Elementary Number Theory 2022

August 24, 2022

– Notation –

Put

$$\mathrm{Spec}(\mathbb{Z}) := \left\{ p \in \mathbb{Z} \;\middle|\; p \text{ er et primtall} \right\}.$$

This is called the **spectrum** of $\mathbb{Z}$[(a)].

Sometimes there is a red/pink circle with an E inside, placed in the margin. This indicates that there is an exercise hiding in the text.

The set (ring) of all polynomials with coefficients in $\mathbb{Z}$, is denoted $\mathbb{Z}[x]$, indicating that x is the variable[(b)].

(a) More generally, if R is a ring,

$$\mathrm{Spec}(R) := \left\{ \mathfrak{p} \subset R \mid \mathfrak{p} \text{ prime ideal} \right\}$$

is the **spectrum** of R. If $(0) \in \mathrm{Spec}(R)$, then the ring is an **integral domain**.

(b) We can replace $\mathbb{Z}$ with any commutative ring if so desired (but we won't use this here).

– Division algorithm –

The following should be well-known to everybody since elementary school:

Definition 1. Let $a, b \in \mathbb{Z}$ where $a \geq b$. Then there are *unique* $q, r \in \mathbb{Z}$, such that

$$a = qb + r, \quad 0 \leq r < b.$$

The number q is the **quotient** and r is the **residue**. One says that r is the residue of a **modulo** b.

If $r = 0$ we say that b **divides** a and we write $b \mid a$; in the opposite case, we write $b \nmid a$.

It is important to note the following:

(1) The residue is **strictly** less than b. Think about what it would mean otherwise.

(2) We have the following equivalence

$$b \mid a \iff \text{there is a unique } t \in \mathbb{Z} \text{ such that } a = tb.$$

The following theorem is fundamental.

Theorem 1. Let $a, b, c, d \in \mathbb{Z}$. Then

(i) $b \mid a \implies b \mid ac$;

(ii) $b \mid a$ and $b \mid c \implies b \mid (a \pm c)$;

(iii) $b \mid a$ and $d \mid c \implies (bd) \mid (ac)$;

(iv) $b \mid a$ and $a \mid c \implies b \mid c$;

(v) la $b \neq 0$; $b \mid a$ and $b \mid c \implies b \mid (na \pm mc)$, for all $n, m \in \mathbb{Z}$.

Proof. We will prove (ii), (iv) and (v) and let (i) and (iii) be an exercise for you.

(ii) That $b \mid a$ is equivalent with the existence of a unique $r \in \mathbb{Z}$ such that $a = rb$; similarly, $c = sb$ for some unique $s \in \mathbb{Z}$. This gives that $a \pm c = rb \pm sb = (r+s)b$, which, by definition, means that $b \mid (a \pm c)$.

(iv) By definition: $a = rb$ and $c = sa$. Substitution gives $c = sa = s(rb) = (rs)b$, which is equivalent to $b \mid c$.

(v) Once again, by definition, $a = rb$ and $c = sb$. It is obvious that this means that $b \mid na$ fra (i). Analogously, we see $b \mid mc$. Therefore (ii) gives that $b \mid (na \pm mc)$. E

As said, (i) and (iii) are exercises. □

– Greatest common divisor –

Definition 2. Let $a, b \in \mathbb{Z}$. Then the **greatest common divisor between** a **and** b, $\gcd(a,b)$, is the unique number $d \in \mathbb{Z}_{\geq 1}$ such that $d \mid a$ and $d \mid b$.

When $\gcd(a,b) = 1$ we say that a and b are **relatively prime**.

Lemma 1. We have

$$\gcd(a,n) = \gcd(b,n) = 1 \iff \gcd(ab,n) = 1.$$

Proof. $\Rightarrow$) Suppose $\gcd(a,n) = \gcd(b,n) = 1$. Since there are no common factors between a and n or b and n, there can be no common factors between ab and n.

$\Leftarrow$) Suppose $\gcd(a,n) = d > 1$. Then $\gcd(ab,n) > 1$ since d divides both n and ab. □

The following relation is referred to as **Bézout's identity**:

Theorem 2 (Bézout)**.** Let $\gcd(a,b) = d$. Then there are $x, y \in \mathbb{Z}$ such that

$$d = xa + yb.$$

Observe that we are not saying anything about how to go about finding these x, y. This is done by using the **extended Euclidean algorithm**.

To compute $\gcd(a,b)$, x and y one uses the following iterative procedure, called the **extended Euclidean algorithm**.

Suppose, $a \geq b$. Put

$$\begin{pmatrix} r_0 \\ s_0 \\ t_0 \end{pmatrix} = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} r_1 \\ s_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$$

Then, successive use of the division algorithm, the extended Euclidean algorithm can be written on matrix form as the recursion

$$\begin{pmatrix} r_{i+1} \\ s_{i+1} \\ t_{i+1} \end{pmatrix} = \begin{pmatrix} r_{i-1} \\ s_{i-1} \\ t_{i-1} \end{pmatrix} - q_i \begin{pmatrix} r_i \\ s_i \\ t_i \end{pmatrix}.$$

The first relation $r_{i+1} = r_{i-1} - q_i r_i$ defines the quotient q_i.

