Elementary Number Theory
20th October 2021

1. Congruences

It was the genius of C-F Gauss that defined the notion as well as notation of congruences.

Given a natural number m, two integers a and b are said to be congruent modulo m, if m divides the integer $a - b$. One uses the notation $a \equiv b \mod m$.
The relation of congruence generalizes equality of numbers and satisfies the basic properties

$$a \equiv b \ mod \ m,$$

$$c \equiv d \ mod \ m$$

implies $a + c \equiv b + d, ac \equiv bd \ mod \ m$.
Also, if $ab \equiv ac \mod m$ and $(a, m) = 1$, then $b \equiv c \mod m$.
The fact that for any positive integer m and a coprime integer a, the GCD 1 can be expressed as $ax + my$ can be rephrased as asserting that $ax \equiv 1 \mod m$ has a solution x. One calls x the 'multiplicative inverse' of $a \mod m$. This is meaningful as x is unique mod m by the last property above.

Fermat's little theorem can be re-stated as saying that if p is a prime number then for any integer a, we have $a^p \equiv a \mod p$; further, if a is coprime to p, then $a^{p-1} \equiv 1 \mod p$.

Nice fact: *If $f(x)$ is a polynomial with integer coefficients, then $f(a) \equiv f(b) \ mod \ a - b$ for integers $a \neq b$.*
The proof is easy as follows. Write

$$f = a_0 + a_1 x + \cdots + a_n x^n.$$

Then, $\frac{f(b)-f(a)}{b-a} = \sum_{r=1}^{n} a_r \frac{b^r - a^r}{b-a} \in \mathbb{Z}$.

This observation has some interesting applications. For instance, recall problem 18 we had discussed earlier:
Suppose f is an integer polynomial such that $f(a_1) = f(a_2) = f(a_3) = 2$ for distinct integers a_1, a_2, a_3. Then, 3 cannot be an integral value of f.

A generalization of Fermat's little theorem is the so-called Euler's congruence. To discuss it, we introduce two notions:
Given a positive integer $m > 1$, call a set of m integers $a_1, \cdots, a_m$ a

complete residue system mod m if, modulo m, these are the m integers $0, 1, \cdots, m-1$.
A *reduced residue system mod* m is a set of (distinct) integers $r_1, r_2, \cdots, r_k$ such that every integer coprime to m is congruent modulo m to exactly one of the r_i's.
The number k is denoted by $\phi(m)$ and ϕ is called the totient function.

Fact. If $\{r_1, \cdots, r_k\}$ is a reduced residue system mod m and a is an integer coprime to m, then $\{ar_1, \cdots, ar_k\}$ is also a reduced residue system mod m.
Indeed, ar_d is coprime to m for each i and, if $ar_i \equiv ar_j \bmod m$, then $r_i \equiv r_j \bmod m$. Hence, we have the assertion. This implies:

Euler's congruence. *If* m *is any positive integer, and* $(a, m) = 1$, *then* $a^{\phi(m)} \equiv 1$ *mod* m.
Proof. The sets $\{r_i \bmod m : 1 \leq i \leq \phi(m)\}$ and $\{ar_i \bmod m : 1 \leq i \leq \phi(m)\}$ are equal. Therefore,

$$a^{\phi(m)}\left(\prod_{i=1}^{\phi(m)} r_i\right) \equiv \prod_{i=1}^{\phi(m)} r_i \ mod\ m.$$

As $(\prod_{i=1}^{\phi(m)} r_i, m) = 1$, we have the asserted congruence of Euler.

