CIMPA research school on Group Actions in Arithmetic and Geometry

Finite fields – tutorial session
Solutions

February 26, 2020 — updated March 4, 2020

1. For each prime $p \leq 13$ and also for $p = 31$, list the values $a \in \mathbb{F}_p^\times$ which are primitive roots modulo p (i.e. generators of the cyclic group $\mathbb{F}_p^\times$). Next, for each a and for $n = 1, 2, \ldots, p-1$, compute a^n. Deduce a table of the discrete logarithm modulo p with respect to the primitive root a.

Solution.

For each primitive root α modulo p, we give the table of the exponentials in basis α, namely α^n for $n = 0, 1, \ldots, p-2$. One can view the values of n modulo $p-1$, while the values of α^n are modulo p. It is plain to deduce the table of the logarithms with respect to the primitive root α. We give explicitly this table only for $p = 31$ and $\alpha = 3$.

(a) $p = 2$, $\alpha = 1$

(b) $p = 3$, $\alpha = 1$ or $\alpha = 2$.

(c) $p = 5$, $\alpha = 2$ or $\alpha = 3$.

	$n =$	0	1	2	3
α^n :	$\alpha = 2$	1	2	4	3
	$\alpha = 3$	1	3	4	2

(d) $p = 7$, $\alpha = 3$ or $\alpha = 5$.

	$n =$	0	1	2	3	4	5
α^n	$\alpha = 3$	1	3	2	6	4	5
	$\alpha = 5$	1	5	4	6	2	3

(e) $p = 11$

From $2^5 = 32 \equiv -1 \pmod{11}$ it follows that 2 is a primitive root modulo 11 (a generator of the cyclic group $\mathbb{F}_{11}^\times$):

$n =$	0	1	2	3	4	5	6	7	8	9
$2^n =$	1	2	4	8	5	10	9	7	3	6

We have $\varphi(10) = 4$, $(\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$, the primitive roots modulo 11 are 2, $2^3 = 8$, $2^7 = 7$, $2^9 = 6$.

To get the table of exponentials 8^n we take the shift of the table for 2^n by 3:

$n =$	0	1	2	3	4	5	6	7	8	9
$8^n =$	1	8	9	6	4	10	3	2	5	7

To get the table of exponentials 7^n we reverse the order of the table for 8^n (since $7 = 8^{-1}$):

$n =$	0	1	2	3	4	5	6	7	8	9
$7^n =$	1	7	5	2	3	10	4	6	9	8

To get the table of exponentials 6^n we reverse the order of the table for 2^n (since $6 = 2^{-1}$):

$n =$	0	1	2	3	4	5	6	7	8	9
$6^n =$	1	6	3	7	9	10	5	8	4	2

(f) $p = 13$

We have $\varphi(12) = 4$, the primitive roots modulo 13 are 2, $2^5 = 6$, $2^7 = 11$, $2^{11} = 7$.

The table of 2^n for $n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ is

$n =$	0	1	2	3	4	5	6	7	8	9	10	11
$2^n =$	1	2	4	8	3	6	12	11	9	5	10	7

The table for 6^n is obtained by shifting by 5 the table for 2^n:

$$6^n : \qquad 1,\ 6,\ 10,\ 8,\ 9,\ 2,\ 12,\ 7,\ 3,\ 5,\ 4,\ 11.$$

The table for 11^n is the reverse of the table for 6^n:

$$11^n : \qquad 1,\ 11,\ 4,\ 5,\ 3,\ 7,\ 12,\ 2,\ 9,\ 8,\ 10,\ 6.$$

The table for 7^n is the reverse of the table for 2^n:

$$7^n : \qquad 1,\ 7,\ 10,\ 5,\ 9,\ 11,\ 12,\ 6,\ 3,\ 8,\ 4,\ 2.$$

(g) $p = 31$

Since $\varphi(30) = 8$, there are 8 primitive roots modulo 31.

From $2^5 \equiv 1 \pmod{31}$, it follows that 2 has order 5 in $\mathbb{F}_{31}^{\times}$, hence is not a primitive root modulo 31.

