MEETING 6 - MODULAR ARITHMETIC AND INTRODUCTORY CRYPTOGRAPHY

In this meeting we go through the foundations of modular arithmetic. Before the meeting it is assumed that you have watched the videos and worked through Kapitel 5: Modulär aritmetik och egenskaper hos heltalen. We will do some Peer Instruction on these themes and follow up some of the questions that came in.

Deepening the understanding of the congruence class as a mathematical object

We have introduced the *congruence class* (in Swedish "restklass") as all the numbers congruent to a particular modulus. In IDK Kapitel 5 a congruence class was denoted in bold style, like this: **0**,**1**, etc. Now we will however use another notation, the bar notation so instead of **0**,**1**, etc. we write $\overline{0}$, $\overline{1}$, etc. Examples:

1. All even numbers: $\{\ldots,-4,-2,0,2,4,6,8,\ldots\} = \{2k; k \in \mathbb{Z}\}$. Written as $\overline{0}$, when the modulus 2 is implicitely determined. (Even numbers are the numbers divisible by 2, that is gives remainder 0 when divided by 2.)
2. All odd numbers: $\{\ldots,-3,-1,1,3,5,7,\ldots\} = \{2k+1; k \in \mathbb{Z}\}$. Written as $\overline{1}$, when the modulus 2 is implicitely determined. (Odd numbers are the numbers that give remainder 1 when divided by 2.)
3. All numbers that give remainder 3 when we divide by 5: $\{\ldots,-12,-7,-2,3,8,13,18,\ldots\} = \{5k+3; k \in \mathbb{Z}\}$. Written as $\overline{3}$, when the modulus 2 is implicitely determined.

We consider again the multiplication tables for $\mathbb{Z}_7$ and $\mathbb{Z}_{10}$:

$\mathbb{Z}_7$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_{10}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

In kapitel 5 we saw how we can introduce operations on the congruence classes. Now we can compare that to the earlier situation when we introduced mathematical objects such as numbers, vector or matrices - let us call them mathematical objects, or just *objects*. We learned to calculate with them and calculate means adding, subtracting, multiplying etc. Can we divide also? Let us understand just what division means, we formulate this by clarifying what subtraction means:

To *subtract* an object a from an object b we want to find the object x that fulfills this:

$$a + x = b$$

we denote the object x by $b - a$ and this is something we have done since we started school, it is not a difficult thing to understand when we think or ordinary numbers but it works also with vectors and matrices. But let us now apply the same reasoning to multiplication and division as a reverse to multiplication:

The question of how to *divide* an object b by an object a arises from the question of asking which object x do I need to use if I want to multiply an object a and obtain b? That is, which x fulfills this:

$$a \cdot x = b$$

we denote the object x by $\frac{b}{a}$ and we know from working with numbers or matrices that not all objects are allowed, when it comes to numbers we cannot have $a = 0$. And when it comes to matrices, as you probably remember from the theory of matrices, the equation

$$A \cdot X = B$$

could not be solved for all B if the matrix A was not invertible - but when the inverse existed we could write the solution as $X = A^{-1} \cdot B$. The matrix A^{-1} was called the *inverse* of A. A longer name for it is the *multiplicative inverse* of A. It is this route we will take when introducing division with congruences. Take a look at the multiplication tables above, can we always solve the equation

$$a \cdot x = b$$

when a, x and b are congruence classes?

As it turns out, for some a this equation have no solutions when we are working in $\mathbb{Z}_{10}$, for example if $b = \overline{4}$ and $a = \overline{5}$ we cannot have any x so that $a \cdot x = b$. It would mean $\overline{5} \cdot x = \overline{4} \Leftrightarrow 5 \cdot x \equiv 4 \pmod{10}$ which is impossible. Why is this impossible?

