University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Homework questions – Week 4

Jean-Baptiste Campesato

February 8th, 2021 to February 12th, 2021

Exercise 1.
Compute $\gcd(3^{123} - 5, 25)$.

Exercise 2.
Prove that $\forall n \in \mathbb{Z},\ 6 | n(n+1)(n+2)$

Exercise 3.

1. Prove that $\forall n \in \mathbb{Z},\ \gcd(2n, 2n+2) = 2$.
2. Prove that $\forall n \in \mathbb{Z},\ \gcd(2n-1, 2n+1) = 1$.
3. Prove that for $a, b \in \mathbb{Z}$ not both zero, $\gcd(5a+3b, 13a+8b) = \gcd(a, b)$.

Exercise 4.
Find all the integer solutions of

(a) $xy = 2x + 3y$ (b) $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$ (c) $x + y = xy$

(d) $9x + 15y = 11$ (e) $9x + 15y = 18$ (f) $1665x + 1035y = 45$

Exercise 5.

1. Prove that if $a, b \in \mathbb{Z}$ are not both zero then there exist $a', b' \in \mathbb{Z}$ such that $\gcd(a', b') = 1$, and $a = da'$ and $b = db'$ where $d = \gcd(a, b)$.
2. Prove that $\forall a, b, c \in \mathbb{Z} \setminus \{0\},\ c | ab \implies c | \big(\gcd(a, c) \gcd(b, c)\big)$

Exercise 6.

1. Prove *Sophie Germain's identity*: $a^4 + 4b^4 = \big((a+b)^2 + b^2\big)\big((a-b)^2 + b^2\big)$.
2. Prove that $3^{44} + 4^{29}$ is a composite number.
3. Prove that for every natural number $n > 1$, $n^4 + 4^n$ is a composite number.
   Hint: study the parity of n.

Exercise 7.
Prove that there are infinitely many integers that can't be written as the sum of a square with a prime number.
Hint: *look at* $(3k+2)^2$ *for* $k \in \mathbb{N} \setminus \{0\}$.

Exercise 8.
Prove that $\forall n \in \mathbb{N},\ n | (n-1)! + 1 \implies n$ is prime.

Exercise 9.
Let $n \in \mathbb{N} \setminus \{0\}$. Find n consecutive natural numbers such that none of them is a prime number.

Exercise 10.
Prove that the following numbers are not rationals using the prime factorization theorem.

1. $\log_{10} 2$
2. $\sqrt{2}$

For this question you can use what you know about $\mathbb{Q}$ *and* $\mathbb{R}$.

Exercises 11 to 14 are more difficult!

Exercise 11.
Prove that $\forall n \in \mathbb{Z},\ 49 \nmid n^3 - n^2 - 2n + 1$

Exercise 12.
Prove that there are infinitely many prime numbers of the form $p = 4k + 3$ where $k \in \mathbb{N}$.

Exercise 13. *Goldbach's theorem about Fermat numbers*

1. Prove that $\forall n \in \mathbb{N},\ \forall k \in \mathbb{N} \setminus \{0\},\ 2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$.
2. Let $m, n \in \mathbb{N}$. Prove that if $m \neq n$ then $2^{2^n} + 1$ and $2^{2^m} + 1$ are coprime.

Exercise 14.
Let $a, n \geq 2$ be two natural numbers.
1. Prove that if $a^n - 1$ is prime then $a = 2$ and n is prime.
   A number of the form $M_n = 2^n - 1$ is called a Mersenne number.
2. Is the converse true?

Exercise 15.
Three brothers inherit n gold pieces weighing $1, 2, \ldots, n$.
For what $n \in \mathbb{N} \setminus \{0\}$ can they be split into three equal heaps?

Exercise 16.
A sea pirate wants to share a treasure with its sailors.
The treasure is made of 69 diamonds, 1150 pearls and 4140 gold coins.
He is able to share fairly the treasure such that everyone (including himself) receive the same amount of each object.
How many sailors are there?

