University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Homework questions – Week 7

Jean-Baptiste Campesato

March 8th, 2021 to March 12th, 2021

I forgot to give the following result in Chapter 2, so let's prove it now and I will add it in the lecture notes.

Exercise 1.
Let $a, b, c \in \mathbb{Z}$. Prove that if $a|c$, $b|c$ and $\gcd(a, b) = 1$ then $ab|c$.

Exercise 2.
Either prove or find a counter-example to $\forall a, b \in \mathbb{N} \setminus \{0\},\ \varphi(ab) = \varphi(a)\varphi(b)$.

Exercise 3.
What's the remainder of the Euclidean division of $1 + 2 + 2^2 + 2^3 + \cdots + 2^{100}$ by 125?

Exercise 4.
Find the last 3 digits of 3^{2021} (written in decimal).

Exercise 5.
Prove that $\forall n, k \in \mathbb{N} \setminus \{0\},\ \varphi\left(n^k\right) = n^{k-1}\varphi(n)$.

Exercise 6.
Prove that $\forall a, b \in \mathbb{N} \setminus \{0\},\ \gcd(a, b) = 1 \implies a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Exercise 7.
Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Prove that if $\gcd(a, n) = \gcd(a - 1, n) = 1$ then $\displaystyle\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0 \pmod{n}$.

Exercise 8.
Prove that $\forall a \in \mathbb{N} \setminus \{0, 1\},\ \forall k \in \mathbb{N} \setminus \{0\},\ k|\varphi\left(a^k - 1\right)$.

Exercise 9.
We define a sequence by $u_0 \in \mathbb{N} \setminus \{0\}$ and $u_{k+1} = \varphi(u_k) \in \mathbb{N} \setminus \{0\}$ for $k \in \mathbb{N}$.
Prove that the sequence $(u_k)_k$ is eventually constant equal to 1.

Exercise 10.
Assume that $n = pq$ where p, q are distinct prime numbers.
Find a way to easily recover p and q from the knowledge of n and $\varphi(n)$.

Exercise 11.
In order to prove that RSA works, we check that if p and q are two distinct prime numbers then

(1) $\quad \forall l \in \mathbb{N},\ \forall m \in \mathbb{Z},\ m^{1+l\varphi(pq)} \equiv m \pmod{pq}$

The proof seen in class relies on Euler's theorem: $m^{1+l\varphi(pq)} = m \times \left(m^{\varphi(pq)}\right)^l \equiv m \times 1^l \pmod{pq} \equiv m \pmod{pq}$.
Therefore it holds only when $\gcd(m, pq) = 1$, i.e. it doesn't hold when $p|m$ or $q|m$.[1].
Prove that (1) holds with no restriction on m.

[1] That's already quite good: it works for $m \in \{0, 1, \dots, pq - 1\} \setminus (\{p, 2p, \dots, (q - 1)p\} \cup \{q, 2q, \dots, (p - 1)q\})$ but $\frac{pq-(p-1)-(q-1)}{pq} = 1 + \frac{2}{pq} - \frac{1}{q} - \frac{1}{p}$ is small when p and q are large, so this proof works for almost all possible messages.

Exercise 12.

1. Check that $(n, e) = (5917, 17)$ and $(n, d) = (5917, 2033)$ are suitable respectively public and private keys.
   Note that $n = 61 \times 97$.

2. Bob wants to send the message $m = 42$ to Alice using the above keys. What should he send to Alice?
   You don't have to compute it by hand.
   Check that Alice can decrypt this message.

3. Alice just received the ciphered message $c = 3141$ from Bob. What is the original message?

Exercise 13.
Eve intercepted the message $c = 271$ sent to Alice from Bob.
She finds Alice's public key $(n, e) = (1003, 11)$ on her website.
What is the original message sent by Bob?

Exercise 14. *Digital signature*
Another common problem related to communations is the following: how can the recipient be sure that the sender is not an impostor?
Explain how RSA can be used to solve this issue.

Sample solutions to Exercise 1.
Let $a, b, c \in \mathbb{Z}$ be such that $a|c$, $b|c$ and $\gcd(a,b) = 1$.
Since $a|c$ and $b|c$, there exist $k, l \in \mathbb{Z}$ such that $c = ak$ and $c = bl$.
Since $\gcd(a,b) = 1$, by Bézout's identity, there exists $u, v \in \mathbb{Z}$ such that $au + bv = 1$.
Then $c = auc + bvc = aubl + bvak = ab(ul + vk)$, so that $ab|c$.

Sample solutions to Exercise 2.
This property is false: $\varphi(2\times 2) = 2^2 - 2 = 2$ but $\varphi(2)\varphi(2) = 1 \times 1$.

