Foundations of informatics: a bridging course
Week 2: Mathematical tools

MICHAEL NÜSKEN, 26.-30.09.05

1. Number theory

Exercise 1.1 (EEA, modular inverse). Use paper and pencil for this exercise. For each of the following pairs (a, b) compute two integers $s \in \mathbb{Z}$ and $t \in \mathbb{Z}$ such that $1 = sa + tb$ or prove that they do not exist. For the remaining items compute the wanted inverses if possible.

(i) $a = 33$, $b = 54$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	33		1	0	
1	54	0	0	1	$33 = 0 \cdot 54 + 33$
2	33	1	1	0	$21 = 1 \cdot 33 + 54$
3	21	1	-1	1	$12 = 1 \cdot 21 + 33$
4	12	1	2	-1	$9 = 1 \cdot 12 + 21$
5	9	1	-3	2	$3 = 1 \cdot 9 + 12$
6	3	3	5	-3	$0 = 3 \cdot 3 + 9$
7	0		-18	11	

So we get the gcd $3 = 5 \cdot 33 + -3 \cdot 54$. ◯

(ii) $a = 77$, $b = 89$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	77		1	0	
1	89	0	0	1	$77 = 0 \cdot 89 + 77$
2	77	1	1	0	$12 = 1 \cdot 77 + 89$
3	12	6	-1	1	$5 = 6 \cdot 12 + 77$
4	5	2	7	-6	$2 = 2 \cdot 5 + 12$
5	2	2	-15	13	$1 = 2 \cdot 2 + 5$
6	1	2	37	-32	$0 = 2 \cdot 1 + 2$
7	0		-89	77	

So we get the gcd $1 = 37 \cdot 77 + -32 \cdot 89$. ◯

(iii) $a = 579$, $b = 982$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	579		1	0	
1	982	0	0	1	$579 = 0 \cdot 982 + 579$
2	579	1	1	0	$403 = 1 \cdot 579 + 982$
3	403	1	-1	1	$176 = 1 \cdot 403 + 579$
4	176	2	2	-1	$51 = 2 \cdot 176 + 403$
5	51	3	-5	3	$23 = 3 \cdot 51 + 176$
6	23	2	17	-10	$5 = 2 \cdot 23 + 51$
7	5	4	-39	23	$3 = 4 \cdot 5 + 23$
8	3	1	173	-102	$2 = 1 \cdot 3 + 5$
9	2	1	-212	125	$1 = 1 \cdot 2 + 3$
10	1	2	385	-227	$0 = 2 \cdot 1 + 2$
11	0		-982	579	

So we get the gcd $1 = 385 \cdot 579 + -227 \cdot 982$. ◯

(iv) 12^{-1} in $\mathbb{Z}_{23}$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	23		1	0	
1	12	1	0	1	$11 = 1 \cdot 12 + 23$
2	11	1	1	-1	$1 = 1 \cdot 11 + 12$
3	1	11	-1	2	$0 = 11 \cdot 1 + 11$
4	0		12	-23	

So we get the gcd $1 = -1 \cdot 23 + 2 \cdot 12$ and thus $12^{-1} = 2$ in $\mathbb{Z}_{23}$.

Alternatively, we can use the symmetric remainder system giving a shorter euclidean algorithm scheme:

i	r_i	q_i	s_i	t_i	comment
0	23		1	0	
1	12	2	0	1	$-1 = 2 \cdot 12 + 23$
2	-1	-12	1	-2	$0 = -12 \cdot -1 + 12$
3	0		12	-23	

So we get the gcd $-1 = 1 \cdot 23 + -2 \cdot 12$ and thus again $12^{-1} = 2$ in $\mathbb{Z}_{23}$. ◯

(v) 12^{-1} in $\mathbb{Z}_{21}$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	21		1	0	
1	12	1	0	1	$9 = 1 \cdot 12 + 21$
2	9	1	1	-1	$3 = 1 \cdot 9 + 12$
3	3	3	-1	2	$0 = 3 \cdot 3 + 9$
4	0		4	-7	

So we get the gcd $3 = -1 \cdot 21 + 2 \cdot 12$ and since it is not 1 (nor -1) there is no inverse of 12 in $\mathbb{Z}_{21}$. ◯

(vi) 23^{-1} in $\mathbb{Z}_{100}$.

