Numbers Made Dumber

Rohan Baijal
Vivek Kumar Singh
Yatharth Goswami

Lecture 3

13-05-2021

1.1 Modular Arithmetic

Many problems involving large integers can be simplified by a technique called *modular arithmetic*, where we use congruences in place of equations. The basic idea is to choose an integer n and replace every integer with its remainder when divided by n.

Using this technique we can often answer questions related to calendars, etc. Let's consider one example though.

Example 1.1.

Is 22051946 a perfect square? Instead of using square roots or brute force checking, let us make an important observation.
A perfect square must leave remainder 1 or 0 when divided by 4.
Here, by looking at the last 2 digits (46), we notice that the remainder will be 2. Hence, the number is not a square. Simple!
NOTE : Had the remainder been 1 or 0, we would have had to use other methods to verify if the number is a perfect square.

Exercise 1.1.

Show that the last decimal digit of a perfect square cannot be 2, 3, 7 or 8.

Definition Let n be a positive integer, and let a and b be any integers. We say that a is congruent to b mod (n), or a is a residue of b mod (n), written

$$a \equiv b \ mod \ (n),$$

if a and b leave the same remainder when divided by n. (Other notations for this include $a \equiv b$ (mod n) and $a \equiv_n b$; we will often use simply $a \equiv b$ if the value of n is understood.) To be more precise, we use the division algorithm to put $a = qn + r$ with $0 \leq r < n$, and $b = q'n + r'$ with $0 \leq r' < n$, and then we say that $a \equiv b$ mod (n) if and only if $r = r'$.

Lemma 1.1.1. *For any fixed $n \geq 1$ we have $a \equiv b \ mod \ (n)$ if and only if $n|(a - b)$.*

Proof. Putting $a = qn + r$ and $b = q'n + r'$ as above, we have $a - b = (q - q')n + (r - r')$ with $-n < r - r' < n$. If $a \equiv b$ mod (n) then $r = r'$, so $r - r' = 0$, and $a - b = (q - q')n$, which is divisible by n. Conversely, if n divides $a - b$ then it divides $(a - b) - (q - q')n = r - r'$; now the only integer strictly between $-n$ *and* n which is divisible by n is 0, so $r - r' = 0$, giving $r = r'$ and hence $a \equiv b$ mod (n). □

Lemma 1.1.2. *For any fixed $n \geq 1$*
(a) $a \equiv a$ for all integers a.
(b) if $a \equiv b$ then $b \equiv a$.
(c) if $a \equiv b$ and $b \equiv c$, then $a \equiv c$.

Proof. (a) We have $n|(a - a) \forall a$.
(b) If $n|(a - b)$ *then* $n|(b - a)$.
(c) If $n|(a - b)$ and $n|(b - c)$ then $n|(a - b) + (b - c) = a - c$. □

These three properties are the reflexivity, symmetry and transitivity axioms for an equivalence relation, so Lemma 1.1.2 proves that for each fixed n, congruence mod (n) is an equivalence relation on $\mathbb{Z}$. It follows that $\mathbb{Z}$ is partitioned into disjoint equivalence classes; these are the congruence classes

$$[a] = \{b \in \mathbb{Z} | a \equiv b \mod (n)\} = \{..., a-2n, a-n, a, a+n, a+2n\}$$

for $a \in \mathbb{Z}$. (If we want to emphasise the particular value of n being used, we can use the notation $[a]_n$ here.) Each class corresponds to one of the n possible remainders $r = 0, 1, ..., n-1$ on division by n, so there are n different congruence classes. They are

$$\begin{aligned} [0] &= \{..., -2n, -n, 0, n, 2n, ...\} \\ [1] &= \{..., 1-2n, 1-n, 1, 1+n, 1+2n, ...\} \\ [n-1] &= \{..., -n-1, -1, n-1, 2n-1, ...\} \end{aligned}$$

There are no further classes distinct from these: for example, [0] = [n].
More generally, $[a] = [b]$ iff $a \equiv b \mod (n)$.

When n = 1 all integers are congruent to each other, so there is a single congruence class, coinciding with $\mathbb{Z}$. When $n = 2$ the two classes $[0] = [0]_2$ *and* $[1] = [1]_2$ consist of the even and odd integers respectively.

