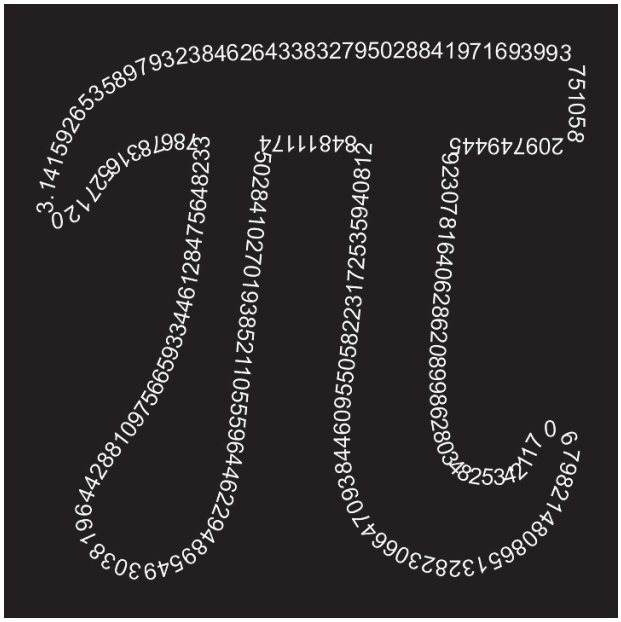
MATHS BASIC COURSE FOR UNDERGRADUATES



Leire Legarreta, Iker Malaina and Luis Martínez

Faculty of Science and Technology

Department of Mathematics

University of the Basque Country

5th SUBJECT: CONGRUENCES

Congruences. Divisibility criteria. Linear congruences. Euler's ρ function. Chinese remainder theorem.

1 Congruences

The language of congruences can be used to solve problems of divisibility. This language was studied by Gauss in 1801, in Disquisitiones Arithmaticae.

Definition. *Let n be a positive integer number. The integer numbers a and b are said to be congruent modulo n, and we will address it as $a \equiv b$ (mod n), if when they are divided by n, we obtain the same remainder. The number n is said to be the modulo of the congruence.*

Examples. *The following are some special cases:*

(i) *When any integer number is divided by $n = 1$, the remainder is 0, this is, all the numbers are congruent each one to each other modulo 1.*

(ii) *If $n = 2$, the only possible remainders are 0 and 1. The ones with remainder 0 are the even numbers, while the ones with remainder 1 are the odd ones.*

(iii) *If $n = 5$, then $9 \equiv 19$ (mod 5), $-13 \equiv 2$ (mod 5) or $5 \equiv -5$ (mod 5). In general, all integer numbers can be divided in 5 classes (mod 5).*

Proposition. *$a \equiv b$ (mod n) if and only if $a - b$ is a multiple of n.*

Proof. *If $a \equiv b$ (mod n), we can write:*

$$a = q_1 n + r \quad \text{and} \quad b = q_2 n + r, \quad \text{where } 0 \leq r < n.$$

By subtracting the previous expressions, we have $a - b = (q_1 - q_2)n$, and we have finished. On the contrary, lets suppose now that $a - b$ is a multiple of n. Lets also suppose that

$$a = q_1 n + r_1 \quad \text{and} \quad b = q_2 n + r_2 \quad \text{where } 0 \leq r_1, r_2 < n.$$

Again, subtracting the previous two expressions, we get $a - b = (q_1 - q_2)n + (r_1 - r_2)$, and isolating $r_1 - r_2$, we obtain that $r_1 - r_2 = (a - b) - (q_1 - q_2)n$ is a multiple of n. Consequently, $r_1 - r_2 = 0$ or $r_1 = r_2$ (what we wanted).