Sample solutions to Exercise 3.
$1 + 2 + 2^2 + 2^3 + \cdots + 2^{100} = \sum_{k=0}^{100} 2^k = \frac{1 - 2^{101}}{1-2} = 2^{101} - 1$ (geometric sum, Cherge's favorite formula).
Note that $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$.
Therefore, since $\gcd(2, 101) = 1$, Euler's theorem gives

$$2^{101} - 1 = 2 \times 2^{100} - 1 \equiv 2 \times 1 - 1 \pmod{125} \equiv 1 \pmod{125}$$

Hence the remainder of the Euclidean division of $1 + 2 + 2^2 + 2^3 + \cdots + 2^{100}$ by 125 is 1.

Sample solutions to Exercise 4.
Note that $\varphi(1000) = \varphi(2^3 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$.
Therefore, since $\gcd(1000, 3) = 1$, Euler's theorem gives

$$\begin{aligned} 3^{2021} = 3^{5\times 400 + 21} = (3^{400})^5 3^{21} &\equiv 1^5 \times 3^{21} \pmod{1000} \\ &\equiv 3^{10}3^{10}3 \pmod{1000} \\ &\equiv 59049 \times 59049 \times 3 \pmod{1000} \\ &\equiv 49 \times 49 \times 3 \pmod{1000} \\ &\equiv 7203 \pmod{1000} \\ &\equiv 203 \pmod{1000} \end{aligned}$$

Thus the last 3 digits of 3^{2021} are 203.

Sample solutions to Exercise 5.
Let $n, k \in \mathbb{N} \setminus \{0\}$.
Write the prime factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ where the p_i are pairwise distinct prime numbers and $\alpha_i \in \mathbb{N} \setminus \{0\}$.
Then $n^k = \prod_{i=1}^{r} p^{k\alpha_i}$ and $\varphi\left(n^k\right) = \prod_{i=1}^{r}\left(p_i^{k\alpha_i} - p_i^{k\alpha_i - 1}\right) = \prod_{i=1}^{r} p_i^{(k-1)\alpha_i} \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) = n^{k-1}\varphi(n)$.

Sample solutions to Exercise 6.
Let $a, b \in \mathbb{N} \setminus \{0\}$. Assume that $\gcd(a,b) = 1$.
Since $\gcd(a,b) = 1$, by Euler's theorem $a^{\varphi(b)} \equiv 1 \pmod{b}$.
Since $\varphi(a) \geq 1$, $b^{\varphi(a)} \equiv 0 \pmod{b}$.
Thus $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{b}$, i.e. $b|a^{\varphi(b)} + b^{\varphi(a)} - 1$.
Swapping a and b, we get similarly that $a|a^{\varphi(b)} + b^{\varphi(a)} - 1$.
Since $\gcd(a,b) = 1$, we derive from Exercise 1 that $ab|a^{\varphi(b)} + b^{\varphi(a)} - 1$, i.e. $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Sample solutions to Exercise 7.
Let $a \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $\gcd(a,n) = \gcd(a-1, n) = 1$.
Since $\gcd(a,b) = 1$, by Euler's theorem we get

$$(a-1)\sum_{k=0}^{\varphi(n)-1} a^k = a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

So $n \Big| (a-1) \displaystyle\sum_{k=0}^{\varphi(n)-1} a^k$.

By Gauss' lemma, since $\gcd(n, a-1) = 1$, we get that $n \Big| \displaystyle\sum_{k=0}^{\varphi(n)-1} a^k$, i.e. $\displaystyle\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0 \pmod n$.

Sample solutions to Exercise 8.
Let $a \in \mathbb{N} \setminus \{0,1\}$ and $k \in \mathbb{N} \setminus \{0\}$.
By Euclidean division, there exist $q, r \in \mathbb{Z}$ such that $\varphi\left(a^k - 1\right) = kq + r$ and $0 \leq r < k$.
Since $\gcd(a^k - 1, a) = \gcd(-1, a) = 1$, we deduce from Euler's theorem that $a^{\varphi(a^k-1)} \equiv 1 \pmod{a^k - 1}$.
But $a^{\varphi(a^k-1)} = a^{kq+r} = (a^k)^q a^r \equiv 1^q a^r \pmod{a^k-1} \equiv a^r \pmod{a^k-1}$.
Therefore $a^r \equiv 1 \pmod{a^k-1}$, i.e. $a^k - 1 | a^r - 1$.
But since $0 \leq r < k$, we get that $0 \leq a^r - 1 < a^k - 1$.
Thence, $a^r - 1 = 0$, i.e. $r = 0$.
So $\varphi\left(a^k - 1\right) = kq$, i.e. $k | \varphi\left(a^k - 1\right)$.

Sample solutions to Exercise 9.
First note that if $n \in \mathbb{N} \setminus \{0\}$ then $\begin{cases} \varphi(n) \leq n-1 & \text{if } n \geq 2 \\ \varphi(n) = 1 & \text{if } n = 1 \end{cases}$.
Therefore $u_{k+1} = \varphi(u_k) \leq u_k$, so that the sequence is decreasing.
Since it is bounded from below then it is eventually constant.
Assume by contradiction that $\forall k \geq N$, $u_{k+1} = u_k > 1$, then $u_{k+1} = \varphi(u_k) \leq u_k - 1 < u_k$. Which is a contradiction.
Therefore the sequence $(u_k)_k$ is eventually constant equal to 1.

