Problem 6.1.

1. Compute the following:
   (a) $6^{365} \bmod 7$,

   Solution:

   We have $6 \equiv -1 \bmod 7$, so $6^{365} \equiv -1 \equiv 6 \bmod 7$.

   (b) $2^{981} \bmod 5$,

   Solution:

   We have $2^2 \equiv -1 \bmod 5$, so

   $$2^{981} = 2 \cdot 4^{490} \equiv 2 \cdot (-1)^{490} = 2 \bmod 5.$$

   (c) $3^{23} \cdot 5^{24} \bmod 16$,

   Solution:

   We have

   $$3^{23} \cdot 5^{24} = 5 \cdot 15^{23} \equiv (-1)^{23} \cdot 5 \equiv -5 \equiv 11 \bmod 16.$$

   (d) $392 \cdot 26019 \bmod 13$.

   Solution:

   Observe that $392 = 13 \cdot 30 + 2$ and $26019 = 13 \cdot 2000 + 19$, so $392 \cdot 26019 \equiv 2 \cdot 19 \equiv 38 \equiv 12 \bmod 13$.

   Relevant slide : 330

2. Prove that for any integer x that is not divisible by 3, and any even integer n, we have $x^n \equiv 1 \bmod 3$.

   Solution:

   Let $n = 2m$. Since 3 does not divide x, it does not divide x^m either. Then, either $x^m \equiv 1 \bmod 3$ or $x^m \equiv 2 \bmod 3$. If $x^m \equiv 1 \bmod 3$, then

   $$x^n = (x^m)^2 \equiv 1^2 = 1 \bmod 3,$$

   and if $x^m \equiv 2 \bmod 3$, then

   $$x^n = (x^m)^2 \equiv 2^2 = 4 \equiv 1 \bmod 3.$$

   Relevant slide : 330

3. Compute the remainder of $2^{761^{435}+97!}$ modulo 3.

Solution:

We have $2 \equiv -1 \bmod 3$. Since $761^{435} + 97!$ is odd, $2^{761^{435}+97!} \equiv -1 \equiv 2 \bmod 3$.
An alternative solution makes use of the previous question: $761^{435} + 97!$ is odd, so $761^{435} + 97! - 1$ is even. From the previous question, $2^{761^{435}+97!-1} \equiv 1 \bmod 3$. So

$$2^{761^{435}+97!} \equiv 2 \cdot 2^{761^{435}+97!-1} \equiv 2 \bmod 3.$$

Relevant slides : 330, 334

4. Show that there is no number n which is congruent to 3 mod 4 and to 5 mod 8.

Solution:

If n is congruent to 5 mod 8, then $n = 5+8\cdot k$ for some integer k, so $n = 5+4(2\cdot k)$, i.e. $n \equiv 5 \equiv 1 \bmod 4$, so n can not be congruent to 3 mod 4.

5. Let m, x and e be positive integers. Let $e = (b_k \dots b_0)_2$ be the binary representation of e (i.e., $b_i \in \{0, 1\}$, and $e = \sum_{i=0}^{k} b_i 2^i$). Let $x_0 = x \bmod m$ and for each $i > 0$, let $x_i = x_{i-1}^2 \bmod m$. Show that

$$x^e \equiv \prod_{i=0}^{k} x_i^{b_i} \bmod m.$$

Solution:

Let us compute $x^e \bmod m$:

$$\begin{aligned}
x^e &\equiv x^{\sum_{i=0}^{k} b_i 2^i} \bmod m \\
&\equiv x^{b_0 + 2b_1 + \cdots + 2^k b_k} \bmod m \\
&\equiv x^{b_0} x^{2b_1} \cdots x^{2^k b_k} \bmod m \\
&\equiv (x^{b_0} \bmod m)(x^{2b_1} \bmod m) \cdots (x^{2^k b_k} \bmod m) \\
&\equiv x_0^{b_0} [x_0^2]^{b_1} \cdots [x_0^{2^k}]^{b_k} \bmod m \\
&\equiv x_0^{b_0} x_1^{b_1} \cdots x_k^{b_k} \bmod m \\
&\equiv \prod_{i=0}^{k} x_i^{b_i} \bmod m.
\end{aligned}$$