Proposition. *Let $n > 1$ be a positive integer number and a, b, c, d, k be integer numbers. The following properties are fulfilled:*

(i) *Reflexivity:* $a \equiv a$ *(mod* n*).*

(ii) *Symmetry: if* $a \equiv b$ *(mod* n*), then* $b \equiv a$ *(mod* n*).*

(iii) *Transitivity: if* $a \equiv b$ *(mod* n*) and* $b \equiv c$ *(mod* n*), then* $a \equiv c$ *(mod* n*).*

(iv) *If* $a \equiv b$ *(mod* n*) and* $c \equiv d$ *(mod* n*), then*

$$a + c \equiv b + d \text{ (mod } n) \quad \text{and} \quad ac \equiv bd \text{ (mod } n).$$

(v) *If* $a \equiv b$ *(mod* n*), then*

$$a \pm k \equiv b \pm k \text{ (mod } n) \quad \text{and} \quad ak \equiv bk \text{ (mod } n).$$

(vi) *If* $a \equiv b$ *(mod* n*), then* $a^m \equiv b^m$ *(mod* n*), for any positive integer* m*.*

(vii) *If* $a \equiv b$ *(mod* n*) and* $p(x)$ *is a polynomial in the variable* x *with integer coefficients, then* $p(a) \equiv p(b)$ *(mod* n*).*

Proof. *properties i), ii) and iii) are immediate, and therefore "being congruent modulo* n*" is an equivalence relation in the group* $\mathbb{Z}$*.*

iv) If $a \equiv b$ *(mod* n*) and* $c \equiv d$ *(mod* n*), then* $a - b = q_1 n$ *and* $c - d = q_2 n$*. Merging the previous two expressions, we obtain* $(a + c) - (b + d) = (q_1 + q_2)n$*, and this is a multiple of* n*, or equivalently,* $a + c \equiv b + d$ *(mod* n*). Analogously, since* $a = b + q_1 n$ *and* $c = d + q_2 n$*, by multiplying both equations we obtain,*

$$ac = (b + q_1 n)(d + q_2 n) = bd + (bq_2 + dq_1 + q_1 q_2 n)n,$$

hence, $ac - db$ *is a multiple of* n*.*

v) is a consequence of iv), since $k \equiv k$ *(mod* n*).*

vi) can also obtain as a consequence of iv), multiplying the congruence $a \equiv b$ *(mod* n*) by itself* m *times. And vii) is a consequence of iv), v) and vi).*

Proposition. *If* $ak \equiv bk$ *(mod* n*), then* $a \equiv b$ *(mod* $\frac{n}{d}$*), where* $d = gcd(k, n)$*.*

Proof. *Since* $d = gcd(k, n)$*, we can write* $k = dk'$ *and* $n = dn'$*, where* $gcd(k', n') = 1$*. From the hypothesis, we have that* $ka - kb = qn$*, for some integer number* q*. This is,* $dk'a - dk'b = qdn'$*, and now dividing by* d*, we have* $k'a - k'b = qn'$*. Therefore,* $n' \mid k'(a - b)$*, this is,* $a \equiv b$ *(mod* n'*).*

Corollary. *If* $ak \equiv bk$ *(mod* n*) and* k *and* n *are coprime numbers, then* $a \equiv b$ *(mod* n*).*

Corollary. *If* $ak \equiv bk$ *(mod* p*), being* p *a prime number and if* $p \nmid k$*, then* $a \equiv b$ *(mod* p*).*

Examples. *Some applications of the previous results are the following:*

(i) $6 \equiv 4$ *(mod* 2*) can be changed to* $3 \equiv 2$ *(mod* $\frac{2}{d}$*), where* $d = gcd(2, 2)$*; this is,* $3 \equiv 2$ *(mod* 1*).*

(ii) $44 \equiv 8$ *(mod* 9*) can be changed to* $11 \equiv 2$ *(mod* $\frac{9}{d}$*), where* $d = gcd(4, 9)$*, this is,* $11 \equiv 2$ *(mod* 9*).*

Example. *An integer number expressed in decimal form is divisible by* 9 *if and only if the sum of its digits is divisible by* 9*. Let us write* n *in decimal form,*

