Advanced information, computation, communication I
EPFL - Fall semester 2021-2022

Week 9 - solutions

November 19, 2021

1 Open questions

Exercise 1. (*) *Prove that if a and b are nonzero integers, a divides b, and $a + b$ is odd, then a is odd.*

We prove by contradiction. Suppose that a and b are nonzero integers, a divides b, and $a + b$ is odd, but a is even. Since a divides b, there is an integer q such that $b = aq$. Hence, $a + b = a + aq = a(1 + q)$. Now, a is even, so there is an integer k such that $a = 2k$. It yields that $a + b = 2k(1 + q)$ where $k(1 + q)$ is an integer. Hence, $a + b$ is even, which contradicts that $a + b$ is odd.

Exercise 2. (*) *Let m be a positive integer. Show that $a \equiv b$ (**mod** m) if a **mod** $m = b$ **mod** m.*

Given: m is a positive integer and $a \bmod m = b \bmod m$
To proof: $a \equiv b \pmod m$
a **mod** $m = b$ **mod** m indicates that there exist an integer q_1 such that:

$$a \textbf{ mod } m = mq_1 + b$$

b **mod** $m = a$ **mod** m indicates that there exist an integer q_2 such that:

$$b \textbf{ mod } m = mq_2 + a$$

Since a **mod** $m = b$ **mod** m:

$$mq_2 + a = mq_1 + b$$

Subtract b from each side of the equation:

$$mq_2 + a - b = mq_1$$

Subtract mq_2 from each side of the equation:

$$a - b = mq_1 - mq_2$$

Factorise the right side of the equation:

$$a - b = m(q_1 - q_2)$$

Since q_1 and q_2 are both integers, their difference $q_1 - q_2$ is also an integer.
By the definition of divides, we have then shown that m divides $a - b$. By the definition of equivalent modulo m:

$$a \equiv b (\bmod\ m)$$

Exercise 3. (**) *Suppose that a and b are integers, $a \equiv 11$ (mod 19), and $b \equiv 3$ (mod 19). Find the integer c with $0 \leq c \leq 18$ such that:*

1. *$c \equiv 13a$ (mod 19).*
2. *$c \equiv 7a + 3b$ (mod 19).*

3. $c \equiv a^3 + 4b^3 \pmod{19}$.

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

1. $c \equiv 13a \pmod{19} = 13 \times 11 \pmod{19} = 143 \pmod{19} = 10 \pmod{19}$. We then obtain $c = 10$ with $0 \leq c \leq 18$.
2. $c \equiv 7a + 3b \pmod{19} = 7 \times 11 + 3 \times 3 \pmod{19} = 77 + 9 \pmod{19} = 86 \pmod{19} = 10 \pmod{19}$. We then obtain $c = 10$ with $0 \leq c \leq 18$.
3. $c \equiv a^3 + 4b^3 \pmod{19} = 11^3 + 4 \times 3^3 \pmod{19} = 1331 + 4 \times 27 \pmod{19} = 1439 \pmod{19} = 14 \pmod{19}$. We then obtain $c = 14$ with $0 \leq c \leq 18$.

Exercise 4. (**) *Show that the hexadecimal expansion of a positive integer can be obtained from its binary expansion by grouping together blocks of four binary digits, adding initial zeros if necessary, and translating each block of four binary digits into a single hexadecimal digit.*

Let n be an integer. The binary representation of n is then $a_k...a_2a_1a_0$ such that:

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + ... + a_7 \cdot 2^7 + a_6 \cdot 2^6 + a_5 \cdot 2^5 + a_4 \cdot 2^4 + a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0$$

It is safe to assume that $k + 1$ is a multiple of 4 (if not, then we add zero terms in front of a_k until the number of digits in the binary representation increased by 1 is a multiple of 4).

