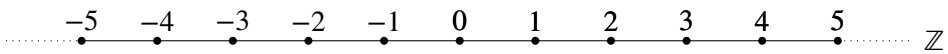
University of Toronto – MAT246H1-S – LEC0201/9201 – Winter 2021

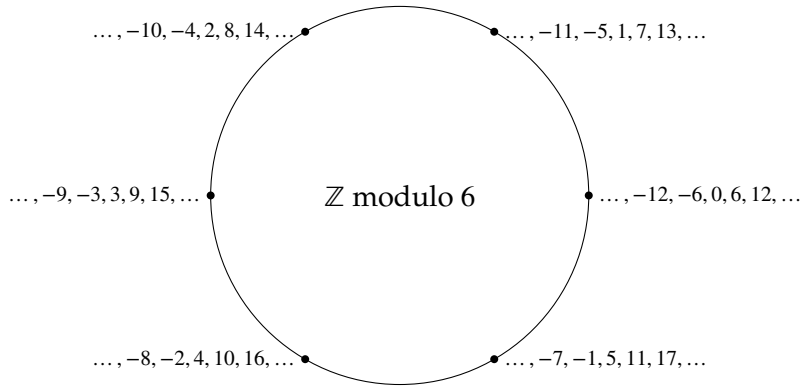
*Concepts in Abstract Mathematics*

# 4 - Modular arithmetic

Jean-Baptiste Campesato

Modular arithmetic was introduced by Gauss during the beginning of the 19th century. Working modulo a natural number $n > 0$ means that, given an integer $a$, we identify it with its remainder $r$ for the Euclidean division by $n$. Basically, it means that we *force* $a$ to be equal to $r$ (of course, not as integers, but equal *modulo* $n$). Informally, we wind $\mathbb{Z}$ on itself as represented below.




This extra layer of abstraction allowed Gauss, and subsequently other mathematicians, to obtain simpler proofs of already known results concerning integers but also to prove new theorems, simply by introducing this new efficient notation which has many good properties.

## Contents

# 1 Congruences

**Definition 1.** We say that a binary relation $\mathcal{R}$ on a set $E$ is an *equivalence relation* if
(i) $\forall x \in E,\ x\mathcal{R}x$ (*reflexivity*)
(ii) $\forall x, y \in E,\ x\mathcal{R}y \implies y\mathcal{R}x$ (*symmetry*)
(iii) $\forall x, y, z \in E,\ \big(x\mathcal{R}y \text{ and } y\mathcal{R}z\big) \implies x\mathcal{R}z$ (*transitivity*)

**Definition 2.** Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$. We say that $a$ and $b$ are *congruent modulo n* if $n|a-b$, which we denote by $a \equiv b \pmod{n}$.

**Proposition 3.** *Congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

*Proof.*
- *Reflexivity.* Let $a \in \mathbb{Z}$ then $n|0 = a - a$. Hence $a \equiv a \pmod{n}$.
- *Symmetry.* Let $a, b \in \mathbb{Z}$ be such that $a \equiv b \pmod{n}$. Then $n|b - a = -(a-b)$ hence $b \equiv a \pmod{n}$.
- *Transitivity.* Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n|a-b$ and $n|b-c$. Hence $n|a - c = (a-b) + (b-c)$. Thus $a \equiv c \pmod{n}$.

■

**Proposition 4.** *Let $n \in \mathbb{N} \setminus \{0\}$ and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have same remainder for the Euclidean division by n.*

*Proof.*
$\Rightarrow$. Assume that $a \equiv b \pmod{n}$, then $b - a = kn$ for some $k \in \mathbb{Z}$. By Euclidean division, $a = nq + r$ for $q, r \in \mathbb{Z}$ satisfying $0 \leq r < n$. Hence $b = a + kn = nq + r + kn = (q+k)n + r$.
$\Leftarrow$. Assume that $a$ and $b$ have same remainder for the Euclidean division by $n$, then $a = nq_1 + r$ and $b = nq_2 + r$ where $q_1, q_2, r \in \mathbb{Z}$ with $0 \leq r < n$.
Hence $a - b = nq_1 + r - (nq_2 + r) = n(q_1 - q_2)$. Thus $n|a-b$, i.e. $a \equiv b \pmod{n}$. ■

**Proposition 5.** *Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$. Then a is congruent modulo n to exactly one element of $\{0, 1, \dots, n-1\}$.*