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

where a_i *are in* $0 \leq a_i \leq 9$*. Since* $10 \equiv 1$ *(mod* 9*), applying one of the previous properties (vi),* $10^i \equiv 1$ *(mod* 9*) and* $a_i \cdot 10^i \equiv a_i$ *(mod* 9*). Thus,* $n \equiv a_1 + a_2 + \cdots + a_n$ *(mod* 9*).*

2 Divisibility criteria

Theorem. *(Fermat's Little Theorem.) If* p *is a prime number and* $p \nmid a$*, then*

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

Proof. *Let us take the first different* $p - 1$ *multiples of* a*:* $a, 2a, \ldots, (p-1)a$*. In pairs, these numbers are not congruent modulo* p*. In fact, if* $sa \equiv ta$ *(mod* p*), being* $s \neq t$*, then cancelling* a*, we would achieve* $s \equiv t$ *(mod* p*), and this is impossible since* s *and* t *are smaller than* p*. Thus, since in pairs, they are not congruent modulo* p*, when we divide them by* p *we obtain* $p - 1$ *different remainders. None of those remainders is* 0*. On the contrary, if* $sa \equiv 0$ *(mod* p*), then cancelling* a*, we would obtain* $s \equiv 0$ *(mod* p*) which is impossible since* $1 \leq s \leq p-1$*. Consequently, with the previous* $p-1$ *numbers, we obtain the remainders* $1, 2, \ldots p - 1$*. Therefore, the numbers* $a, 2a, \ldots (p-1)a$*, in certain order, are congruent modulo* p *with* $1, 2, \ldots p - 1$*. Now multiplying all these congruences, we obtain:*

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \text{ (mod } p),$$

this is,

$$1 \cdot 2 \cdot 3 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \text{ (mod } p),$$

and after cancelations, we have $a^{p-1} \equiv 1$ *(mod* p*).*

Proposition. *If* p *and* q *are two different prime numbers and* a *is an integer fulfilling that* $p \nmid a$ *and* $q \nmid a$*, then* $a^{(p-1)(q-1)} \equiv 1$ *(mod* pq*).*

Proof. *Because of Fermat's Little Theorem, we know that* $a^{p-1} \equiv 1$ *(mod* p*). By applying a previous property (vi), we have* $a^{(p-1)(q-1)} \equiv 1$ *(mod* p*). Similarly, we have* $a^{q-1} \equiv 1$ *(mod* q*), and consequently,* $a^{(p-1)(q-1)} \equiv 1$ *(mod* q*). Now, since* $p \mid a^{(p-1)(q-1)} - 1$ *and* $q \mid a^{(p-1)(q-1)} - 1$*, and* p *and* q *are different prime numbers, we have* $pq \mid a^{(p-1)(q-1)} - 1$*, or equivalently,* $a^{(p-1)(q-1)} \equiv 1$ *(mod* pq*).*

3 Linear congruences

Definition. *If* m *is a positive integer number and* $a, b \in \mathbb{Z}$*, we denote the equation* $ax \equiv b$ *(mod* m*), with the variable* $x \in \mathbb{Z}$*, as a linear congruence.*

Example. *Solve the linear congruence* $4x \equiv 2$ *(mod* 28*). If* $x \in \mathbb{Z}$ *is a solution for the linear congruence, then* $4x = 2 + 28q$*, for some* $q \in \mathbb{Z}$*, and is noticeable that this is impossible, since the left side of the equality is divisible by* 4*, while the right side is not.*

Example. *Solve the linear congruence* $13x \equiv 2$ *(mod* 31*). If* $x \in \mathbb{Z}$ *is a solution for the linear congruence, then* $13x = 2 + 31q$*, for some* $q \in \mathbb{Z}$*. Notice that gcd*$(13, 31) = 1$*, and then, because Bezout's identity, there exist two integer numbers* s, t *for which* $1 = 13s + 31t$*. Thus,* $13s \equiv 1$ *(mod* 31*), and multiplying the congruence by* 2*, we obtain* $13(2s) \equiv 2$ *(mod* 31*). This is,* $x = 2s$ *(*$s \in \mathbb{Z}$*) is a solution for the initial congruence.*

The previous examples give us the key to find the solutions for linear congruences and to prove their existence.

