AN INTRODUCTION TO ARITHMETICS
MATHEMATICAL FOUNDATIONS (Ó.R.)

The aim of this class is to give a brief introduction to some basic aspects of congruences, without entering too much in the language of ring theory. The reader must be aware that many of these concepts can be formulated with much more generality, but we content here with a first approach.
The most elementary questions that arise in the study of arithmetics are concerned with the so-called (arithmetic) modules. Roughly speaking, we are interested in working with the residue classes we obtain when dividing by n, and to have there a notion of addition, multiplication and so on. For this purpose, there are two natural approaches:

1. We can define $\mathbb{Z}/n\mathbb{Z}$ set-theoretically, as $\mathbb{Z}/\sim$, where $x \sim y$ if $x - y$ is a multiple of n. Then, we can put to this set two operations, a sum and a product, and check that with this structure $\mathbb{Z}/n\mathbb{Z}$ is a ring.

2. We can consider that $\mathbb{Z}$ is a ring and that $n\mathbb{Z}$ is an ideal (a set of elements I satisfying that if $a, b \in I$, then $a + b \in I$ and that $xa \in I$ for all x in the ring). Then, it makes sense to consider the quotient $\mathbb{Z}/n\mathbb{Z}$ and the ring morphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$; the quotient inherits (as in the case of vector spaces) the operations of the ring $\mathbb{Z}$. In addition, $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ can also be seen as $\mathbb{Z}$-modules, and in general, as $\mathbb{Z}$-algebras (observe the similitude with the case of vector spaces, where you have worked with k-algebras over a field, for instance $\mathrm{End}(V)$, where V is a k-vector space).

Hence, we can assume that we already have our fundamental element of study, the ring $\mathbb{Z}/n\mathbb{Z}$, and that the elements there are given by the class of the integers i, with $0 \leq i \leq n - 1$.

1 Euclid's algorithm and invertible elements

A first natural question is to ask ourselves by the invertible elements in the ring $(\mathbb{Z}/n\mathbb{Z})$. Before giving an answer, we recall the following:

Proposition 1. *The equation $ax + by = d$, where $a, b, d \in \mathbb{Z}$ has a solution over $\mathbb{Z}$ if and only if $\gcd(a, b)|d$.*

Sketch of the proof. Observe that $ax + by$ always divides the greatest common divisor of a and b, and hence one implication is trivial.
To see the converse, we can restrict to the case of $ax + by = 1$, with a, b relatively prime integers, and here Euclid's algorithm (in its extended version) tells us that there are always a solution. We can formalize this by induction on $\max\{a, b\}$: if $a = bq + r$ (with $a > b$), by induction hypothesis we have that $bx' + ry' = 1$, and then

$$bx' + (a - bq)y' = ay' + b(x' - qy') = 1.$$

□

Let us work an example: take $a = 11, b = 25$. Then,

$$25 = 2 \cdot 11 + 3,$$

$$11 = 3 \cdot 3 + 2,$$
$$3 = 1 \cdot 2 + 1,$$
$$2 = 2 \cdot 1.$$

In particular,

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11 = 4 \cdot (25 - 2 \cdot 11) - 1 \cdot 11 = 4 \cdot 25 - 9 \cdot 11.$$

We conclude that the gcd obtained via the Euclid's algorithm can always be represented in terms of a and b.

Now, we are ready to solve the previous question: what are the invertible elements in $\mathbb{Z}/n\mathbb{Z}$? For an element a to be invertible, we require that

$$ax = ny + 1$$

has a solution, and this happens if and only if a and n are relatively prime.

Problem 1. *$\phi(n)$ is the number of positive integers less than n that are relatively prime with n. If $n = \prod_{i=1}^{r} p_i^{e_i}$, give two proofs of the fact that*

$$\phi(n) = \prod_{i=1}^{n} (p_i - 1) p_i^{e_i - 1}.$$

1. *First of all, recall that*

$$\Big| \bigcup_{i=1}^{n} A_i \Big| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} | \cap_{i=1}^{n} A_i|.$$

   Let A_i be the set of positive integer less than n that are not relatively prime with p_i. Then, taking into account that

$$\phi(n) = n - \Big| \bigcup_{i=1}^{n} A_i \Big|$$

   conclude the proof of the result.

2. *Use the Chinese remainder theorem to show that $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m, n) = 1$. Then, show that $\phi(p^n) = p^{n-1}(p - 1)$ and conclude the proof.*

The following observation will be crucial from now on: the set of invertible elements in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ forms a group under multiplication.
We begin by giving two proofs of the Euler's theorem,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

whenever $\gcd(a, n) = 1$. In particular, if n is a primer number, this statement is usually called *Fermat's little theorem*:

$$a^{p-1} \equiv 1 \pmod{p},$$

whenever $p \nmid a$.