Since $0 \leq r_n < r_{n-1}$ in every step we see that, after a finite number of steps, we must end up with a zero residue (why?). The last non-zero residue, r_n, is then the $\gcd(a, b)$ since r_n divides every step up the recursion. In addition, $x = s_n$ og $y = t_n$:

$$\begin{pmatrix} \gcd(a,b) \\ x \\ y \end{pmatrix} = \begin{pmatrix} r_n \\ s_n \\ t_n \end{pmatrix}$$

The reason why the algorithm works is a bit complicated to explain so I won't do that.

Bézout's identity can actually be extended to an equivalence when $d = 1$:

Theorem 3. Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there are $x, y \in \mathbb{Z}$ such that $xa + yb = 1$.

Proof. $\Rightarrow$) follows from Bézout's theorem. To show the other implication, suppose that there are $x, y \in \mathbb{Z}$ such that $xa + yb = 1$ and where $d := \gcd(a, b) > 1$. Since $d \mid a$ and $d \mid b$ we find that $d \mid (xa + yb)$. Therefore $d \mid 1$. If $d \mid 1$ then there must be an $n \in \mathbb{Z}$ such that $1 = nd$ which is impossible unless $d = \pm 1$. This implies that $d = 1$ (gcd > 0 by definition). $\square$

Corollary 4. Suppose $\gcd(a, b) = d$. Then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof. Bézout's theorem shows that there are $x, y \in \mathbb{Z}$ such that $xa + yb = d$. Since $d \mid a$ and $d \mid b$, $xa + yb = d$ implies that $x(a/d) + y(b/d) = 1$. The result now follows directly from theorem 3. $\square$

Corollary 5. Let $\gcd(a, b) = 1$. Then

$$a \mid c, \ \ b \mid c \implies (ab) \mid c.$$

Proof. Since $\gcd(a, b) = 1$ we (once again) have that $xa + yb = 1$ for some $x, y \in \mathbb{Z}$. Multiply this equation by c to get $cxa + cyb = c$. By $a \mid c$ and $b \mid c$ we find that there are s, t such that $c = sa$ and $c = tb$. Inserting this into $cxa + cyb = c$ we find

$$xsab + ytab = c \iff ab(xs + yt) = c \iff (ab) \mid c,$$

which is the desired conclusion. □

Theorem 6. Let $\gcd(a, b) = 1$. Then

$$a \mid (bc) \quad \implies \quad a \mid c.$$

Proof. The overall idea here is the same as in the above proof. Since $\gcd(a, b) = 1$ we have

$$xa + by = 1 \implies xac + ybc = c.$$

By the hypothesis $a \mid (bc)$, we have $bc = sa$, for some s. Multiplying by c gives $xac + ybc = c$ and we get the equivalence

$$xac + ysa = c \iff a(xc + ys) = c \iff a \mid c,$$

since $bc = sa$. □

It is important that $\gcd(a, b) = 1$. For instance, $12 \mid 8 \cdot 9$, but $12 \nmid 8$, $12 \nmid 9$.

Theorem 7. Let $p \in \operatorname{Spec}(\mathbb{Z})$ and $\gcd(a, b) = 1$. Then,

$$p \mid (ab) \quad \implies \quad p \mid a \text{ or } p \mid b.$$

Proof. Since $\gcd(a, b) = 1$ we once again have $xa + yb = 1$, for some x, y. Suppose that $p \nmid a$ or $p \nmid b$. This means that

$$\gcd(a, p) = \gcd(b, p) = 1$$

since p is prime. However, this gives a contradiction to the conclusion of lemma 1 since, by hypothesis, $p \mid (ab)$. □

– Congruences –

Definition 3. Let $a, b, n \in \mathbb{Z}$. We say that a **is congruent** b **modulo** n, if

$$n \mid (a - b)$$

and write this as $a \equiv b \pmod{n}$. The number n is called the **modulus** of the congruence.

The following equivalences are extremely important to observe:

$$a \equiv b \pmod{n} \iff n \mid (a-b) \iff a-b = kn \\ \iff a = kn + b.$$

Compare this with the division algorithm but be aware that b is not necessarily a residue.

Theorem 8 (Congruence rules)**.** Let $a, b, c, d \in \mathbb{Z}$. Then the following holds:

(a) The relation $\equiv$ is an **equivalence relation**, which means that

(i) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ (**symmetry**);

(ii) $a \equiv a \pmod{n}$ (**reflexivity**), and

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then

$$a \equiv c \pmod{n} \quad (\textbf{transitivity}).$$

(b) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a \pm c \equiv b \pm d \pmod{n} \quad \text{og} \quad ac \equiv bd \pmod{n}.$$

(c) If $\gcd(a, n) = 1$ then there is an r such that

$$ar \equiv 1 \pmod{n};$$

in other words, there is an **inverse** to a modulo n.

(d) If $a \equiv b \pmod{n}$, then

$$a^k \equiv b^k \pmod{n} \quad \text{for all } k \in \mathbb{Z}_{\geq 0}.$$

Proof. We will prove parts of (b), (c) and (d), leaving the rest as exercises.

E

(b) That $a \equiv b \pmod{n}$ is equivalent to $a = rn + b$ and $c \equiv d \pmod{n}$ is equivalent to $c = sn + d$. Adding/subtracting gives us

$$a \pm c = (rn + b) \pm (sn + d) = (r \pm s)n + b \pm d \\ \iff a \pm c \equiv b \pm d \pmod{n}.$$

(c) Suppose $\gcd(a, n) = 1$. From Bézout's identity we find x, y such that $xa + yn = 1$. This means that

$$xa - 1 = yn \iff xa \equiv 1 \pmod{n}.$$

(d) This proof will use **induction**. Clearly the conclusion holds if $k = 0$ and $k = 1$. Assume now that it holds for $k - 1$. We need to prove that it holds for k also[c].

