Collection of exercises to practice notation and the theoretical contents of the unit. You can search for the solution or ask for help through the corresponding forum. Use the forum for each unit to share the solutions to the proposed problems with other students. In these forums, all students can pose or answer questions. Peer collaboration is a very powerful tool for improving abilities associated to problem solving.

Exercise 1. Verify through induction:

a) $(\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(n+2)\right)$

b) $(\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2\right)$

c) $(\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} k^3 = \binom{n+1}{2}^2\right)$

d) $P(n) = (\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}\right)$

Exercise 2. Verify the following affirmations:

a) If $d = gcd(a,b)$ and a', b' are such that $a = da'$ and $b = d \cdot b'$ then a' and b' are coprime.

b) If a and b are coprime and there exists $k \in \mathbb{Z}$ such that $a|b \cdot k$ then $a|k$.

c) If x and n are coprime then $n - x$ and n are also coprime.

d) $gcd(ka, kb) = k \cdot gcd(a,b)\ \forall k, a, b \in \mathbb{Z}$

Exercise 3. Solve the following diophantine equations:

a) $365x + 72y = 18$

b) $28x + 36y = 44$

c) $66x + 550y = 88$

Exercise 4. Prove that:

a) For every non-prime natural number $n \geq 2$, there is a prime number p such that $p|n$ and $p^2 \leq n$

b) Using the prior proof, 373 is prime (were it not, it would have a prime number divisor $p \leq 19$)

Exercise 5. Using identity $2^{rs} - 1 = (2^r - 1)\left(2^{(s-1)r} + 2^{(s-2)r} + \ldots + 2^r + 1\right)$

a) Prove that if $2^n - 1$ is a prime number, then n is a prime number.

b) Calculate the lesser value of n so that the inverse is false.

Exercise 6. Factorize the following numbers through Fermat's method

a) 23711

b) $2^{11} - 1$.

c) 1357

Exercise 7. A band of 17 pirates joins to share a coffer with more than 100 gold coins. After an equal share of the loot, a single coin remains undistributed. In the ensuing brawl for ownership of the coin, one pirate dies. The loot is again equally shared but again, a single coin remains unallocated. What is the minimum number of coins that the coffer can contain?
Assuming that the solution is the real number of coins contained by the coffer and that the allocation mechanism remains unchanged (that is, any time that a coin is left over there is a brawl where one pirate dies), how many pirates must die so that there are no coins left after sharing the loot?

Exercise 8. Which conditions must be verified by $b, k \in \mathbb{Z}$ so that line $87x + by = K$ does not pass through any point with integer coordinates?

Exercise 9. For each $n \in \mathbb{N}$ be it $P_1(n)$ the affirmation that $n^2 + n + 11$ is prime, and $P_2(n)$ the predicate that $(3n + 2)$ is a multiple of 3.

1. Knowing that $P_1(1), P_1(2), \ldots, P_1(9)$ are all true, can we affirm that $P_1(n)$ is true $\forall n \in \mathbb{N}$?
2. Knowing that $P_2(k) \rightarrow P_2(k+1)$ is true $\forall k \in \mathbb{N}$, can we affirm that $\mathbb{N} = \{n \in \mathbb{N}, P_2(n) \text{ is true}\}$?

Exercise 10. Prove that $\forall n \in \mathbb{N}$ it is verified that $n^4 - 4n^2$ is multiple of 3
Notes: It can be useful to remember the behavior of the divisors of a number with regard to its factors.

Exercise 11. Four equal bags of candy were distributed among three groups of children. In the first group, composed by five children, two bags of candy were distributed, with a single candy being left over. In the second group, formed by six children, one bag was distributed, with two pieces of candy being left over. The last bag was delivered in a group of seven children and 3 pieces of candy were left over. If the total amount was lesser than 500 pieces of candy, how many pieces of candy were there in each of the bags?

Exercise 12. Prove that if $gcd(a, b) = 1$ then $gcd(a + b, a - b)$ is one or two.
b
Exercise 13. Prove that $gcd(ka, kb) = k \cdot gcd(a, b)$

Exercise 14. Prove that if $gcd(a, x) = 1$ and $gcd(b, x) = 1$ then $gcd(a \cdot b, x) = 1$.

Exercise 15. Three ships follow different routes, synchronizing their depart on the 1st of January of a non-leap year. Knowing their round trip times are 6, 8, and 10 days respectively, when will they meet again? How many trips will have each one completed by then?