Problem 2. *Prove Euler's theorem and recover Fermat's little theorem.*

Solution: Let $X = \{r_1, \ldots, r_{\phi(n)}\}$ be the set of classes of integers relatively prime with n (those integers smaller than n and coprime with it. Consider now the set $Y = \{ar_1, \ldots, ar_{\phi(n)}\}$. Clearly, these $\phi(n)$ integers are coprime with n since both a and r_i are coprime with n. Further, all of them give different remainders modulo n, since in the case that $ar_i \equiv ar_j \pmod{n}$, we have that $a(r_i - r_j)$ is a multiple of n, and because a is relatively prime with n and r_i, r_j are both between 1 and $n-1$, this is not possible. Hence, the sets X and Y consist on the same elements (modulo n) and hence, the product of all of them gives the same remainder modulo n. In particular

$$r_1 \cdots r_{\phi(n)} \equiv a^{\phi(n)} r_1 \cdots r_{\phi(n)} \pmod{n},$$

and since the product of the r_i is relatively prime with n we can cancel out this terms and we obtain that

$$r^{\phi(n)} \equiv 1 \pmod{n},$$

as desired. In the particular case that $n = p$, $\phi(n) = p - 1$ and we recover Fermat's little theorem.
We can give an alternative proof based on group theory.

Proposition 2 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. Then, $|H|$ divides $|G|$.*

Proof. Let $b_1, \ldots, b_n$ be the elements of G. Then, two sets b_iH, b_jH are either equal or disjoint (prove this). Hence, there must exist a set of indexes $a_1, \ldots, a_k$ such that $a_1H, \ldots, a_kH$ is the whole group and each element is in exactly one of the cosets. Then, $k|H| = |G|$. □

In particular, we can consider the subgroup generated by a, say all the elements of the form a^i, inside the multiplicative group that has order $\phi(n)$. We conclude that the order of a must divide $\phi(n)$.
A natural question now is: for a number a relatively prime with n, which is the smallest positive number i such that $a^i \equiv 1 \pmod{n}$? This number is called the order of a modulo n, and is denotes as $\mathrm{ord}_n(a)$.

Problem 3. *Prove that $a^x \equiv 1 \pmod{n}$ if and only if x is a multiple of the order. Prove also that $\mathrm{ord}_n(a^x) = \mathrm{ord}_n(a)/\gcd(\mathrm{ord}_n(a), x)$.*

In particular, we know that $\phi(n)$ must be a multiple of the order.

2 The structure of $(\mathbb{Z}/p^k\mathbb{Z})^\times$

We now want to study the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$, and for that we need the following three facts:

1. By the Chinese remainder theorem that we recall later on, we can study separately the structure of $(\mathbb{Z}/p_i^{e_i})^\times$ for the different primes appearing in the factorization of n.

2. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

3. $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is also cyclic. This comes from combining the previous statement with the technique of lifting the exponent.

During the proof of the following proposition, we use this lemma:

Lemma 1. *Show that*

$$\frac{1}{n}\sum_{d|n}\phi(d) = 1.$$

Proof. In the additive group $\mathbb{Z}/n\mathbb{Z}$ the order has to be a divisor of n. Let us count those numbers whose order is d, for a fixed divisor d of n. In particular, we are looking for those numbers a such that ad is a multiple of n and ai is not a multiple of n for any $i < d$. Then, it must be $a = nk/d$, with $0 \leq k \leq d-1$ and k relatively prime with d. We conclude that there are $\phi(d)$ such numbers. In particular,

$$\sum_{d|n}\phi(d) = n.$$

□

Proposition 3. $(\mathbb{Z}/p\mathbb{Z})^\times$ *is a cyclic group.*

Proof. First of all, we observe that the order of an element must divide the order of the group, that is, a divisor of $m := \phi(p)$. For each divisor $d|m$, we have that an element of order d satisfies $x^d - 1 = 0$, and no other equation of the form $x^i - 1$, with $i|d$. But observe that if x has order exactly d, then all the numbers $x^0, \ldots, x^{d-1}$ are solutions of $x^d - 1 = 0$, and this equation cannot have more solutions since we are working over a field, $\mathbb{Z}/p\mathbb{Z}$. Then, between these d solutions, exactly $\phi(d)$ have order exactly d, since the order of x^i is the order of x divided by $\gcd(d, i)$. We conclude that the number of elements with order exactly d is either 0 or $\phi(d)$. But observe that the order must divide m, and hence

$$\sum_{d|m}\text{number of elements of order } d \leq \sum_{d|m}\phi(d) = m,$$

and we conclude that all the inequalities are in fact equalities. In particular, there are $\phi(p)$ elements of order $p-1$. □