*Proof.* By Euclidean division $a = nq + r$ where $0 \leq r < n$ so that $a \equiv r \pmod{n}$.
Conversely, if $a \equiv r' \pmod{n}$ where $r' \in \{0, 1, \dots, n-1\}$, then $a - r' = nq$ for some $q \in \mathbb{Z}$. So $a = nq + r'$.
By uniqueness of the Euclidean division, $r = r'$. ■

**Proposition 6.** *Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$ then*
- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

*Proof.* Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$. Hence $a - b = nk$ and $c - d = nl$ for some $k, l \in \mathbb{Z}$. Then
- $(a+c) - (b+d) = (a-b) + (c-d) = nk + nl = n(k+l)$, hence $a + c \equiv b + d \pmod{n}$.
- $ac - bd = (b+nk)(d+nl) - bd = bnl + dnk + n^2kl = n(bl + dk + nkl)$, hence $ac \equiv bd \pmod{n}$.

■

**Example 7.** $1729 \times 16 \equiv 12 \times (-1) \pmod{17} \equiv -12 \pmod{17} \equiv 5 \pmod{17}$

**Corollary 8.** *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N} \setminus \{0\}$. Then $\forall k \in \mathbb{N}$, $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$.*

*Proof.* We prove the statement by induction on $k$.
*Base case at $k = 0$:* $a^0 = b^0 = 1$ hence $a^0 \equiv b^0 \pmod{n}$.
*Induction step:* assume that $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$ for some $k \in \mathbb{N}$.
If $a \equiv b \pmod{n}$ then by induction hypothesis we also have $a^k \equiv b^k \pmod{n}$. Hence, combining both previous congruences, we get that $a^k a \equiv b^k b \pmod{n}$, i.e. $a^{k+1} \equiv b^{k+1} \pmod{n}$. Which proves the induction step. ■

**Remark 9.** Therefore addition, substraction (which is a special case of addition in $\mathbb{Z}$), multiplication and exponentiation are compatible with congruences.
Beware: division is **not** compatible with congruences: $10 \equiv 4 \pmod{6}$ but $5 \not\equiv 2 \pmod{6}$.

**Proposition 10.** *Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}\setminus\{0\}$. Then $a$ has a multiplicative inverse modulo $n$ if and only if* $\gcd(a,n) = 1$. *Otherwise stated,*

$$\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \gcd(a,n) = 1$$

*Proof.* $\exists b \in \mathbb{Z},\ ab \equiv 1 \pmod{n} \Leftrightarrow \exists b, c \in \mathbb{Z},\ ab + nc = 1 \Leftrightarrow \gcd(a,n) = 1$ ■

**Remark 11.** Then the multiplicative inverse is unique modulo $n$. Indeed if $ab \equiv 1 \pmod{n} \equiv ab' \pmod{n}$ then $n|(b-b')a$. Since $\gcd(a,n) = 1$, using Gauss' lemma, we get that $n|b-b'$, i.e. $b \equiv b' \pmod{n}$.

**Remark 12.** There is no cancellation law for congruences. For instance, $50 \equiv 20 \pmod{15}$ but $5 \not\equiv 2 \pmod{15}$. Nonetheless, we have the following proposition.

**Proposition 13.** *Let $n \in \mathbb{N}\setminus\{0\}$ and $a, x, y \in \mathbb{Z}$ satisfying $ax \equiv ay \pmod{n}$ and* $\gcd(a,n) = 1$. *Then $x \equiv y \pmod{n}$.*

*Proof.* Since $\gcd(a,n) = 1$, $a$ admits an inverse modulo $n$, i.e. there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$. Then $ax \equiv ay \pmod{n} \implies bax \equiv bay \pmod{n} \implies x \equiv y \pmod{n}$. ■

## 2 Applications: divisibility criteria

In our everyday life, we usually use a base ten positional notation. It allows use to write all natural numbers using only 10 digits although $\mathbb{N}$ is infinite. The idea is that the position of a digit changes its value.

Indeed, using the well-ordering principle and Euclidean division, it is possible to prove that any $n \in \mathbb{N}$ can be uniquely written as $n = \sum_{k=0}^{r} a_k 10^k$ where $a_k \in \{0, 1, \dots, 9\}$ and $a_r \neq 0$ (*see the appendix for a proof*).