Wilson's theorem. *For any positive integer* $m > 1$, *we have* $(m-1)! \equiv -1$ *mod* m *if, and only if,* m *is prime.*
Here is a proof.
Let p be prime. Observe that every integer a between 1 and $p-1$ is coprime to p and hence admits a unique multiplicative inverse b of a mod p that is between 1 and $p-1$; so $ab \equiv 1 \bmod p$.
Start by pairing each a between 1 and $p-1$ with a b as above; note that a gets paired with itself if and only if $a^2 \equiv 1 \bmod p$ which means $p|(a^2-1)$ and thus has the two solutions $a = 1, p-1$. Hence $(p-1)! \equiv 1(p-1) \equiv -1 \bmod p$.
If $m > 1$ is composite, then clearly any divisor $1 < d < m$ divides $(m-1)!$ which is, therefore, 0 mod m.

Surprisingly, Fermat's little theorem and Wilson's theorem for a prime p can be deduced from each other!
We leave "Wilson implies Fermat's little" as an exercise and discuss the opposite implication which has some new features.

We show that Fermat's little theorem implies Wilson's theorem using the so-called forward difference operator.

For a function f, one has its 'forward difference' function Δf defined as $(\Delta f)(x) = f(x+1) - f(x)$.
If $\Delta^r f$ denotes Δ iterated r times, it follows (again by induction on $n!$) that

$$(\Delta^n f)(x) = \sum_{r=0}^{n} (-1)^r \binom{n}{r} f(x+n-r).$$

Let f be a polynomial of degree $d \geq 1$. Then, observe Δf is a polynomial of degree $d-1$. Also, if f is a constant, Δf is the zero function. Therefore, if $n > d$, we have $(\Delta^n f)(x) = 0 \ \forall \ x$.
Further, $\Delta^d f$ is not any constant but the constant $d! a_d$ where a_d is the leading coefficient of f - this is seen once again by induction - this time on d.
Writing this out for the polynomial $f(x) = x^d$ gives us

$$d! = \sum_{r=0}^{d} (-1)^r \binom{d}{r} (x+d-r)^d \ \forall \ x.$$

In particular,

$$d! = \sum_{r=0}^{d-1} (-1)^r \binom{d}{r} (d-r)^d.$$

Reading the last equality

$$(p-1)! = \sum_{r=0}^{p-2} (-1)^r \binom{p-1}{r} (p-1-r)^{p-1}$$

modulo p, by Fermat's little theorem, we obtain

$$(p-1)! \equiv \sum_{r=0}^{p-2} (-1)^r \binom{p-1}{r} \ mod \ p.$$

However, $\sum_{r=0}^{p-2} (-1)^r \binom{p-1}{r} = -1$ since

$$(-1)^{p-1} + \sum_{r=0}^{p-2} (-1)^r \binom{p-1}{r} = \sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} = (1-1)^{p-1} = 0.$$

Thus, we obtain Wilson's congruence $(p-1)! \equiv -1 \bmod p$.

We mention an important congruence:

Wolstenholme's theorem. *For a prime $p > 3$, we have $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{p^2 a}{b}$ with $(pa, b) = 1$.*

Before proving this, let us introduce the notion of congruence between rational numbers.
Once that notion is introduced, Wolstenholme's theorem can be rewritten as $\sum_{r=1}^{p-1} \frac{1}{r} \equiv 0 \ mod\ p^2$ when p is a prime > 3.
Given a prime p, one can talk about a rational number a/b modulo p when p does not divide b; define :
$\frac{a}{b} + \frac{c}{d} \equiv ab' + cd' \bmod p$
where $bb' \equiv 1 \equiv dd' \bmod p$ for unique positive integers $b', d' < p$ as above.
Why does the above make sense?
First, note that when b, d are not divisible by p, we have $(bd)' \equiv b'd' \bmod p$ because

$$bd((bd)' - b'd') = (bd)(bd)' - bb'dd' \equiv 1 - 1 = 0 \ mod\ p$$

which means p divides $(bd)' - b'd'$ as p does not divide bd. Hence,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \equiv (ad + bc)(bd)'$$
$$\equiv (ad + bc)b'd' \equiv ab'dd' + cd'bb' \equiv ab' + cd' \ mod\ p.$$

Thus, congruence modulo p, respects addition and multiplication of rational numbers mod p provided we are looking at rational numbers whose denominators are not divisible by p.