As an example, consider $(\mathbb{Z}/7\mathbb{Z})^\times$. There must be exactly 2 elements of order 6, that are 3 and 5.
Now, we move to the prime-power case, where the key ingredient will be the technique of lifting the exponent. We will do the detailed proof for the case of p odd, and the case $p = 2$ follows the same argument but taking as the base step that we know that $(\mathbb{Z}/4\mathbb{Z})^\times$ is cyclic.
We will use the notation $v_p(n) = k$ to indicate that $p^k|n$ and that $p^{k+1} \nmid n$. We also write in this case $p^k||n$.

Lemma 2. *Let a, b be integer numbers and p an odd prime number such that $p|(a-b)$ and such that $p \nmid a$. Then,*

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

Proof. Write $a = b + k$, where $v_p(k) = v_p(a-b)$. We will proceed by induction over $v_p(n)$. When $v_p(n) = 0$

$$a^n - b^n = (b+k)^n - b^n = b^n + nkb^{n-1} + (\text{terms divisible by higher powers of } p) - b^n,$$

so $v_p(a^n - b^n) = v_p(k) = v_p(a-b)$, as desired.
Before going to the inductive step, we proof the case $n = p$. Here

$$a^p - b^p = (b+k)^p - b^p = pkb^{p-1} + (\text{terms divisible by higher powers of } p),$$

since p always divides $\binom{p}{i}$ when $1 \leq i \leq p-1$. Then, $v_p(a^p - b^p) = v_p(a-b) + 1$.
Assume that the result is true when $v_p(n) = s$ and we prove it for $s+1$. In particular, assume that $n = p^{s+1} \cdot r$, with $\gcd(p, r) = 1$. Then,

$$v_p(a^n - b^n) = v_p((a^{p^s r})^p - (b^{p^s r})^p) = v_p(a^{p^s r} - b^{p^s r}) + v_p(p) = v_p(a-b) + s + 1.$$

□

Problem 4. *Extend (with some modifications) the lemma for the case $p = 2$.*

Proposition 4. *The group $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic.*

Proof. We know that $\mathbb{Z}/p\mathbb{Z}$ is cyclic. Take a generator of $\mathbb{Z}/p\mathbb{Z}$ and consider the p^{k-1} elements of $\mathbb{Z}/p^k\mathbb{Z}$ that are congruent with it. We claim that some of these numbers has order $p^{k-1}(p-1)$. In fact, for one such a to be a generator, $p^{k-1}(p-1)$ must be the smaller positive number such that $a^i \equiv 1 \pmod p)^k$. To have $a^i \equiv 1 \pmod p$, it must be $i = r(p-1)$. First of all, observe that for two numbers like these, say a, b, we have that $v_p(a^{p-1} - b^{p-1}) = v_p(a-b)$. In particular, of these p^{k-1} numbers, $(p-1)p^{k-2}$ satisfy that $v_p(a^{p-1} - 1) = 1$. Take one such number a. Then,

$$v_p(a^{r(p-1)} - 1) = v_p(a^{p-1} - 1) + v_p(r) = 1 + v_p(r),$$

and for this number to be k we require that $v_p(r) = k-1$. Then, the smallest number satisfying the condition is $(p-1)p^{k-1}$, as desired. □

Observe that when $k \geq 2$ we have proved that there are exactly $\phi(p-1)(p-1)p^{k-2}$ generators of the group, as expected, since

$$\phi(\phi(p^k)) = \phi((p-1)p^{k-1}) = \phi(p-1)\phi(p^{k-1}) = \phi(p-1)(p-1)p^{k-2},$$

where we have used again that the ϕ-function is weakly multiplicative.
We continue by studying another classical question.