[c] Since we know the conclusion is true for $k - 1 = 2$, then we would know that it is true for $k = 3$ and then it would be true for $k = 4$, e.t.c..

From (b) we have the following implication

$$a \equiv b \pmod{n} \text{ and } a^k \equiv b^k \pmod{n} \implies aa^{k-1} \equiv bb^{k-1} \pmod{n}$$

which clearly is equivalent to $a^k \equiv b^k \pmod{n}$.

The parts of the theorem promised are proved. □

E

It is important to observe that the following implication is false:

$$a^k \equiv b^k \pmod{n} \implies a \equiv b \pmod{n}.$$

Exercise 8 asks you to find a counterexample.

The following example shows one way in which theorem 8 is used.

Example 1. We know from theorem 8 (d) that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$. Therefore, say $a = 5$, $k = 364$ and $n = 3$. We have that $5 \equiv 2 \pmod{3}$ so

$$5^{364} \equiv 2^{364} \pmod{3}.$$

Now $364 = 4 \cdot 7 \cdot 13$, so, since $2^4 = 16 \equiv 1 \pmod{3}$,

$$(2^4)^{7\cdot 13} \equiv 1^{7\cdot 13} = 1 \pmod{3}$$

from which it follows that

$$5^{364} \equiv 1 \pmod{3}.$$

Lemma 2. Put $\gcd(\alpha, n) = d$. Then

$$\alpha x \equiv \alpha y \pmod{n} \iff x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right).$$

E

Proof. This follows from corollary 4. See exercise 17. □

– Congruence equations –

Let $a, b, n \in \mathbb{N}$ such that $\gcd(a, n) = 1$. Then theorem 8 (iii) assures the existence of an inverse to a modulo n. Therefore the **congruence equation**, or simply **congruence**,

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

has the solution $x = a^{-1}b$. Notice that we do not assume that $n \in \operatorname{Spec}(\mathbb{Z})$.

The fact of the matter is that we do not even have to assume that $\gcd(a, n) = 1$:

Theorem 9. Let $\gcd(a, n) = d$. Then the congruence

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

has a solution if and only if $d \mid b$.

Proof. If $ax \equiv b \pmod{n}$ we have to have $d \mid b$ since

$$ax \equiv b \pmod{n} \iff b = ns - ax.$$

Suppose now that $d \mid b$. Then $a = \alpha d$, $b = \beta d$ and $n = \nu d$. Lemma 2 implies that

$$ax \equiv b \pmod{n} \iff \alpha x \equiv \beta \pmod{\nu}.$$

Since $\gcd(\alpha, \nu) = 1$ we are assured from theorem 8 (iii) of the existence of an inverse to α modulo ν. Therefore is $x = \alpha^{-1}\beta$ a solution to $\alpha x \equiv \beta \pmod{\nu}$. The above equivalence then implies that x also is a solution to $ax \equiv b \pmod{n}$. □

E

Obviously there is nothing in the way of looking at congruence equations defined by higher degree polynomials.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. Then it is natural to wonder if

$$f(x) \equiv b \pmod{n}$$

has a solution[d]. Observe that we can assume that $b = 0$ since otherwise we can simply subtract b from both sides of the congruence.

[d] Exercise 11.

Recall that not all polynomials over $\mathbb{R}$ are solvable in $\mathbb{R}$; one needs to extend to $\mathbb{C}$ to be guaranteed solutions. Analogously, not all congruence equations have solutions; one needs to extend to something bigger (we will come to this later). The existence of solutions is dependent on both $f(x)$ and n. For fixed $f(x)$ there are infinitely many n such that $f(x) \equiv b \pmod{n}$ has a solution.

The following two examples will be of utmost importance later.

Example 2. Let $f(x) = x^2 + 1$. Then

- $f(x) \equiv 0 \pmod{5}$ has the solutions $\{2, 3\}$;
- $f(x) \equiv 0 \pmod{13}$ has the solutions $\{5, 8\}$;
- $f(x) \equiv 0 \pmod{19}$ has no solution;
- $f(x) \equiv 0 \pmod{23}$ has no solution;
- $f(x) \equiv 0 \pmod{34}$ has the solutions $\{13, 21\}$;
- $f(x) \equiv 0 \pmod{794653}$ has the solutions $\{330106, 464547\}$.

Observe the difference between whether the modulus is a prime or not.

We shall now look at the general congruence equation

$$f(x) \equiv 0 \pmod{n}$$

when $f(x) = x^2 + a$, $a \in \mathbb{Z}_{\geq 2}$.

There are two distinct cases:

(1) $a \in \mathrm{Spec}(\mathbb{Z})$, or

(2) a can be non-trivially factored.

We will handle these two cases separately.

Example 3. Put $f(x) = x^2 + 557$ (557 is a prime). Obviously, $x = 1$ is always a solution of multiplicity two modulo 2 so we assume below that $n \neq 2$.