We usually write $\overline{a_r a_{r-1} \dots a_0}^{10}$ for $\sum_{k=0}^{r} a_k 10^k$ but we may omit the line over the digits when there is no possible confusion. For instance, $590743 = 5\times 10^5 + 9\times 10^4 + 0\times 10^3 + 7\times 10^2 + 4\times 10^1 + 3\times 10^0$.

Note that we also use other bases: base 2 and base 16 are quite common nowadays in computer sciences. And other bases were also commonly used by human beings in various places in the past: we still have the influence of a base 60 positional system when describing time (1 hour is 60 minutes), and the influence of a base 20 positional system in several languages (in French 96 is litteraly pronounced $4\times 20 + 16$).

In this section, we are going to use modular arithmetic in order to prove some divisibility criteria using our base ten positional notation.

**Proposition 14.** $3|\overline{a_r a_{r-1} \dots a_0}^{10}$ *if and only if* $3|\sum_{k=0}^{r} a_k$.

*Proof.* Note that $10 \equiv 1 \pmod{3}$, hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{r} a_k 1^k \pmod{3} \equiv \sum_{k=0}^{r} a_k \pmod{3}$$

Thus,

$$\begin{aligned} 3|\overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{3} \\ &\Leftrightarrow \sum_{k=0}^{r} a_k \equiv 0 \pmod{3} \\ &\Leftrightarrow 3|\sum_{k=0}^{r} a_k \end{aligned}$$

■

**Examples 15.**

- 91524 is divisible by 3 since $9+1+5+2+4 = 21 = 7\times 3$ is.
- Let's study whether 8546921469 is a multiple of 3 or not:

$$\begin{aligned} 3|8546921469 &\Leftrightarrow 3|8+5+4+6+9+2+1+4+6+9 = 54 \\ &\Leftrightarrow 3|5+4=9 \end{aligned}$$

But $9 = 3\times 3$, hence 3|8546921469.

**Proposition 16.** $9|\overline{a_r a_{r-1}\dots a_0}^{10}$ *if and only if* $9|\sum_{k=0}^{r} a_k$.

*Proof.* That's a similar proof since $10 \equiv 1 \pmod 9$. ∎

**Proposition 17.** $4|\overline{a_r a_{r-1}\dots a_0}^{10}$ *if and only if* $4|\overline{a_1 a_0}^{10}$.

*Proof.* Note that $10^2 = 4\times 25$ hence $10^k \equiv 0 \pmod 4$ for $k \geq 2$. Hence

$$\begin{aligned} 4|\overline{a_r a_{r-1}\dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1}\dots a_0}^{10} \equiv 0 \pmod 4 \\ &\Leftrightarrow \sum_{k=0}^{r} a_k 10^k \equiv 0 \pmod 4 \\ &\Leftrightarrow a_1\times 10 + a_0 \equiv 0 \pmod 4 \\ &\Leftrightarrow \overline{a_1 a_0}^{10} \equiv 0 \pmod 4 \\ &\Leftrightarrow 4|\overline{a_1 a_0}^{10} \end{aligned}$$

∎

**Examples 18.**

- $4 \nmid 856987454251100125$ since $4 \nmid 25$.
- $4|98854558715580$ since $4|80 = 4\times 20$.

## 3 Fermat's little theorem

**Lemma 19.** *Let $p$ be a prime number. Then* $\forall n \in \{1,\dots,p-1\}$, $\binom{p}{n} \equiv 0 \pmod p$.

*Proof.* Let $n \in \{1,\dots,p-1\}$. Remember that $n\binom{p}{n} = p\binom{p-1}{n-1}$. Hence, $p|n\binom{p}{n}$.
Since $\gcd(p,n) = 1$, by Gauss' lemma, we get that $p|\binom{p}{n}$. ∎

**Theorem 20** (Fermat's little theorem, version 1)**.**
*Let $p$ be a prime number and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod p$.*

*Proof.* We first prove the theorem for $a \in \mathbb{N}$ by induction.
*Base case at $a = 0$:* $0^p = 0 \equiv 0 \pmod p$.
*Induction step:* assume that $a^p \equiv a \pmod p$ for some $a \in \mathbb{N}$. Then

$$\begin{aligned} (a+1)^p &= \sum_{n=0}^{p}\binom{p}{n}a^n \text{ by the binomial formula} \\ &\equiv a^p + 1 \pmod p \quad \text{since, by the above lemma, } p|\binom{p}{n} \text{ for } 1 \leq n \leq p-1 \\ &\equiv a+1 \pmod p \quad \text{by the induction hypothesis} \end{aligned}$$

Which ends the induction step.