Exercise 16. Reason whether 327 and 145 have an inverse in $\mathbb{Z}_{625}$. If so, calculate them.

Exercise 17. Using Fermat's method, calculate the remainder of dividing 3^{47} by 23.

Exercise 18. Calculate the number in the units position of 7^{1986}

Exercise 19. Calculate:

a) $7^{1968}\, mod\, 20$

b) $49^{2345}\, mod\, 1350$

Exercise 20. Indicate which of the following congruencies have a solution. Reason your answer and calculate the solution whenever it is possible.

a) $12x = 7\, mod\, 21$

b) $12x = 7\, mod\, 73$

c) $12x = 6\, mod\, 30$

d) $111x = 27\, mod\, 321$

e) $111x = 10\, mod\, 321$

f) $111x = 9\, mod\, 300$

Exercise 21. Solve the following congruency systems:

a) $\begin{cases} x = 12\, mod\, 17 \\ x = 13\, mod\, 64 \\ x = 8\, mod\, 27 \end{cases}$

b) $\begin{cases} 2x = 1\, mod\, 5 \\ x = 2\, mod\, 6 \\ x = 3\, mod\, 7 \end{cases}$

c) $\begin{cases} x = 2\, mod\, 5 \\ 2x = 1\, mod\, 7 \\ 3x = 4\, mod\, 11 \end{cases}$

Exercise 22. Solve the following congruency systems whenever it is possible.

a) $\begin{cases} x + 2y = 3\, mod\, 7 \\ 3x + y = 2\, mod\, 7 \end{cases}$

b) $\begin{cases} x + 2y = 4\, mod\, 7 \\ 4x + 3y = 4\, mod\, 7 \end{cases}$

c) $\begin{cases} x + 2y = 4\, mod\, 5 \\ 4x + 3y = 4\, mod\, 5 \end{cases}$

d) $\begin{cases} x + 2y = 4\, mod\, 5 \\ 4x + 2y = 4\, mod\, 5 \end{cases}$

Exercise 23. Prove that $\forall n \in \mathbb{N}$, if $p \in \mathbb{N}$ is prime, it is verified that $n^p = n\, mod\, p$. Use the proof to verify that the last number of n and n^5 base 10 are equal.

Exercise 24. Prove that the set of the prime numbers is infinite through *reductio ad absurdum* and congruencies.

Exercise 25. Solve the following equations:

1. $5x = 12\, mod\, 13$
2. $x^2 - x - 1 = 0$ in Z_{11}

Exercise 26. Supposing that p is a prime number:

1. Prove that the equation $x = x^{-1}$ in $\mathbb{Z}_p$ implies that $x^2 - 1 = 0\, mod\, p$ and then 1 and -1 are the only elements in $\mathbb{Z}_p$ that are equal to their own inverse.
2. Deduce from the prior affirmation that integer numbers lesser than p (except for $p - 1$ and 1) can be grouped in twos such that one of the members of the group is an inverse of the other in $\mathbb{Z}_p$.
3. Wilson's theorem: prove that $(p - 1) \neq -1\, mod\, p$

Exercise 27. Prove that:

a) If $2^n - 1$ is a prime number, then either n is an odd number or $n = 2$

b) If p is a prime number different from 2 or 5, then either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

Exercise 28. Prove the following properties:

a. $\forall n \in \mathbb{N}$, if $p \in \mathbb{N}$ is a prime number such that $mcd(n, p) = 1$ it is verified that $n^p = n\, mod\, p$. Use this to prove that the remainder of dividing 23^7 by 7 is 2.

b. $(\forall n \in \mathbb{N}) \left(\sum_{k=1}^{n} k^3 = \binom{n+1}{2}^2 \right)$

References

Herbert B. Enderton, "A mathematical introduction to logic", Elsevier, 2001.

Norman L. Biggs, "Discrete mathematics". Oxford University Press, 2002.

R. Johnsonbaugh, "Discrete mathematics". Prentice Hall, 1997.

Ralph P Grimaldi, "Discrete and Combinatorial Mathematics: An Applied Introduction". Addison-Wesley, 1994.

W. K. Grassmann and J.P. Tremblay, "Logic and discrete mathematics : a computer science perspective". Prentice Hall, 1996.