Advanced information, computation, communication I
EPFL - Fall semester 2020-2021

Week 9 - solutions

November 17, 2020

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 $q2$ 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:

$$a - b = mq_1 - mq_2$$

Factorize 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:

$$a \equiv b (\text{mod } m)$$

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. $c \equiv a^3 + 4b^3$ *(mod 19).*

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

1. $c \equiv 13a \pmod{19} = 13 \times 11 \pmod{m} = 143 \pmod{m} = 10 \pmod{19}$. 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 $c = 18$ 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 ak 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:

$= 2^{k-3}(a_k \cdot 2^3 + a_{k_1} \cdot 2^2 + ak_2 \cdot 2^1 + a_{k_3} \cdot 2^0)$
$+....$
$+2^4(a_7 \cdot 2^3 + a_6 \cdot 2^2 + a_5 \cdot 2^1 + a_4 \cdot 2^0)$
$+(a_3 \cdot 2^3 + a_2 \cdot 2^2 + a_1 \cdot 2 + a_0)$

We then note that each block $a_i \cdot 2^3 + ai_1 \cdot 2^2 + a_{i_2} \cdot 2^1 + ai_3 \cdot 2_0$ 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. Since the base b expansion of n is $n = (a_m a_{m-1} ... a_1 a_0)_b$:

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

Let us next determine an expression for $b^2 n$:

$$\begin{aligned} b^2 n &= b^2 (a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0) \\ &= a_m b^{m+2} + a_{m-1} b^{m+1} + ... + a_1 b^3 + a_0 b^2 \\ &= a_m b^{m+2} + a_{m-1} b^{m+1} + ... + a_1 b^3 + a_0 b^2 + 0b + 0 \end{aligned}$$

This then implies that the base b expansion of $b^2 n$ is $(a_m a_{m-1} ... a_1 a_0 00)_b$.

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:

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

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

$$m = 1(7^{n-1}) + 1(7^{n-2}) + 1(7) + 1$$
$$7^{n-1} + 7^{n-2} + ... + 7 + 1$$

$$= \sum_{i=1}^{n-1} 7^i = \frac{7^n - 1}{7 - 1} = \frac{1}{6}(7^n - 1)$$

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 initialize a loop from 2 to $N - 1$ to and check the divisibility. The following is the pseudo-code 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 factorization 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)
  end while
  j := j + 1
  if n mod prime(i) ≠ 0 then
    factor := factor ∪ prime(i)^j
  end if
end for
if factor = ∅ then
  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. *Determine how we can use the decimal expansion of an integer n to determine whether n is divisible by:*

1. 4: n is divisible by 4 if and only if the two rightmost digits of the decimal expansion, viewed as a two-digit integer (or the single digit if it's a one-digit integer), is divisible by 4.
2. 25: n is divisible by 25 if and only if the two rightmost digits are 00 (or 0 if it's a one-digit integer), 25, 50, or 75.

3. 20: n is divisible by 20 if and only if the rightmost digit of the decimal expansion is 0 and the digit in the tens place (if it's not a one-digit integer) is 0, 2, 4, 6, or 8.

Exercise 12. *Describe an algorithm for finding the difference of two binary expansions.*

procedure subtract(a, b: positive integers, $a > b$, $a = (a_{n-1}a_{n-2}...a_1a_0)_2$, $b = (b_{n-1}b_{n-2}...b_1b_0)_2$)
$B := 0$ {B is the borrow}
for $j := 1$ to $n - 1$ **do**
  if $a_j \geq b_j + B$ **then**
    $s_j := a_j - b_j - B$
    $B := 0$
  else
    $s_j := a_j + 2 - b_j - B$
    $B := 1$
  end if
end for
{$(s_{n-1}s_{n-2}...s_1s_0)_2$ is the difference}

Exercise 13. *Show that $a^m + 1$ is composite if a and m are integers greater than 1 and m is odd. [Hint: Show that $x + 1$ is a factor of the polynomial $x^m + 1$ if m is odd.]*

Write $n = rs$, where $r > 1$ and $s > 1$. Then $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + (2^r)^{s-3} + ... + 1)$. The first factor is at least $2^2 - 1 = 3$ and the second factor is at least $2^2 + 1 = 5$. This provides a factoring of $2^n - 1$ into two factors greater than 1, so $2^n - 1$ is composite.

Exercise 14. *Find gcd(92928, 123552) and lcm(92928, 123552), and verify that gcd(92928, 123552)·lcm(92928, 123552) = 92928·123552.*

gcd (92928, 123552) = 1056; lcm(92928, 123552) = 10,872,576; both products are 11,481,440,256.