$= (a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + a_{k-3} \cdot 2^{k-3})$
$+....$
$+(a_7 \cdot 2^7 + a_6 \cdot 2^6 + a_5 \cdot 2^5 + a_4 \cdot 2^4)$
$+(a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0)$

Factor out powers of 2 out of each block of 4 terms:

$= 2^{k-3}(a_k \cdot 2^3 + a_{k-1} \cdot 2^2 + a_{k-2} \cdot 2^1 + a_{k-3} \cdot 2^0)$
$+....$
$+2^4(a_7 \cdot 2^3 + a_6 \cdot 2^2 + a_5 \cdot 2^1 + a_4 \cdot 2^0)$
$+(a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0)$

We then note that each block $a_i \cdot 2^3 + a_{i-1} \cdot 2^2 + a_{i-2} \cdot 2^1 + a_{i-3} \cdot 2^0$ is a hexadecimal digit:

$= h_{(k-3)/4} \cdot 2^{k-3} + ... + h_2 \cdot 2^8 + h_1 \cdot 2^4 + h_0$
$= h_{(k-3)/4} \cdot 16^{k-3}/4 + ... + h_2 \cdot 16^2 + h_1 \cdot 16 + h_0$

The corresponding hexadecimal expansion of n is then $h_{(k-3)/4}...h_2h_1h_0$.

Exercise 5. (*) *Find the sum and product of each of these pairs of numbers. Express your answers as a hexadecimal expansion.*

1. $(1AE)_{16}, (BBC)_{16}$

			1	1	
			1	A	E
+			B	B	C
			D	6	A

				1	A	E
	×			B	B	C
			1	4	2	8
		1	2	7	A	
+	1	2	7	A		
	1	3	B	5	C	8

2. $(ABCDE)_{16}, (1111)_{16}$

	A	B	C	D	E
+		1	1	1	1
	A	C	D	E	F

				A	B	C	D	E
			×		1	1	1	1
				A	B	C	D	E
			A	B	C	D	E	
		A	B	C	D	E		
×	A	B	C	D	E			
	B	7	4	1	4	8	B	E

Exercise 6. *(**) Suppose that n and b are positive integers with $b \geq 2$ and the base b expansion of n is $n = (a_m a_{m-1} ... a_1 a_0)_b$. Find the base b expansion of:*

1. The number b^n can be written in base b as :

$$b^n = a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0$$

To have an equality on the left side and right side we must have

$$a_n = 1$$
$$a_{n-1} = a_{n-2} = \ldots = a_1 = a_0 = 0$$

This then implies that the base b expansion of b^n is $(1\underbrace{00...000}_{n \text{ zeros}})_b$.

2. Since the base b expansion of n is $n = (a_m a_{m-1} ... a_1 a_0)_b$:

$$n = a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0$$

Divide each side of the previous equation by b:

$$\frac{n}{b} = \frac{a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0}{b}$$
$$= a_m b^{m-1} + a_{m-1} b^{m-2} + ... + a_2 b + a_1 + \frac{a_0}{b}$$

Since $a_m b^{m-1} + a_{m-1} b^{m-2} + ... + a_2 b + a_1$ is an integer while $0 \leq \frac{a_0}{b} < 1$ (as $0 \leq a_0 < b$).

$$\lfloor n/b \rfloor = a_m b^{m-1} + a_{m_1} b^{m-2} + ... + a_2 b + a_1$$

This then implies that the base b expansion of $\lfloor n/b \rfloor$ is $(a_m a_{m-1} ... a_1)_b$.

Exercise 7. (**) *Find the decimal expansion of the number with the $n-$digit base seven expansion $(111...111)_7$ (with n 1's). [Hint: Use the formula for the sum of the terms of a geometric progression.]*

By the definition of the base 7 representation of an integer m:

$$m = a_k 7^k + a_{k-1}7^{k-1} + ... + a_1 8 + a_0$$

In this case, $k = n - 1$ *and* $a_i = 1$ *for* $i = 0, 1, 2, ..., k - 1$.

$$\begin{aligned} m &= 1(7^{n-1}) + 1(7^{n-2}) + ... + 1(7) + 1 \\ &= 7^{n-1} + 7^{n-2} + ... + 7 + 1 \\ &= \sum_{i=0}^{n-1} 7^i = \frac{7^n - 1}{7 - 1} = \frac{1}{6}(7^n - 1) \end{aligned}$$

Exercise 8. *(**) Express in pseudocode the trial division algorithm for determining whether an integer is prime.*