Sample solutions to Exercise 1.
The positive divisors of 25 are 1, 5 and 25. Hence, $\gcd(3^{123}-5, 25)$ has to be equal to one of these numbers. Assume by contradiction that $\gcd(3^{123}-5, 25) = 5$ or $\gcd(3^{123}-5, 25) = 25$. In both cases, $5|3^{123}-5$ and so $5|3^{123} = (3^{123}-5)+5$. Contradiction.
Therefore $\gcd(3^{123}-5, 25) = 1$.

Sample solutions to Exercise 2.
Let $n \in \mathbb{Z}$.
Since n, $n+1$ and $n+2$ are three consecutive integers, one is divisible by 2 and one is divisible by 3.
Hence $n(n+1)(n+2) = 2k$ and $n(n+1)(n+2) = 3l$ for some $k, l \in \mathbb{Z}$.
Then $2k = 3l$, so that $2|3l$. Besides $\gcd(2,3) = 1$ thus $2|l$ by Gauss' lemma, i.e. $l = 2m$ for some $m \in \mathbb{Z}$.
Therefore $n(n+1)(n+2) = 3l = 6m$ and $6|n(n+1)(n+2)$.

Sample solutions to Exercise 3.
In my solutions I use that $\gcd(a,b) = \gcd(a+kb, b)$ (see Proposition 35 of Chapter 2).

1. $\gcd(2n, 2n+2) = \gcd(2n, (2n+2)-2n) = \gcd(2n, 2) = \gcd(2n - 2\times n, 2) = \gcd(0,2) = 2$.
2. $\gcd(2n-1, 2n+1) = \gcd(2n-1, (2n+1)-(2n-1)) = \gcd(2n-1, 2) = \gcd((2n-1)-2\times n, 2) = \gcd(-1,2) = 1$.
3. $$\begin{aligned}\gcd(5a+3b, 13a+8b) &= \gcd(5a+3b, (13a+8b) - 2\times(5a+3b))\\ &= \gcd(5a+3b, 3a+2b) = \gcd((5a+3b)-(3a+2b), 3a+2b)\\ &= \gcd(2a+b, 3a+2b) = \gcd(2a+b, (3a+2b)-(2a+b))\\ &= \gcd(2a+b, a+b) = \gcd((2a+b)-b, b)\\ &= \gcd(a+b, b) = \gcd(a,b)\end{aligned}$$

Sample solutions to Exercise 4.
(a) Let $x, y \in \mathbb{Z}$. Then

$$\begin{aligned}xy = 2x+3y &\Leftrightarrow (x-3)(y-2) = 6\\ &\Leftrightarrow (x-3, y-2) \in \{(1,6), (2,3), (3,2), (6,1), (-1,-6), (-2,-3), (-3,-2), (-6,-1)\}\\ &\Leftrightarrow (x,y) \in \{(4,8), (5,5), (6,4), (9,3), (2,-4), (1,-1), (0,0), (-3,1)\}\end{aligned}$$

(b) Let $x, y \in \mathbb{Z} \setminus \{0\}$. Then

$$\begin{aligned}\frac{1}{x}+\frac{1}{y} = \frac{1}{5} &\Leftrightarrow 5y+5x = xy\\ &\Leftrightarrow (x-5)(y-5) = 25\\ &\Leftrightarrow (x-5, y-5) \in \{(1,25), (5,5), (25,1), (-1,-25), (-25,-1)\} \quad \text{since } x, y \neq 0\\ &\Leftrightarrow (x,y) \in \{(6,30), (10,10), (30,6), (4,-20), (-20,4)\}\end{aligned}$$

(c) Let $x, y \in \mathbb{Z}$. Then

$$\begin{aligned}x+y = xy &\Leftrightarrow x+y-xy+1 = 1\\ &\Leftrightarrow (x-1)(y-1) = 1\\ &\Leftrightarrow (x-1, y-1) = (-1,-1) \text{ or } (x-1, y-1) = (1,1)\\ &\Leftrightarrow (x,y) = (0,0) \text{ or } (x,y) = (2,2)\end{aligned}$$

(d) For the next questions, look at the slides from Feb 2 and/or the last part of Chapter 2.

Sample solutions to Exercise 5.