Sample solutions to Exercise 10.

$$\begin{aligned}
& \varphi(n) = (p-1)(q-1) \\
\Leftrightarrow\ & \varphi(n) = pq - p - q + 1 \\
\Leftrightarrow\ & \varphi(n) = n - p - \frac{n}{p} + 1 \\
\Leftrightarrow\ & p\varphi(n) = pn - p^2 - n + p \\
\Leftrightarrow\ & p^2 - (n - \varphi(n) + 1)p + n = 0
\end{aligned}$$

Therefore p (and similarly for q) is a root of the equation $X^2 - (n - \varphi(n) + 1)X + n = 0$.

Sample solutions to Exercise 11.
Let $l \in \mathbb{N}$ and $m \in \mathbb{Z}$.

- Let's prove that $m^{1+l\varphi(pq)} \equiv m \pmod p$.
  - If $p|m$ then both sides are congruent to $0 \pmod p$, therefore $m^{1+l\varphi(pq)} \equiv m \pmod p$.
  - If $p \nmid m$ then $\gcd(m^{q-1}, p) = 1$ (*check it*), therefore, using Fermat's little theorem, we get that

    $$\left(m^{q-1}\right)^{p-1} \equiv 1 \pmod p$$

    Thus $m^{1+l\varphi(pq)} = m \times m^{l(p-1)(q-1)} = m \times \left(\left(m^{q-1}\right)^{p-1}\right)^l \equiv m \times 1^l \pmod p \equiv m \pmod p$.
- We prove similarly that $m^{1+l\varphi(pq)} \equiv m \pmod q$.

Therefore $p | m^{1+l\varphi(pq)} - m$ and $q | m^{1+l\varphi(pq)} - m$.
Since $\gcd(p, q) = 1$, we deduce from Exercise 1 that $pq | m^{1+l\varphi(pq)} - m$, i.e. $m^{1+l\varphi(pq)} \equiv m \pmod{pq}$

Sample solutions to Exercise 12.

1. Here $\varphi(n) = (61-1)(97-1) = 60 \times 96 = 5760$.
   Note that $5760 = 338 \times 17 + 14$, so $\gcd(\varphi(n), e) = \gcd(5760, 17) = \gcd(14, 17) = 1$.
   Therefore $e = 17$ is a suitable choice for $n = 5917$.
   Furthermore $ed = 17 \times 2033 = 34561 = 6 \times 5760 + 1 \equiv 1 \pmod{\varphi(n)}$.
   Therefore d is a suitable choice for $e = 17$ and $n = 5917$.

2. $m^e = 42^{17} \equiv 3838 \pmod{5917}$, so Bob should send $c = 3838$ to Alice.
   Then Alice will perform the computation $c^d = 3838^{2033} \equiv 42 \pmod{5917}$.

3. $c^d = 3141^{2033} \equiv 4630 \pmod{5917}$, therefore the original message is 4630.

Sample solutions to Exercise 13.

Using a computer, it is easy to see that $1003 = 17 \times 59$.
Therefore $\varphi(n) = 16 \times 58 = 928$. Let's look for a multiplicative inverse of $e = 11$ modulo $\varphi(n) = 928$.
We apply Euclid's algorithm:

$$\begin{aligned} 928 &= 11 \times 84 + 4 \\ 11 &= 4 \times 2 + 3 \\ 4 &= 3 \times 1 + 1 \end{aligned}$$

Therefore

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 4 \times 2) \\ &= 4 \times 3 - 11 \\ &= (928 - 11 \times 84) \times 3 - 11 \\ &= 928 \times 3 - 11 \times (84 \times 3 + 1) \\ 1 &= 928 \times 3 + 11 \times (-253) \end{aligned}$$

Note that we want $d > 0$, so we take $d = -253 + \varphi(n) = 928 - 253 = 675$.
Therefore we may decipher the message with the private key $(n, d) = (1003, 675)$.
Finally $c^d = 271^{675} \equiv 951 \pmod{1003}$. So the original message sent by Bob to Alice is 951.

Sample solutions to Exercise 14.

Alice keys are (n, e) and (n, d).
She wants to send the message $m \in \{0, 1, \dots, n-1\}$ to Bob in a way that Bob can authenticate her as the sender.
For this purpose she finds the unique $s \in \{0, \dots, n-1\}$ such that $s \equiv m^d \pmod{n}$ (using her *private* key), i.e. s is the remainder of m^d by n.
She sends to Bob both the message m and the signature s.
Then Bob checks that $m \equiv s^e \pmod{n}$. If so, then Alice was the sender (or at least someone knowing Alice's private key).