Solution.

i	r_i	q_i	s_i	t_i	comment
0	100		1	0	
1	23	4	0	1	$8 = 4 \cdot 23 + 100$
2	8	2	1	-4	$7 = 2 \cdot 8 + 23$
3	7	1	-2	9	$1 = 1 \cdot 7 + 8$
4	1	7	3	-13	$0 = 7 \cdot 1 + 7$
5	0		-23	100	

So we get the gcd $1 = 3 \cdot 100 + -13 \cdot 23$. ○

Exercise 1.2 (Repeated squaring). Use paper and pencil for this exercise. How many multiplications do you need to compute x^{382}?

(i) Find an algorithm that uses 14 multiplications.

Solution. Noting that $382 = (1\,0111\,1110)_2$ the standard repeated squaring algorithm gives us the following 14 steps:

i	x^e	binary(e)
0	x^1	1
1	x^2	10
2	x^4	100
3	x^5	101
4	x^{10}	1010
5	x^{11}	1011
6	x^{22}	1 0110
7	x^{23}	1 0111
8	x^{46}	10 1110
9	x^{47}	10 1111
10	x^{94}	101 1110
11	x^{95}	101 1111
12	x^{190}	1011 1110
13	x^{191}	1011 1111
14	x^{382}	1 0111 1110

○

(ii) Find an algorithm that uses 12 multiplications.

Solution. We could try the ternary representation $382 = 112011_3$ but since cubing costs two multiplications this also gives a 14 step algorithm. It could be enhanced to give a 13 step algorithm if we use that 11_3 is computed and appears twice as a digit pattern. Yet, that's it. But we can use $382 = 2 \cdot 191$ and $190 = 2 \cdot 5 \cdot 19$: First, compute x^{19}, then raise that to the fifth power, then square to obtain x^{190}. Multiplying by x and squaring yields x^{382}. This gives

the following 12 step algorithm:

i	x^e	binary(e)
0	x	1
1	x^2	10
2	x^4	100
3	x^8	1000
4	x^9	1001
5	x^{18}	1 0010
6	x^{19}	1 0011
7	x^{38}	10 0110
8	x^{76}	100 1100
9	x^{90}	101 1111
10	x^{190}	1011 1110
11	x^{191}	1011 1111
12	x^{382}	1 0111 1110

○

(iii) Can you find an algorithm that uses 11 multiplitations?

Solution. It is very difficult to find such an algorithm. Actually, any algorithm to get x^{191} will always need at least 11 steps. So first computing that and then squaring gives nothing better than 12 steps. Thus if anything better shall be found we must look for another decomposition of 382 as a sum of two smaller numbers. After some trying, $382 = 198 + 184$ proves to work. We have to choose the algorithm leading to 184 such that the remaining 14 that miss to 198 are already computed. This is the resulting algorithm:

i	x^e	binary(e)
0	x	1
1	x^2	10
2	x^4	100
3	x^5	101
4	x^9	1001
5	x^{14}	1110
6	x^{23}	1 0111
7	x^{46}	10 1110
8	x^{92}	101 1100
9	x^{184}	1011 1000
10	x^{198}	1 0111 0000
11	x^{382}	1 0111 1110

○

Some side calculations: $382 = 101111110_2 = 112011_3 = 11332_4 = 3012_5 = 1434_6 = 1054_7 = 576_8$, $382 = 2 \cdot 191$, $190 = 2 \cdot 5 \cdot 19$, $189 = 7 \cdot 3^3$.

Exercise 1.3 (Modular calculations). Use paper and pencil for this exercise. Calculate $2^{1234567} \bmod 11$. Explain your reasoning.