A primitive root modulo 31 is 3. The table of 3^n for $n = 1, 2, \ldots, 30$ is given by

$n =$	0	1	2	3	4	5	6	7	8	9
$3^n =$	1	3	9	27	19	26	16	17	20	29

$n =$	10	11	12	13	14	15	16	17	18	19
$3^n =$	25	13	8	24	10	30	28	22	4	12

$n =$	20	21	22	23	24	25	26	27	28	29
$3^n =$	5	15	14	11	2	6	18	23	7	21

The primitive roots modulo 31 are

$$3,\ 3^7 = 17,\ 3^{11} = 13,\ 3^{13} = 24,\ 3^{17} = 22,\ 3^{19} = 12,\ 3^{23} = 11,\ 3^{29} = 21.$$

One checks indeed that the numbers

$$3 \times 21 = 63,\ 17 \times 11 = 187,\ 13 \times 12 = 156,\ 24 \times 22 = 528$$

are congruent to 1 modulo 31.

The table for 17^n is the shift by 7 of the table for 3^n, the table for 13^n is the shift by 4 of the table for 17^n, the table for 24^n is the shift by 2 of the table for 13^n, and we get the other tables by reversing the order.

The table of the discrete logarithms with respect to 3 modulo 31 is the following (the first row is 3^n modulo 31, the second row is n modulo 30):

1	2	3	4	5	6	7	8	9	10
0	24	1	18	20	25	28	12	2	14
11	12	13	14	15	16	17	18	19	20
23	19	11	22	21	6	7	26	4	8
21	22	23	24	25	26	27	28	29	30
29	17	27	13	10	5	3	16	9	15

2. Binary error correcting codes.

Let $n \in \{1, 2, 3, 4\}$. Among 2^n playing cards, you select one without telling me which one it is. I display some of them and I ask you whether the card you selected is one of them. You answer yes or no.

(a) How many questions should I ask in order to know which card you selected?

(b) Same problem, but now you are allowed to give me at most one wrong answer, and I want to decide whether or not all you answers were right. If you gave always the right answer, I want to know which card you selected (*error detecting code*).

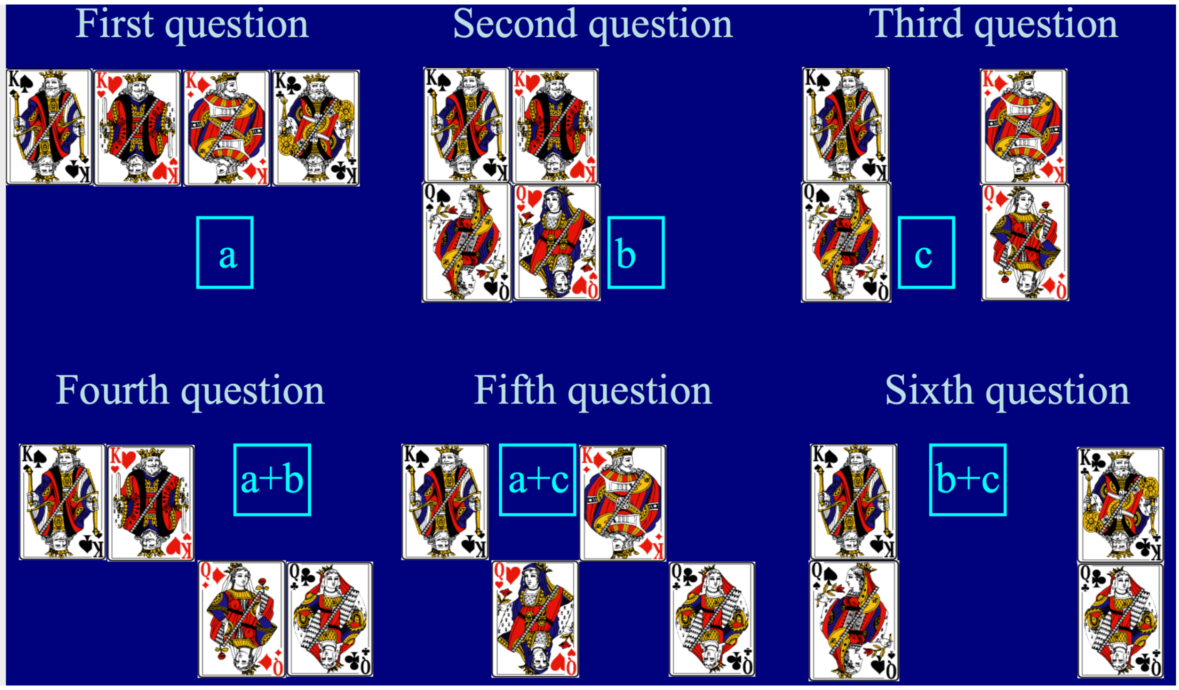
(c) Same problem, again you are allowed to give me at most one wrong answer, but now, I want to know which card you selected, even if one of your answers was wrong (*error correcting code*).