The interesting feature to notice in the tables above is that the equation

$$a \cdot x = b$$

has a solution for every b if we have all the possible b's occurring in the row that is determined by a. For example, if we choose $a = \overline{3}$ we see that the row determined by this a is

$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$

and each possible b here occurs so that for example, if we wanted to have an x such that $\overline{3} \cdot x = \overline{8}$, we check on top of the table in the column where we find $\overline{8}$, at the top we find $\overline{6}$ which means that $x = \overline{6}$ is the solution to the equation.

Inspecting the multiplication table for $\mathbb{Z}_{10}$, we can draw the conclusion that

$$a \cdot x = b$$

has a solution for all b if and only if $a = \overline{1}$ or $a = \overline{3}$ or $a = \overline{7}$ or $a = \overline{9}$. So what is the pattern here? What do we have to demand on a for the equation to have a solution?

We may get a clue from this by studying the multiplication table for $\mathbb{Z}_7$, here *every* row contains every element in $\mathbb{Z}_7$, we conclude that the equation $a \cdot x = b$ has a solution in $\mathbb{Z}_7$ for every a (except of course $a = \overline{0}$). For example, working in $\mathbb{Z}_7$, what is the solution to $\overline{4} \cdot x = \overline{6}$? Well, look on the row determined by $a = \overline{4}$ and try to find $\overline{6}$, it is found in the column that has $\overline{5}$ at the top - so that $x = \overline{5}$ is the solution. This can be done with any a and any b in $\mathbb{Z}_7$... But NOT in $\mathbb{Z}_{10}$.

If we ponder a while about the mechanism of this we end up realizing that the central thing here is that a must be relatively prime to the modulus (that is n) for a solution to always exist. Let us make a statement of a theorem about this:

Theorem: Let n be a positive modulus. (That is just a positive integer greater than 1.) Then the equation

$$a \cdot x = b$$

in $\mathbb{Z}_n$ has a solution in x for every possible choice of b if a and n are relatively prime.

Proof: (In this proof we shall alternate between using the same symbol for integers and congruence classes - that we can do so is granted by an earlier result.) Let a, n be relatively prime. Then there exists integers s, t such that $sa + tn = 1$. (They can be found with the use of the Euclidean algorithm.) This means that, in $\mathbb{Z}_n$ we have $sa = \overline{1}$. For any equality in $\mathbb{Z}_n$ we can then write

$$ap = q \Rightarrow sap = sq \Rightarrow p = sq \Rightarrow ap = asq \Rightarrow ap = q$$

so that we can always write

$$ap = q \Leftrightarrow p = sq.$$

(With numbers and matrices, s would be the multiplicative inverse, for numbers $s = \frac{1}{a}$ and for matrices $s = A^{-1}$.) Now use this on the equation, we then get

$$a \cdot x = b \Leftrightarrow sax = sb \Leftrightarrow x = sb$$

but this then means that we have found the x and the equation has a solution. The proof is complete.

Corollary: If the modulus n is a prime number, then every equation of the form $ax = b$ in $\mathbb{Z}_n$ has a solution for every $b \neq \overline{0}$.

Proof: This is just the same theorem stated when the modulus is a prime, the condition a, n relatively prime is then automatically met.

We actually call the element s above a multiplicative inverse and we introduce it with a definition:

Definition: Let n be a positive modulus. Then, for any $a \in \mathbb{Z}_n$, if $sa = \overline{1}$, we call s a *multiplicative inverse* of a.

We can only have one multiplicative inverse, if we would have two multiplicative inverses, s_1, s_2 of the same a, then

$$s_1 = s_1 \cdot 1 = s_1 \cdot (a \cdot s_2) = (s_1 \cdot a) \cdot s_2 = 1 \cdot s_2 = s_2.$$

So there is at most one multiplicative inverse.

Let us study an exam question from the 9 of April 2015:

Use the Euclidean algorithm to find the multiplicative inverse of $23 \pmod{17}$ and use it to find all integers x that satisfy $23x \equiv 337 \pmod{17}$.