For a given $n \geq 1$, we denote the set of n equivalence classes mod (n) by $\mathbb{Z}_n$, known as the set of integers mod (n). Our next aim is to show how to do arithmetic with these congruence classes, so that $\mathbb{Z}_n$ becomes a number system with properties very similar to those of $\mathbb{Z}$. We do this by using the operations of addition, subtraction and multiplication in $\mathbb{Z}$ to define the corresponding operations on the congruence classes in $\mathbb{Z}_n$. If [a] and [b] are elements of $\mathbb{Z}_n$ (that is, congruence classes mod (n)), we define their sum, difference and product to be the classes

$$\begin{aligned} [a] + [b] &= [a+b], \\ [a] - [b] &= [a-b], \\ [a][b] &= [ab] \end{aligned}$$

The problem of division is left for later because a/b need not always be an integer.

Before going further, we need to show that these three operations are well- defined, in the sense that the right-hand sides of the three equations defining them depend only on the classes $[a]$ and $[b]$, and not on the particular elements a and b we have chosen from those classes. More specifically, we must show that if $[a] = [a']$ and $[b] = [b']$, then $[a+b] = [a'+b']$, $[a-b] = [a'-b']$ and $[ab] = [a'b']$. These follow immediately from the following result:

Lemma 1.1.3. *For a given $n \geq 1$, if $a' \equiv a$ and $b' \equiv b$ then $a'+b' \equiv a+b$, $a'-b' \equiv a-b$ and $a'b' \equiv ab$.*

Proof. If $a' \equiv a$ then $a' = a + kn$ for some integer k, and similarly we have $b' = b + ln$ for some integer l; then $a' \pm b' = (a \pm b) + (k \pm l)n \equiv a \pm b$, and $a'b' = ab + (al + bk + kln)n \equiv ab$.
□

It follows that addition, subtraction and multiplication of pairs of classes in $\mathbb{Z}_n$ are all well-defined. In particular, by repeated use of the addition and multiplication parts of this lemma

we can define arbitrary finite sums, products and powers of classes in $\mathbb{Z}_n$ by

$$[a_1] + [a_2] + ... + [a_k] = [a_1 + a_2 + ... + a_k]$$
$$[a_1][a_2]...[a_k] = [a_1 a_2 ... a_k]$$
$$[a]^k = [a^k]$$

for any integer $k \geq 2$.

To emphasise why we have to be so careful about checking that the operations of arithmetic in $\mathbb{Z}_n$ are well-defined, let us look at what happens if we try to define exponentiation of classes in $\mathbb{Z}_n$ in the obvious way. We could define

$$[a]^{[b]} = [a^b]$$

restricting b to non-negative values to ensure a^b is an integer. If we take $n = 3$, this gives

$$[2]^{[1]} = [2^1] = [2].$$

unfortunately, $[1] = [4]$ in $\mathbb{Z}_3$ and out definition would also give us

$$[2]^{[4]} = [2^4] = [16] = [1] \neq [2];$$

thus we can get different congruence classes for $[a]^{[b]}$ by choosing different elements b and b' in the same class $[b]$, namely $b = 1$ and $b' = 4$. This is because $a' \equiv a$ and $b' \equiv b$ do not imply $(a')^{b'} \equiv ab$, so exponentiation of congruence classes is not well-defined. We therefore confine arithmetic in $\mathbb{Z}_n$ to operations which are well-defined, like addition, subtraction, multiplication and powers; we shall see later that a restricted form of division can also be defined.
A set of n integers, containing one representative from each of the n congruence classes in $\mathbb{Z}_n$, is called a complete set of residues mod (a). A sensible choice of such a set can ease calculations considerably. One obvious choice is provided by the division algorithm: we can divide any integer a by n to give $a = qn + r$ for some unique r satisfying $0 \leq r < n$; thus each class $[a] \in \mathbb{Z}_n$ contains a unique $r = 0, 1, ..., n-1$, so these n integers form a complete set of residues, called the *least non-negative residues* mod (n). For many purposes these are the most convenient residues to use, but sometimes it is better to replace it with a remainder r satisfying $-n/2 < r \leq n/2$. These remainders are the *least absolute residues* mod (n), those with least absolute value; when n is odd they are $0, 1, 2, ..., (n-1)/2$, and when n is even they are $0, 1, 2, ..., (n-2)/2, n/2$. The following calculations illustrate these complete sets of residues.

