Summary on Lecture 11, March 6, 2019

• **The Euclidian Algorithm.** Recall: let $m, n \in \mathbf{Z}$, and $n \neq 0$. Then there exist unique integers $q \in \mathbf{Z}$ and $r \in \{0, 1, \dots, n-1\}$ such that $m = n \cdot q + r$. We look at the division:

$$m = q \cdot n + r, \quad 0 \leq r \leq n - 1.$$

The following fact is very important for us: it gives a key to compute $\gcd(m, n)$ for arbitrary integers m and n.

Lemma 1. $\gcd(m, n) = \gcd(n, r)$.

Examples. We compute few examples:

$$\gcd(27, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$
$$\gcd(183, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$$

• **The algorithms.** Below are three algorithms. We will use them for particular examples.

The algorithms $\mathbf{GCD}(k, n)$ and $\mathbf{GCD}^+(k, n)$ compute the greatest common divisor $\gcd(k, n)$. The last one, $\mathbf{EuclidianAlgorithm}^+(k, n)$, computes also integers s, t satisfying the identity $sk + tn = d$.

$\mathbf{GCD}(k, n)$
`Input:` `integers` $k, n \geq 0$`, both not equal to zero`
`Output:` $\gcd(k, n)$
  $a := k,\ b := n$
`while` $b \neq 0$ `do`
  $(a, b) := (b, a \text{ MOD } b)$
`return` a

$\mathbf{GCD}^+(k, n)$
`Input:` `integers` $k, n \geq 0$`, both not equal to zero`
`Output:` $\gcd(k, n)$
  $a := k$,
  $b := n$
`while` $b \neq 0$ `do`
  $q := a \text{ DIV } b \qquad (a, b) := (b, a - qb)$
  $d := a$
`return` d

$\mathbf{EuclidianAlgorithm}^+(k, n)$
`Input:` `integers` $k, n \geq 0$`, both not equal to zero`
`Output:` $d = \gcd(k, n)$`,` $s, t \in \mathbf{Z}$ `such that` $sk + tn = d$
  $a := k,\ a' := n$,
  $s := 1,\ s' := 0$,
  $t := 0,\ t' := 1$,
`while` $a' \neq 0$ `do`
  $q := a \text{ DIV } a' \qquad (a, a') := (a', a - qa')$
  $(s, s') := (s', s - qs')$
  $(t, t') := (t', t - qt')$
  $d := a$
`return` d, s, t

Examples:

(1) We compute $\gcd(73,17)$. We have that $\gcd(73,17) = \gcd(17,5) = \gcd(5,2) = \gcd(2,1) = 1$:

$$\begin{array}{lcl} 73 & = & 17\cdot 4 + 5 \\ 17 & = & 5\cdot 3 + 2 \\ 5 & = & 2\cdot 2 + 1 \end{array} \qquad \begin{array}{lcl} 5 & = & 73 - 17\cdot 4 \\ 3 & = & 17 - 5\cdot 3 \\ 1 & = & 5 - 2\cdot 2 \end{array}$$

Now we have:

$$\begin{aligned} 1 &= 5 - 2\cdot 2 = 5 - (17 - 5\cdot 3)\cdot 2 = 5\cdot 7 - 17\cdot 2 \\ &= (73 - 17\cdot 4)\cdot 7 - 17\cdot 2 = 73\cdot 7 - 17\cdot 28 - 17\cdot 2 \\ &= 73\cdot 7 - 17\cdot 30. \end{aligned}$$

We obtain: $73\cdot 7 - 17\cdot 30 = 1$.

(2) We start with **EuclidianAlgorithm**$^{+}(73,17)$. We list the steps:

	a	a'	s	s'	t	t'	q	$a = s\cdot 73 + t\cdot 17$
0	73	17	1	0	0	1	4	$73 = 1\cdot 73 + 0\cdot 17$
1	17	5	0	1	1	-4	3	$17 = 0\cdot 73 + 1\cdot 17$
2	5	2	1	-3	-4	13	2	$5 = 1\cdot 73 - 4\cdot 17$
3	2	1	-3	7	13	-30	2	$2 = -3\cdot 73 + 13\cdot 17$
4	**1**	0	**7**	$*$	-30	$*$	$*$	$1 = 7\cdot 73 - 30\cdot 17$

We obtain: $1 = 7\cdot 73 - 30\cdot 17$.