Solution: The Euclidean algorithm consists of repeated application of The Division Algorithm to 23 and 17, so we get

$$23 = 1 \cdot 17 + 6, \quad 17 = 2 \cdot 6 + 5, \quad 6 = 1 \cdot 5 + 1$$

so that $1 = 6 - 1 \cdot 5 = 6 - 1 \cdot (17 - 2 \cdot 6) = 3 \cdot 6 - 17 = 3 \cdot (23 - 17) - 17 = 3 \cdot 23 - 4 \cdot 17$. This means that the multiplicative inverse of $23 \pmod{17}$ is 3. Hence we can multiply both sides of the congruence by 3. However, let us first reduce 337 to what it is congruent with $\pmod{17}$, we easily see that $337 \equiv 14 \pmod{17}$ so that we have the following equivalent congruences

$$23x \equiv 337 \pmod{17} \Leftrightarrow 23x \equiv 14 \pmod{17} \Leftrightarrow 3 \cdot 23x \equiv 3 \cdot 14 \pmod{17}$$

which can be written$1 \cdot x \equiv 3 \cdot 14 \pmod{17} \Leftrightarrow x \equiv 8 \pmod{17}$.

So we can always use the Euclidean Algorithm to find the multiplicative inverse. Let us consider another example.

Example: Find the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}_{19}$.

Solution: We seek integers s, t such that $s \cdot 17 + t \cdot 19 = 1$. These integers exist for sure since $17, 19$ are relatively prime. (Why?) The Euclidean algorithm gives

$$19 = 1 \cdot 17 + 2 \qquad 17 = 8 \cdot 2 + 1 \qquad 1 = 19 - 8 \cdot (19 - 17) \Leftrightarrow 1 = 9 \cdot 17 - 8 \cdot 19$$

This means that $s = 9$ and $t = -8$ will satisfy $s \cdot 17 + t \cdot 19 = 1$ which means that the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}_{19}$ will be $\overline{9}$.

you can yourself choose any two prime numbers, p, q, and practice to find the multiplicative inverse of $\overline{p}$ in $\mathbb{Z}_q$, do this for as many prime numbers as you want. (Maybe it is good to do $p, q = 11, 13$, $p, q = 11, 17$, $p, q = 23, 29$, $p, q = 23, 37$.)

Investigating multiplicative inverses in $\mathbb{Z}_p$

We can also formulate the results in the previous section like this:

Proposition: Let n be a positive modulus. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

or, if we use the congruence class notation, we express ourselves like this:

Proposition: Let n be a positive modulos. If $\overline{a} \cdot \overline{c} = \overline{b} \cdot \overline{c}$ and $\gcd(c, n) = 1$, then $\overline{a} = \overline{b}$.

Now if we are using a prime modulus then each nonzero element will be relatively prime to the modulus, so then we can express ourselves like this:

Proposition: Let p be a prime number. If $ac \equiv bc \pmod{p}$ and $c \neq 0$, then $a \equiv b \pmod{p}$.

or, if we use the congruence class notation, we express ourselves like this:

Proposition: Let p be a prime number. If $\overline{a} \cdot \overline{c} = \overline{b} \cdot \overline{c}$ and $\overline{c} \neq \overline{0}$, then $\overline{a} = \overline{b}$.

This last formulation is particularly interesting, it means that $\mathbb{Z}_p$ works exactly as the ordinary real numbers: we can add, subtract, multiply and divide with nonzero numbers!

Let us explore the properties of $\mathbb{Z}_p$, where p is a prime number. Then, each nonzero element has a multiplicative inverse. That is for example in $\mathbb{Z}_7$, the elements $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ all have multiplicative inverses, if these elements are denoted x, we can always find an s such that $sx = \overline{1}$. (What about $\overline{7}$?) We can look in the multiplication table above and find these inverses, consulting the table we get $\overline{1} \cdot \overline{1} = \overline{1}$ so that the multiplicative inverse of $\overline{1}$ is $\overline{1}$ itself (of course!), further $\overline{2} \cdot \overline{4} = \overline{1}$ so that the multiplicative inverse of $\overline{2}$ is $\overline{4}$.

