> The good Christian should beware of mathematicians, and all those who make empty prophecies. The danger already exists that the mathematicians have made a covenant with the devil to darken the spirit and to confine man in the bonds of Hell. (*Quapropter bono christiano, sive mathematici*[1], *sive quilibet impie divinantium, maxime dicentes vera, cavendi sunt, ne consortio daemoniorum irretiant.*)
>
> St. Augustine, De Genesi ad Litteram, Book II, xviii, 37.
>
> (1) Note, however, that *mathematici* was most likely used to refer to astrologers.

Question 1. Calculate the least non-negative residue of 20! mod 23. Also, calculate the least non-negative residue of 20! mod 25. (Hint: Use Wilson's theorem.)

Question 2. The order of an invertible congruence class $a \bmod m$ is the smallest positive integer n such that $a^n \equiv 1 \bmod m$. Find the order of every non-zero element of $\mathbb{Z}/19\mathbb{Z}$

Question 3. Find the least non-negative residue of $2^{47} \bmod 23$.

Question 4. Show that $n^{13} - n$ is divisible by $2, 3, 5, 7$ and 13 for all $n \geq 1$.

Question 5. Show that $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer for all n.

Question 6. Let $m = 2^{15} - 1 = 32767$. Prove the following:

(a) The order of 2 mod m is 15.

(b) The number 15 does not divide $m - 1 = 32766$.

(c) Use the previous parts to conclude that m is not prime (you are not allowed to find a factorization of m).

Question 7. Prove that $n^{101} - n$ is divisible by 33 for all $n \geq 1$.

Question 8. Find the following values of Euler's phi function:

$$\varphi(5), \varphi(6), \varphi(16), \varphi(11), \varphi(77), \varphi(10), \varphi(100), \varphi(100^n) \quad \text{for all } n \geq 1.$$

Question 9. Prove that $\varphi(p^n) = p^{n-1}(p-1) = p^n - p^{n-1}$ if p is prime, where φ is the Euler phi function, i.e., $\varphi(m)$ is the number of elements in $(\mathbb{Z}/m\mathbb{Z})^\times$.

Question 10. For each pair (a, b) below, calculate separately $\varphi(ab)$, $\varphi(a)$ and $\varphi(b)$, and then verify that $\varphi(ab) = \varphi(a)\varphi(b)$.

$$(i)\ a = 3, b = 5, \quad (ii)\ a = 4, b = 7, \quad (iii)\ a = 5, b = 6, \quad \text{and} \quad (iv)\ a = 4, b = 6$$

Question 11. The goal of this exercise is to provide an alternative proof of $\varphi(ab) = \varphi(a)\varphi(b)$ if $(a, b) = 1$.

1. First, we will prove that $\varphi(30) = \varphi(6)\varphi(5)$ as follows. Write down all the numbers $1 \leq n \leq 30$ in 6 rows of 5 numbers

1	7	13	19	25
2	8	14	20	26
3	9	15	21	27
4	10	16	22	28
5	11	17	23	29
6	12	18	24	30

(a) Show that each row is a complete residue system modulo 5, hence each row has $\varphi(5)$ numbers relatively prime to 5.

(b) Show that each column is a complete residue system modulo 6, hence each column has $\varphi(6)$ numbers relatively prime to 6. Show that all the numbers in each row are congruent modulo 6.

(c) Show that if a number is relatively prime to 30, then there are in total $\varphi(5)$ numbers in the same row that are relatively prime to 30.

(d) Conversely, show that if a number is **not** relatively prime to 6, then none of the numbers in the same row are relatively prime to 30.

(e) Conclude that

$$\begin{aligned}\varphi(30) &= \varphi(6)\varphi(5) \\ &= (\varphi(6) \text{ rows with units modulo } 30)(\varphi(5) \text{ units in each row }).\end{aligned}$$

2. Generalize the previous argument to prove that $\varphi(ab) = \varphi(a)\varphi(b)$ if $(a, b) = 1$.

RSA: Public Key Cryptography

Question 12. Read Section 7.5.3 in the book on RSA Public Key Cryptography.

Question 13. Suppose there is a public key $n = 2911$ and $e = 1867$ and you intercept an encrypted message:

0785 0976 1594 0481 1560 2128 0917.

1. Can you crack the code and decipher the message?

2. Another message is sent with public key $n = 54298697624741$ and $e = 1234567$. Could you crack this code? How would you do it? In other words, find a factorization of n to compute $\varphi(n)$, and compute (if possible) the decryption key d such that $de \equiv 1 \bmod \varphi(n)$.