1. Let $a, b \in \mathbb{Z}$ not both zero. Set $d = \gcd(a, b)$.
   Since $d|a$ and $d|b$, we know that $a = da'$ and that $b = db'$ for some $a', b' \in \mathbb{Z}$.
   Then $d = \gcd(a, b) = \gcd\left(da', db'\right) = d \gcd\left(a', b'\right)$. Hence $\gcd(a', b') = 1$.

2. **Method 1:** Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ be such that $c|ab$.
   Set $d = \gcd(a, c)$ and $\delta = \gcd(b, c)$. Then $a = da'$, $c = dc'$, $b = \delta b''$, $c = \delta c''$ where $\gcd(a', c') = 1$ and $\gcd(b'', c'') = 1$.
   Therefore $c|ab$ becomes $dc'|da'\delta b''$, hence $c'|a'\delta b''$. Since $\gcd(a', c') = 1$, by Gauss' lemma, $c'|\delta b''$.
   Hence $\delta c'' = c = dc'|d\delta b''$, so that $c''|db''$. Since $\gcd(c'', b'') = 1$, by Gauss' lemma, $c''|d$.
   Finally $c = \delta c''|\delta d|da'\delta b'' = ab$.

   Method 2: Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ be such that $c|ab$.
   Write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ and $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ where the p_i are prime numbers and $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$.
   Then $\gcd(a, c) = p_1^{\min(\alpha_1,\gamma_1)} p_2^{\min(\alpha_2,\gamma_2)} \cdots p_r^{\min(\alpha_r,\gamma_r)}$ and $\gcd(b, c) = p_1^{\min(\beta_1,\gamma_1)} p_2^{\min(\beta_2,\gamma_2)} \cdots p_r^{\min(\beta_r,\gamma_r)}$.
   Hence $\gcd(a, c)\gcd(b, c) = p_1^{\min(\alpha_1,\gamma_1)+\min(\beta_1,\gamma_1)} p_2^{\min(\alpha_2,\gamma_2)+\min(\beta_2,\gamma_2)} \cdots p_r^{\min(\alpha_r,\gamma_r)+\min(\beta_r,\gamma_r)}$.
   Thus $c|\gcd(a, c)\gcd(b, c)$ if and only if $\gamma_1 \leq \min(\alpha_1, \gamma_1) + \min(\beta_1, \gamma_1)$, ..., $\gamma_r \leq \min(\alpha_r, \gamma_r) + \min(\beta_r, \gamma_r)$.
   First case: if $\min(\alpha_i, \gamma_i) = \gamma_i$ or $\min(\beta_i, \gamma_i) = \gamma_i$ then $\gamma_i \leq \min(\alpha_i, \gamma_i) + \min(\beta_i, \gamma_i)$.
   Otherwise: $\min(\alpha_i, \gamma_i) + \min(\beta_i, \gamma_i) = \alpha_i + \beta_i$ but since $c|ab$, we know that $\gamma_1 \leq \alpha_1 + \beta_1$, ..., $\gamma_r \leq \alpha_r + \beta_r$.

Sample solutions to Exercise 6.

1. $$\begin{aligned}\left((a+b)^2 + b^2\right)\left((a-b)^2 + b^2\right) &= \left(a^2 + 2b^2 + 2ab\right)\left(a^2 + 2b^2 - 2ab\right) \\ &= \left(a^2 + 2b^2\right)^2 - (2ab)^2 \\ &= a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = a^4 + 4b^4\end{aligned}$$

2. $3^{44} + 4^{29} = (3^{11})^4 + 4 \times (4^7)^4 = \left(\left(3^{11} + 4^7\right)^2 + 4^{14}\right)\left(\left(3^{11} - 4^7\right)^2 + 4^{14}\right)$ is non-trivial (i.e. none of the factor is ± 1, check it).

3. If $n = 2k$ with $k \in \mathbb{N} \setminus \{0\}$ then $n^4 + 4^n$ is even and greater than 2, so it is composite.
   If $n = 2k + 1$ with $k \in \mathbb{N} \setminus \{0\}$ then $n^4 + 4^n = (2k + 1)^4 + 4 \times (2^k)^4$ which has a non-trivial factorization using Germain's identity (check it), so it is a composite.