We can make a table:

$\mathbb{Z}_7$	Inverses
$\overline{0}$	*Missing*
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{5}$
$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{3}$
$\overline{6}$	$\overline{6}$

Consider this question: do any of the elements in $\mathbb{Z}_p$ have themselves as multiplicative inverse? That is, which elements x in $\mathbb{Z}_p$ satisfy $x \cdot x = \overline{1}$? If we write $x \cdot x$ as x^2 we are asking which x in $\mathbb{Z}_p$ satisfy the equation

$$x^2 = \overline{1}.$$

Now since p is a prime number, then $\mathbb{Z}_p$ works as the real numbers so we can solve this equation as usual:

$$x^2 = \overline{1} \Leftrightarrow x^2 - \overline{1} = \overline{0} \Leftrightarrow (x + \overline{1}) \cdot (x - \overline{1}) = \overline{0} \Leftrightarrow x + \overline{1} = \overline{0} \vee x - \overline{1} = \overline{0} \Leftrightarrow x = \overline{-1} = \overline{p-1} \vee x = \overline{1}$$

so the only two possibilities for an element in $\mathbb{Z}_p$ to be its own multiplicative inverse is if it is $\overline{1}$ or $\overline{p-1}$. This means that for every other element in $\mathbb{Z}_p$, that is the $p - 3$ elements $\overline{2}, \overline{3}, \ldots, \overline{p-2}$, they must all have a multiplicative inverse that is not themselves. And indeed, we can have a look at the table above, the only elements in $\mathbb{Z}_7$ which are their own inverses are $\overline{1}$ and $\overline{6} = \overline{7-1}$. What is the use of this? Well, we are studying congruences and they are very useful and it is useful to learn about their properties. We will use this fact in proving Wilson's Theorem in the next meeting, for now we look an immensely important application of all this: Cryptography.

Cryptology by use of the RSA-algorithm

RSA is an acronym, it stands for Rivest, Shamir, and Adleman who were the three originators of the application of number theory that is used for cryptology. The meaning of the word "cryptography" means "hidden writing" and the objective of a cryptographic application is to ensure that two parties, usually called Alice and Bob can communicate privately over a channel which a third party can eavesdrop on, that is hear what is being communicated. The eavesdropper, commonly called Eve, is able to hear all signals that are being sent over the channel, but the cryptographic application needs to ensure that, to Eve, the signals that are sent has no meaning, that they are indistinguishable from just white noise, that is random signals.

One very interesting feature of modern cryptology is that a cryptographic application gets safer if it is publicly known how the encryption procedure is performed. Not in exact, concrete detail of course, there must exist a secret element called a *key*. How can this be? How can an algorithm be safer if it is known how it works? There is a very simple answer to that and this is that if it known how an algorithm works and it works over many years, then it is not likely that it will contain any loopholes, someone ought to have found out. By now the RSA algorithm has been employed successfully over many years and it is very unlikely that it will contain a vulnerability.

Let us introduce some terminology.

Definition: A *crypto-scenario* is a situation where we have three parties *Alice*, *Bob*, and *Eve*. The two parties *Alice* and *Bob* wishes to exchange information over a channel whose signals *Eve* also can hear. A message T that everyone can understand is called a *cleartext*, a message C that only *Alice* and *Bob* can understand is called a *cryptotext*. An *encryption* is an **one-to-one** function e defined on the set of all *possible cleartexts*, called L (for *Language*). A *decryption* is a function d defined on $e(L)$ such that $\forall T \in L : d(e(T)) = T$.