By definition, a prime number is a number greater than 1, which is only divisible by 1 and itself. Therefore, we initialise a loop from 2 to $N - 1$ to and check the divisibility. The following is the pseudocode for the approach:

```
i ← 2
while i ≤ N − 1 do
  if N mod i = 0 then
    return Composite
  end if
end while
return Prime
```

Exercise 9. (***) *Express in pseudocode an algorithm for finding the prime factorisation of an integer.*

```
factor := ∅
prime := set of all prime numbers from 2 to √n
m := numebr of elements in the set prime
for i ≤ m do
  j ← 0
  while n mod prime(i) = 0 do
    n := n/prime(i)
    j := j + 1
    if n mod prime(i) ≠ 0 then
      factor := factor ∪ prime(i)^j
    end if
  end while
end for
if n > 1 or factor = ∅ then
  factor := factor ∪ {n}
end if
return factor
```

Exercise 10. (*) *Show that a positive integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3.*

Let $a = (a_{n-1}a_{n-2}...a_1a_0)_{10}$. Then $a = 10^{n-1}a_{n-1}+10^{n-2}a_{n-2}+...+10a_1+a_0 \equiv a_{n-1}+a_{n-2}+...+a_1+a_0$ (mod 3), because $10^j \equiv 1$ (mod 3) for all nonnegative integers j. It follows that $3|a$ if and only if 3 divides the sum of the decimal digits of a.

Exercise 11. (**) *Find gcd(92928, 123552) and lcm(92928, 123552), and verify that gcd(92928, 123552)·lcm(92928, 123552) = 92928·123552.*

The numbers are even, so we can consider trying to factorise the numbers, or speedup the process by removing some small factors.

- The number 92928 is even. Then 2 is a factor. We divide by 2 and obtain another even number. We continue like this until we obtain the first odd number – $92928 = 2^8 \cdot 363$. Now obviously 363 is divisible by 3; $363 = 3 \cdot 121$. Finally, by trial and error, or by remembering the multiplication table, we can see that $121 = 11^2$. We obtain

$$92928 = 2^8 \cdot 3 \cdot 11^2.$$

- The number 123552 is also even. We keep dividing it by 2 until we obtain $123552 = 2^6 \cdot 3861$. A careful observer will notice that 3861 is divisible by 3, and that $3861/3 = 1287$ is also divisible by 3, and in fact that $1287/3 = 429$ is again divisible by 3. This leads us to $123552 = 2^5 \cdot 3^3 \cdot 143$. Finally, a simple calculation shows that $143 = 11 \cdot 13$ and therefore

$$1235552 = 2^5 \cdot 3^3 \cdot 11 \cdot 13.$$

Now we can easily compute the gcd and the lcm of the two numbers.

$$\gcd(92928, 123552) = \gcd(2^8 \cdot 3 \cdot 11^2\ ,\ 2^5 \cdot 3^3 \cdot 11 \cdot 13) = 2^5 \cdot 3 \cdot 11,$$
$$\operatorname{lcm}(92928, 123552) = \operatorname{lcm}(2^8 \cdot 3 \cdot 11^2\ ,\ 2^5 \cdot 3^3 \cdot 11 \cdot 13) = 2^8 \cdot 3^3 \cdot 11^2 \cdot 13.$$

Finally, to confirm that $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b$, we can use the their prime factorisations

$$\underbrace{(2^5 \cdot 3 \cdot 11)}_{\gcd(92928,123552)} \cdot \underbrace{(2^8 \cdot 3^3 \cdot 11^2 \cdot 13)}_{\operatorname{lcm}(92928,123552)} = 2^{13} \cdot 3^4 \cdot 11^3 \cdot 13 = \underbrace{(2^8 \cdot 3 \cdot 11^2)}_{92928} \cdot \underbrace{(2^5 \cdot 3^3 \cdot 11 \cdot 13)}_{123552}$$

2 Exam questions

Exercise 12. (***) *The sum* $((AAAAAA)_{16}^{(AAAAAA)_{16}} + (BBBBBB)_{16}^{(BBBBBB)_{16}})(\mod 8)$ *is:*

