Exercises

Giulia Mauri

Politecnico di Milano

email: *giulia.mauri@polimi.it*
website: *http://home.deib.polimi.it/gmauri*

April 22, 2015

Overview

1. The Euclidean Algorithm

2. Block Ciphers

References:
[1] SAGE: http://sagemath.org
[2] PYTHON: http://docs.python.org

Greatest Common Divisor

Definition (Greatest Common Divisor)

The greatest common divisor of a and b is the largest positive integer dividing both a and b and is denoted $gcd(a, b)$.

Definition (Relatively Prime)

We say that a and b are relatively prime if $gcd(a, b) = 1$.

There are two standard ways for finding the gcd:

1. If you can factor a and b into primes, do so.
2. If a and b are large numbers, the gcd can be computed by using the Euclidean algorithm.

The Euclidean algorithm - An example

Example

Compute gcd(482,1180).

$$
\begin{aligned}
1180 &= 2 \cdot 482 + 216 \\
482 &= 2 \cdot 216 + 50 \\
216 &= 4 \cdot 50 + 16 \\
50 &= 3 \cdot 16 + 2 \\
16 &= 8 \cdot 2 + 0
\end{aligned}
$$

The last non zero remainder is the gcd, which is 2 in this case.

The Euclidean algorithm - Formal description

Suppose that a is greater than b. Represent a in the form:

$$a = q_1 b + r_1$$

If $r_1 = 0$, then b divides a and the greatest common divisor is b. If $r_1 \neq 0$, then continue by representing b in the form:

$$b = q_2 r_1 + r_2$$

Continue in this way until the remainder is zero:

$$\begin{aligned} r_1 &= q_3 r_2 + r_3 \\ \vdots &= \vdots \quad \vdots + \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

The conclusion is that:

$$gcd(a, b) = r_k$$

The Euclidean algorithm - Exercise

Exercise

Compute $d = gcd(360, 294)$ *in two ways: (i) by factoring each of the two numbers and then factorizing* d*; (ii) using the Euclidean algorithm.*

The Euclidean algorithm - Exercise

Exercise

Compute $d = gcd(360, 294)$ *in two ways: (i) by factoring each of the two numbers and then factorizing* d*; (ii) using the Euclidean algorithm.*

Solution

(i) Factorization:

$360 = 6^2 \cdot 10 = 2^3 \cdot 3^2 \cdot 5; \quad 294 = 2 \cdot 3 \cdot 7^2$

$d = 2 \cdot 3 = 6$

(ii) Euclidean algorithm:

$$\begin{aligned} 360 &= 1 \cdot 294 + 66 \\ 294 &= 4 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned}$$

$d = 6$

The extended Euclidean algorithm

The Euclidean algorithm can be used to determine if a positive integer $b < n$ has a multiplicative inverse modulo n by checking if $r_k = gcd(n, b) = 1$.

Definition

We define the following recursions:

$$s_k = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{if } k = 1 \\ s_{k-2} - q_{k-1}s_{k-1} & \text{if } k \geq 2 \end{cases}$$

$$t_k = \begin{cases} 0 & \text{if } k = 0 \\ 1 & \text{if } k = 1 \\ t_{k-2} - q_{k-1}t_{k-1} & \text{if } k \geq 2 \end{cases}$$

It follows that s_k and t_k always satisfy the following equality:

$$r_k = r_0 s_k + r_1 t_k$$

where $r_0 = \max(a, b)$ and $r_1 = \min(a, b)$.

The extended Euclidean algorithm

Definition (Multiplicative Inverse)

Suppose $gcd(r_0, r_1) = 1$. Then $r_1^{-1} \bmod r_0 = t_k \bmod r_0$

Proof.

From previous definition, we have that:

$$1 = gcd(r_0, r_1) = r_0 s_k + r_1 t_k.$$

Reducing this equation modulo r_0, we obtain:

$$t_k r_1 \equiv 1 \pmod{r_0}$$

The result follows. $\square$

The Euclidean algorithm - Exercise

Exercise

Find $d = gcd(841, 294)$ *and express* d *as* $r_0 s_k + r_1 t_k$.

The Euclidean algorithm - Exercise

Exercise

Find $d = gcd(841, 294)$ *and express* d *as* $r_0 s_k + r_1 t_k$.