Example: Let us take an extremely simple example called the Ceasar crypto. (This was how secrets of state were handled in the ancient Roman Empire.) Choose an offset, for example 3. Then the encryption function d is formed by replacing A with D, B with E and so on, replacing each letter in the alphabet with the one 3 steps ahead. When we get to the three last letters, X, Y, Z we start over and replace X with A, Y with B, and Z with C. The watchful people understands that this is offsetting letters with an index of 3 and then doing it modulo the alphabet. When we encrypt a cleartext T we do it letter by letter. Thus if $T =$ "$SECRET$" we get the cryptotext $C =$ "$VHFUHX$". We can also write this in terms of functions $C =$ "$VHFUHX$" $= e($"$SECRET$"$)$. The decryption function applied to this cryptotext of course recovers the original cleartext so that we have: $d($"$VHFUHX$"$) =$ "$SECRET$".

The central mathematical object in cryptography is the encryption function - and of course the decryption function that is used together with the encryption function. Basically we use number theory to create an encryption function which we can describe using integers. If we apply this to the function described above, numbering the letters in the alphabet from 0 to 28, the encryption function would simply be $e(t) = t + 3(mod 29)$ and the decryption function would just be $d(c) = c - 3(mod 29)$. It is clear that $d(e(t)) = t$ for all integers t. When we move to more advanced cryptography we will create a much larger interval, something like $0, 1, 2, \dots, N - 1$ where N is a very large number. Our encryption function will then be a one-to-one function onto this interval and therefor it will actually be a bijection. Similarly the decryption function will also be a bijection of this large interval onto itself. We will formulate this in a couple of examples, we will start small and go larger.

Example: A very small instance of the RSA-crypto. We deal with the integers $L = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and set

$$e(t) = t^7 (mod 10) \quad \text{and} \quad d(c) = c^7 (mod 10).$$

Then we have two different so-called keys for encryption (7) and decryption (3). The decryption key is held secret and the encryption key can be made public together with the modulus, 10. We can study the values of the two functions e and d in a table:

t	$e(t)$	$d(e(t))$	
0	$e(0) = 0$	$d(0) = 0$	(Computation: $e(0) = 0^7 (mod 10) = 0$.)
1	$e(1) = 1$	$d(1) = 1$	(Computation: $e(1) = 1^7 (mod 10) = 1$.)
2	$e(2) = 8$	$d(8) = 2$	(Computation: $e(2) = 2^7 (mod 10) = 128 (mod 10) = 8$.)
3	$e(3) = 7$	$d(7) = 3$	(Computation: $e(3) = 3^7 (mod 10) = 2187 (mod 10) = 7$.)
4	$e(4) = 4$	$d(4) = 4$	
5	$e(5) = 5$	$d(5) = 5$	
6	$e(6) = 6$	$d(6) = 6$	
7	$e(7) = 3$	$d(3) = 7$	
8	$e(8) = 2$	$d(8) = 8$	
9	$e(9) = 9$	$d(9) = 9$	

This illustrates a very small (and practically useless) instance of the RSA-algorithm that can be used to send one of the numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ in a secret way. The procedure is as follows: Alice publishes to everyone the numbers $(10, 7)$, this is the so-called *public key*. Anyone can encrypt numbers with these two numbers by forming the encryption function e. We study the example when Bob wants to secretely send the number 8 to Alice. Alice has beforehand published the public key $(10, 7)$ and now Bob uses this to encrypt the cleartext 8, he forms $e(8)$ by computing $8^7 (mod 10)$ which is 2. So the cryptotext is 2 which is sent over the channel that Eve also listens to. It arrives at Alice and Eve, who listens, but only Alice knows the secret decryption key which is 3. So Alice forms $d(2)$ by computing $2^3 (mod 10)$ which is 8 and thereby understands that Bob has sent her an 8. Eve on the other hand does not know which of the numbers is the decryption key and so cannot know that it was 8 that was sent.

In practice of course the numbers are much larger than this. We will study a slightly larger example.