Now, we proceed to prove Wolstenholme's theorem.

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$
$$= (1 + \frac{1}{p-1}) + (\frac{1}{2} + \frac{1}{p-2}) + \cdots + (\frac{1}{(p-1)/2} + \frac{1}{(p+1)/2})$$
$$= p(\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{(p-1)(p+1)/4}).$$

Now, since $p - r \equiv -r \bmod p$, we get
$\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{(p-1)(p+1)/4} \equiv \frac{-1}{1^2} + \frac{-1}{2^2} + \cdots + \frac{-1}{((p-1)/2)^2} \bmod p$.
We need to show that when $p > 3$, the right hand side is a rational number of the form pa/b.
Note that for each r between 1 and $r - 1$, $-r^2$ is congruent to exactly one term above. Thus,

$1^2 + 2^2 + \cdots + (p-1)^2 \equiv 2(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{((p-1)/2)^2}) \bmod p$.
But, the left hand side equals $\frac{(p-1)p(2p-1)}{6}$ which is clearly a multiple of p when $p \neq 2, 3$ and we have the result.

Square-root of -1 mod p.
For which primes p is it true that there exists an integer a such that $a^2 \equiv -1 \bmod p$?
We prove that this happens if, and only if, either $p = 2$ or $p \equiv 1 \bmod 4$.
If $p = 1$, the result is clear with $a = 1$.
Let p be an odd prime. If $a^2 \equiv -1 \bmod p$, then raising both sides to the $(p-1)/2$-th power, we have $a^{p-1} \equiv (-1)^{(p-1)/2} \bmod p$. By Fermat's little theorem, the LHS is 1 mod p. Hence, $(p-1)/2$ must be even; i.e. p must be 1 mod 4 for a solution to exist.
Finally, we show the main nontrivial assertion that if $p \equiv 1 \bmod 4$ is a prime, then indeed $a^2 \equiv -1 \bmod p$ does have a solution. Indeed, Wilson't congruence $(p-1)! \equiv -1 \bmod p$ can be rewritten (using $p - i \equiv -i \bmod p$ for $i \leq (p-1)/2$) as $((p-1)/2)!^2(-1)^{(p-1)/2} \equiv -1 \bmod p$. As $(p-1)/2$ is even, we have the solution $a = ((p-1)/2)!$ is a solution of $a^2 \equiv -1 \bmod p$.

Primes expressible as sums of two squares

We prove the beautiful result due to Fermat:

A prime p is expressible as $a^2 + b^2$ for integers a, b if, and only if, $p = 2$ or $p \equiv 1$ mod 4. Further, if $p \equiv 3$ mod 4 is a prime dividing a number of the form $a^2 + b^2$, then $p|a, p|b$.
Proof.
If $p = 2$, clearly we have a solution $a = b = 1$. Let $p \equiv 1 \bmod 4$. Start with t such that $t^2 \equiv -1 \bmod p$. Consider the numbers $u + tv$ as u, v vary over $0, 1, \cdots, [\sqrt{p}]$. These are $([\sqrt{p}] + 1)^2 > p$ numbers, which implies by the pigeon-hole principle that there exist two different pairs (u_1, v_1) and (u_2, v_2) such that $u_1 + tv_1 \equiv u_2 + tv_2 \bmod p$. Then $a = u_1 - u_2$ and $b = v_1 - v_2$ satisfy $a^2 \equiv -b^2 \bmod p$. Thus, $p|(a^2 + b^2)$. But, clearly $|a|, |b| < \sqrt{p}$ which implies $0 < a^2 + b^2 < 2p$. Hence $p = a^2 + b^2$.
Now, we prove the second assertion from which it will follow that primes $\equiv 3 \bmod 4$ are not expressible as sums of two squares.
Suppose $p \equiv 3 \bmod 4$ and assume $p|(a^2 + b^2)$. If $(p, a) = 1$, then get $ac \equiv 1 \bmod p$ which implies $1 \equiv a^2c^2 \equiv -(tc)^2 \bmod p$, a contradiction

of the fact that -1 cannot be a square mod such primes. Hence, $p|a$ and similarly $p|b$.