We still need to prove the theorem for $a < 0$. Then $-a \in \mathbb{N}$, hence, from the first part of the proof, $(-a)^p \equiv -a \pmod{p}$. Multiplying both sides by $(-1)^p$ we get that $a^p \equiv (-1)^{p+1} a \pmod{p}$.
If $p = 2$ then either $a \equiv 0 \pmod 2$ or $a \equiv 1 \pmod 2$, and the statement holds for both cases.
Otherwise, $p$ is odd, and hence $(-1)^{p+1} = 1$. Thus $a^p \equiv a \pmod{p}$. ■

**Theorem 21** (Fermat's little theorem, version 2)**.**
*Let $p$ be a prime number and $a \in \mathbb{Z}$. If $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.*

*Proof.* By the first version of Fermat's little theorem, $a^p \equiv a \pmod{p}$. Hence $p | a^p - a = a(a^{p-1} - 1)$.
Since $\gcd(a, p) = 1$, by Gauss' lemma, $p | a^{p-1} - 1$. Thus $a^{p-1} \equiv 1 \pmod{p}$. ■

**Remark 22.** Note that both versions of Fermat's little theorem are equivalent.

## 4 Wilson's theorem

**Lemma 23.** *Let $p$ be a prime number. Then*

$$\forall a \in \mathbb{Z},\ a^2 \equiv 1 \pmod{p} \implies \big(a \equiv -1 \pmod{p} \text{ or } a \equiv 1 \pmod{p}\big)$$

*Proof.* Let $p$ be a prime number and $a \in \mathbb{Z}$ satisfying $a^2 \equiv 1 \pmod{p}$. Then $p | a^2 - 1 = (a - 1)(a + 1)$.
By Euclid's lemma, either $p | a - 1$ or $p | a + 1$, i.e. $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ■

**Theorem 24** (Wilson's theorem)**.** *Let $n \in \mathbb{N} \setminus \{0, 1\}$. Then $n$ is prime if and only if $(n - 1)! \equiv -1 \pmod{n}$.*

*Proof.* Let $n \in \mathbb{N} \setminus \{0, 1\}$.

- *Assume that $n$ is a composite number.* Then there exists $k \in \mathbb{N}$ such that $k | n$ and $1 < k < n$.
  Assume by contradiction that $(n - 1)! \equiv -1 \pmod{n}$ then $n | (n - 1)! + 1$ and hence $k | (n - 1)! + 1$.
  But $k | (n - 1)!$, thus $k | \big((n - 1)! + 1 - (n - 1)!\big)$, i.e. $k | 1$. So $k = 1$ which leads to a contradiction.

- *Assume that $n$ is prime.*
  Let $a \in \{1, 2, \dots, n - 1\}$ then $\gcd(a, n) = 1$. Hence $a$ admits a multiplicative inverse modulo $n$, so there exists $b \in \{1, 2, \dots, n - 1\}$ such that $ab \equiv 1 \pmod{n}$.
  Note that this $b$ is unique by Remark 11.
  By the above lemma, $a = 1$ and $a = n - 1$ are the only $a$ as above being their self-multiplicative inverse (i.e. such that $a^2 \equiv 1 \pmod{n}$). Otherwise $b \neq a$.
  Thus $(n - 1)! = 1 \times 2 \times \cdots \times (n - 1) \equiv 1 \times (n - 1) \pmod{n} \equiv -1 \pmod{n}$.
  Indeed, in the previous product each term simplifies with its multiplicative inverse except 1 and $n - 1$.

■

**Examples 25.**
- Take $p = 17$ then $(17 - 1)! + 1 = 20922789888001 = 17 \times 1230752346353$.
- Take $p = 15$ then $(15 - 1)! + 1 = 87178291201 = 15 \times 5811886080 + 1$.

**Remark 26.** Wilson's theorem is a very inefficient way to check whether a number is prime or not. Nonetheless, it has some interesting theoretical applications.

## 5 Chinese remainder theorem

**Theorem 27** (Chinese remainder theorem)**.**
*Let* $n_1, n_2 \in \mathbb{N} \setminus \{0,1\}$ *be such that* $\gcd(n_1, n_2) = 1$ *and let* $a_1, a_2 \in \mathbb{Z}$.
*Then there exists* $x \in \mathbb{Z}$ *satisfying* $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$
*Besides, if* $x_1, x_2 \in \mathbb{Z}$ *are two solutions of the above system then* $x_1 \equiv x_2 \pmod{n_1 n_2}$.

