4 Application: RSA cryptography

There are many interesting applications of number theory and abstract algebra, especially in computer-related subjects. We shall look closer at one famous application to cryptography.

4.1 The problem of secure communication

Suppose that two persons want to communicate with each other, and they want to protect their communication from being overheard by a third party. This could for example be any of the following situations:

- I want to buy a book at the online bookshop Amazon. To do this, I send them my credit card number through the Internet, so that they can deduct the correct amount of money from my bank account. A skilled hacker can easily interrupt the communication, get hold of my credit card number, and use it to take all the money in my account.
- The American CIA agent John MacAgent has infiltrated the North Korean military, and wants to send some secret information back to his colleagues in the US. If someone can interrupt and understand his message, he will immediately be killed by the North Koreans.
- Sarah is deeply in love with Otieno, but her parents thinks she is too young to have a boyfriend. So Sarah needs to send secret messages to Otieno that her parents cannot understand, even if they manage to find one of the messages.
- The researchers at the company Amazing Machines Ltd has come up with an idea for a machine that could produce large amounts of electricity very cheaply. They want to discuss these ideas through email with some leading physicists in Japan, but if someone else manages to interrupt the email communication, they could steal the idea, and the company could lose millions of dollars.

So how can these problems be solved? How can these people communicate in a safe way? These kinds of problems are investigated in the field of cryptography.
The simplest way of solving the problem is to agree on some kind of encoding scheme. For example, Sarah and Otieno could agree that in their letters, every A means B, every B means C, every C means D etc. In this case, Otieno could for example send a letter with the message

H KNUD XNT

and Sarah would be very happy, and write back:

H KNUD XNT SNN, RVDDSHD!

If her mother found the piece of paper with these letters, she would not understand, and Sarah could probably convince her that this is just the password for her webmail.
There are many other, much more complicated, ways of encoding messages (any such method is called an encoding scheme) so that they are not easily readable to others. However, there are two possible problems with all of these methods.

- Problem 1: If the code is not complicated enough, it could easily be cracked by someone with a computer (perhaps Sarah's mother has computer programming as a hobby... scary!)
- Problem 2: Suppose that Sarah's father gets hold of the *first* letter, where they write down which encoding scheme to use! Then he would be able to understand *every* subsequent letter he can find, with catastrophic consequences!

The first problem can perhaps be solved by making the encoding complicated enough, but the second is a major problem! If for example my computer system agrees with the Amazon website on how to encode the credit card number, and someone gets hold of this information, then they will be able to read my credit card number even if it is encoded!
This problem can actually be overcome, by using something called *RSA cryptography*.

4.2 Factoring large numbers

One of the ideas behind the RSA cryptography is that it is very hard to factor large integers, even if you use a computer. You have learnt how to factor small numbers, but how would you find the prime factorization of an integer n with 200 digits? Of course, you could start by checking the primes $2, 3, 5, 7$ and so on, to see if any of them divides the large number. However, such a number is so large, that you would become old and probably die before you have checked all primes up to $\sqrt{n}$, even if you used a computer. I mentioned earlier that if you can find the factorization of the number

74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359

then you would be awarded a sum of US$ 30,000. Such a prize exists to encourage research in this area, because it has an enormous impact on the millions of messages and financial transations that take place every day through the Internet and other communication channels.

4.3 Any message can be expressed in terms of integers

It is easy to transform any message written with letters to a message written in integers. We could use any of the common methods used in computers, such as ASCII, Unicode and so on. In this course, we will simply write 1 instead of A, 2, instead of B, and so on, up to 26 instead of Z. We will also write 0 instead of an empty space. So we could send the numbers

$$8\ 9\ 0\ 20\ 8\ 5\ 18\ 5$$

instead of the message "HI THERE".