Sample solutions to Exercise 7.

Let $k \in \mathbb{N} \setminus \{0\}$. Assume by contradiction that $(3k + 2)^2 = n^2 + p$ where $n \in \mathbb{N}$ and p is a prime number.
Then $p = (3k + 2)^2 - n^2 = (3k - n + 2)(3k + n + 2)$.

- If $3k - n + 2 = 1$ then $n = 3k + 1$ so $p = 3k + n + 2 = 6k + 3 = 3(2k + 1)$ is not prime, which leads to a contradiction.
- If $3k + n + 2 = 1$ then $3k = -n - 1 < 0$, which is not possible since $k > 0$.

Therefore p admits a non-trivial factorization. Which is a contradiction.

Sample solutions to Exercise 8.

Compare with Wilson's theorem from Chapter 4.
We are going to prove the contrapositive: $\forall n \in \mathbb{N}$, n is not prime $\implies n \nmid (n-1)! + 1$.
Let $n \in \mathbb{N}$. Assume that n is not prime. Then there exists $k \in \mathbb{N}$ such that $1 < k < n$ and $k|n$.
Assume by contradiction that $n|(n-1)! + 1$. Then $k|(n-1)! + 1$. But $k|(n-1)!$ since $1 < k < n$.
Thus $k|(n-1)! + 1 - (n-1)! = 1$. Which is a contradiction.
Therefore $n \nmid (n-1)! + 1$.

Sample solutions to Exercise 9.

Let $n \in \mathbb{N} \setminus \{0\}$. Consider the following n consecutive natural numbers

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \dots, (n+1)!+(n+1)$$

Take $(n+1)!+k$ in the previous list (i.e. $k = 2, \dots, (n+1)$). Then $k|(n+1)!+k$ but $1 < k < (n+1)!+k$. Therefore $(n+1)!+k$ has a non-trivial divisor.

Sample solutions to Exercise 10.

1. Assume by contradiction that $\log_{10} 2 = \frac{a}{b} \in \mathbb{Q}$. Then

$$\frac{\log 2}{\log 10} = \frac{a}{b} \Leftrightarrow b \log 2 = a \log 10 \Leftrightarrow \log(2^a) = \log(10^b) \Leftrightarrow 2^a = 10^b \Leftrightarrow 2^a = 2^b 5^b$$

   By uniqueness of the prime factorization, $a = b = 0$. Contradiction.

2. Assume by contradiction that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. Then $2b^2 = a^2$.
   The prime factorization of the LHS has an odd number of primes (counted with exponents) whereas the RHS has an even number of primes (counted with exponents). Which is impossible since the prime factorization is unique up to order.

Sample solutions to Exercise 11.

Assume by contradiction that $49|n^3 - n^2 - 2n + 1$ for some $n \in \mathbb{Z}$.
Note that $n^3 - n^2 - 2n + 1 = (n+2)^3 - 7n^2 - 14n - 7$.
Since $7|49|n^3 - n^2 - 2n + 1$ and $7|7n^2 + 14n + 7$ then $7|(n^3 - n^2 - 2n + 1) + 7n^2 + 14n + 7 = (n+2)^3$.
By Euclid's lemma, since 7 is prime, $7|(n+2)^2$ and similarly $7|n+2$.
Therefore, there exists $k \in \mathbb{Z}$ such that $n = 7k - 2$.
Then $n^3 - n^2 - 2n + 1 = 49(7k^3 - 7k^2 + 2k) - 7$.
Therefore $49|49(7k^3 - 7k^2 + 2k) - (n^3 - n^2 - 2n + 1) = 7$. Which is a contradiction.

Sample solutions to Exercise 12.

