> 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.)

Solution:
Since 23 is a prime, by Wilson's theorem we know that $22! \equiv -1 \mod 23$. Therefore $20! \cdot (21 \cdot 22) \equiv -1 \mod 23$. Moreover $21 \cdot 22 \equiv (-2)(-1) \equiv 2 \mod 23$. Thus: $20! \cdot 2 \equiv -1 \mod 23$ and since the inverse of 2 is 12, we get $20! \equiv -12 \equiv 11 \mod 23$.

On the other hand 20! is divisible by 25, so $20! \equiv 0 \bmod 25$.

Question 2. Find the order of every non-zero element of $\mathbb{Z}/19\mathbb{Z}$

Solution:
Here is a list of congruence classes and their orders:

class	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
order	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

You can calculate each one of these directly, but we will see better ways to calculate orders in Chapter 8, as follows: the modulus 19 is prime, thus, the order of any element must divide 18, so it must be $1, 2, 3, 6, 9$ or 18. To finish the problem, simply go through the congruence classes $1, 2, 3, \ldots, 18$ and find their order by calculating

$$a, a^2, a^3, a^6, a^9, a^{18} \bmod 19$$

and stop once you find the first instance such that one of them is 1 mod 19.

Notice that once you know that the order of 2 is 18, you can use the formula

$$\text{ord}(2^n) = \frac{18}{\gcd(18, n)}$$

to find the order of every class.

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

Solution:
Since 23 is prime and 2 is not divisible by 23, FLT applies and $2^{22} \equiv 1 \bmod 23$. Moreover, $47 = 2 \cdot 22 + 3$. Thus:

$$2^{47} \equiv (2^{22})^2 \cdot 2^3 \equiv 1 \cdot 8 \equiv 8 \bmod 23.$$

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

Solution:
We will use repeatedly the fact that $n^p \equiv n \bmod p$, for all $n \geq 1$. In all cases we will show that $n^{13} \equiv n \bmod p$ for $p = 2, 3, 5, 7$ adn 13.

- By 2: $n^{13} \equiv (n^2)^6 \cdot n \equiv n^6 \cdot n \equiv (n^2)^3 \cdot n \equiv n^4 \equiv (n^2)^2 \equiv n^2 \equiv n \bmod 2$.
- By 3: $n^{13} \equiv (n^3)^4 \cdot n \equiv n^5 \equiv n^3 \cdot n^2 \equiv n \cdot n^2 \equiv n^3 \equiv n \bmod 3$.
- By 5: $n^{13} \equiv (n^5)^2 \cdot n^3 \equiv n^2 \cdot n^3 \equiv n^5 \equiv n \bmod 5$.
- By 7: $n^{13} \equiv n^7 \cdot n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \bmod 7$.
- By 13: $n^{13} \equiv n \bmod 13$.

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

Solution:
If the number $N = \frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer, then $15N = 3n^5 + 5n^3 + 7n$ is an integer. Conversely, if $3n^5 + 5n^3 + 7n$ is an integer divisible by 15, then N is an integer. So let us prove that $M = 3n^5 + 5n^3 + 7n$ is always divisible by 15. Since $15 = 3 \cdot 5$, it suffices to show that M is divisible by 3 and 5:

- By 3: $M = 3n^5 + 5n^3 + 7n \equiv 2n^3 + n \equiv 2n + n \equiv 3n \equiv 0 \bmod 3$. Notice that we used FLT to prove $n^3 \equiv n \bmod 3$ for all n.
- By 5: $M = 3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n \equiv 3n + 2n \equiv 0 \bmod 5$. Here we used $n^5 \equiv n \bmod 5$, by FLT.

Thus 3 and 5 divide M, so 15 divides M, and hence $N = M/15$ is an integer.

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).

Solution:

- The order of $2 \bmod m$ is 15. Indeed, $2^{15} \equiv 1 \bmod m$ because $m = 2^{15} - 1$, and $2^d \not\equiv 1 \bmod m$ for any $d < 15$ because $2^d - 1 < m$ for any $d < 15$.
- 15 does not divide $m - 1 = 32766$. Indeed, $m - 1 = 32766$ is clearly not divisible by 5, so it cannot be divisible by 15.

Therefore, m cannot be prime because if m was prime, Fermat's Little theorem would imply that $2^{m-1} \equiv 1 \bmod m$ and, therefore, the order of 2 (which is 15) would divide $m - 1$. Thus m cannot be prime.

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

Solution:
We prove that $n^{101} - n$ is divisible by 3 and 11.

- By 3: if $n \equiv 0 \bmod 3$ then $n^{101} \equiv 0 \equiv n \bmod 3$. If $n \not\equiv 0 \bmod 3$, then $n^2 \equiv 1 \bmod 3$ and $n^{101} \equiv (n^2)^{50} n \equiv n \bmod 3$.
- By 11: if $n \equiv 0 \bmod 11$ then $n^{101} \equiv 0 \equiv n \bmod 11$. If $n \not\equiv 0 \bmod 11$ then $n^{10} \equiv 1 \bmod 11$ and $n^{101} \equiv (n^{10})^{10} n \equiv n \bmod 11$.

Thus, $n^{101} - n$ is always divisible by 3 and 11, so it is divisible by 33.

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

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

Solution:
Recall that $\phi(p^n) = p^{n-1}(p-1)$ if p is a prime and $\phi(ab) = \phi(a)\phi(b)$ if $(a, b) = 1$. The values are now a simple calculation. For example:

$$\phi(100^n) = \phi(2^{2n} \cdot 5^{2n}) = \phi(2^{2n})\phi(5^{2n}) = 2^{2n-1}(2-1)5^{2n-1}(5-1) = 2^{2n+1} \cdot 5^{2n-1}.$$

Question 9. Prove that $\varphi(p^n) = p^{n-1}(p-1) = p^n - p^{n-1}$ if p is prime.

