Summary on Lecture 11, November 10, 2014

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

We look at the division:

$$m = q \cdot n + r, \quad 0 \leq r < b.$$

The following fact is very important for us: it gives a key to compute $\gcd(m, n)$ for arbitrary integers m and n. Euclid has discovered this property around 2,300 years ago.

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

Proof. We will show that every common divisor of m and n is also a common divisor of n and r, and that every common divisor of n and r is also a common divisor of m and n.

Indeed, let $d|m$ and $d|n$. Then, since $r = m - q \cdot n$, $d|r$. Thus d is a common divisor of n and r.

Let $d|n$ and $d|r$. Then, since $m = q \cdot n + r$, $d|m$. Thus d is a common divisor of m and n.

Now, since the common divisors of the pairs (m, n) and (n, r) coincide, the greatest common divisor is the same, i.e., $\gcd(m, n) = \gcd(n, r)$. □

Examples. We compute few examples:

$$\begin{aligned}
&\gcd(27, 5) = \gcd(5, 2) = \gcd(2, 1) = 1 \\
&\gcd(183, 15) = \gcd(15, 3) = \gcd(3, 0) = 3 \\
&\gcd(2014, 323) = \gcd(323, 76) = \gcd(76, 19) = \gcd(19, 0) = 19.
\end{aligned}$$

We introduce the notations: $(m \ \mathsf{DIV}\ n) := q$, and $(m \ \mathsf{MOD}\ n) := r$. Thus we can write:

$$m = (m \ \mathsf{DIV}\ n) \cdot n + (m \ \mathsf{MOD}\ n).$$

We fix $n > 0$ and then we say that m and m' are equal **mod** n iff $(m - m' \ \mathsf{MOD}\ n) = 0$, i.e. that $m - m'$ is divisible by n.

Example. Let $n = 5$. Then there are only possible remainders are $0, 1, 2, 3, 4$. Thus we can put together all integers in 5 different classes:

$$\mathbf{0} := \{0, \pm 5, \pm 2 \cdot 5, \ldots\}, \quad \mathbf{1} := \{1, 1 \pm 5, 1 \pm 2 \cdot 5, \ldots\}, \quad \mathbf{2} := \{2, 2 \pm 5, 2 \pm 2 \cdot 5, \ldots\},$$
$$\mathbf{3} := \{3, 3 \pm 5, 3 \pm 2 \cdot 5, \ldots\}, \quad \mathbf{4} := \{4, 4 \pm 5, 4 \pm 2 \cdot 5, \ldots\}.$$

Now we can add the classes: say, let $4 + 5j \in \mathbf{4}$, and $1 + 5i \in \mathbf{1}$. Then

$$4 + 5j + 1 + 5i = 5(1 + i + j) \in \mathbf{0},$$

and we choose different numbers in $\mathbf{4}$ and $\mathbf{1}$, the result will be the same. Thus we have that $\mathbf{4} + \mathbf{1} = \mathbf{0}$. Similarly, we can multiply. Say, let $2 + 5j \in \mathbf{2}$, and $3 + 5i \in \mathbf{3}$. Then

$$(2 + 5j)(3 + 5i) = 6 + 5 \cdot 3i + 5 \cdot 2j + 5 \cdot 5ji = 1 + 5(3i + 2j + 5ji) \in \mathbf{1}.$$

Thus $\mathbf{2} \cdot \mathbf{3} = \mathbf{1}$. Here are the addition and multiplication tables **mod** 5:

+	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**3**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