4.4 The RSA Cryptosystem

Suppose that I want to be able to receive secret messages from other people. The fundamental idea is the following. I find a "one-way function", call it E, such that everyone can compute E, but only I can compute the inverse of E. Then anyone can send me a secret message x, by computing $E(x)$, and sending this value to me. Since I am the only one who can compute the inverse of E, I and no-one else can retrieve x.

4.4.1 Creating a one-way function

This is how I create a one-way function E.

1. I pick two large primes p and q, and I put $n = pq$.
2. I compute $\varphi(n) = (p-1)(q-1)$
3. I choose an integer e which is coprime to $\phi(n)$, and which satisfies $1 < e < \phi(n)$.
4. I find an integer d such that $ed \equiv 1 \pmod{\varphi(n)}$
5. I define a function by
$$\begin{aligned} E : \mathbb{Z}_n &\to \mathbb{Z}_n \\ x &\mapsto x^e \end{aligned}$$
6. I make the numbers n and e available to everyone, so that anyone can compute E.

As we will prove, the inverse of E is the function $x \mapsto x^d$, so I can easily compute the inverse, since I know d. Although everyone knows the number n and the number e, note the following:

- It is HARD for anyone else to factor n, i.e. to find p and q.

- It is HARD for anyone else to compute $\varphi(n)$, since they don't know the factorization of n.
- It is IMPOSSIBLE for anyone to find d, unless they know $\varphi(n)$.

In these points, the word HARD means that it takes an enormous amount of time - so in practice it is impossible. Of course, we assume that p and q are very large, otherwise it would be easy to factor n, and anyone could find d.

Theorem 28. The inverse of E is the function $x \mapsto x^d$.

Proof. We must prove that $x^{ed} \equiv x \pmod{n}$, in other words, that n divides $(x^{ed} - x)$. Since $n = pq$, it is enough to show that p and q both divide $(x^{ed} - x)$. Consider first the case of p. If p divides x, then clearly p also divides $(x^{ed} - x)$. If p does not divide x, then Euler's theorem says

$$x^{p-1} \equiv 1 \pmod{p} \tag{2}$$

Since $(p-1)$ divides $\varphi(n)$, and $\varphi(n)$ divides $(ed-1)$, we see that $(p-1)$ divides $(ed-1)$. In other words, there is an integer b such that

$$b(p-1) = ed - 1$$

Raise both sides of the congruence (2) to b. We get

$$x^{ed-1} \equiv 1 \pmod{p}$$

and multiplying both sides by x gives the desired congruence. We can use exactly the same argument for q, and conclude that $x^{ed} \equiv x \pmod{n}$. □

4.4.2 How someone sends me a message

Suppose that Arnold Schwarzenegger wants to send me a message. He writes the message as a sequence of integers $m_1, m_2, \ldots$ as explained above. He then computes the numbers $E(m_1), E(m_2), \ldots$ and sends these numbers to me. Even if someone interrupts the message, he can not compute the integers m_i, because he does not know the number d.

4.4.3 How I decrypt a message I receive

I receive the numbers $E(m_1), E(m_2), \ldots$ from Arnold. I can then compute

$$\begin{aligned} m_1 &= E(m_1)^d \\ m_2 &= E(m_2)^d \end{aligned}$$

and so on. Then I translate these numbers into letters, and reads the message.

4.5 An example

Let us take an example. First I create a one-way function E.

1. I choose the primes $p = 23$ and $q = 11$. Of course, these are far to small to give an effective encryption for real life applications, but it will provide us with an example that is easy to follow. We get $n = 253$
2. I compute $\varphi(253) = 22 \cdot 10 = 220$
3. I must choose an integer e which is coprime to 220, and which satisfies $1 < e < 220$. I choose $e = 13$
4. I find an integer d such that $13d \equiv 1 \pmod{220}$. I can take $d = 17$. (See section 4.6 for more explanation on how to find d.)
5. I make the numbers $n = 253$ and $e = 13$ available to everyone, so that anyone can compute E.