Solution

k	r_k	q_k		s_k	t_k	$r_0 s_k + r_1 t_k$
0	841			1	0	841
1	294	2		0	1	294
2	253	1	$841 = 2{\cdot}294 + 253$	1	-2	253
3	41	6	$294 = 1{\cdot}253 + 41$	-1	3	41
4	7	5	$253 = 6 \cdot 41 + 7$	7	-20	7
5	6	1	$41 = 5 \cdot 7 + 6$	-36	103	6
6	1	6	$7 = 1 \cdot 6 + 1$	43	-123	1
7	0		$6 = 6 \cdot 1 + 0$	-294	841	0

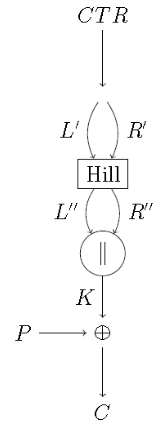
The last non null remainder is obtained for $k = 6$*, the two numbers are coprime and the two required coefficients are* $s = 43$ *and* $t = -123$.

Block Ciphers

Block ciphers encrypt blocks of several letters or number simultaneously. A change of one character in a plaintext block should change potentially all the characters in the corresponding ciphertext block. The Hill cipher is an example of block cipher.

Exercise

Consider the following cryptosystem operating in counter mode.



The Hill cipher operates in $\mathbb{Z}_{26}$ *and is defined by the equation:*

$$(L''R'') = (L'R')M \bmod 26$$

The key is:

$$M = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$$

The initial value of the counter is $IV = 9$.

Modes of operation - Exercise

Exercise

1. *Verify that the key of the Hill cipher is valid.*
2. *Find the inverse key and verify it.*
3. *Cipher the plaintext P=01100 10011 10101 01010.*
4. *Knowing that for $IV = 3$ the plaintext P=10100 01100 10111 10101 corresponds to the ciphertext C=00010 10101 10100 10000, find M.*

Solution (1-2)

It should be: $gcd(det(M), 26) = 1$.

$det(M) = 23 \rightarrow gcd(23, 26) = 1$

$inverse\_mod(23, 26) = 17$

$M^{-1} = 17 \begin{pmatrix} 5 & -2 \\ -4 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 10 & 17 \end{pmatrix} \; M \cdot M^{-1} = I$

$\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Modes of operation - Exercise

Solution (3)

At step 1 the counter is:

$$CTR_1 = 9 = 1001 = (10 \quad 1)$$

We have expressed the counter first in binary form and then as a vector of numbers in $\mathbb{Z}_{26}$*.*
The output of the Hill cipher is:

$$(10 \quad 1) \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = (14 \quad 25)$$

The first bits of the keystream, K_1*, are:*

$$K_1 = (14 \quad 25) = 01110 \quad 11001$$

Solution (3)

Therefore the ciphertext is:

$$C_1 = P_1 \oplus K_1 = 0110010011 \oplus 0111011001 = 0001001010$$

The procedure is the same for the second block, considering $CTR_2 = IV + 1 = 10$.

$$CTR_2 = 10 = 1010 = \begin{pmatrix} 10 & 10 \end{pmatrix}$$

The output of the Hill cipher is:

$$\begin{pmatrix} 10 & 10 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 24 & 18 \end{pmatrix}$$

The other bits of the keystream, K_2, *are:*

$$K_2 = \begin{pmatrix} 24 & 18 \end{pmatrix} = 11000 \quad 10010$$

Solution (3-4)

Therefore the ciphertext is:

$$C_2 = P_2 \oplus K_2 = 1010101010 \oplus 1100010010 = 0110111000$$

To find the key, the matrix M, remember that the Hill cipher do not operate on the plaintext but on the counter and gives the keystream as output. In this case, the keystream is $K = C \oplus P = 101101100100011 00101$, and the corresponding bits of the counter are $CTR = 3||4 = 00110100$. The bits of the keystream and the counter must be expressed as elements of $\mathbb{Z}_{26}$ and organized in a matrix to obtain the equation:

$$M = CTR^{-1}K = \begin{pmatrix} 0 & 11 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 22 & 25 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 19 & 0 \end{pmatrix} \begin{pmatrix} 22 & 25 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}$$