(a) $n \in \mathrm{Spec}(\mathbb{Z}) \setminus \{2\}$. There are two possibilities

(i) the congruence has no solution;

(ii) there are exact two solutions.

For example are $\{36, 73\}$ solutions to

$$x^2 + 557 \equiv 0 \pmod{109},$$

while $x^2 + 557 \equiv 0 \pmod{43}$ has no solution.

(b) Suppose now that $n \notin \mathrm{Spec}(\mathbb{Z}) \setminus \{2\}$. In this case there are many possibilities. For instance,

– $n = 22$ has the solutions $\{9, 13\}$;

– $n = 69$ has the solutions $\{8, 31, 38, 61\}$:

– $n = 91$ has no solution;

– $n = 561$ has the solutions

$$\{2, 53, 134, 185, 376, 427, 508, 559\}.$$

The maximal number of solutions in the interval $[0, 10^5]$ is 16, which happens for the first time for $n = 12903$.

Example 4. Now, let $f(x) = x^2 + 31682$, where

$$31682 = 2 \cdot 7 \cdot 31 \cdot 73.$$

In this case $x = 1$ is not a solution modulo 2.

The first we can observe is that if $n \in \{2, 7, 31, 73\}$ the the congruence equation has the *unique* solution $x = 0$.

Otherwise we have the same possibilities as in the previous example:

(a) $n \in \mathrm{Spec}(\mathbb{Z})$. Two possibilities:

(i) no solution;

(ii) exactly two solutions.

For instance, $\{62, 129\}$ are solutions to

$$x^2 + 31682 \equiv 0 \pmod{191},$$

while $x^2 + 31682 \equiv 0 \pmod{193}$ has no solution at all.

(b) Suppose now that $n \notin \mathrm{Spec}(\mathbb{Z})$. In that case there are, as in the previous example, many possibilities:

- $n = 26$ gives the solutions $\{8, 18\}$;
- $n = 99$ gives the solutions $\{14, 41, 58, 85\}$:
- $n = 110$ has no solution;
- $n = 759$ has the solutions

$$\{14, 124, 239, 377, 382, 520, 635, 745\}.$$

Also in this case, the maximal number of solutions in the interval $[0, 10^5]$ is 16, which happens first for $n = 9867$.

Finally a third degree polynomial. For simplicity we only consider congruences $f(x) \equiv 0 \pmod{p}$ where $p \in \mathrm{Spec}(\mathbb{Z})$. Obviously composite moduli is also possible.

Example 5. Let $f(x) = x^3 + x + 103$. Then the congruence

- $f(x) \equiv 0 \pmod{59}$ has the solutions $\{25, 45, 48\}$;
- $f(x) \equiv 0 \pmod{191}$ has the solution $\{36\}$;
- $f(x) \equiv 0 \pmod{251}$ has no solution;
- $f(x) \equiv 0 \pmod{271}$ has the solutions $\{38, 252\}$;
- $f(x) \equiv 0 \pmod{39869}$ has the solutions $\{2262, 9213, 28394\}$.

Polynomials of degree three will be very important when we discuss elliptic curves.

To solve the above congruences, I wrote a (definitively not optimised!) Python program. I leave to you, as an exercise (exercise 21), to write such a program.

E

– The Chinese Remainder Theorem –

We now have the following fundamental theorem:

Theorem 10. Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}_{\geq 1}$ be relatively prime integers (i.e., $\gcd(n_i, n_j) = 1$ for all $i \neq j$). Then the system of congruences

$$\begin{cases} x \equiv \alpha_1 \pmod{n_1} \\ x \equiv \alpha_2 \pmod{n_2} \\ \quad\vdots \\ x \equiv \alpha_k \pmod{n_k}, \end{cases}$$

for $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}$, has a simultaneous solution that is unique modulo $n_1 n_2 \cdots n_k$.

The proof is **effective** in the sense that it supplies a method for computing the solution, so be sure to read it carefully.

Proof. Put $N := n_1 n_2 \cdots n_k$ and form the numbers

$$M_i := N/n_i = n_1 \cdot n_2 \cdots n_{i-1} \cdot n_{i+1} \cdots n_k.$$

Since $\gcd(n_i, n_j) = 1$ for $i \neq j$, we find that $\gcd(M_i, n_i) = 1$.

Therefore, the congruence $M_i x \equiv 1 \pmod{n_i}$ has a unique solution, say β_i. Put

$$\boldsymbol{\beta} := \alpha_1 M_1 \beta_1 + \alpha_2 M_2 \beta_2 + \cdots + \alpha_k M_k \beta_k.$$

Since $n_j \mid M_i$ for $i \neq j$ we have that $M_i \equiv 0 \pmod{n_i}$. Hence

$$\boldsymbol{\beta} \equiv \alpha_i M_i \beta_i \pmod{n_i}.$$

Since $M_i \beta_i \equiv 1 \pmod{n_i}$ we find that

$$\boldsymbol{\beta} \equiv \alpha_i \pmod{n_i}$$

for all $1 \leq i \leq k$. Therefore, $\boldsymbol{\beta}$ is a solution to the system.