Proposition. *The linear congruence* $ax \equiv b$ *(mod* m*), being* $x \in \mathbb{Z}$*, has a solution if and only if* $d = gcd(a, m)$ *divides* b*. Besides, in this case, there exist exactly* d *non congruent solutions modulo* m*.*

Proof. *First of all, let us suppose that* $x_0 \in \mathbb{Z}$ *is a solution of the linear congruence. Then,* $ax_0 = b + qm$*, for some* $q \in \mathbb{Z}$*. Since* $d \mid a$ *and* $d \mid m$*, we conclude that* $d \mid b$*. On the contrary, let us suppose that* $d \mid b$ *and write* $b = kd$*, for some* $k \in \mathbb{Z}$*. By Bezout's identity, there exist two integer numbers* s, t *for which* $d = sa + tm$*. Multiplying the previous equality by* k*, we have* $b = kd = ksa + ktm$*, and then* $aks = b - ktm \equiv b$ *(mod* m*). This is,* ks *is a solution for the given congruence. On the other hand, if* x_0 *and* x_1 *are two different solutions for the congruence* $ax \equiv b$*(mod* m*), then* $ax_1 \equiv ax_0$ *(mod* m*), and cancelling* a*, we obtain* $x_1 \equiv x_0$ *(mod* $\frac{m}{d}$*). Thus, the* d *different solutions for the congruence which are non congruent modulo* m *are:*

$$\{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\}.$$

Example. *Prove Wilson's Theorem. If* p *is a prime number, then* $(p-1)! + 1 \equiv 0$ *(mod* p*). By Fermat's Little Theorem, the congruence* $x^{p-1} \equiv 1$ *(mod* p*), or equivalently the congruence* $x^{p-1} - 1 \equiv 0$ *(mod* p*), has* $p - 1$ *different solutions; specifically:*

$1, 2, \ldots, p-1$. *Thus,*

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \text{ (mod } p).$$

Since any value of x fulfills this congruence, by taking $x = 0$ we have the following:

$$-1 \equiv (-1)(-2)\ldots(-(p-1)) \text{ (mod } p) \equiv (-1)^{p-1} 1 \cdot 2 \ldots (p-1) \text{ (mod } p),$$

this is, $(-1)^{p-1} \cdot (p-1)! + 1 \equiv 0$ (mod p). If $p = 2$, we have $-1 + 1 \equiv 0$ (mod 2), and if p is an odd number, we have $(p-1)! + 1 \equiv 0$ (mod p).

4 Euler's ρ function

Definition. *If $n \in \mathbb{N}$, we call $\rho(n)$ to the number of positive integers that are smaller or equal to n and at the same time, are coprimes to n. By definition, $\rho(1) = 1$, and it is called Euler's ρ function.*

Proposition. *If p is a prime number, then $\rho(p) = p - 1$.*

Proposition. *If p is a prime number and $n \in \mathbb{N}$, then $\rho(p^n) = p^n - p^{n-1}$.*

Proof. *The positive integer numbers smaller or equal to p^n and that at the same time are not coprimes to p^n are:*

$$p, 2p, 3p, \ldots, p(p-1), p^2, (p+1)p, (p+2)p, \ldots, 2p^2, 3p^2, \ldots,$$

$$(p-1)p^2, p^3, \ldots, p^{n-2}, 2p^{n-2}, 3p^{n-2}, \ldots p^{n-1}p,$$

and counting them, there are p^{n-1} positive integer numbers. Thus, $\rho(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(p - \frac{1}{p})$.