Finally, we can deduce from the above results that:

Theorem. *A positive integer n is expressible as a sum of two squares of integers if, and only if, each prime divisor of n which is $\equiv 3$ mod 4 appears with an even power.*
The necessity follows from above. For the sufficiency, one just needs to observe Brahmagupta's identity

$$(a^2+b^2)(c^2+d^2) = (ad-bc)^2 + (ac+bd)^2.$$

Now, we observe a result on solvability of linear congruences.

Proposition. *Let $m > 0$, and a, b be integers. Then, the congruence $ax \equiv b$ mod m has an integer solution for x if, and only if, (a, m) divides b. Further, if this condition is satisfied, the set of solutions is the arithmetic progression with common difference $m/(a, m)$.*
Proof.
Clearly, if x is an integer solution of the congruence $ax \equiv b \bmod m$, then there is an integer y so that $ax + my = b$. Clearly, (a, m) divides b. Conversely, if (a, m) divides b, say $b = (a, m)B$, then expressing $(a, m) = au + mv$ for some integers u, v, we have $b = a(uB) + m(vB)$. So, $ax \equiv b \bmod m$ has a solution in integers x. Finally, if x_1, x_2 are two integer solutions of $ax \equiv b \bmod m$, then $ax_1 \equiv b \equiv ax_2 \bmod m$ and so $m|a(x_1 - x_2)$. Dividing m and a by their GCD, we have that $\frac{m}{(a,m)} \Big| \frac{a}{(a,m)}(x_1 - x_2)$. As $\left(\frac{m}{(a,m)}, \frac{a}{(a,m)}\right) = 1$, it follows that $\frac{m}{(a,m)} \Big| (x_1 - x_2)$; so, any two solutions differ by a multiple of $\frac{m}{(a,m)}$. Conversely, for any integer x satisfying $ax \equiv b \bmod m$, each of the integers $x_k := x + \frac{km}{(a,m)}$ (as k varies over integers) satisfies $ax_k = ax + \frac{kam}{(a,m)} \equiv b \bmod m$.

Some Problems on Congruences from section 2.1

Q 12, P. 57. If $19|(4n^2+4)$, then $n^2 \equiv -1 \bmod 19$ which is impossible as $19 \equiv 3 \bmod 4$.

Q 26, P. 57. Note $504 = (7)(8)(9)$. Now,

$$(n^3-1)n^3(n^3+1) = n^7 - n \equiv 0 \; mod \; 7.$$

Also, if n is even, then $8|n^3$. If n is odd, then $n^3 \pm 1$ are even and one of them is a multiple of 4.
Also, if $3|n$, then $9|n^3$. If $(9, n) = 1$, then Euler's congruence shows $n^6 \equiv 1 \bmod 9$ as $\phi(9) = 6$.

Q 28,29,30, P. 57.
Each of these follows by noting that powers of a fixed integer modulo a fixed modulus is periodic by pigeon-hole principle. Hence, we have:
$2^n \bmod 10$ going as $2, 4, 8, 6, 2, \cdots$;
$3^n \bmod 10$ going as $3, 9, 7, 1, 3, \cdots$ and;
3^n modulo 100 going as $3, 9, 27, 81, 43, 29, 87, 61, 83, 49, 47, 41, 23, 69, 07, 21, 63, 89, 67, 01, 03, \cdots$
Of course, we can also use Euler's congruence for $3^n \bmod 10$ and mod 100.