It remains to prove that $\boldsymbol{\beta}$ is unique. Suppose that $\boldsymbol{\beta}'$ is another solution,

$$\boldsymbol{\beta}' \equiv \alpha_i \pmod{n_i} \iff \boldsymbol{\beta}' \equiv \boldsymbol{\beta} \pmod{n_i}, \quad 1 \leq i \leq k,$$

the equivalence following from the fact that both $\boldsymbol{\beta}$ and $\boldsymbol{\beta}'$ are congruent α_i modulo n_i. By definition,

$$\boldsymbol{\beta}' \equiv \boldsymbol{\beta} \pmod{n_i} \iff n_i \mid (\boldsymbol{\beta} - \boldsymbol{\beta}'), \quad 1 \leq i \leq k.$$

Now, since $\gcd(n_i, n_j) = 1$, corollary 5 implies that

$$(n_1 n_2 \cdots n_k) \mid (\boldsymbol{\beta} - \boldsymbol{\beta}'),$$

which proves the desired conclusion. □

Observe the following important corollary.

Corollary 11. Let $n = n_1 \cdot n_2 \cdots n_k$, with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then any solution to the system

$$\begin{cases} x \equiv \alpha \pmod{n_1} \\ x \equiv \alpha \pmod{n_2} \\ \quad \vdots \\ x \equiv \alpha \pmod{n_k}, \end{cases}$$

is also a solution to the congruence

$$x \equiv \alpha \pmod{n}.$$

Proof. This follows immediately from corollary 5 and theorem 10. □

– *Residue classes* –

When $a \geq n$ the division algorithm gives that $a = qn + r$ where $0 \leq r < n$. This means that the residues when dividing a by n are elements in the set

$$\mathbb{Z}/n := \{0, 1, 2, \ldots, n-1\},$$

and this set includes *all* possible residues modulo n.

Theorem 12. If $a \equiv b \pmod{n}$ then

$$a = q_a n + r_a, \quad \text{og} \quad b = q_b n + r_b \quad \Longrightarrow \quad r_a = r_b,$$

where q_a, q_b are the quotients and r_a, r_b the residues.

Expressed in words: if $a \equiv b \pmod{n}$, then a and b have the same residue modulo n.

Proof. The division algorithm gives that $r_a, r_b < n$ and therefore is $r_a - r_b < n$. From $a = q_a n + r_a$ and $b = q_b n + r_b$ we get by subtraction,

$$a - b = (q_a - q_b)n + (r_a - r_b).$$

Since $a \equiv b \pmod{n}$, the right-hand side must be a multiple of n. On the other hand, since $r_a - r_b < n$ we must have $r_a = r_b$ (otherwise, the right-hand side can not be a multiple of n). □

Let $a \in \mathbb{Z}$. Then the division algorithm gives that $a = q_a n + r_a$. We say that r_a is the **reduction of** a **modulo** n. This is often denoted by $\bar{a}$. The set of all $x \in \mathbb{Z}$ having the same residue as a is denoted $[a]$, and is called the **residue class** of a. Observe that this is a set!

Since the residue is unique, dependent only on a and n, the reduction is also unique. On the other hand, given a residue r modulo n, there are many $x \in \mathbb{Z}$ such that $\bar{x} = r$. In fact, the theorem above says that all $x, y \in \mathbb{Z}$ with $x \equiv y \pmod{n}$ all have the same residue. Expressed differently,

$$a \equiv b \pmod{n} \iff \bar{a} = \bar{b} \in \mathbb{Z}/n = \{0, 1, 2, \ldots, n-1\}.$$

More correctly, the elements in $\mathbb{Z}/n$ are *sets*, where $r \in \mathbb{Z}/n$ **represents** all those a that has r as residue modulo n. Therefore, in the name of precision, one should write

$$\mathbb{Z}/n = \{[0], [1], [2], \ldots, [n-1]\}$$

and remember that the elements in $\mathbb{Z}/n$ are sets and not numbers.

Hence, we can express the discussion above as

$$\begin{aligned} [a] &= \left\{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \right\} \\ &= \left\{ b \in \mathbb{Z} \mid \bar{a} = \bar{b} \text{ modulo } n \right\} \\ &= \left\{ b \in \mathbb{Z} \mid a \text{ og } b \text{ have the same residue modulo } n \right\} \in \mathbb{Z}/n \end{aligned}$$

and the set $[a]$ can be *represented* by this residue.

Observe that $\overline{0}$ is the set of all $x \in \mathbb{Z}$ that are divisible by n.

The above discussion also justifies the notation $\mathbb{Z}/n$: "division by n". In correct mathematical notation this should be written as $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ but I kind of like the notation $\mathbb{Z}/n$ since it highlights that we are actually dealing with division by n.

Definition 4. Let $\overline{a}, \overline{b} \in \mathbb{Z}/n$ be two residue classes. The following operations define addition/subtraction and multiplication of residue classes:

(a) $[a] \pm [b] \stackrel{\text{def.}}{=} [a \pm b]$;

(b) $[a] \cdot [b] \stackrel{\text{def.}}{=} [a \cdot b]$.

Here one needs to be careful. Remember that $[a]$ is the *set* of all numbers having the same residue as a. We need to show that the above definitions are *well-defined*, i.e., independent on which representatives we choose from the sets. The choices are made in the right-hand side of the definitions.

Theorem 13. The arithmetic operations defined in definition 4 are well-defined.