×	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

Example. Let $n = 6$. Then there are only possible remainders are $0, 1, 2, 3, 4, 5$. Thus we can put together all integers in 6 different classes:

$$\mathbf{0} := \{0, \pm 6, \pm 2 \cdot 6, \ldots\}, \quad \mathbf{1} := \{1, 1 \pm 6, 1 \pm 2 \cdot 6, \ldots\}, \quad \mathbf{2} := \{2, 2 \pm 6, 2 \pm 2 \cdot 6, \ldots\},$$
$$\mathbf{3} := \{3, 3 \pm 6, 3 \pm 2 \cdot 6, \ldots\}, \quad \mathbf{4} := \{4, 4 \pm 6, 4 \pm 2 \cdot 6, \ldots\}, \quad \mathbf{5} := \{5, 5 \pm 6, 5 \pm 2 \cdot 6, \ldots\}.$$

Similarly, we can add and multiply. Here are the addition and multiplication tables **mod** 6:

+	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

×	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**
2	**0**	**2**	**4**	**0**	**2**	**4**
3	**0**	**3**	**0**	**3**	**0**	**3**
4	**0**	**4**	**2**	**0**	**4**	**2**
5	**0**	**5**	**4**	**3**	**2**	**1**

We notice that $\mathbf{2} \cdot \mathbf{3} = \mathbf{0}$, $\mathbf{4} \cdot \mathbf{3} = \mathbf{0}$, and $\mathbf{3} \cdot \mathbf{3} = \mathbf{3}$.

Exercise. Write the addition and multiplication tables for $n = 10$ and $n = 11$.

Example. Compute last three digits of the following integer: 2014^{79}.

In other words, we have to compute 2014^{79} **mod** 1000. To warm-up, we compute 2014^{2^k} **mod** 1000 for several values of k:

$$\begin{array}{lllll} 2014^1 & = 14 & = 14 & \textbf{mod } 1000, \\ 2014^2 & = 14^2 & = 196 & \textbf{mod } 1000, \\ 2014^{2^2} & = 196^2 & = 416 & \textbf{mod } 1000, \\ 2014^{2^3} & = 416^2 & = 56 & \textbf{mod } 1000, \\ 2014^{2^4} & = 56^2 & = 136 & \textbf{mod } 1000, \\ 2014^{2^5} & = 136^2 & = 496 & \textbf{mod } 1000, \\ 2014^{2^6} & = 496^2 & = 16 & \textbf{mod } 1000. \end{array}$$

Now we find a binary decomposition of 79: We have: $79 = 1 + 2 + 4 + 8 + 64 = 1 + 2 + 2^2 + 2^3 + 2^6$. Then we have:

$$\begin{array}{rcll} 2014^{79} & = & 2014^1 \cdot 2014^2 \cdot 2014^{2^2} \cdot 2014^{2^3} \cdot 2014^{2^6} & \\ & = & 14 \cdot 196 \cdot 416 \cdot 56 \cdot 16 & \textbf{mod } 1000 \\ & = & (14 \cdot 196) \cdot (416 \cdot 56) \cdot 16 & \textbf{mod } 1000 \\ & = & 744 \cdot 296 \cdot 16 & \textbf{mod } 1000 \\ & = & (744 \cdot 296) \cdot 16 & \textbf{mod } 1000 \\ & = & 224 \cdot 16 & \textbf{mod } 1000 \\ & = & 584 & \textbf{mod } 1000 \end{array}$$

The answer: $2014^{79} = 584$ **mod** 1000.

Exercise. Compute last two digits of the integer 2014^{2014}.

• **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 ≥ 0, both not equal to zero
Output:  gcd(k,n)
      a := k, b := n
while b ≠ 0 do
      (a,b) := (b, a MOD b)
return a
```

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

$\mathbf{EuclidianAlgorithm}^+(k,n)$
```
Input:  integers k,n ≥ 0, both not equal to zero
Output:  d = gcd(k,n),  s,t ∈ Z such that sk + tn = d
      a := k, a' := n,
      s := 1, s' := 0,
      t := 0, t' := 1,
while a' ≠ 0 do
      q := a DIV a'        (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 $\gcd(73,17)=\gcd(17,5)=\gcd(5,2)=\gcd(2,1)=1$:

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

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