Solution.

(a) Given 2^n card, label them starting from 0 to $2^n - 1$; write the labels in binary form. Ask n questions, for the k–th one, display the cards having a label with 1 for the k–th binary digit. The sequence of yes and no gives you the binary expansion of the answer, with the digit 1 for yes and 0 for no.

(b) In order to detect a wrong answer, ask one more question using the parity bit. The number of questions is $n + 1$.

(c) In order to correct a wrong answer, use an error correcting code.
• For $n = 1$ and 2 cards, ask 3 questions using the repetition code (display the same card 3 times). The corresponding error correcting code is Example 80 in the notes [1].
• For $n = 2$ and 4 cards, ask 5 questions: repeat twice the two questions which give the solution when there is no wrong answer, and for the last one use the parity bit. The corresponding error correcting code is Example 82 in the notes [1].
• For $n = 3$ and 8 cards, ask 6 questions: questions 1,2,3 are the ones which give the solution when there is no wrong answer, the next 3 questions are the parity bits between questions (1 and 2), (2 and 3), (1 and 3). The corresponding error correcting code is Example 83 in the notes [1].



- For $n = 4$ and 16 cards, ask 7 questions only using Hamming's code.

3. Three people are in a room, each has a hat on his head, the colour of which is black or white. Hat colours are chosen randomly. Everybody sees the colour of the hat of everyone else, but not on ones own. People do not communicate with each other. Everyone tries to guess (by writing on a piece of paper) the colour of their hat. They may write: Black/White/Abstain.

   The people in the room win together or lose together as a team. The team wins if at least one of the three persons does not abstain, and everyone who did not abstain guessed the colour of their hat correctly.

   (a) What could be the strategy of the team to get the highest probability of winning? What is this probability?

   (b) Same questions with seven people.

   Solution.

   (a) With three people, one solution is that the team bets that the three colours are not the same. When they see twice the same colour on the heads of the two other people, they bet that their own hat is not of that colour. If they see two different colours, they abstain.

   There are 8 possible distributions of the colours, two of them where the hats have all the same colours (white–white–white or black–black–black); in this case they all bet the wrong colour and the team looses. In the remaining 6 cases, the team wins. Hence the probability of winning is $3/4 = 75\%$.

   This is the best probability for this game, but there are other equivalent strategies: they select two distributions of colours which have no common element, like white–black–white and black–white–black, and they bet that these two distributions do not correspond to the correct answer.

   (b) With seven people, use the $[7, 4]$ Hamming code in place of the $[3, 1]$ repetition code. Replace the two colours by 0 and 1, so that the distribution of colours corresponds to an element in $\mathbb{F}_2^7$. The team bets that the distribution of colours is not an element of the Hamming code. When one member of the team sees the 6 other colours, he or she looks at the two possible elements in $\mathbb{F}_2^7$ which correspond to the distribution of hats. If one of them lies in the Hamming code, he or she writes the colour corresponding to the other element. Otherwise, the two possible answers correspond to elements which lie in two different Hamming balls of radius 1, this person does not know which is the center of the Hamming ball containing the right solution and in this case he or she abstains. The team looses in 16 cases, there are $2^7 = 128$ possible distributions, so he wins in $2^7 - 2^4 = 128 - 16 = 112$ cases, the probability of winning is $7/8 = 87.5\%$, and this is optimal.

The optimality for each of the questions in the exercises 2 and 3 is proved by counting the number of Hamming balls of radius 1 and the number of points in each such ball.

References

[1] `http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/FiniteFields.pdf`

[2] `http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/Coding.pdf`

Remark. *These exercises and the solutions are now included in the version of the notes* [1] *revised on March 3, 2020.*