*Proof.*

- *Existence.* By Bézout's identity, there exist $m_1, m_2 \in \mathbb{Z}$ such that $n_1 m_1 + n_2 m_2 = 1$.
  Note that $n_1 m_1 \equiv 0 \pmod{n_1}$ and that $n_1 m_1 \equiv n_1 m_1 + n_2 m_2 \pmod{n_2} \equiv 1 \pmod{n_2}$.
  Similarly $n_2 m_2 \equiv 0 \pmod{n_2}$ and $n_2 m_2 \equiv 1 \pmod{n_1}$.
  Thus, if we set $x = a_2 n_1 m_1 + a_1 n_2 m_2$ then
  - $x \equiv a_2 \times 0 + a_1 \times 1 \pmod{n_1} \equiv a_1 \pmod{n_1}$,
  - $x \equiv a_2 \times 1 + a_1 \times 0 \pmod{n_2} \equiv a_2 \pmod{n_2}$.
- *Uniqueness modulo* $n_1 n_2$. Let $x_1, x_2 \in \mathbb{Z}$ be two solutions.
  Then $x_1 - x_2 \equiv 0 \pmod{n_1}$ so $x_1 - x_2 = k n_1$ for some $k \in \mathbb{Z}$. Similarly $n_2 | x_1 - x_2 = k n_1$.
  Since $\gcd(n_1, n_2) = 1$, by Gauss' lemma, $n_2 | k$. So there exists $l \in \mathbb{Z}$ such that $k = n_2 l$.
  Thus $x_1 - x_2 = l n_1 n_2$ and therefore $x_1 \equiv x_2 \pmod{n_1 n_2}$.

■

## 6 Euler's theorem

**Definition 28.** *Euler's totient function* is the function $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ defined by

$$\varphi(n) \coloneqq \#\left\{k \in \mathbb{N} \ : \ 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\right\}$$

**Proposition 29.** $\forall n_1, n_2 \in \mathbb{N} \setminus \{0\}$, $\gcd(n_1, n_2) = 1 \implies \varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$

*Proof.* If $n_1 = 1$ or $n_2 = 1$ then there is nothing to prove. So let's assume that $n_1, n_2 \geq 2$.
Define

$$S_i = \left\{r \in \mathbb{N} \ : \ 1 \leq r \leq n_i \text{ and } \gcd(r, n_i) = 1\right\}, \ i = 1, 2$$

and

$$T = \left\{k \in \mathbb{N} \ : \ 1 \leq k \leq n_1 n_2 \text{ and } \gcd(k, n_1 n_2) = 1\right\}$$

For $k \in T$, write the Euclidean divisions $k = n_1 q_1 + r_1$ with $0 \leq r_1 < n_1$ and $k = n_2 q_2 + r_2$ where $0 \leq r_2 < n_2$.
Let's prove that $r_i \in S_i$:

- Assume that $r_i = 0$ then $n_i | k$ and $n_i | n_1 n_2$ so that $n_i | \gcd(k, n_1 n_2) = 1$: contradiction. So $1 \leq r_i < n_i$.
- $\gcd(r_i, n_i) = \gcd(k - n_i q_i, n_i) = \gcd(k, n_i) | \gcd(k, n_1 n_2) = 1$, hence $\gcd(r_i, n_i) = 1$.

Therefore we can define $f : T \to S_1 \times S_2$ by $f(k) = (r_1, r_2)$. Let's prove that $f$ is a bijection.
Let $(r_1, r_2) \in S_1 \times S_2$. Then by the Chinese remainder theorem, there exists a unique $k \in \{1, 2, \dots, n_1 n_2\}$ such that $k \equiv r_1 \pmod{n_1}$ and $k \equiv r_2 \pmod{n_2}$.
Note that $\gcd(k, n_1) = \gcd(r_1 + l n_1, n_1) = \gcd(r_1, n_1) = 1$ (for some $l \in \mathbb{Z}$).
Similarly $\gcd(k, n_2) = \gcd(r_2, n_2) = 1$.
Then $\gcd(k, n_1 n_2) = 1$ by Exercise 3 of Problem Set 2, so that $k \in T$.
We proved that $\forall (r_1, r_2) \in S_1 \times S_2$, $\exists! k \in T$, $(r_1, r_2) = f(k)$, i.e. that $f$ is bijective.
Therefore, $\#T = \#(S_1 \times S_2) = \#S_1 \# S_2$, i.e. $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$. ■