A more rigorous approach would consist in replacing the dots $(\cdots)$ from the expressions above by an induction step. In this case the proof is as follows. First note that for each i, $x_i \equiv x^{2^i} \bmod m$. Indeed, $x_0 \equiv x \equiv x^{2^0} \bmod m$; suppose by induction that $x_i \equiv x^{2^i} \bmod m$ for a certain index $i \geq 0$; then

$$x_{i+1} \equiv x_i^2 \equiv \left(x^{2^i}\right)^2 = x^{2^{i+1}} \bmod m,$$

concluding the induction. Now,

$$\prod_{i=0}^{k} x_i^{b_i} \equiv \prod_{i=0}^{k} \left(x^{2^i}\right)^{b_i} \equiv \prod_{i=0}^{k} x^{b_i 2^i} \equiv x^{\sum_{i=0}^{k} b_i 2^i} \equiv x^e \bmod m.$$

6. Use the previous question to compute $5^{59} \bmod 23$.

Solution:

We have $59 = (111011)_2$. Define

$$\begin{aligned}
x_0 &= 5,\\
x_1 &= 5^2 \bmod 23 = 2,\\
x_2 &= 2^2 \bmod 23 = 4,\\
x_3 &= 4^2 \bmod 23 = 16,\\
x_4 &= 16^2 \bmod 23 = 256 \bmod 23 = 3,\\
x_5 &= 3^2 \bmod 23 = 9.
\end{aligned}$$

Then,

$$\begin{aligned}
5^{59} &\equiv x_0 \cdot x_1 \cdot x_3 \cdot x_4 \cdot x_5 \equiv 5 \cdot 2 \cdot 16 \cdot 3 \cdot 9\\
&\equiv (5 \cdot 4) \cdot (8 \cdot 3) \cdot 9 = -3 \cdot 1 \cdot 9 \equiv -27 \equiv 19 \bmod 23.
\end{aligned}$$

This method of exponentiation is called "square and multiply". It is a very efficient algorithm used to compute modular exponentiations with huge numbers. Note that this algorithm uses at most $2k$ multiplications (k multiplications while computing x_i, $i = 0, \ldots, 5$ and another k when multiplying them), where $k = \lfloor log_2 e \rfloor$.

Problem 6.2.

(This problem mostly requires the same techniques of the previous one. You can solve this to practise more on modular arithmetic.)

1. Compute the following without using a calculator:
   (a) $37^{121} \bmod 7$,

   Solution:

   We have $37 \equiv 2 \bmod 7$. Also, $2^3 \equiv 1 \bmod 7$, so

   $$37^{121} \equiv 2^{3 \cdot 40 + 1} \equiv (8)^{40} \cdot 2 \equiv 2 \bmod 7.$$

   (b) $18^{243} \bmod 19$,

   Solution:

   We have $18 \equiv -1 \bmod 19$, so

   $$18^{243} \equiv (-1)^{243} \equiv -1 \equiv 18 \bmod 19.$$

   (c) $3^{17!} \bmod 27$,

   Solution:

   We have $3^3 = 27 \equiv 0 \bmod 27$, so

   $$3^{17!} \equiv 3^3 \cdot 3^{17!-3} \equiv 0 \bmod 27.$$

(d) $460002 \cdot 25 \bmod 23$,

Solution:

We have $460002 = 23 \cdot 20000 + 2$, so $460002 \equiv 2 \bmod 23$. Therefore

$$460002 \cdot 25 \equiv 2 \cdot 2 \equiv 4 \bmod 23.$$

(e) $1112233445566778899753100246813 79 \bmod 8$,

Solution:

$$\begin{aligned} 10^0 &\equiv 1 \bmod 8 \\ 10^1 &\equiv 2 \bmod 8 \\ 10^2 &\equiv 4 \bmod 8 \\ 10^n &\equiv 0 \bmod 8 \quad \forall\, n \geq 3 \end{aligned}$$