Example: Set

$$e = 17, \qquad d = 2753, \qquad N = 3233.$$

Then this defines an instance of the RSA-crypto by the encryption and decryption functions

$$e(t) = t^{17} (mod 3233) \quad \text{and} \quad d(c) = c^{2753} (mod 3233).$$

This instance of RSA can encrypt the numbers $0, 1, 2, 3, \dots, 3233 - 1 = 3232$, that is we can use it to shuffle 3233 integers (of course 0 and 1 are shuffled so we forget about them). For example to encrypt 123 we form

$$e(123) = 123^{17} (mod 3233) =$$

$$337587917446653715596592958817679803 (mod 3233) = 855.$$

And to decrypt 855 we compute

$$d(855) = 855^{2753} (mod 3233) =$$

5043288895841606873442289912739446663145387836003550931555496756450105562861208255997874424542811005438349865428933638493024645144150785172091796654782635307099638035387326500896686074771829745822950342950407903581845940956377938586598936883808360284013250976862076697739667533250542826093475735137988063256482639334453092594385562429233017519771900169249169128091505960191787601713497254392792156967017899021343071464689712796102771813783945869677289869342365240311693217089269617643726521315665833158712459759803042503144006837883246101784830717585474547252069688925995892544366701432205469543174002285500923863694244485597333306305160738530286321930291350374547194675777671357 9

54965202919790505781532871558392070303159585937493663283548602090830
63550704455658896319318011934122017826923344101330116480696334024075
04695258866987658669006224024102088466507530263953870526631933584734
81094876156227126037327597360375237388364148088948438096157757045380
08107946980066734877795883758289985132793070353355127509043994817897
90548993381217329458535447413268056981087263348285463816885048824346
58897839333466254454006619645218766694795528023088412465948239275105
77049113329025684306505229256142730389832089007051511055250618994171
23177795157979429711795475296301837843862913977877661298207389072796
76720235011399271581964273076407418989190486860748124549315795374377
12441601438765069145868196402276027766869530903951314968319097324505
45234594477256587887692693353918692354818518542420923064996406822184
49011913571088542442852112077371223831105455431265307394075927890822
60604317113339575226603445164525976316184277459043201913452893299321
61307440532227470572894812143586831978415597276496357090901215131304
15756920979851832104115596935784883366531595132734467524394087576977
78908490126915322842080949630792972471304422194243906590308142893930
29158483087368745078977086921845296741146321155667865528338164806795
45594189100695091965899085456798072392370846302553545686919235546299
57157358790622745861957217211107882865756385970941907763205097832395
71346411902500470208485604082175094910771655311765297473803176765820
58767314028891032883431850884472116442719390374041315564986995913736
51621084511374022433518599576657753969362812542539006855262454561419
25880943740212888666974410972184534221817198089911953707545542033911
96453936646179296816534265223463993674233097018353390462367769367038
05342644821735823842192515904381485247388968642443703186654199615377
91396964900303958760654915244945043600135939277133952101251928572092
59788751160195962961569027116431894637342650023631004555718003693586
05526491000090724518378668956441716490727835628100970854524135469660
84481161338780654854515176167308605108065782936524108723263667228054
00387941086434822675009077826512101372819583165313969830908873174174
74535988684298559807185192215970046508106068445595364808922494405427
66329674592308898484868435865479850511542844016462352696931799377844
30217857019197098751629654665130278009966580052178208139317232379013
23249468260920081998103768484716787498919369499791482471634506093712
56541225019537951668976018550875993133677977939527822273233375295802
63122665358948205566515289466369032083287680432390611549350954590934
06676402258670848337605369986794102620470905715674470565311124286290
73548884929899835609996360921411284977458614696040287029670701478179
49024828290748416008368045866685507604619225209434980471574526881813
18508591501948527635965034581536416565493160130613304074344579651083
80304062240278898042825189094716292266898016684480963645198090510905
79651307570379245958074479752371266761011473878742144149154813591743
92799496956415653866883891715446305611805369728343470219206348999531
91764016110392490439179803398975491765395923608511807653184706473318
01578207412764787592739087492955716853665185912666373831235945891267
87095838000224515094244575648744840868775308453955217306366938917023
94037184780362774643171470855830491959895146776294392143100245613061
11429937000557751339717282549110056008940898419671319709118165542908
76109008324997831338240786961578492341986299168008677495934077593066
02207814943807854996798945399364063685722697422361858411425048372451
24465580270859179795591086523099756519838277952945756996574245578688
38354442368572236813990212613637440821314784832035636156113462870198
51423901842909741638620232051039712184983355286308685184282634615027
44187358639504042281512399505995983653792227285847422071677836679451
34363807086579774219853595393166279988789721695963455346336497949221
13017661316207477266113107012321403713882270221723233085472679533015
07998062253835458948024820043144726191596190526034069061930939290724
10284948700167172969517703467909979440975063764929635675558007116218