It is a special case of Dirichlet's theorem on arithmetic progressions.
Assume that there are only finitely many primes $3 = p_1 < p_2 < \cdots < p_r$ such that $p_m = 4k_m + 3$ with $k_m \in \mathbb{R}$.
Set $n = 4p_1 p_2 \cdots p_r - 1$. Then $n = 4(p_1 p_2 \cdots p_r - 1) + 3$
Write $n = \prod_{i=1}^{s} q_i$ as a product of prime numbers.
Note that each q_i is not one of the p_m nor 2 (otherwise $q_i|1$ or $2|1$).
Therefore $q_i = 4r_i + 1$ (the only possible remainder is 1).
Hence $n = \prod_{i=1}^{s}(4r_i + 1) = 4\alpha + 1$ for some $\alpha \in \mathbb{N}$.
We obtain a contradiction with the uniqueness of the Euclidean division (the remainder of the Euclidean division of n by 4 can't 3 and 1).

Sample solutions to Exercise 13.

1. Let $n \in \mathbb{N}$. We are going to prove by induction on $k \geq 1$ that

$$\forall k \in \mathbb{N} \setminus \{0\},\ 2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$$

Base case at $k = 1$: $\left(2^{2^n} - 1\right) \times \prod_{i=0}^{0} \left(2^{2^{n+i}} + 1\right) = \left(2^{2^n} - 1\right) \times \left(2^{2^n} + 1\right) = \left(2^{2^n}\right)^2 - 1^2 = 2^{2^{n+1}} - 1.$

Induction step. Assume that $2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$ holds for some $k \geq 1$. Then

$$\begin{aligned}
\left(2^{2^n} - 1\right) \times \prod_{i=0}^{(k+1)-1} \left(2^{2^{n+i}} + 1\right) &= \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k} \left(2^{2^{n+i}} + 1\right) \\
&= \left(2^{2^n} - 1\right) \times \left(\prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)\right) \times \left(2^{2^{n+k}} + 1\right) \\
&= \left(2^{2^{n+k}} - 1\right) \times \left(2^{2^{n+k}} + 1\right) \quad \text{by the induction hypothesis} \\
&= \left(\left(2^{2^{n+k}}\right)^2 - 1^2\right) \\
&= \left(2^{2^{n+k+1}} - 1\right)
\end{aligned}$$

Which ends the induction step.

2. We may assume without lost of generality that $n < m$, i.e. $m = n + k$ for some $k \in \mathbb{N} \setminus \{0\}$.
Write $F_i = 2^{2^i} + 1$ then from the first question we get that

$$F_m + 2 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} F_{n+i}$$

Let $g = \gcd(F_m, F_n)$. Then d divides F_m and F_n thus d divides $2 = \left(2^{2^n} - 1\right) \times \left(\prod_{i=0}^{k-1} F_{n+i}\right) - F_m$.
So either $d = 2$ or $d = 1$. Since F_m is even, we get that $d = 1$.
Therefore $\gcd(F_m, F_n) = 1$.

Sample solutions to Exercise 14.

1. Assume that $a^n - 1$ is prime.
Note that $a^n - 1 = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + \cdots + a + 1\right)$.
Since $a^n - 1$ is prime, then it has no trivial divisor, therefore either $a - 1 = 1$ or $a - 1 = a^n - 1$.
The latter is not possible since $a, n \geq 2$, thus $a - 1 = 1$, i.e. $a = 2$.

Assume that $n = pq$ with $p, q \in \mathbb{N}$. Then $2^n - 1 = 2^{pq} - 1 = (2^p - 1)\left((2^p)^{q-1} + (2^p)^{q-2} + \cdots + 2^p + 1\right)$.
Since $2^n - 1$ is a prime number, then either $2^p - 1 = 1$ or $2^p - 1 = 2^{pq} - 1$.
In the first case $p = 1$ and in the other case $p = pq = n$.
Hence the only positive divisors of n are 1 and itself, i.e. n is a prime number.

2. No, $2^{11} - 1 = 2047 = 23 \times 89$.

Sample solutions to Exercise 15.

Since $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ must be divisible by 3, either $3|n$ or $3|n + 1$. It is easy to check that this necessary condition is also sufficient when $n > 3$.

Sample solutions to Exercise 16.

Note that $69 = 3 \times 23$, $1150 = 2 \times 5^2 \times 23$ and $4140 = 2^2 \times 3^2 \times 5 \times 23$. Note that only positive common divisors are 1 and 23. Assuming the pirate is not alone, the treasure is shared between 23 people so there are 22 sailors.