Proof. Clearly $\bar{a} \in [a], \bar{b} \in [b]$. Now, take arbitrary $\bar{\alpha} \in [a]$ and $\bar{\beta} \in [b]$. This is equivalent to $a \equiv \alpha \pmod{n}$ and $b \equiv \beta \pmod{n}$. We need to show that

$$\bar{a} + \bar{b} = \bar{\alpha} + \bar{\beta},$$

where we, according to the definition, have

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta}.$$

In other words, we need to show that

$$\overline{a+b} = \overline{\alpha + \beta}$$

which is equivalent to showing (remember: equal residues) that

$$(a+b) \equiv (\alpha + \beta) \pmod{n}.$$

Now we have $a \equiv \alpha \pmod{n}$ and $b \equiv \beta \pmod{n}$. Adding these two congruences gives, by theorem 8 (ii),

$$(a+b) \equiv (\alpha + \beta) \pmod{n},$$

exactly what we needed to show. $\square$

The above defines a **ring structure** on $\mathbb{Z}/n$, and reduction is a **ring homomorphism**.

If $n = p$ is prime then one puts

$$\mathbb{F}_p := \mathbb{Z}/p,$$

for reasons to be explained later. It is important to note that, one does *not* write

$$\mathbb{F}_{p^k} := \mathbb{Z}/p^k,$$

for $k > 1$.

– Eulers teorem –

Definition 5. The function $\varphi : \mathbb{N} \to \mathbb{N}$ defined by

$$\varphi(n) = \#\Big\{1 \leq a \leq n-1 \;\Big|\; \gcd(a,n) = 1\Big\},$$

is called the **Euler totient function**.

Theorem 14. The totient function is **weakly multiplicative**: suppose $n, m \in \mathbb{Z}$ and $\gcd(n,m) = 1$, then

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m), \quad n, m \in \mathbb{Z}.$$

Proof. The proof is quite tricky and is omitted. □

Clearly,

$$\varphi(p) = p - 1 \quad \text{for } p \in \operatorname{Spec}(\mathbb{Z}).$$

More generally,

Theorem 15. For $p \in \operatorname{Spec}(\mathbb{Z})$,

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right), \quad k \geq 0.$$

Proof. Since $\gcd(p^k, n) = 1$ if and only if $p \nmid n$, there are p^{k-1} numbers between 1 and p^k that are divisible by p:

$$p, 2p, 3p, \ldots, p^{k-1}p.$$

Hence the set

$$\Big\{1 \leq a \leq p^k \;\Big|\; \gcd(p^k, a) = 1\Big\},$$

$a \in \mathbb{Z}$, have $p^k - p^{k-1}$ elements. □

We won't give proofs of the following two theorems:

Theorem 16. Suppose $n \in \mathbb{Z}$ has prime factorisation

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}, \quad p_i \in \operatorname{Spec}(\mathbb{Z}).$$

Then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right).$$

Proof. This is an induction argument. □

Theorem 17. For $n \geq 3$, $\varphi(n)$ is an even number.

Lemma 3. Let $a, n > 1$, $\gcd(a,n) = 1$ and

$$A = \left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\} = \left\{1 \leq s < n \;\middle|\; \gcd(s,n) = 1\right\}.$$

Then the set

$$B = \left\{aa_1, aa_2, \ldots, aa_{\varphi(n)}\right\}$$

is congruent to A, in the sense that every element in B is congruent with **exactly** one element in A.

Proof. We cannot have that $aa_i \equiv aa_j (\text{mod } n)$ when $i \neq j$. Indeed, suppose that $i \neq j$ and that $aa_i \equiv aa_j (\text{mod } n)$. Since $\gcd(a,n) = 1$ we can eliminate a from the congruence to get $a_i \equiv a_j (\text{mod } n)$. This is a contradiction to the definition of A (all elements are distinct modulo n; indeed, they are all distinct and less than n, therefore distinct modulo n). Hence $aa_i \not\equiv aa_j (\text{mod } n)$.

Furthermore, from Lemma 1, we have

$$\gcd(a,n) = \gcd(a_i, n) = 1 \quad \Longrightarrow \quad \gcd(aa_i, n) = 1.$$

Thus we know that the elements in B are distinct and relatively prime to n.

For every aa_i there is a unique $1 \leq b_i < n$ such that

$$aa_i \equiv b_i (\text{mod } n).$$

From this follows, since $\gcd(aa_i, n) = 1$, that

$$\gcd(b_i, n) = 1.$$

Indeed, the congruence $aa_i \equiv b_i (\text{mod } n)$ is equivalent to the statement that $aa_i = b_i + kn$. If $\gcd(b_i, n) = d > 1$, d would have to divide aa_i. However, $\gcd(aa_i, n) = 1$ so this is impossible. We can therefore conclude that b_i have to be one, and only one, of the elements of A. □

Theorem 18 (Euler)**.** Let $n > 1$, $a \in \mathbb{Z}$ and $\gcd(a,n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 (\text{mod } n).$$

Proof. From lemma 3 we see that

$$\left\{aa_1, aa_2, \ldots, aa_{\varphi(n)}\right\} \equiv \left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\} \pmod{n}.$$

In other words,

$$aa_i \equiv b_i (\text{mod } n), \quad b_i \in \left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\}, \quad 1 \leq i \leq \varphi(n).$$

Multiplying all these congruences gives

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv b_1 b_2 \cdots b_{\varphi(n)} \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}.$$

The left-hand side is

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) = a^{\varphi(n)}a_1a_2\cdots a_{\varphi(n)},$$

so

$$a^{\varphi(n)}a_1a_2\cdots a_{\varphi(n)} \equiv a_1a_2\cdots a_{\varphi(n)} \pmod{n}.$$

