime, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.
3. If n is a prime, then $\varphi(n^k) = n^k - n^{k-1}$

<u>Examples:</u>

Use the above rules to calculate $\varphi(11), \varphi(6), \varphi(9)$ and $\varphi(18)$:

$\varphi(11) = 11 - 1 = 10.$

$\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = (2 - 1) \cdot (3 - 1) = 2$

$\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6.$

$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = (2 - 1) \cdot (3^2 - 3^1) = 6.$

Introduction to modular arithmetic

The following slides contains a short introduction to modular arithmetic. We will continue this topic next week!

Intro to modular arithmetic

We'll start with an example:

Remember that we can e.g. write the remainder of 10 after division by 3 as $\mathrm{rem}(10,3) = 1$. Let's consider what happens when we take the remainder of increasing numbers after division by 3:

$$\begin{aligned}
\mathrm{rem}(0,3) &= 0\\
\mathrm{rem}(1,3) &= 1\\
\mathrm{rem}(2,3) &= 2\\
\mathrm{rem}(3,3) &= 0\\
\mathrm{rem}(4,3) &= 1\\
\mathrm{rem}(5,3) &= 2\\
\mathrm{rem}(6,3) &= 0\\
&\vdots
\end{aligned}$$

The number we are taking the remainder with respect to is called the **modulus**

Notice that only 3 different numbers occur (0, 1, and 2), and that there is a clear pattern: as the number on the left increases by 1 in each line, the remainders run through 0, 1, 2, 0, 1, 2 and so on.

Intro to modular arithmetic

In modular arithmetic, we **only** care about the remainder of numbers after division by some number, called the **modulus.** When the modulus is 3 (as in the last slide), any two numbers which have the same remainder after division by 3 are called **congruent** to each other. For example, 1 and 10 are congruent when the modulo is 3 because

$$\mathrm{rem}(10,3) = \mathrm{rem}(1,3).$$

Remainders can also be written using the modulus notation, e.g.:

$$\mathrm{rem}(10,3) = 10 \bmod 3$$

Calculation rules in modular arithmetic

Consider the following expressions. Which are true?

- $(2+5) \bmod 4 = \big((2 \bmod 4) + (5 \bmod 4)\big) \bmod 4$

  Left hand side: $(2+5) \bmod 4 = 7 \bmod 4 = 3$

  Right hand side: $\big((2 \bmod 4) + (5 \bmod 4)\big) \bmod 4 = (2+1) \bmod 4 = 3$

- $(2 \cdot 5) \bmod 4 = \big((2 \bmod 4) \cdot (5 \bmod 4)\big) \pmod 4$

  Left hand side: $(2 \cdot 5) \bmod 4 = 10 \bmod 4 = 2$

  Right hand side: $\big((2 \bmod 4) \cdot (5 \bmod 4)\big) \bmod 4 = (2 \cdot 1) \bmod 4 = 2$

- $2^5 \bmod 4 = \left(2^{5 \bmod 4}\right) \bmod 4$

  Left hand side: $(2^5) \bmod 4 = 32 \bmod 4 = 0$

  Right hand side: $\left(2^{5 \bmod 4}\right) \bmod 4 = (2^1) \bmod 4 = 2$

Calculation rules in modular arithmetic

The first two "experiments" in the last slide generalizes to the following calculation rules:

- $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

  In words: If you have to add two numbers modulo m, you can start by finding the modulo of each number and then add these instead

- $(a \cdot b) \bmod 4 = \big((a \bmod m) \cdot (b \bmod m)\big) \pmod m$

  In words: If you have to multiply two numbers modulo m, you can start by finding the modulo of each number and then multiply these instead

However, the last experiment showed that, in general:

- $a^b \bmod m \neq \left(a^{b \bmod m}\right) \bmod m$

  In words: If you have to do an exponentiation modulo m, it is not generally true that you can start by finding the modulo of the exponent and then carry out the exponentiation!