Problem 5 (Wilson)**.** *Prove that $(p-1)! \equiv -1 \pmod p$.*

Solution: If $p = 2$ the result is trivial. Otherwise, observe that each element in $1, 2, \ldots, p-1$ has an inverse modulo p. The only elements that are self-inverse are 1 and -1, since the equation $x^2 \equiv 1 \pmod p$ forces $(x-1)(x+1) \equiv 0 \pmod p$, and since $\mathbb{Z}/p\mathbb{Z}$ is a field, it must be either $x = 1$ or $x = -1$. The other $p-3$ elements must have an inverse that is different from theirselves and is unique; in addition, if a is the inverse of b, b is the inverse of a. Hence, we can group the remaining $p-3$ elements in $(p-3)/2$ pairs (a_i, b_i) such that $a_i b_i \equiv 1 \pmod n$. Hence

$$(p-1)! \equiv 1 \cdot (-1) \cdot \prod_{i=1}^{\frac{p-3}{2}} a_i b_i \equiv 1 \cdot -1 \cdot 1 = -1 \pmod p.$$

Observe that when p is not a prime number the result is false. If $n \neq p^2$, we can take a divisor of n different from 1 and n, say m, and observe that $m \cdot n/m$ is already a multiple of m, hence the congruence is 0. If $n = p^2$ and $p \geq 3$, there are at least two multiples of p smaller than n, and then it is also 0. When $n = 4$, $3! \equiv 2 \pmod 4$.

3 The Chinese remainder theorem

We frequently have to deal with system of congruences, in which one would like to determine all the integers x that verify, for instance, that are congruent with 5 modulo 6 and with 3 modulo 7. Here, one check that $17, 17+42, 17+84, \ldots$ all work. But this cannot always be done. For instance, we cannot find an integer number congruent with 5 modulo 6 and with 2 modulo 8. The reason is that 6 and 8 are not coprime, so forcing a certain congruence modulo 6 determines the congruence in all its divisors (for instance 2) so we are saying twice the congruence modulo 2 and this information can be (and in this case is what happens) contradictory. But this does not occur if the numbers are relatively prime.

Theorem 1 (Chinese remainder)**.** *Let $n_1, \ldots, n_r$ be a collection of relatively prime integer numbers. Then, for any integer numbers $a_1, \ldots, a_r$ there is a unique integer x between 0 and $n_1 \cdots n_r - 1$ (or a unique residue class in $\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z}$) such that $x \equiv a_i \pmod{n}_i$ for all i. Then, $y \in \mathbb{Z}$ satisfies this congruence if and only it is congruent with x modulo $n_1 \ldots n_r$.*

Proof. It is enough to prove the theorem when $r = 2$ since then we can proceed for induction, taking $\tilde{n}_1 = n_1 \cdots n_{r-1}$ and $\tilde{n}_2 = n_r$, because if n_r is coprime with $n_1, \ldots, n_{r-1}$ it is also coprime with their product.
Then, we can restrict to the following easier result: given m and n relatively prime natural numbers, and $a, b \in \mathbb{Z}$ we must prove that there is one and only one number x between 0 and $mn - 1$ such that $x \equiv a$ modulo m and $x \equiv b$ modulo n.
Let $\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be the application that sends the residue class of x modulo mn to $(x \pmod m, x \pmod n)$. Suppose that $\phi(x) = \phi(y)$. Then, $\phi(x-y) = 0$, and hence $x - y$ is a multiple of both m and n, and consequently, a multiple of mn. This implies that x and y are the same element modulo mn. Then, ϕ is injective and since both sets have the same cardinality, ϕ must be a bijection (in particular, it is surjective). □

Remark: From the preceding, we conclude that to know $z \pmod{n_1 \cdots n_r}$ is the same as knowing it modulo each of the n_i. In fact, any statement modulo a number N can be reduced to a statement modulo each of its prime powers.
This proof has the advantage of being very simple, but has the drawback that it is not constructive. However, it is relatively easy to observe that obtaining a solution can be done applying Bézout's identity. For instance, imagine that we want x congruent with 3 modulo 8 and with 4 modulo 5.
Let us begin constructing a number congruent with 3 modulo 8 and with 0 modulo 5. For this, just take the Bézout identity

$$8x + 5y = 1,$$

that has $x = 2$ and $y = -3$ as a solution, and observe then that

$$8 \cdot 6 + 5 \cdot (-9) = 3,$$

or alternatively

$$5 \cdot (-9) = 3 - 8 \cdot 6.$$

The number $5 \cdot (-9)$ is clearly a multiple of 5 and by construction, it is congruent with 3 modulo 8. Then, -45 works, and so $-45 + 40 \cdot 2 = 35$ too.

In the same way we get a number congruent with 0 modulo 8 and with 4 modulo 5, say 24. Now, adding up the two numbers, we have $35 + 24 \equiv 19 \pmod{40}$ and by the properties of congruences, it verifies the two requirements.

We now come back to the previous problem, the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$. When n is odd, the Chinese remainder theorem asserts that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/(p_i - 1)p_i^{e_i - 1}\mathbb{Z}).$$

When $2|n$, the factor corresponding to $\mathbb{Z}/2^k\mathbb{Z}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$. In particular, observe that the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic (has a generator) if and only if $n = 2, 4, p^k$ or $2p^k$.