Thus,

$$\begin{aligned} &1112233445566778899753100246813 79 \equiv 379 \equiv 3 \times 4 + 7 \times 2 + 1 \\ &\equiv 4 + 6 + 1 \equiv 3 \bmod 8. \end{aligned}$$

Relevant slide : 330

2. Compute $65363549000917 \bmod 9$.

Solution:

As seen in class, a decimal number is congruent to the sum of its digits modulo 9, so

$$\begin{aligned} 65363549000917 &\equiv 6 + 5 + 3 + 6 + 3 + 5 + 4 + 9 + 9 + 1 + 7 \\ &\equiv 58 \equiv 5 + 8 \equiv 13 \equiv 1 + 3 \equiv 4 \bmod 9. \end{aligned}$$

Relevant slides : 337 - 338

3. Decide whether or not the multiplication

$$6453601 \cdot 23456 = 151975665056$$

is correct by reducing mod 9.

Solution:

By the same method, we get $6453601 \equiv 7 \bmod 9$ and $23456 \equiv 2 \bmod 9$, so $6453601 \cdot 23456 \equiv 5 \bmod 9$. But $151975665056 \equiv 2 \bmod 9$, so the multiplication is incorrect.

Relevant slides : 337 - 338

4. Prove that given a number represented in base 10 as $n = (d_k \dots d_1 d_0)_{10}$ (with digits $d_i \in \{0, 1, \dots, 9\}$), we have $n \equiv \sum_{i=0}^{k} (-1)^i d_i \bmod 11$.

Solution:

We have $10 \equiv -1 \bmod 11$, so

$$n = \sum_{i=0}^{k} 10^i d_i \equiv \sum_{i=0}^{k} (-1)^i d_i \bmod 11.$$

5. Using the previous question, compute 9760145571116 mod 11.

Solution:

We have

$$\begin{aligned} 9760145571116 &\equiv 9 - 7 + 6 - 0 + 1 - 4 + 5 - 5 + 7 - 1 + 1 - 1 + 6 \\ &\equiv 17 \equiv -1 + 7 \equiv 6 \bmod 11. \end{aligned}$$

6. Given a number n represented in base 10, find a similar method to compute n modulo 1001, and use it to compute 4067007258442 modulo 1001.

Solution:

Consider $n = (d_k \dots d_1 d_0)_{10}$. Without loss of generality, suppose that the number of digits is divisible by 3 (if necessary, add one or two leading zeros to the representation of n). Write $k = 3\ell - 1$. Grouping the digits of n three by three, we have

$$n = \sum_{i=0}^{\ell-1} 1000^i (d_{3i+2}\ d_{3i+1}\ d_{3i})_{10}.$$

Since $1000 \equiv -1 \bmod 1001$, we get

$$n \equiv \sum_{i=0}^{\ell-1} (-1)^i (d_{3i+2}\ d_{3i+1}\ d_{3i})_{10} \bmod 1001.$$

Therefore,

$$4067007258442 \equiv 4 - 67 + 7 - 258 + 442 \equiv 128 \bmod 1001.$$

7. Which of the following numbers are multiples of 11?

$$\begin{aligned} a &= 67^{9876543210112277} + 21^{1231239875566} + 9 \\ b &= 109^{4648731230355} + 56^{65659313514739945} + 1 \\ c &= 36^{102498765} + 90^{907864310} + 7 \end{aligned}$$

Solution:

The numbers are obviously too big to be calculated directly on a computer. We use instead the theory of modular arithmetic. First, notice that $67 = 66 + 1$ such that

$$67 \equiv 66 + 1 \equiv 0 + 1 \equiv 1 \pmod{11}$$

Thus,

$$67^n \equiv 1^n \equiv 1 \pmod{11}$$

Therefore,

$$67^{9876543210112277} \equiv 1 \pmod{11}$$

Similarly,

$$21 \equiv 22 - 1 \equiv 0 - 1 \equiv -1 \pmod{11}$$

Thus,

$$21^{1231239875566} \equiv (-1)^{1231239875566} \equiv 1 \pmod{11}$$

since 1231239875566 is even. Putting everything together, we obtain

$$a \equiv 1 + 1 + 9 \equiv 11 \equiv 0 \pmod{11}$$

So a is indeed a multiple of 11.
For b, notice that

$$109^n \equiv (-1)^n \pmod{11}$$

Thus,

$$109^{4648731230355} \equiv (-1) \pmod{11}$$

since 4648731230355 is odd. We also notice that

$$56^{65659313514739945} \equiv 1 \pmod{11}$$

Therefore,

$$b \equiv (-1) + 1 + 1 \equiv 1 \pmod{11}$$

So b is not a multiple of 11.
For c, notice that $36 = 12 \cdot 3$. Then, $12 \equiv 1 \pmod{11}$, so we are left with $3^{102498765}$. The exponent is a multiple of 5, and one can check that $3^5 \equiv 1 \pmod{11}$, so that we can conclude that $3^{102498765} \equiv 1 \pmod{11}$.
For the second term, we can write $90 = 45 \cdot 2$. Then, $45 \equiv 1 \pmod{11}$, so we are left only with $2^{907864310}$.
The exponent is a multiple of 10. One can check that $2^5 \equiv -1 \pmod{11}$, so that $2^{10} = (2^5)^2 \equiv 1 \pmod{11}$ and we can conclude that $2^{907864310} \equiv 1 \pmod{11}$.
Hence, summing up modulo 11 we have that

$$36^{102498765} + 90^{907864310} + 7 \equiv 1 + 1 + 7 \equiv 9 \pmod{11}$$

Therefore, c is not a multiple of 11.

Problem 6.3.

1. Let $x = 021395789400$. Perform (by hand) the Euclidean division of x by 97.

Solution:

In order to avoid calculations with large numbers, we start by writing $x = 100x_0$ where $x_0 = 213957894$. Then, since $100 \equiv 3 \pmod{97}$,

$$x \equiv 100x_0 \equiv 3x_0 \pmod{97}$$

To compute the remainder of the division of x_0 by 97, we write x_0 as

$$x_0 = 2\times10^8+1\times10^7+3\times10^6+9\times10^5+5\times10^4+7\times10^3+8\times10^2+9\times10^1+4\times10^0$$

Furthermore, we calculate the remainders for the division of powers of 10 by 97:

$$\begin{aligned}
10 &\equiv 10 \pmod{97}\\
10^2 &\equiv 3 \pmod{97}\\
10^3 &\equiv 30 \pmod{97}\\
10^4 &\equiv (10^2)^2 \equiv 9 \pmod{97}\\
10^5 &\equiv 90 \pmod{97}\\
10^6 &\equiv 10^4 \times 10^2 \equiv 27 \pmod{97}\\
10^7 &\equiv 270 \equiv 76 \pmod{97}\\
10^8 &\equiv (10^4)^2 \equiv 81 \pmod{97}
\end{aligned}$$

Therefore,

$$\begin{aligned}
x_0 &\equiv 2\times 81 + 1\times 76 + 3\times 27 + 9\times 90 + 5\times 9 + 7\times 30 + 8\times 3 + 9\times 10 + 4\times 1\\
&\equiv 1502\\
&\equiv 1\times 30 + 5\times 3 + 0\times 10 + 2\\
&\equiv 47 \pmod{97}
\end{aligned}$$

Going back to x, we find $x \equiv 3\times 47 \equiv 141 \equiv 44 \pmod{97}$, which means that the remainder of the division of x by 97 is $r = 44$.
Thus the quotient can be obtained as

$$q = \frac{x-r}{97} = 220575148$$

Compute the two control digits MOD 97-10 for the telephone number $x_1 = 021\ 395\ 7894$.