- ◯ *1*
- ✓ *3*
- ◯ *5*
- ◯ *7*

We need to compute some values modulo 8, and those values are expressed in base 16. Therefore it is enough to consider only the first digit of those values since

$$a_m 16^m + a_{m-1} 16^{m-1} + ... + a_1 16 + a_0 \equiv a_0 \mod 8.$$

We know that $(A)_{16} = (10)_{10}$ and $(B)_{16} = (11)_{10}$ so $(A)_{16} \equiv 2 \mod 8$ and $(B)_{16} \equiv 3 \mod 8$. Therefore the above expression is equivalent to

$$(2^{(AAAAAA)_{16}} + 3^{(BBBBBB)_{16}}) \mod 8$$

The exponent $(BBBBBB)_{16}$ of 3 is an odd number (which is easy to check). It can be written as $(BBBBBB)_{16} = 1 + 2 \cdot b$ for some integer b. Then $3^{(BBBBBB)_{16}} = 3^1 \cdot 3^{2b}$. However we have $3^2 = 9 \equiv 1 \mod 8$, so $3^{2b} \equiv 1^b \equiv 1 \mod 8$. Therefore $3^{(BBBBBB)_{16}} \equiv 3 \cdot 1^b \equiv 3 \mod 8$.

Note that the exponent $(AAAAAA)_{16}$ of 2 is greater than 3 (which is easy to check), we have $2^3 \mid 2^{(AAAAAA)_{16}}$ and so $2^{(AAAAAA)_{16}} = 0 \mod 8$. Therefore:

$$(AAAAAA)_{16}^{(AAAAAA)_{16}} + (BBBBBB)_{16}^{(BBBBBB)_{16}} \equiv 0 + 3 \equiv 3 \mod 8.$$

Exercise 13. (***) *The maximum number of divisions performed when executing the Euclidean algorithm to compute the* $\gcd(n_1, n_2)$ *for two integers* n_1, n_2 *with* $25 \geq n_1 \geq n_2 \geq 0$ *is:*

◯ *4*

◯ *5*

✓ *6*

◯ *7*

The Euclidean algorithm is least efficient when executed on two consecutive Fibonacci numbers. This is exactly the case when all quotients of Euclidean divisions are equal to 1, so we never obtain a remainder which is less than half the quotient.

The largest Fibonacci pair smaller than 25 is $n_1 = 21$, $n_2 = 13$. The $\gcd(21, 13)$ is computed by consecutively setting $\gcd(n_1, n_2) = \gcd(n_2, n_1 \mod n_2)$ as follows:

Step	n_1	n_2	$n_1 = n_2 \cdot q + r$
1	21	13	$21 = 13 \cdot 1 + 8$
2	13	8	$13 = 8 \cdot 1 + 5$
3	8	5	$8 = 5 \cdot 1 + 3$
4	5	3	$5 = 3 \cdot 1 + 2$
5	3	2	$3 = 2 \cdot 1 + 1$
6	2	1	$2 = 1 \cdot 2 + 0$
7	1	0	//

In total there are 6 Euclidean divisions.

Exercise 14. (*) *Let* R *be a relation on the set of integers such that* $(x, y) \in R$ *if* $\gcd(x, y)$ *is a prime number. Then:*

◯ *R is an equivalence relation*

◯ *R is reflexive and symmetric but not transitive*

✓ *R is symmetric but not reflexive and not transitive*

◯ *R is symmetric and transitive, but not reflexive*

The relation R is not reflexive because $\gcd(1, 1) = 1$ implies that $(1, 1) \notin R$ (note that 1 is not a prime number, but if you prefer you can prove the same with $(4, 4)$ for example).

The relation R is symmetric because $\gcd(x, y) = \gcd(y, x)$.

The relation R is not transitive, which we will show with an example. Note that $(2, 6), (6, 3) \in R$ because $\gcd(2, 6) = 2$ is prime and $\gcd(6, 3) = 3$ is prime. However $\gcd(2, 3) = 1$ and therefore $(2, 3) \notin R$. You can use $(10, 6), (6, 15)$ if you prefer not to obtain 1, but rather a composite number in the proof.

Therefore R is symmetric but not reflexive and not transitive.

$*$ = *easy exercise, everyone should solve it rapidly*

$**$ = *moderately difficult exercise, can be solved with standard approaches*

$***$ = *difficult exercise, requires some idea or intuition or complex reasoning*