**Proposition 30.** *Let $p_1, \dots, p_r$ be pairwise distinct prime numbers and $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$, then*

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

*Proof.*

- *First case:* let $p$ be a prime number and $\alpha \in \mathbb{N} \setminus \{0\}$. Then $\gcd(p^\alpha, m) > 1$ if and only if $p|m$. Hence $\varphi(p^\alpha) = \#\left(\{1, 2, \dots, p^\alpha\} \setminus \{1 \times p, 2 \times p, \dots, p^{\alpha-1} \times p\}\right) = p^\alpha - p^{\alpha-1}$.
- *General case:* using Proposition 29 and the first case, we get that

$$\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

■

**Remark 31.** Assuming that we have already some knowledge about $\mathbb{Q}$, we can also write for $n = \prod_{i=1}^{r} p_i^{\alpha_i}$:

$$\varphi(n) = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

**Theorem 32** (Euler's theorem)**.** *Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

**Remark 33.** Note that Fermat's little theorem is a special case of Euler's theorem: indeed, if $p$ is a prime number then $\varphi(p) = p - 1$.

*Proof of Euler's theorem.*
Write $S = \left\{k \in \mathbb{N} \,:\, 1 \le k \le n \text{ and } \gcd(k, n) = 1\right\} = \left\{k_1, k_2, \dots, k_{\varphi(n)}\right\}$.
We will use the following two facts:

(i) Given $k_i \in S$, there exists $k_j \in S$ such that $ak_i \equiv k_j \pmod{n}$.
Let $k_i \in S$ then $\gcd(ak_i, n) = 1$ by Exercise 3 of Problem Set 2.
Thus $ak_i \equiv k_j \pmod{n}$ for some $k_j \in S$.

(ii) $\forall k_i, k_j \in S$, $ak_i \equiv ak_j \pmod{n} \implies k_i = k_j$.
Indeed, then $n|a(k_i - k_j)$ and hence $n|k_i - k_j$ by Gauss' lemma.
Thus $k_i \equiv k_j \pmod{n}$.
Finally, $k_i = k_j$ since $1 \le k_i, k_j \le n$.

For $i \in \{1, 2, \dots, \varphi(n)\}$, there exists a unique $l_i \in \{0, 1, \dots, n-1\}$ such that $l_i \equiv ak_i \pmod{n}$.
Then, $\{l_1, l_2, \dots, l_{\varphi(n)}\} = \{k_1, k_2, \dots, k_{\varphi(n)}\}$.
Indeed, by (i), $\{l_1, l_2, \dots, l_{\varphi(n)}\} \subset \{k_1, k_2, \dots, k_{\varphi(n)}\}$. And by (ii), $\#\{l_1, l_2, \dots, l_{\varphi(n)}\} = \#\{k_1, k_2, \dots, k_{\varphi(n)}\}$.
Hence $\prod_{i=1}^{\varphi(n)} k_i = \prod_{i=1}^{\varphi(n)} l_i \equiv \prod_{i=1}^{\varphi(n)} ak_i \pmod{n} \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i \pmod{n}$.
Therefore $n|(a^{\varphi(n)} - 1)\prod_{i=1}^{\varphi(n)} k_i$.
Since $\gcd\left(n, \prod_{i=1}^{\varphi(n)} k_i\right) = 1$ by Exercise 3 of Problem Set 2, we deduce from Gauss' lemma that $n|a^{\varphi(n)} - 1$, i.e. $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

# A Positional numeral system with base $b$

**Theorem 34.** *Let $b \geq 2$ be an natural number. Then any natural number $n \in \mathbb{N}$ admits a unique expression*

$$n = \sum_{k \geq 0} a_k b^k$$

*where $a_k \in \{0, 1, \dots, b-1\}$ and $a_k = 0$ for all but finitely many $k \geq 0$.*

**Notation 35.** We write $\overline{a_r a_{r-1} \dots a_1 a_0}^b$ for $\sum_{k=0}^{r} a_k b^k$.

*Proof of Theorem 34.*
**Existence.**
We are going to prove by strong induction that for any $n \geq 0$, there exist $a_k \in \{0, 1, \dots, b-1\}$, $k \in \mathbb{N}$, all but finitely many equal to 0 such that $n = \sum_{k \geq 0} a_k b^k$.