Problem 6. *Find the number of solutions of $x^2 = x$ in $\mathbb{Z}/60\mathbb{Z}$.*

Solution: We require $x(x-1) \equiv 0 \pmod{60}$. From $x(x-1) \equiv 0 \pmod{4}$ and $\gcd(x, x-1) = 1$ we see that either x or $x-1$ must be a multiple of 4. For the same reason, either x or $x-1$ is a multiple of 3 and again either x or $x-1$ is a multiple of 5. We have therefore 8 possibilities that are independent due to the Chinese remainder theorem. For instance, if $x \equiv 0 \pmod{4}, x \equiv 0 \pmod{3}, x \equiv 1 \pmod{5}$ we obtain that 36 is one possible solution. The other solutions are $25, 21, 40, 16, 45, 0$ and 1 (eight in total).

Problem 7. *Use the Chinese remainder theorem to find the number of solutions of*

$$x^2 \equiv 1 \pmod{n}.$$

4 Problems

Problem 8. *Use Euclid's algorithm to find all the integer solutions of*

$$6x + 8y = 10.$$

Problem 9. *Show that the equation*

$$x^2 + 3y^2 = 2z^2$$

cannot have any integer solution different from $(0, 0, 0)$.

Problem 10. *Find the last three digits of 2009^{2011}.*

Problem 11. *Find all integer number satisfying*

$$\begin{cases} n \equiv 0 \pmod{2} \\ n \equiv 2 \pmod{3} \\ n \equiv 6 \pmod{7}. \end{cases}$$

Problem 12. *Give a criterion to determine when the equation*

$$ax \equiv b \pmod{n}$$

has at least one solution. In these cases, determine the number of solutions.

Problem 13. *Let n be a positive integer, and let S denote the set of positive integers smaller or equal than n which are relatively prime with n. The n-th cyclotomic polynomial $\Phi_n(x)$ is defined as*

$$\Phi_n(x) = \prod_{i \in S} (x - \zeta_n^i) \in \mathbb{C}[X],$$

where $\zeta_n = e^{2\pi i/n}$.

1. *Show that for any p prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$.*
2. *Show that*
$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$
3. *Show that $\Phi_n(x) \in \mathbb{Z}[X]$.*
4. *Consider the reduction of $\Phi_{p-1}(x)$ modulo p. Show that $\Phi_{p-1}(x)$ is a monic polynomial whose roots all have multiplicity one and agree with the $\phi(p-1)$ primitive roots modulo p. For instance,*
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1,$$
and over $\mathbb{F}_{11}[X]$ the roots are 2, 6, 7 and 8.

5 Challenging problems

Problem 14. *Determine how many elements in $(\mathbb{Z}/N\mathbb{Z})^\times$ have even order.*

Problem 15. *Find the least positive integer n such that for any set of integer numbers $\{a_1, \ldots, a_n\}$ there are two distinct elements a_i, a_j such that 2009 divides either $a_i - a_j$ or $a_i a_j - 1$.*

Problem 16. *Let p, q be relatively prime positive integers. Prove that*

$$\sum_{k=0}^{pq-1} (-1)^{\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even,} \\ 1 & \text{if } pq \text{ is odd.} \end{cases}$$

Problem 17. *Given $x \in (0,1)$, let $y \in (0,1)$ be the number whose n-th digit after the decimal point is the 2^n-th digit after the decimal point of x. Prove that if x is rational, then y is also rational.*

Problem 18. *Prove that, for any n, there are n consecutive numbers such that any of them is divisible by the sum of its digits.*

Problem 19. *Prove that 2 is a primitive root modulo 5^k (also called generator of the multiplicative group).*

Problem 20. *In a board of dimensions $n \times n$ we place the numbers $1, 2, \ldots, n^2$ in some order. n positions are said to be disperse if there are no two in the same row or column. A board is said to be good if all the products of n numbers written in n disperse positions give the same remainder when divided by $n^2 + 1$. Determine if there exist good boards for $n = 8$ and $n = 10$.*

Problem 21. *Let k be a positive integer and $a_1, \ldots, a_k$ digits. Prove that there exists a positive integer n such that the last $2k$ digitis of 2^n are, in this order,*

$$a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$$

for certain digits $b_1, b_2, \ldots, b_k$.

Problem 22. *Find the greatest value of k such that 1991^k divides*

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Problem 23. *Determine all positive integers n such that $\frac{2^n+1}{n^2}$ is an integer number.*