Q 36, P. 58. If $p = 2, 3$ or 5, we can easily verify $(p-1)! + 1$ is a power of p. Let $p > 5$ be a prime. Then, each of the three numbers $2, (p-1)/2, p-1$ occurs separately in the product $(p-1)!$; therefore, $(p-1)^2$ divides $(p-1)!$.
Now, if $(p-1)! = p^k - 1$ for some k, then $(p-1)^2|(p^k-1)$. As we have seen, $p^k - 1 \equiv k(p-1) \bmod (p-1)^2$ (expanding p^k as $(p-1_1)^k$). Hence, we must have $(p-1)|k$ if $(p-1)! = p^k - 1$. But then $p^{p-1} - 1 \leq p^k - 1 = (p-1)!$ which is impossible as $p \geq 7$ (by induction on $n \geq 7$, we have $n^{n-1} - 1 > (n-1)!$).

Q 37, P. 58. By exercise 36, for any prime $p > 5$, we have that $(p-1)! + 1$ is not a power of p. But, it is a multiple of p by Wilson; hence, it is divisible by at least another prime different from p.

Q 44.

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!} \equiv \frac{(-1)^k k!}{k!} = (-1)^k.$$

Q 51. We need to prove that $(p-1)! \equiv p-1 \bmod (1+2+\cdots+(p-1))$ if p is a prime.

As $(p-2)! \equiv 1 \bmod p$ for $p > 2$ prime, we have

$$\frac{(p-1)! - (p-1)}{p(p-1)/2} = \frac{2((p-2)! - 1)}{p} \in \mathbb{Z}.$$

Q 52. We have to show $(p-2)! \equiv 1 \bmod p$ but that $(p-2)! - 1$ is not a power of p if $p \geq 5$.
The first assertion is clear from Wilson. For the second one, note that for odd p, considering modulo $p-1$, we have

$$(p-2)! \equiv (-1)(-2)\cdots(-(p-2)) = (-1)^{p-2}(p-2)!$$

which gives $2(p-2)! \equiv 0 \bmod p-1$.
Therefore, if $(p-2)! = 1 + p^k$ for some k, then the RHS is $\equiv 2 \bmod p-1$). Multiplying by 2, we have

$$0 \equiv 4 \; mod (p-1).$$

This gives $p = 2, 3$ or 5.

Q 15, P.63, NZM.

$$\binom{p^\alpha - 1}{k} = \binom{p^\alpha}{k} - \binom{p^\alpha - 1}{k-1}$$
$$= \binom{p^\alpha}{k} - \binom{p^\alpha}{k-1} + \binom{p^\alpha}{k-2}$$

etc. Using $\binom{p^\alpha}{k} \equiv 0 \bmod p$ if $0 < k < p^\alpha$, this gives for $k \leq p^\alpha - 1$ that

$$\binom{p^\alpha - 1}{k} \equiv (-1)^k \; mod \; p.$$

Q 16. We will prove something more general than what is asked for; this is the so-called Lucas's theorem.
Indeed, let p be a prime and write the base p expansions

$$n = n_0 + n_1 p + \cdots + n_r p^r$$
$$k = k_0 + k_1 p + \cdots + k_r p^r$$

where $0 \leq n_i, k_i < p$. Consider the polynomial $(1+x)^n \in (\mathbb{Z}/p\mathbb{Z})[X]$. Clearly

$$(1+X)^n = (1+X)^{n_0}(1+X^p)^{n_1}\cdots(1+X^{p^r})^{n_r}$$

because $(1+X)^{p^d} = 1 + X^{p^d}$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. The coefficient of X^k is $\binom{n}{k}$ looking at the LHS. Looking at the RHS, the coefficient is clearly

$$\binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_r}{k_r}.$$

Hence, we obtain Lucas's theorem: for any prime p, we have modulo p,

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_r}{k_r}.$$

Q 17. If the numbers c_i are defined by the power series identity:

$$(1 + x + \cdots + x^{p-1})/(1 - x)^{p-1} = 1 + c_1 x + c_2 x^2 + \cdots$$

we need to prove that $p|c_i$ for each i.
We simply multiply the numerator and denominator of the LHS by $1 - x$ to obtain

$$(1 - x^p)/(1 - x)^p = 1 + c_1 x + \cdots$$

Reading this power series mod p, we get

$$1 \equiv 1 + \bar{c_1} x + \bar{c_2} x^2 + \cdots$$

which clearly proves $p|c_i$ for all i.