Solution. Of course, this can be solved by brute force: compute $2^{1234567}$ (it's a small number: only 371 642 digit number, nothing compared to infinity…) and

then divide by 11 with remainder. If you have a lazy day, then this might enjoy you. Of course, you would be clever and use repeated squareing…

Already much better is to compute $2^{1234567}$ in $\mathbb{Z}_{11}$, namely reducing modulo 11 after each single step. Using repeated squaring this can be done in ten minutes or so…

A little more thinking makes this solvable within a glance: The little theorem of Fermat ('f'ermat) gives us $2^{10} = 1$ in $\mathbb{Z}_{11}$ because 11 is prime and $2 \neq 0$ in $\mathbb{Z}_{11}$ (ie. $\gcd(2, 11) = 1$). Now,

$$2^{1234567} = \big(\underbrace{2^{10}}_{=1}\big)^{123456} \cdot 2^7 = 2^7.$$

Further, $2^5 = -1$ (could have been either this or 1, since its square is 1) and $2^2 = 4$ so $2^7 = -4 = 7$ in $\mathbb{Z}_{11}$ and we are done within moments. ◯

Exercise 1.4 (Polynomials). Polynomials, like $m = x^8 + x^4 + x^3 + x + 1$ in $\mathbb{Z}_2[x]$, behave in various ways like numbers and often operations are easier with them since there is no carry when they are added.

(i) Compute $(x^3 + x + 1) \cdot (x^7 + x^3 + 1)$ in $\mathbb{Z}_2[x]$.

Solution. The only non-standard thing to consider is that $1 + 1 = 0$ when working over $\mathbb{Z}_2$:

$$\begin{aligned}(x^3 + x + 1) \cdot (x^7 + x^3 + 1) &= x^{10} + x^6 + x^3 \\ &\quad + x^8 + x^4 + x \\ &\quad + x^7 + x^3 + 1 \\ &= x^{10} + x^8 + x^7 + x^6 + x^4 + x + 1 \qquad ◯\end{aligned}$$

(ii) Compute the quotient and remainder of $x^{10} + x^2 + x + 1$ on division by m in $\mathbb{Z}_2[x]$.

Solution. Division with remainder with polynomials is almost the same as with numbers. Only there are no carries. Over $\mathbb{Z}_2$ we have the further advantage that $-1 = 1$ and thus adding and subtracting is the same. We get:

$$\begin{array}{rl} x^{10} \qquad\qquad + x^2 + x + 1 = (x^2) \cdot m + (x^6 + x^5 + x^3 + x + 1) & \\ \underline{x^{10} + x^6 + x^5 + x^3 + x^2} & \\ \qquad x^6 + x^5 + x^3 \qquad + x + 1 & \end{array}$$

Thus the quotient is x^2 and the remainder $x^6 + x^5 + x^3 + x + 1$. ◯

Also the Extended Euclidean Algorithm can be carried out with polynomials:

(iii) Compute the inverse $(x^2 + x + 1)^{-1}$ in $\mathbb{Z}_2[x]$ modulo m.

Solution. We simply execute the extended Euclidean algorithm for polynomials (noting that 'small' for polynomials means small degree). We obtain:

i	r_i	q_i	s_i	t_i
0	$x^8 + x^4 + x^3 + x + 1$		1	0
1	$x^2 + x + 1$	$x^6 + x^5 + x^3$	0	1
2	$x + 1$	x	1	$x^6 + x^5 + x^3$
3	1	$x + 1$	x	$x^7 + x^6 + x^4 + 1$
4	0		$x^2 + x + 1$	$x^8 + x^4 + x^3 + x + 1$

So we get the gcd $1 = (x)\cdot(x^8+x^4+x^3+x+1)+(x^7+x^6+x^4+1)\cdot(x^2+x+1)$ and the inverse of x^2+x+1 in $\mathbb{Z}_2[x]/\left\langle x^8+x^4+x^3+x+1\right\rangle$ (or in $\mathbb{Z}_2[x]$ modulo $x^8+x^4+x^3+x+1$, which is no more than another language) is $x^7+x^6+x^4+1$. ◯