Corollary. *If p is a prime number and $n \in \mathbb{N}$, then $\displaystyle\sum_{i=0}^{n} \rho(p^i) = p^n$.*

Proof. *By using the previous proposition,*

$$\sum_{i=0}^{n} \rho(p^i) = \rho(p^0) + \sum_{i=1}^{n} \left(p^i - p^{i-1}\right) = 1 + (p-1) \sum_{i=1}^{n} p^{i-1} =$$

$$\rho(1) + (p-1)\frac{p^n - 1}{p-1} = 1 + p^n - 1 = p^n.$$

Theorem. *If $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ ($n \in \mathbb{N}$) is the canonical factorization of n, then*

$$\rho(n) = \prod_{i=1}^{r} \rho(p_i^{k_i}) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Proof. *The theorem can be proven inductively. The amount of numbers non divisible by p_1 and that at the same time are smaller or equal to n is given by $n - \frac{n}{p_1}$. Let us suppose that the amount of numbers smaller or equal to n and at the same time, non divisible by the primes $p_1, p_2, \ldots, p_s$ (being $s < r$) is given by the following formula:*

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}).$$

Now, the positive integer numbers smaller or equal to n that at the same time are multiples of p_{s+1} are: p_{s+1}, $2p_{s+1}, \ldots, \frac{n}{p_{s+1}}p_{s+1}$. From those, the numbers that are not multiples of $p_1, p_2, \ldots, p_s$ are related to the coefficients of p_{s+1} (this is, $1, 2, 3, \ldots, \frac{n}{p_{s+1}}$) that are not divisible by $p_1, p_2, \ldots, p_s$. By the induction hypothesis, the amount of these positive integer numbers is given by the expression:

$$\frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}).$$

Thus, the amount of positive integer numbers smaller or equal to n that at the same time are non divisible by $p_1, p_2, \ldots p_{s+1}$ is given by the following formula:

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}) - \frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}) =$$

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_{s+1}}).$$

Remark. *Another way to see that $\rho(n) = \prod_{i=1}^{r} \rho(p_i^{k_i})$ in the previous conditions would be: find the numbers that have an inverse for the product in $\mathbb{Z}/n\mathbb{Z}$, or in other words, find the group $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$, and then, notice that there exists an application that is at the same time bijective and an homomorphism between $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ and the cartesian product $\mathbb{U}(\mathbb{Z}/{p_1}^{k_1}\mathbb{Z}) \times \mathbb{U}(\mathbb{Z}/{p_2}^{k_2}\mathbb{Z}) \times \ldots \times \mathbb{U}(\mathbb{Z}/{p_r}^{k_r}\mathbb{Z})$. Consequently, the amount of invertible elements for the product in both groups is related, and therefore their amount can also be counted in two ways.*

Proposition. *If $n > 1$, the sum of the positive integer numbers smaller or equal to n that are coprimes to n is given by $\frac{1}{2}n\rho(n)$.*

Proof. *Let $m_1, m_2, \ldots, m_{\rho(n)}$ be all the positive integers smaller or equal to n that at the same time are coprimes to n. The sum of all these numbers is given by:*

$$S = m_1 + m_2 + \cdots + m_{\rho(n)}.$$

For any index $i \in \{1, \ldots, \rho(n)\}$, since $n - m_i$ and n are coprimes, then all the positive integer numbers smaller or equal to n that are at the same time coprimes to n can be addressed as:

$$(n - m_1), (n - m_2), \ldots, (n - m_{\rho(n)}).$$

Thus,

$$S = (n - m_1) + (n - m_2) + \cdots + (n - m_{\rho(n)}).$$

Joining the two expressions for S, we obtain:

$$2S = n + \overbrace{\cdots}^{\rho(n)} + n = n\rho(n).$$

Proposition. *Euler's ρ function is multiplicative. In other words, if m and n are coprimes, then $\rho(mn) = \rho(m)\rho(n)$.*

Proof. *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ and $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ be the canonical factorization of these integer numbers, where $p_i \neq q_j$ for all the indexes. Then:*