Solution:

The two control digits can be obtained by computing the remainder after division of $x = 021\ 395\ 7894\ 00$ by 97, and then by computing $c = 98 - r$. We have previously computed $r = 44$, hence the control digits are 54.

Relevant slides : 339 - 342

2. Let $\tilde{x}_1$ be the number obtained by replacing 02 with 99 in x_1:

$$\tilde{x}_1 = 991\ 395\ 7894$$

Compare the control digits MOD 97-10 of x_1 and $\tilde{x}_1$.

Solution:

We append two zeros at the end of $\tilde{x}_1$ and obtain $\tilde{x} = 991\ 395\ 7894\ 00$. Following the same method as in part 1, we obtain the remainder after division of $\tilde{x}$ by 97, $\tilde{r} = 44$, which is the same as for x. Thus, x_1 and $\tilde{x}_1$ have the same control digits MOD 97-10.

3. More generally, let z be an integer whose decimal representation includes twice the digit 9 in consecutive positions. Let z' be the number obtained by replacing 99 with 02 in z. Show that $z - z'$ is a multiple of 97.

Solution:

Let $z_n, \ldots, z_0$ be the digits of the decimal representation of z:

$$z = z_n \times 10^n + \cdots + z_1 \times 10^1 + z_0 \times 10^0$$

Let k and $k+1$ be the positions where the two consecutive digits 9 are located, that is, $z_{k+1} = z_k = 9$.
We have

$$\begin{aligned} z &= z_n \times 10^n + \cdots + 9 \times 10^{k+1} + 9 \times 10^k + \cdots + z_1 \times 10^1 + z_0 \times 10^0 \\ z' &= z_n \times 10^n + \cdots + 0 \times 10^{k+1} + 2 \times 10^k + \cdots + z_1 \times 10^1 + z_0 \times 10^0 \end{aligned}$$

Thus,

$$z - z' = 9 \times 10^{k+1} + 7 \times 10^k = 90 \times 10^k + 7 \times 10^k = 97 \times 10^k$$

So $z - z'$ is divisible by 97 (the quotient is 10^k).

If 99 was replaced by mistake with 02, can the control digits of MOD 97-10 detect this error?

Solution:

Let $z_1 = 100z$ and $z'_1 = 100z'$. Since $z - z' \equiv 0 \pmod{97}$, $z_1 - z'_1 \equiv 0 \pmod{97}$ as well. Hence, the control digits of MOD 97-10 will be the same, and the error will not be detected.

Relevant slides : 339 - 342

4. Suppose a bank uses MOD 97-10 to ensure that messages from customers are transmitted to the bank without modifications. It is known that the bank encodes wire transfer orders in the format

$$M = DDDDDDDDDD \| AAAAAAA \| CC$$

where the first part (represented by the D's) is the ten-digit receiving account number, the second part (represented by the A's, padded on the left by zeros if necessary) is the amount to be transferred, and the final part (represented by the C's) is the MOD 97-10 control digits. Note that there are exactly 7 digits in the 'Amount' part; bigger transactions will require in-person confirmation. Recall that '$\|$' denotes the concatenation operator.

You, a software engineer by day, malicious hacker by night, have somehow managed to find a way to modify up to two digits in such messages while they are being transmitted. You are unhappy with your salary of CHF 10′000 a month from your day job. You intercept the following message

$$M_{\text{salary}} = 1461319897001000010$$

for the salary of March '25 from your employer to the bank. How much more money can you make the bank transfer to your account instead?

Solution:

We can easily see that modifying the message first to

$$M_{\text{modified}} = 1461319897901000010$$

will be the first step, since it gains you the most money by modifying a single digit. However, you can only modify one more digit and also make sure that the control digits match the rest of the message. Thankfully, using the result from the previous part, you can add another CHF 700′000 in the uncoded part and escape detection, resulting in a net gain of CHF 9′700′000 (check that the control digits remain the same in this case). Your final message is thus

$$M_{\text{modified}} = 1461319897971000010$$

Good luck, it is only a matter of time before your employer will start noticing!