2. (Sun-Tzu/Arybhata) Chinese remainder theorem

The strange title above alludes to the fact that the result was stated in the 3rd century by Sun-Tzu but no proof or complete method of proof was given and later Aryabhata in the 6th century gave an algorithm. The theorem generalizes the last result proved in the previous section and is the following:

CRT. *Let $n_1, \cdots, n_r$ be $r \geq 2$ positive integers which are pairwise coprime (that is, $(n_i, n_j) = 1$ for all $i \neq j$). Let $a_1, \cdots, a_r$ be arbitrary integers. Then, there exists an integer x which simultaneously satisfies the congruences $x \equiv a_i$ mod n_i for each $i = 1, \cdots, r$. Further the solution x is unique mod $n_1 n_2 \cdots n_r$.*

Proof.
Firstly, notice that the last assertion is easy to see because the difference of any two solutions is a multiple of each n_i and hence, of the product $n_1 n_2 \cdots n_r$ which is their LCM.
For the existence, we give two proofs - one existential and the other constructive.

First Proof. For any positive integer n, let us use the symbol $\mathbb{Z}_n$ to denote the set $\{1, 2, \cdots, n\}$. Then, for $n = n_1 n_2 \cdots n_r$, we have a "function"

$$T : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_r}$$

given by

$$b \mapsto (b_1, b_2, \cdots, b_r)$$

where b_i is the unique element of $\mathbb{Z}_{n_i}$ such that $b \equiv b_i$ mod n_i. We see that T is a 1-1 function because if $T(b) = T(c)$, then $b - c \equiv 0$ mod n_i for each $i \leq r$; so, $b - c \equiv 0$ mod $n_1 n_2 \cdots n_r$ as the LCM of the n_i's is their product. Now, both sides have the same number n of elements; so, any 1-1 map must be onto. Finally, each $a_i \equiv b_i \in \mathbb{Z}_{n_i}$ for a unique b_i. Hence, if $T(a) = (b_1, \cdots, b_r)$, then $a \equiv a_i$ mod n_i for each $i \leq r$.

Second Proof. Let $m_i = n/n_i = \prod_{j \neq i} n_j$. Then, for each $i \leq r$, we have $(m_i, n_i) = 1$ by the assumption of pairwise coprimality of the m_j's. Then, we know that there exists m_i' such that $m_i m_i' \equiv 1$ mod n_i for each $i \leq r$. Also, clearly $n_j | m_i$ for each $j \neq i$. Consider the integer

$$a = a_1 m_1 m_1' + a_2 m_2 m_2' + \cdots + a_r m_r m_r'.$$

Clearly, $a \equiv a_i$ mod n_i for each $i \leq r$. This finishes the proof.

Proposition. *Let k, n be arbitrary positive integers and suppose a_{ij} are integers (for $1 \leq i \leq k, 1 \leq j \leq n$). Suppose $m_1, \cdots, m_k$ are pairwise coprime integers and $b_1, \cdots, b_r$ be arbitrary integers. Then, the k simultaneous congruences*

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \ (mod\ m_1),$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \ (mod\ m_2),$$

$$\cdots\cdots\cdots\cdots$$

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n \equiv b_k \ (mod\ m_k)$$

have a solution in integers $x_1, \cdots, x_n$ if and only if, for each $i \leq k$, the GCD of $a_{i1}, a_{i2}, \cdots, a_{in}, m_i$ divides b_i.

Proof.

We apply induction on k to prove the theorem. The proof is constructive modulo the Euclidean division algorithm (which is also constructive).