Since all a_i are relatively prime to n, we conclude, by using lemma 2 several times, that $a_1a_2\cdots a_{\varphi(n)}$ also is. Therefore, we can eliminate $a_1a_2\cdots a_{\varphi(n)}$ from the congruence to get

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

which was what had to be proven. □

Corollary 19. The set

$$a \in (\mathbb{Z}/n)^{\times} := \left\{a \in \mathbb{Z}/n \;\middle|\; \gcd(a,n) = 1\right\}$$

is the set of all $\varphi(n)$**-roots of unity** modulo n. In other words, for $x \in (\mathbb{Z}/n)^{\times}$, we have that $x^{\varphi(n)} = 1$ in $\mathbb{Z}/n$.

Theorem 20 (Fermat's "little" theorem)**.** Let $a \in \mathbb{Z}$, $p \in \operatorname{Spec}(\mathbb{Z})$ and $\gcd(a,p) = 1$. Then

$$a^{p-1} \equiv 1(\text{mod } p).$$

In particular,

$$a^{p} \equiv a(\text{mod } p).$$

Proof. This follows directly from Euler's theorem since $\varphi(p) = p-1$ for $p \in \operatorname{Spec}(\mathbb{Z})$. □

Example 6. We shall prove that

$$a^{37} \equiv a \pmod{1729},$$

for all $a \in \mathbb{Z}$.

First we observe that $1729 = 7 \cdot 13 \cdot 19$ and so

$$\varphi(1729) = \varphi(7)\varphi(13)\varphi(19) = 6 \cdot 12 \cdot 18 = 36^2.$$

We then have

$$a^{37} = a^{36+1} = a^{36}a \equiv 1 \cdot a \pmod{1729},$$

since

$$a^{\varphi(1729)} = \left(a^{36}\right)^{36} \equiv 1 \pmod{1729}.$$

– Exercises –

Exercise 1. Finish the exercises in the text.

Exercise 2. Write a Python program that has the following functions:

(i) a function that finds the quotient and residue in the division algorithm, *without* using built-in functions in Python;

(ii) a function that implements the extended Euclidean algorithm in Python. (Here you *may* use the built-in quotient and remainder Python functions.)

Exercise 3. Show that

(i) $2 \mid (n^2 - n)$;

(ii) $6 \mid (n^3 - n)$, and

(iii) $30 \mid (n^5 - n)$

Exercise 4. Show that $4 \nmid (n^2 + 2)$.

Exercise 5. Show that

(a) $n^2 \equiv 1 \pmod{8}$ when n is odd.

(b) $n^3 \equiv 0, 1, \text{ or } 6 \pmod{7}$, for $n \in \mathbb{Z}$.

(c) $n^4 \equiv 0, \text{ or } 1 \pmod{5}$, for $n \in \mathbb{Z}$.

(d) If n is not divisible by 2 or 3 then $n^2 \equiv 1 \pmod{24}$, for $n \in \mathbb{Z}$.

Exercise 6. Use congruences to calculate the remainders when

(a) 2^{50} is divided by 7, and

(b) when 41^{65} is divided by 7.

Exercise 7. Use congruences to prove the following:

(a) For each $n \geq 1$

$$7 \mid (5^{2n} + 3 \cdot 2^{5n-2}).$$

(b) For each $n \geq 1$

$$27 \mid (2^{5n+1} + 5^{n+2}).$$

Exercise 8. Find a counterexample to the implication

$$a^k \equiv b^k \pmod{n} \quad \Longrightarrow \quad a \equiv b \pmod{n}.$$

Exercise 9. Let $p \in \mathrm{Spec}(\mathbb{Z})$. Show

$$a^2 \equiv b^2 \pmod{p} \quad \Longrightarrow \quad p \mid (a+b) \text{ or } p \mid (a-b).$$

Why is this not in opposition to exercise 8?

Exercise 10. Suppose $d > 0$ and that $d \mid n$. Show the implication

$$a \equiv b \pmod{n} \implies a \equiv b \pmod{d}.$$

Exercise 11. Let $P(x) \in \mathbb{Z}[x]$. If $a \equiv b \pmod{n}$, use exercise 8 to show that

$$P(a) \equiv P(b) \pmod{n}.$$

Exercise 12. Solve the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Don't forget to check your solution.

Exercise 13. Solve the following system of congruences:

$$\begin{cases} x \equiv \;\, 5 \pmod{11} \\ x \equiv 14 \pmod{29} \\ x \equiv 15 \pmod{31} \end{cases}$$

Don't forget to check your solution.

Exercise 14. Solve the following system of congruences:

$$\begin{cases} 2x \equiv \;\, 1 \pmod{5} \\ 3x \equiv \;\, 9 \pmod{6} \\ 4x \equiv \;\, 1 \pmod{7} \\ 5x \equiv 9 \pmod{11} \end{cases}$$

You will have to invoke lemma 2 to solve this. Don't forget to check your solution.

Exercise 15. Use corollary 11 to solve the congruence

$$13x \equiv 3 \pmod{77}.$$

Don't forget to check your solution.

Exercise 16. Use corollary 11 to solve the congruence

$$23x \equiv 95 \pmod{276}.$$

Don't forget to check your solution.