- *Base case at $n = 0$:* $0 = \sum_{k \geq 0} 0 b^k$.
- *Induction step.* Assume that $0, 1, \dots, n$ admit an expression in base $b$, for some $n \geq 0$.
  By Euclidean division, $n + 1 = bq + r$ where $q, r \in \mathbb{N}$ satisfy $0 \leq r < b$.
  Note that if $q \neq 0$ then $q < bq \leq bq + r = n + 1$. Thus $0 \leq q \leq n$.
  Therefore, by the induction hypothesis, $q = \sum_{k \geq 0} a_k b^k$ where $a_k \in \{0, 1, \dots, b-1\}$ and $a_k = 0$ for all but finitely many $k \geq 0$.
  Hence, $n + 1 = bq + r = \sum_{k \geq 0} a_k b^{k+1} + r b^0$.

**Uniqueness.**
Write $\sum_{k \geq 0} a_k b^k = \sum_{k \geq 0} a'_k b^k$ where $a_k, a'_k \in \{0, 1, \dots, b-1\}$ are zero for all but finitely many $k \geq 0$.
Assume by contradiction there exists $k \geq 0$ such that $a_k \neq a'_k$.
Since $\{k \in \mathbb{N} \,:\, a_k \neq a'_k\}$ is finite and non-empty, it admits a greatest element $\ell$.
WLOG, we may assume that $a_\ell < a'_\ell$.

Then $0 = \sum_{k \geq 0} a_k b^k - \sum_{k \geq 0} a'_k b^k = \sum_{k \geq 0} (a_k - a'_k) b^k = \sum_{k=0}^{\ell} (a_k - a'_k) b^k$. So that $(a'_\ell - a_\ell) b^\ell = \sum_{k=0}^{\ell-1} (a_k - a'_k) b^k$.

Therefore $(a'_\ell - a_\ell) b^\ell \leq \sum_{k=0}^{\ell-1} |a_k - a'_k| b^k \leq \sum_{k=0}^{\ell-1} (b-1) b^k = b^\ell - 1 < b^\ell \leq (a'_\ell - a_\ell) b^\ell$.

Hence a contradiction. ∎

**Remark 36.** In order to pass from a base 10 expression to a base $b$ expression, we can perform successive Euclidean divisions as shown below (to pass from a base $b$ expression to a base 10 we may simply compute the sum).

**Example 37.**

$$\begin{aligned}
42 &= 2 \times 21 + 0 \\
&= 2 \times (2 \times 10 + 1) + 0 \\
&= 2 \times (2 \times (2 \times 5 + 0) + 1) + 0 \\
&= 2 \times (2 \times (2 \times (2 \times 2 + 1) + 0) + 1) + 0 \\
&= 2 \times (2 \times (2 \times (2 \times (2 \times 1 + 0) + 1) + 0) + 1) + 0 \\
&= 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0
\end{aligned}$$

Hence $\overline{42}^{10} = \overline{101010}^2$.