If n had been very large, no-one would be able to factor n, or find $\varphi(n)$, or find d.
Arnold now wants to send me the message "YEAH". He knows n and e. The message is written as a sequence of numbers as

$$25 \quad 5 \quad 1 \quad 8$$

Arnold now computes (remember that we use arithmetic mod 253).

$$\begin{aligned} E(25) &= 25^e = 25^{13} = 27 \\ E(5) &= 15^e = 15^{13} = 136 \\ E(1) &= 1^e = 1^{13} = 1 \\ E(8) &= 8^e = 8^{13} = 248 \end{aligned}$$

and sends me the sequence

$$27 \quad 136 \quad 1 \quad 248$$

When I receive this sequence, I compute (raising each number to d)

$$\begin{aligned} 27^{17} &= 25 \\ 136^{17} &= 5 \\ 1^{17} &= 1 \\ 248^{17} &= 8 \end{aligned}$$

and I translate these numbers into the message "YEAH".

4.6 More about linear combinations

Given e and m, how do find an integer d such that $ed \equiv 1 \pmod{m}$? Well, there are several ways. You could try to put $d = 1$, then $d = 2$, then $d = 3$ and so on, and for each d, check whether $ed \equiv 1 \pmod{m}$, until you find a value of d that satisfies this congruence. A faster way is to check the numbers $m + 1$, $2m + 1$, $3m + 1$, etc until you find a number which is divisible by e. Divide this number by e to find d.

There is an even more effective (but also more complicated) method, which uses the Euclidean algorithm. To do this, we must learn how to express the integer 1 as a linear combination of two coprime integers. Knowing this, we can find integers x and y such that

$$1 = xe + ym$$

and then we can take $d = x$. How do we find the integers x and y? Answer: we can actually use the Euclidean algorithm. We show two examples below to illustrate the method. The steps are as follows:

1. Go through Euclid's algorithm. Whenver you have computed m_i, write out the equation
$$m_{i-2} = q \cdot m_{i-1} + m_i$$
2. Work your way backwards through the steps of the Euclidean algorithm to express 1 as a linear combination $xe + ym$ of e and m. When doing this, you use the equations
$$m_i = m_{i-2} - q \cdot m_{i-1}$$
3. Check your answer (i.e. check that $1 = xe + ym$), so that you have not made a mistake in the calculations

Example 50. Write 1 as a linear combination of 7 and 18.
We first go through Euclid's algorithm:

$$\begin{aligned} m_1 &= 18 \\ m_2 &= 7 \\ m_3 &= r(18, 7) = 4 \qquad \text{so } 18 = 2 \cdot 7 + 4 \\ m_4 &= r(7, 4) = 3 \qquad \text{so } 7 = 1 \cdot 4 + 3 \\ m_5 &= r(4, 3) = 1 \qquad \text{so } 4 = 1 \cdot 3 + 1 \\ m_6 &= r(3, 1) = 0 \end{aligned}$$

Now we can use these steps to express 1 as a linear combination of 7 and 18, as follows:

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (18 - 2 \cdot 7) - 7 = 2 \cdot 18 - 5 \cdot 7$$

Example 51. In the RSA example above, we wanted to find an integer d such that

$$13d \equiv 1 \pmod{220}$$

We first express 1 as

$$1 = 13x + 220y$$

using the Euclidean algorithm:

$$\begin{aligned} m_1 &= 220 \\ m_2 &= 13 \\ m_3 &= r(220, 13) = 12 \qquad \text{so } 220 = 16 \cdot 13 + 12 \\ m_4 &= r(13, 12) = 1 \qquad \text{so } 13 = 1 \cdot 12 + 1 \\ m_5 &= r(12, 1) = 0 \end{aligned}$$

So using back-substitution we get

$$1 = 13 - 12 = 13 - (220 - 16 \cdot 13) = 17 \cdot 13 - 1 \cdot 220$$

so we can take $x = 17$, $y = -1$. As explained, we can now take $d = 17$.