Exercise 17. Prove lemma 2.

Exercise 18. Find the addition and multiplication tables for

(a) $\mathbb{Z}/5$;

(b) $\mathbb{Z}/6$;

(c) $\mathbb{Z}/7$, and

(d) $\mathbb{Z}/8$.

Exercise 19. If A and B are two sets $A \times B$ denotes the set

$$A \times B := \Big\{(a, b) \mid a \in A,\ b \in B\Big\}.$$

In other words, the set of all pairs of element from A and B Observe that, generally $A \times B \neq B \times A$. Also, (a, b) is not the same as (b, a) unless $a = b$.

Now, let $A := \mathbb{Z}/n$ and $B := \mathbb{Z}/m$. Define addition and multiplication component-wise :

$$(a, b) + (c, d) := (a + c, b + d), \quad (a, b) \cdot (c, d) := (ac, bd).$$

Compute the addition and multiplication tables for

(a) $\mathbb{Z}/2 \times \mathbb{Z}/2$ (this is the so-called **Klein Viergruppe**);

(b) $\mathbb{Z}/2 \times \mathbb{Z}/3$, and

(c) $\mathbb{Z}/3 \times \mathbb{Z}/3$.

Exercise 20. Construct a bijective function ϕ between $\mathbb{Z}/2 \times \mathbb{Z}/3$ and $\mathbb{Z}/6$ such that the addition and multiplication tables are compatible, or, expressed in fancy language, such that ϕ is a **ring homomorphism**.

In other words, if ϕ is such a function

$$\phi : \mathbb{Z}/6 \to \mathbb{Z}/2 \times \mathbb{Z}/3,$$

and if $a, b \in \mathbb{Z}/6$, then

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

Observe that that the tables are different on the left-hand side and right-hand side; in the left-hand side it is the tables for $\mathbb{Z}/2 \times \mathbb{Z}/3$, and in the right-hand side the tables for $\mathbb{Z}/6$.

Remember that a **bijective** function $f : A \to B$ is a function that is

(i) **injective**: $f(x) = f(y) \implies x = y$, and

(ii) **surjective**: for each $y \in B$, there is an $x \in A$ such that $y = f(x)$.

Exercise 21. Write a Python program that solves

$$f(x) \equiv 0 \pmod{n}$$

for arbitrary $f \in \mathbb{Z}[x]$ and arbitrary modulus n.

Exercise 22. Show that every element in $\mathbb{F}_p$ has an inverse. In other words, show that for every $a \in \mathbb{F}_p$, there is a $b \in \mathbb{F}_p$ such that

$$ab = ba = 1 \in \mathbb{F}_p.$$

Hint: Use congruences.

On the other hand, show, for instance by finding a counterexample, that the same is *not* true for $\mathbb{Z}/p^2$. (Recall that $\mathbb{F}_{p^2} \neq \mathbb{Z}/p^2$.)

In fact, show that there are elements $a \in \mathbb{Z}_{p^2}$ such that $ab = 0$ for some b. One says that a is a **zero-divisor**.

Exercise 23. Compute the following.

(a) $\varphi(2197)$ (*Hint:* $13 \mid 2197$);

(b) $\varphi(123)$;

(c) $\varphi(61828)$.

Exercise 24. Show that

$$d \mid n \Longrightarrow \varphi(d) \mid \varphi(n).$$

Exercise 25. Write a Python program that computes the value $\varphi(n)$ for all $n \in \mathbb{Z}_{\geq 0}$. Be sure to test it with numbers that you can compute by hand.

Exercise 26. Use Euler's theorem to prove that

(a) $a^{13} \equiv a \pmod{2730}$, for all $a \in \mathbb{Z}$.

(b) $a^{33} \equiv a \pmod{4080}$, for a an odd integer.

(c) Use Euler's theorem and (a) to prove that

$$51 \mid (10^{32n+9} - 7), \quad \text{for all } n \geq 1.$$

Exercise 27. Let $\gcd(a, n) = \gcd(a-1, n) = 1$. Prove that

$$\sum_{i=0}^{\varphi(n)-1} a^i \equiv 0 \pmod{n}.$$

Recall that $\varphi(n)$ is an even number and observe that, for m even,

$$x^m - 1 = (x-1)(1 + x + x^2 + \cdots + x^{m-1}).$$

Exercise 28. Let m be an arbitrary multiple of 9.

(a) Use Fermat's theorem to prove that $3 \mid (10^9 - 7)$.

(b) Prove that $3 \mid (10^m - 7)$.

(c) Use Euler's theorem and (a) to prove that

$$51 \mid (10^{32n+9} - 7), \quad \text{for all } n \geq 1.$$

Exercise 29. Let $p \in \operatorname{Spec}(\mathbb{Z})$.

(a) Show that every $a \in \mathbb{F}_p$ is a $(p-1)^{\text{th}}$-root of unity.

(b) Which elements in $\mathbb{Z}/p^2$ are n^{th}-roots of unity, $n \geq 2$?

(c) In $\mathbb{Z}/p^k$?

Exercise 30. Show that

$$91^{19200} \equiv 1 \pmod{35301}.$$

Hint: Use Euler's theorem.

Exercise 31. Compute the remainder when 2^{100000} is divided by 77. *Hint:* Use Euler's theorem. You might also need to use the Chinese Remainder Theorem[e].

[e] Answer: 23