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s},$$

and by a previous theorem,

$$\rho(mn) = mn(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})(1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \dots (1 - \frac{1}{q_s}) =$$

$$\left(m(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})\right)\left(n(1 - \frac{1}{q_1}) \dots (1 - \frac{1}{q_s})\right) = \rho(m)\rho(n).$$

Remark. *Notice that $\rho(3) = 2$ and $\rho(6) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$, but $\rho(3 \cdot 6) = \rho(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6 \neq \rho(3)\rho(6)$.*

5 Chinese remainder theorem

Proposition. *The following system of linear congruences*

$$x \equiv a_1 (mod\ m_1)$$

$$x \equiv a_2 (mod\ m_2)$$

is solvable if and only if gcd$(m_1, m_2) \mid (a_2 - a_1)$. If x_1 is a solution of the system, then any other solution of the system has the form $x \equiv x_1$(mod lcm(m_1, m_2)).

Proof. *If $x \equiv a_1$(mod m_1), then $x = a_1 + km_1$ where k is an integer number. Substituting in the second linear congruence, $a_1 + km_1 \equiv a_2$(mod m_2), and thus $m_1 k \equiv (a_2 - a_1)$(mod m_2). By a previous proposition, we know that this congruence is solvable if and only if gcd$(m_1, m_2) \mid (a_2 - a_1)$. Suppose that there exists x_0 that is a solution of the new second linear congruence. Now denote $x_1 = a_1 + x_0 m_1$. Any other solution of the new second congruence has the form $x_0 + \frac{m_2}{d} t$, where $d =$ gcd(m_1, m_2) and $t \in \{1, 2, \dots, d - 1\}$. Then, another solution of the first system has the form:*

$$x = a_1 + (x_0 + \frac{m_2}{d} t) m_1 = a_1 + x_0 m_1 + \frac{m_1 m_2}{d} t.$$

Since $x_1 = a_1 + x_0 m_1$ *and* $gcd(m_1, m_2) \cdot lcm(m_1, m_2) = m_1 m_2$ *or* $\frac{m_1 m_2}{gcd(m_1, m_2)} = lcm(m_1, m_2)$*, then we have that* $x \equiv x_1 (mod\ lcm(m_1, m_2))$*.*

Theorem. *(Chinese remainder theorem.) If* $gcd(m_i, m_j) = 1$ *for any value* $i \neq j$*, then the system of congruences*

$$x \equiv a_1 (mod\ m_1)$$

$$x \equiv a_2 (mod\ m_2)$$

$$\cdots\cdots$$

$$x \equiv a_n (mod\ m_n)$$

has a unique solution modulo $m = m_1 \ldots m_n$*.*

Proof. *Denote as* $M_i = \frac{m}{m_i}$ *for any value of* $i \in \{1, \ldots, n\}$*. Then,* $gcd(M_i, m_i) = 1$*. By a previous proposition, the solutions of the following linear conrguences are unique:*

$$M_1 x_1 \equiv 1\ (\ mod\ m_1), M_2 x_2 \equiv 1\ (\ mod\ m_2), \ldots, M_n x_n \equiv 1\ (\ mod\ m_n).$$

Multiplying each of them by the corresponding factor, we obtain:

$$M_1 x_1 a_1 \equiv a_1\ (\ mod\ m_1), M_2 x_2 a_2 \equiv a_2\ (\ mod\ m_2), \ldots, M_n x_n a_n \equiv a_n\ (\ mod\ m_n).$$

Now each congruence of the initial statement is fulfilled if

$$x_0 = M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_n x_n a_n,$$

because M_j *includes the factor* m_i*, if* $i \neq j$*. Hence, the initial system of linear congruences has at least one solution. If* x' *is another solution of the system, we have that* $x' \equiv a_i (mod\ m_i)$*, for certain value of i. In addition,* $x' \equiv x_0 (mod\ m_i)$*, and since* $gcd(m_i, m_j) = 1$ *for the cases where* $i \neq j$*, applying repetitively the previous proposition, we obtain the following :* $x' \equiv x_0\ (\ mod\ m)$*.*