Solution:
By definition, $\varphi(p^n)$ is the number of units in $\mathbb{Z}/p^n\mathbb{Z}$. By definition, the units in $\mathbb{Z}/p^n\mathbb{Z}$ are those numbers between 1 and $p^n - 1$ which are relatively prime to p^n, and thus relatively prime to p. Let's count the number of non-units instead, i.e. the elements of $\mathbb{Z}/p^n\mathbb{Z}$ which *have* a factor of p. These are:

$$0, p, 2p, 3p, \ldots, p \cdot p, (p+1)p, (p+2)p, \ldots, p^n - p = (p^{n-1} - 1)p.$$

Therefore, $\mathbb{Z}/p^n\mathbb{Z}$ has p^n elements and p^{n-1} non-units. Thus, the number of units must be:

$$\varphi(p^n) = p^n - p^{n-1}.$$

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

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

Solution:

- $a = 3$, $b = 5$. $\mathbb{Z}/3\mathbb{Z}$ has 2 units, $\mathbb{Z}/5\mathbb{Z}$ has 4 units (see problem 7) and $\mathbb{Z}/15\mathbb{Z}$ has 8 units:
$$U_{15} = \{1, 2, 4, 7, 11, 13, 14\}.$$
- $a = 4$,$b = 7$. $\mathbb{Z}/4\mathbb{Z}$ has 2 units and $\mathbb{Z}/7\mathbb{Z}$ has 6 units because 7 is prime. $\mathbb{Z}/28\mathbb{Z}$ has 12 units:
$$U_{28} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$
- $a = 5$ and $b = 6$. $\mathbb{Z}/5\mathbb{Z}$ has 4 units and $\mathbb{Z}/6\mathbb{Z}$ has 2 units. $\mathbb{Z}/30\mathbb{Z}$ has 8 units:
$$U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$
- If $a = 4$ and $b = 6$ then $\varphi(24) \neq \varphi(4) \cdot \varphi(6)$. $\mathbb{Z}/4\mathbb{Z}$ has 2 units and $\mathbb{Z}/6\mathbb{Z}$ has 2 units, but $\mathbb{Z}/24\mathbb{Z}$ has 8 units:
$$U_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

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 $(a, b) = 1$.

Solution:
We'll solve part (2) directly. Write the numbers $\leq ab$ in a table as follows:

$$\begin{array}{c|c|c|c|c}
1 & 2 & 3 & \dots & a \\
a+1 & a+2 & a+3 & \dots & 2a \\
2a+1 & 2a+2 & 2a+3 & \dots & 3a \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \dots & ba
\end{array}$$

Note that:

- Each row is congruent to $1, 2, 3, \dots, 0 \bmod a$, thus, each row has exactly $\varphi(a)$ elements relatively prime to a.
- Each column is a complete set of representatives modulo b. Why? Here is why. $\{0, 1, 2, 3, \dots, b-1\}$ is a complete set of representatives modulo b. Since $(a, b) = 1$, a is a unit modulo b, and therefore $\{0, a, 2a, 3a, \dots, (b-1)a\}$ is also a complete set of representatives modulo b. Finally, if we add a constant k to every number in a complete set of representatives, we obviously get back another complete set of representatives (we are simply shifting all numbers by k). Thus, $\{k, a+k, 2a+k, 3a+k, \dots, (b-1)a+k\}$, a column in our table, is a complete set of representatives mod b, for any k.
- Therefore, every column has exactly $\varphi(b)$ elements relatively prime to b.
- Since a unit modulo ab is a number that is relatively prime to both a and b, there will be $\varphi(a)\varphi(b)$ units modulo ab in the table: $\varphi(a)$ columns relatively prime to a and $\varphi(b)$ numbers in every column are relatively prime also to b.

RSA: Public Key Cryptography

Question 12. Read Section 7.5.2 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?

Solution:
In order to crack an RSA code, the fundamental problem is to be able to factor n. In this case, this is easily accomplished because n is small enough. Indeed: $n = 41 \cdot 71$. Hence, we can calculate $\varphi(n) = \varphi(41)\varphi(71) = 40 \cdot 70 = 2800$. Also, we can calculate $d = e^{-1}$ modulo 2800:

$$d \equiv (1867)^{-1} \equiv 3 \bmod 2800.$$

Now, we can start decoding the message, one block at a time:

$$(0785)^3 \equiv 1200 \bmod 2911, \quad (0976)^3 \equiv 1907 \bmod 2911, \dots$$

The full decoded message is:

$$1200\ 1907\ 0818\ 0022\ 0418\ 1412\ 0423$$

When we translate the code back into letters (remember $00 = A,\ 01 = B, \ldots$) we get:

MATHISAWESOMEX

Hence, the original message was "*Math is awesome*" (and a letter X was added at the end to finish a four digit block).

For the second part, one would first use a computer to factor n into primes,

$$n = 54298697624741 = 7368743 \cdot 7368787,$$

so that we can calculate $\varphi(n)$:

$$\varphi(n) = \varphi(7368743 \cdot 7368787) = 7368742 \cdot 7368786 = 54298682887212.$$

Next we would calculate the decoding exponent d as the solution of the linear congruence $ed \equiv 1 \bmod \varphi(n)$, i.e.,

$$1234567 \cdot d \equiv 1 \bmod 54298682887212.$$

The solution is $d = 47898735178447$. Now, if we intercept a message M, then we just *simply* need to calculate $M^d \bmod n$, i.e.,

$$M^d \bmod 54298697624741,$$

again with the help of a computer.