27727603182921790350290486090976266285396627024392536890256337101471
68327404504583060228676314215815990079164262770005461232291921929971
69907690169025946468104141214204472402661658275680524166861473393322
65959127006456304474160852916721870070451446497932266687321463467490
41185886760836840306190695786990096521390675205019744076776510438851
51941619318479919134924388152822038464729269446084915299958818598855
19514906630731177723813226751694588259363878610724302565980914901032
78384821401136556784934102431512482864529170314100400120163648299853
25166349056053794585089424403855252455477792240104614890752745163425
13992163738356814149047932037426337301987825405699619163520193896982
54478631309773749154478427634532593998741700138163198116645377208944
00285485000269685982644562183794116702151847721909339232185087775790
95933267631141312961939849592613898790166971088102766386231676940572
95932538078643444100512138025081797622723797210352196773268441946486
16402961059899027710532570457016332613431076417700043237152474626393
99011899727845362949303636914900881060531231630009010150839331880116
68215163893104666659513782749892374556051100401647771682271626727078
37012242465512648784549235041852167426383189733332434674449039780017
84689726405462148024124125833843501704885320601475687862318094090012
63241969092252022679880113408073012216264404133887392600523096072386
15855496515800103474611979213076722454380367188325370860671331132581
99227975522771848648475326124302804177943090938992370938053652046462
55147267884961527773274119265709116613580084145421487687310394441054
79639308530896880365608504772144592172500126500717068969428154627563
70458838904219177398190648731908014828739058159462227867277418610111
02763247972904122211994117388204526335701759090678628159281519982214
57652796853892517218720090070389138562840007332258507590485348046564
54349837073287625935891427854318266587294608072389652291599021738887
95773647738726574610400822551124182720096168188828493894678810468847
31265541726209789056784581096517975300873063154649030211213352818084
76122990409576427857316364124880930949770739567588422963171158464569
84202455109029882398517953684125891446352791897307683834073696131409
74522985638668272691043357517677128894527881368623965066654089894394
95161912002160777898876864736481837825324846699168307281220310791935
646668401591485826999933744276777252275403853322196852298590851548110
40229657916338257385513314823459591633281445819843614596306024993617
53097925561238039014690665163673718859582772525683119989984646027216
46279764077057074816406450769779869955106180046471937808223250148934
07851137833251073753823403466269553292608813843895784099804170410417
77608463062862610614059615207066695243018438575031762939543026312673
77406936404705896083462601885911184367532529845888040849710922999195
65539701911191919188327308603766775339607722455632113506572191067587
51186812786344197572392195263333856538388240057190102564949233944519
65959203992392217400247234147190970964562108299547746193228981181286
05556588093851898811812905614274085809168765711911224763288658712755
38928438126611991937924624112632990739867854558756652453056197509891
14578114735771283607554001774268660965093305172102723066635739462334
13638045914237759965220309418558880039496755829711258361621890140359
54234930424749053693992776114261796407100127643280428706083531594582
305946326827861270203356980346143245697021484375 (mod 3233) = 123

The number 123 is thus encrypted to 855 and then decrypted back to 123 with the two functions e, d. The computations involve a number containing about 4200 digits, which is a measure of the forces that lie inside the RSA algorithm - it is *only* the correct key that kan undo that great jumble of digits.