Consider first the case $k = 1$.

If the integers $x_1, \cdots, x_n$ satisfy the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \ (mod\ m_1),$$

we have $\sum_{j=1}^{n} a_{1j}x_j - b_1 = m_1 t$ for some integer t. Thus, the greatest common divisor of $a_{11}, a_{12}, \cdots, a_{1n}$ and m_1 divides b_1. This condition is also sufficient by the Euclidean division algorithm. For, if $b_1 = sd$ where $d = \mathrm{GCD}(a_{11}, \cdots, a_{1n}, m_1)$, then writing

$$d = \sum_{j=1}^{n} a_{1j}y_j + m_1 t,$$

we have a solution $x_1 = sy_1, \cdots, x_n = sy_n$ of the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \ (mod\ m_1).$$

Therefore, for a general k, a necessary condition for a common solution is that, for each $i \leq k$, the GCD of $a_{i1}, a_{i2}, \cdots, a_{in}, m_i$ divides b_i.

This condition also ensures that each individual congruence has a solution.

Now, we suppose that the GCD condition suppose we have already gotten a common solution $x_1, \cdots, x_n$ in integers for the first r congruences $(1 \leq r < k)$:

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \equiv b_i \ (mod\ m_i) \ \forall\ 1 \leq i \leq r.$$

Now, we first choose a solution $y_1, \cdots, y_n$ of the $(r+1)$-th congruence

$$a_{r+1,1}x_1 + a_{r+1,2}x_2 + \cdots + a_{r+1,n}x_n \equiv b_{r+1} \ (mod\ m_{r+1}).$$

For each $j \leq n$, choose X_j such that

$$m_1 m_2 \cdots m_r X_j \equiv y_j - x_j \ (mod\ m_{r+1}).$$

These choices are possible because $m_1 m_2 \cdots m_r$ and m_{r+1} relatively prime. We observe that for the new choices

$$x'_j = x_j + m_1 m_2 \cdots m_r X_j \ (1 \leq j \leq n),$$

the first r congruences continue to hold. Moreover,

$$\sum_{j=1}^{n} a_{r+1,j} x'_j \equiv \sum_{j=1}^{n} a_{r+1,j}(x_j + m_1 m_2 \cdots m_r X_j)$$

$$\equiv \sum_{j=1}^{n} a_{r+1,j} y_j \equiv b_{r+1} \ (mod\ m_{r+1}).$$

Therefore, the theorem is proved by induction.

Remarks.

(I) The classical Chinese remainder theorem can be thought of as the special case when the matrix $\{a_{ij}\}$ has only a single column which is non-zero.
(II) If the matrix $\{a_{ij}\}$ has a left inverse (that is an $n \times k$ integer matrix $\{b_{ij}\}$ such that $BA = I_n$, then clearly the necessary condition of the theorem holds for any choice of $b_1, \cdots, b_k$.
In particular, if $k = n$ and $\{a_{ij}\}$ is an $n \times n$ integral matrix whose inverse is also integral, each system of n linear congruences in n variables with pairwise co-prime moduli has a solution.
(III) A special case of the above theorem which is of interest as it produces a solution for arbitrary b_i's, is the following one. In the theorem above, if, for each $i \leq k$, there is some j for which a_{ij} is coprime to m_i, then the necessary condition obviously holds.
(IV) In the classical case of one variable, there is a unique solution modulo $m_1 m_2 \cdots m_k$. In the multivariable case, there is no natural uniqueness assertion possible. The point is that homogeneous congruences in more than one variable have many solutions. So, uniqueness can be asked for only after specifying a box (more precisely, an n-dimensional parallelotope) in which we seek solutions.
For example, both $(1, 4)$ and $(0, -1)$ are simultaneous solutions of the congruences

$$x - y \equiv 1 \ (mod\ 2),$$
$$x + y \equiv 2 \ (mod\ 3).$$