Foundations of informatics: a bridging course
Week 2: Mathematical tools

MICHAEL NÜSKEN, 26.-30.09.05

2. Probability

Exercise 2.1 (Roulette). We consider the american roulette. The center of a game is a spinning disk with 38 small slots at the edge where a heavy metal ball fits that is sent spinning in the opposite direction. Occasionally it will settle in one of the boxes which are labelled with the number 1 through 36, each coloured either red or green, and the special green boxes 0 and 00. The player bets on the outcome of the game. She has various possible things to choose from: she can bet on a single number (also 0 or 00). If she wins (that is the outcome is as predicted) then she gets paid 36 times the amount she placed on the number. More on the game you find at `http://www.glueckspielschule.de/roulette/index.html` in German or at `http://www.ildado.com/roulette_rules.html` in English.

(i) Give the appropriate probability space of a (fair) roulette. (This includes the definition of a distribution!)

Solution. Take $U = \{0, 00, 1, 2, 3, 4, \ldots, 36\}$ and let $P(u) = \frac{1}{38}$ for each possible outcome $u \in U$. (Thus P is the uniform distribution on U. Any other would not be fair.) ◯

For notational convenience let X be the random variable such that $X(u) = u$.

(ii) What is the probability to win if you bet that

(a) the number is even.

Solution. prob(X is even (and not 0 or 00)) $= \frac{18}{38} = \frac{9}{19}$ since there are 18 good outcomes out of $\#U = 38$ possible ones. ◯

(b) the number is in the right column.

Solution. prob(X is in the right column) $= \frac{12}{38} = \frac{6}{19}$ since there are 12 good outcomes out of $\#U = 38$ possible ones. ◯

(c) the number is at a given corner (eg. 1,2,4,5).

Solution. prob(X is on the selected corner) $= \frac{4}{38} = \frac{2}{19}$ since there are 4 good outcomes out of $\#U = 38$ possible ones. ◯

(iii) What is the expected win if you play 1 € on

(a) a single number.

Solution. Let W be the win if we bet 1 € on a single number. Then E(W) = 35 € $\cdot \frac{1}{38}$ + -1 € $\cdot \frac{37}{38} = -\frac{1}{19}$ €, so in average you loose about 5 cent. ◯

Remark: If you have calculated the payout then note that the win is the payout minus the bet, so the net payout.

(b) a half like 'red' or 'even'. Let W be the win if we bet 1 € on a half. Then E(W) = 1 € $\cdot \frac{18}{38}$ + -1 € $\cdot \frac{20}{38} = -\frac{1}{19}$ €, so in average you loose about 5 cent.

Exercise 2.2. Consider playing with three dice.

(i) Give the appropriate probability space for rolling three (fair) dice. (This includes the definition of a distribution!)

Solution. The right space is the cartesian product of three copies of the set $\{1,2,3,4,5,6\}$ of possible outcomes of one die. So

$$U = \{(1,1,1),(1,1,2),\ldots,(6,6,6)\}\,.$$

Since the dice shall be fair we use the uniform distribution on this set: $P(u) = \frac{1}{6^3} = \frac{1}{216}$ for all possible outcomes $u \in U$. ◯

For notational convenience we use the random variables X_1, X_2, X_3, where X_i gives the outcome of the i-th die. (Note that we distinguish the three dice, say the first one is red, the second green and the third blue. It would also be possible to do it otherwise but the resulting space and distribution would be much more complicated…)

As can be seen easily, the three random variables are equally distributed, ie. $\text{prob}(X_1 = x) = \text{prob}(X_2 = x) = \text{prob}(X_3 = x)$ for each $x \in \{1,2,3,4,5,6\}$, and of course $\text{prob}(X_i = x) = \frac{1}{6}$ as can be easily calculated. (Note that all we know at start is $\text{prob}(X_1 = x_1, X_2 = x_2, X_3 = x_3) = \frac{1}{6^3}$. Actually, the three random variables X_i are independent but we do not need that.)