(2) We apply **EuclidianAlgorithm**$^{+}(135,40)$. We list the steps:

	a	a'	s	s'	t	t'	q	$a = s\cdot 135 + t\cdot 40$
0	135	40	1	0	0	1	3	$135 = 1\cdot 135 + 0\cdot 40$
1	40	15	0	1	1	-3	2	$40 = 0\cdot 135 + 1\cdot 40$
2	15	10	1	-2	-3	7	1	$15 = 1\cdot 135 - 3\cdot 40$
3	10	5	-2	3	7	-10	2	$10 = -2\cdot 135 + 7\cdot 40$
4	**5**	0	**3**	$*$	-10	$*$	$*$	$5 = 3\cdot 135 - 10\cdot 40$

We obtain: $5 = 3\cdot 135 - 10\cdot 40$.

(3) We would like to find two integers x and y such that $2000x + 643y = 1$. We use a "simple-minded" algorithm to find $\gcd(2000,643)$. We have that $\gcd(2000,643) = \gcd(643,71) = \gcd(71,4) = \gcd(4,3) = \gcd(3,1) = 1$:

$$\begin{array}{lcl} 2000 & = & 643\cdot 3 + 71 \\ 643 & = & 71\cdot 9 + 4 \\ 71 & = & 4\cdot 17 + 3 \\ 4 & = & 3\cdot 1 + 1 \end{array} \qquad \begin{array}{lcl} 71 & = & 2000 - 643\cdot 3 \\ 4 & = & 643 - 71\cdot 9 \\ 3 & = & 71 - 4\cdot 17 \\ 1 & = & 4 - 3\cdot 1 \end{array}$$

Now we have:

$$\begin{aligned} 1 &= 4 - 3\cdot 1 = 4 - (71 - 4\cdot 17) = 4\cdot 18 - 71\cdot 1 = (643 - 71\cdot 9)\cdot 18 - 71\cdot 1 \\ &= 643\cdot 18 - 71\cdot(9\cdot 18 + 1) = 643\cdot 18 - 71\cdot 163 = 643\cdot 18 - (2000 - 643\cdot 3)\cdot 163 \\ &= 643\cdot(18 + 3\cdot 163) - 2000\cdot 163 = 643\cdot 507 - 2000\cdot 163 = 326{,}001 - 326{,}000. \end{aligned}$$

We obtain: $643\cdot 507 - 2000\cdot 163 = 1$. Now we notice that

$$\begin{aligned} 1 &= 643\cdot 507 - 2000\cdot 163 = 643\cdot 507 + k\cdot 643\cdot 2000 - k\cdot 643\cdot 2000 - 2000\cdot 163 \\ &= 643\cdot(507 + k\cdot 2000) - 2000\cdot(k\cdot 643 + 163). \end{aligned}$$

Then $x = 507 + k\cdot 2000$, $y = k\cdot 643 + 163$. Notice that x is defined uniquely **mod 2000**, and y is defined uniquely **mod 643**.

• **The Fundamental Theorem of Arithmetic.** Let n be a positive integer. Then there exist unique primes $p_1, \dots, p_s$ and positive integers $e_1, \dots, e_s$ such that $n = p_1^{e_1} \cdots p_s^{e_s}$.

Proof. We use that fact (see Lecture 5):

Lemma 1. Let n be an integer. Then either n is a prime or there exists a prime p such that $p|n$.

Assume Theorem fails for some integer n. We form a set

$$S = \{\ n \mid \text{The Fundamental Theorem of Arithmetic fails for } n\ \}$$

Then by assumption, $S \neq \emptyset$. By Well-Ordering Principle, we find the minimal integer $n_0 \in S$. Then n_0 cannot be a prime (otherwise $n_0 \notin S$). Then there exists a prime p such that $n_0 = pn_1$. Since $n_1 < n_0$, the Fundamental Theorem of Arithmetic holds for n_1, and $n_1 = p_1^{e_1} \cdots p_s^{e_s}$. Then $n_0 = p \cdot p_1^{e_1} \cdots p_s^{e_s}$. Contradiction. This prove existence of such decomposition. □

Exercise. Prove that the decomposition $n = p_1^{e_1} \cdots p_s^{e_s}$ is unique.

Example. Let $n = p_1^{e_1} \cdots p_s^{e_s}$. How many divisors of n are there? Clearly, every integer k such that $k|n$ could be written as $k = p_1^{a_1} \cdots p_s^{a_s}$, where $0 \leq a_i \leq e_i$, $i = 1, \dots, s$. Thus we have $(1 + e_1)$ choices for a_1, $(1 + e_2)$ choices for a_2, and so on. Totally, we have

$$(1 + e_1)(1 + e_2) \cdots (1 + e_s) = \prod_{i=1}^{s} (1 + e_i)$$

divisors of $n = p_1^{e_1} \cdots p_s^{e_s}$.

For instance, the integer $2,953,092,457 = 7^3 \cdot 17^2 \cdot 31^3$ has $(1 + 3)(2 + 1)(3 + 1) = 48$ divisors.