The first known positional numeral system is the Babylonian one (circa 2000BC) whose base is 60 and whose digits are:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | 10 | 𒌋 | 20 | 𒎌 | 30 | 𒐐 | 40 | 𒐚 | 50 | 𒐝 |
| 1 | 𒁹 | 11 | 𒌋𒁹 | 21 | 𒎌𒁹 | 31 | 𒐐𒁹 | 41 | 𒐚𒁹 | 51 | 𒐝𒁹 |
| 2 | 𒁹𒁹 | 12 | 𒌋𒁹𒁹 | 22 | 𒎌𒁹𒁹 | 32 | 𒐐𒁹𒁹 | 42 | 𒐚𒁹𒁹 | 52 | 𒐝𒁹𒁹 |
| 3 | 𒁹𒁹𒁹 | 13 | 𒌋𒁹𒁹𒁹 | 23 | 𒎌𒁹𒁹𒁹 | 33 | 𒐐𒁹𒁹𒁹 | 43 | 𒐚𒁹𒁹𒁹 | 53 | 𒐝𒁹𒁹𒁹 |
| 4 | 𒁹𒁹𒁹𒁹 | 14 | 𒌋𒁹𒁹𒁹𒁹 | 24 | 𒎌𒁹𒁹𒁹𒁹 | 34 | 𒐐𒁹𒁹𒁹𒁹 | 44 | 𒐚𒁹𒁹𒁹𒁹 | 54 | 𒐝𒁹𒁹𒁹𒁹 |
| 5 | 𒁹𒁹𒁹𒁹𒁹 | 15 | 𒌋𒁹𒁹𒁹𒁹𒁹 | 25 | 𒎌𒁹𒁹𒁹𒁹𒁹 | 35 | 𒐐𒁹𒁹𒁹𒁹𒁹 | 45 | 𒐚𒁹𒁹𒁹𒁹𒁹 | 55 | 𒐝𒁹𒁹𒁹𒁹𒁹 |
| 6 | 𒁹𒁹𒁹𒁹𒁹𒁹 | 16 | 𒌋𒁹𒁹𒁹𒁹𒁹𒁹 | 26 | 𒎌𒁹𒁹𒁹𒁹𒁹𒁹 | 36 | 𒐐𒁹𒁹𒁹𒁹𒁹𒁹 | 46 | 𒐚𒁹𒁹𒁹𒁹𒁹𒁹 | 56 | 𒐝𒁹𒁹𒁹𒁹𒁹𒁹 |
| 7 | 𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 17 | 𒌋𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 27 | 𒎌𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 37 | 𒐐𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 47 | 𒐚𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 57 | 𒐝𒁹𒁹𒁹𒁹𒁹𒁹𒁹 |
| 8 | 𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 18 | 𒌋𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 28 | 𒎌𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 38 | 𒐐𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 48 | 𒐚𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 58 | 𒐝𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 |
| 9 | 𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 19 | 𒌋𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 29 | 𒎌𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 39 | 𒐐𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 49 | 𒐚𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 | 59 | 𒐝𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹𒁹 |

Let's say that we want to write 13655 using Babylonian cuneiform numerals. For that, we perform successive Euclidean divisions by 60 as follows:

$$13655 = 60 \times 227 + 35 = 60 \times (60 \times 3 + 47) + 35 = 3 \times 60^2 + 47 \times 60^1 + 35 \times 60^0$$

Hence it was written: 𒐝 𒐚𒁹 𒎌𒁹

Originally, there was no positional zero and an empty space was used instead (which can be confusing: 𒎌𒐝 𒁹 and 𒎌𒐝 𒁹 are not equal). The more convenient symbol 𒑚 was later used instead of the empty space (but it is not the number 0, just a placeholder symbol for the positional numeral system).

See below a problem set submission by a MAT246 student circa 1700BC.

Figure 1: YBC 7289, clay tablet, between 1800BC and 1600BC.

It shows (extremely accurate) approximations of $\sqrt{2} \simeq 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}$
and of $30\sqrt{2} \simeq 42 + \frac{25}{60} + \frac{35}{60^2}$ (diagonal of the square of side length 30, see above de square)
*Yale Babylonian Collection,*
*Original picture from* https://commons.wikimedia.org/wiki/File:YBC-7289-OBV-REV.jpg

## B The Chinese Remainder Theorem for more than two equations

You won't need the following result in MAT246, I've just added it because it was asked on Piazza (@82).

**Theorem 38** (Chinese remainder theorem)**.** *Let $k \in \mathbb{N} \setminus \{0,1\}$.*
*Let $n_1, n_2, \dots, n_k \in \mathbb{N} \setminus \{0,1\}$ be pairwise coprine, i.e. $\forall i, j \in \{1, \dots, k\}$, $i \neq j \implies \gcd(n_i, n_j) = 1$.*
*Let $a_1, \dots, a_k \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$ satisfying*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

The proof follows closely the one of Theorem 27 but applied to $n_i$ and $n_1 \dots n_{i-1} n_{i+1} \dots n_k$.

*Proof.* Let $i \in \{1, \dots, k\}$. Then $\gcd(n_i, n_1 \dots n_{i-1} n_{i+1} \dots n_k) = 1$.
So, by Bézout's identity, there exists $u_i, v_i \in \mathbb{Z}$ such that $u_i n_i + v_i n_1 \dots n_{i-1} n_{i+1} \dots n_k = 1$.
Set $e_i = v_i n_1 \dots n_{i-1} n_{i+1} \dots n_k$ then $e_i \equiv 1 \pmod{n_i}$, and for $j \in \{1, \dots, k\} \setminus \{i\}$, $e_i \equiv 0 \pmod{n_j}$.
Therefore $x = \sum_{i=1}^{k} a_i e_i$ is a suitable solution. ∎