(ii) Compute the expected sum of the three dice.

Solution. We have to compute the expected value of the sum $S = X_1 + X_2 + X_3$ of the three dice. Thus

$$\mathrm{E}(S) = \mathrm{E}(X_1) + \mathrm{E}(X_2) + \mathrm{E}(X_3)$$

and $\mathrm{E}(X_i) = 1\cdot\frac{1}{6} + 2\cdot\frac{1}{6} + 3\cdot\frac{1}{6} + 4\cdot\frac{1}{6} + 5\cdot\frac{1}{6} + 6\cdot\frac{1}{6} = \frac{7}{2} = 3.5$, thus $\mathrm{E}(S) = 3\cdot 3.5 = 10.5$. ◯

(iii) Compute the probability that

(a) all three dice show the same number.

Solution. We calculate

$$\begin{aligned}\text{prob}(X_1 = X_2 = X_3) &= \sum_{x\in\{1,\ldots,6\}} \text{prob}(X_1 = x, X_2 = x, X_3 = x)\\ &= 6\cdot\frac{1}{6^3} = \frac{1}{36}.\end{aligned}$$ ◯

(b) all three dice show a different number.

Solution. We calculate

$$\begin{aligned}\text{prob}(X_1 \neq X_2 \neq X_3 \neq X_1) &= \sum_{x\in U, x_1\neq x_2\neq x_3\neq x_1} \text{prob}(X_1 = x_1, X_2 = x_2, X_3 = x_3)\\ &= 6\cdot 5\cdot 4\cdot\frac{1}{6^3} = \frac{5}{9}.\end{aligned}$$ ◯

(iv) Compute the conditional probability that the sum is even given that no six occurs.

Solution. If no six occurs the possible outcomes of each die are $\{1, 2, 3, 4, 5\}$ each with probability $\frac{1}{5}$. That their sum is even means that either all show an even result, so each chooses between 2 and 4 giving $2^3 = 8$ possibilities, or exactly one shows an even result giving three times (depending on which die shows the even result) $2 \cdot 3^2$ possibilities. In total we obtain

$$\text{prob}\,(S \text{ even} \,|\, \forall i \colon X_i \neq 6) = \frac{2^3 + 3 \cdot 2 \cdot 3^2}{5^3} = \frac{62}{125}.$$ ○

Exercise 2.3. Give a further example of a randomized program where a loop terminates only with a certain probability. Compute the running time.

Solution. There are various examples… ○

Foundations of informatics: a bridging course
Week 2: Mathematical tools

MICHAEL NÜSKEN, 26.-30.09.05

3. Linear Algebra

Exercise 3.1 (Linear system of equations and determinants). Solve the linear system

$$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \\ 1 & 0 & 0 \end{bmatrix} x = \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix}$$

over the field $\mathbb{Z}_7$ and calculate the determinant of the matrix.

Solution. We perform the Gauß-Jordan algorithm over $\mathbb{Z}_7$:

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 2 & 1 & -1 \\ 1 & 0 & 0 & 2 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 2 & 1 & -1 \\ 0 & 0 & -3 & -1 \end{array}\right] \quad \begin{array}{l} \\ \text{divide this row by } 2 \\ \text{divide this row by } -3 \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 3 & 3 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & 1 & -2 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & -2 \end{array}\right]$$

Thus we read off that $x = [2, -3, -2]^T$ is the only solution and the determinant of the matrix is $(-1)^0 \cdot 2 \cdot (-3) = 1$ (in $\mathbb{Z}_7$). (Note that the determinant is the product of all those scalars which we used to divide rows by and a (-1) for each swap. Here, we used no swap and we divided the second row by 2 and the third row by -3.) ◯

Of course, there are other possibilities to calculate the determinant but this one is quite cheap (even if you need only the determinant!).