We will now describe the general way to create an instance of the RSA-algorithm, we will use the two examples above to make the description concrete.

Description of how to create an instance of the RSA algorithm.

1. Choose two prime numbers, for example $p = 2$ and $q = 5$. Form the product $pq = 10$, this is N which is the modulus. It is also the number of different symbols that can be encrypted and decrypted by this instance. (In our example only 10.)
2. Choose the encryption number e such that e and $(p-1)(q-1)$ are relatively prime. In our example $(p-1)(q-1) = (2-1)(5-1) = 4$. We can therefore choose $e = 7$ because 7 and 4 are relatively prime. (It is a coincidence that e is also a prime number.)
3. The decryption number d is chosen so that $d \equiv 1(mod(p-1)(q-1))$. In our case above we choose d so that $d \cdot 7 \equiv 1(mod4) \Leftrightarrow 7d \equiv 1(mod4)$. This number can be found by applying the Euclidean Algorithm on 7 and 4, after some computations we arrive at $d = 3$. (Indeed, $d = 7$, or any other d which would have $d \equiv 3(mod4)$.)

The three steps above establishes the values of e, d, N and thereby the encryption and decryption functions e and d are determined. It is a bit unfortunate that we have the same name for the constants e, d as the functions e, d, but it is not so confusing when we work more with concrete examples.

Example: We will look at the same procedure being carried out for the second example.

1. The two prime numbers here were $p = 61$ and $q = 53$. The product is $N = pq = 61 \cdot 53 = 3233$.
2. The encryption number $e > 1$ is chosen so that $gcd(e, (p-1)(q-1)) = 1$. In our example $(p-1)(q-1) = 60 \cdot 52$. The number $e = 17$ is a prime number that does not divide either 60 or 52 and hence the numbers $e = 17$ and $60 \cdot 52$ are relatively prime. So $e = 17$ is chosen.
3. Now it is time to choose the decryption number. The rule is to choose it so that $de \equiv 1(mod(p-1)(q-1))$. in our case we have $(p-1)(q-1) = 60 \cdot 52 = 3120$. This means that we need to find d such that $17 \cdot d \equiv 1(mod3120)$. We employ the Euclidean Algorithm to find d. We have:
$$3120 = 17 \cdot 183 + 9, \quad 17 = 1 \cdot 9 + 8, \quad 9 = 1 \cdot 8 + 1$$
So that
$$1 = 9 - 1 \cdot 8 = 9 - 1 \cdot (17 - 9) = 2 \cdot 9 - 17 = 2 \cdot (3120 - 17 \cdot 183) - 17 = 2 \cdot 3120 - 367 \cdot 17.$$
This means that $17 \cdot (-367) \equiv 1(mod3120)$. Since we want a positive number for d we have to add multiples of the modulus 3120 to -367 until we get a positive number, one 3120 is enough and we find that $-367 + 3120 = 2753$ which is our decryption number. (Observe that in theory -367 would also work, however, in the world of congruence classes the number -367 *is the same* as the number 2753.)

In conclusion: the public key is $(e, pq) = (17, 3233)$ and the private decryption key is $d = 2753$.

Exercise: Verify that the numbers $p = 83$, $q = 89$, $N = 7387$, $e = 17$, and $d = 849$ fulfills the demands of the RSA-crypto.

Exercise: Choose $p = 5$, $q = 7$, then $N = 35$. Find e, d and create an instance of the RSA-crypto based on these numbers.