Example 1.2. C alculate the least non-negative residue of 28×33 mod 35
Notice $28 \equiv -7$ and $33 \equiv -2$. Using Lemma (?),

$$28 \times 33 \equiv (-7) \times (-2) \equiv 14.$$

Since $0 \leq 14 < 35$, 14 is the required least non-negative residue.

Example 1.3. C alculate the least absolute residue of 15×59 mod 75.
We have $15 \times 59 \equiv 15 \times (-16)$. We can do this in several stages now. Thus

$$15 \times (-16) = 15 \times (-4) \times 4 = (-60) \times 4 \equiv 15 \times 4 \equiv -15.$$

And since $-75/2 < -15 \leq 75/2$, the required residue is -15.

Exercise 1.2. (a). Calculate the least non-negative residue of $3^8 \mod (13)$.
(b). Find the remainder when 5^{10} is divided by 19.
(c). Find the final decimal digit of $1! + 2! + 3! + ... + 10!$.

Since n divides m iff $m \equiv 0 \mod (n)$, it follows that problems about divisibility are equivalent to problems about congruences, and these can be easier to solve sometimes.

Exercise 1.3.
Prove that $a(a+1)(2a+1)$ is divisible by 6.
Hint. Try to work with cases using least absolute residues.
Find a quicker proof for this by observing that $6|m$ iff $2|m$ and $3|m$.

Theorem 1.1.4. *Let n have prime-power factorisation*

$$n = p_1^{e_1}...p_k^{e_k},$$

where $p_1, ..., p_k$ are distinct primes. Then, for any integers a and b we have $a \equiv b \mod (n)$ iff $a \equiv b \mod (p_i^{e_i})$ for each $i = 1, 2, ..., k$.

This will later be proved as a corollary of the Chinese Remainder Theorem.

Lemma 1.1.5. *Let $f(x)$ be a polynomial with integer coefficients, and let $n \geq 1$. If $a \equiv b \mod (n)$ then $f(a) \equiv f(b) \mod (n)$.*

Proof. Write $f(x) = c_0 + c_1x + ... + c_kx^k$, where each $c_i \in \mathbb{Z}$. If $a \equiv b \mod (n)$, then repeated use of Lemma (?) implies that $a^i \equiv b^i$ for all $i \geq 0$, so $c_ia^i \equiv c_ib^i$ for all i and hence $f(a) = \sum c_ia^i \equiv \sum c_ib^i = f(b)$. □

For an illustration of this, consider Exercise 1.3 where we take $f(x) = x(x+1)(2x+1) = 2x^3 + 3x^2 + x$ and $n = 6$; Now if $a \equiv 0, \pm1, \pm2$ or 3 then $f(a) \equiv f(0), f(\pm1), f(\pm2)$ or $f(3)$, and all of those are congruent to 0 mod(6).

Suppose that a polynomial $f(x)$, with integer coefficients, has an integer root $x = a \in \mathbb{Z}$, so that $f(a) = 0$. It follows then that $f(a) \equiv 0 \mod (n)$ for all integers $n \geq 1$. We can often use the contrapositive of this to show that certain polynomials $f(x$ have no integer roots: if there exists an integer $n \geq 1$ such that the congruence $f(x) \equiv 0 \mod (n)$ has no solutions x, then the equation $f(x) = 0$ can have no solutions x. If n is small we can check whether $f(x) \equiv 0 \mod (n)$ has any solutions simply by evaluating $f(x_1), ..., f(x_n)$ where $x_1...., x_n$ form a complete set of residues mod (n): each $x \in \mathbb{Z}$ is congruent to some x_i, so Lemma 1.1.5 implies that $f(x) \equiv f(x_i)$, and we simply determine whether any of $f(x_1), ..., f(x_n)$ is divisible by n.

Example 1.4.
Prove that the polynomial $f(x) = x^5 - x^2 + x - 3$ has no integer roots.
Take $n = 4$ and consider the congruence $f(x) \equiv 0 \mod (4)$.
Using the least absolute residues -1,0,1,2 we find that

$$f(0) = -3, f(1) = -2, f(-1) = -6, f(2) = 27$$

None of these values is divisible by 4, so the congruence $f(x) \equiv 0 \mod(4)$ has no solutions and hence the polynomial $f(x)$ has no integer roots.
NOTE : Choosing $n = 4$ is a matter of trial-and-error or insight or experience. You can see that for $n < 4$, the congruence does have a solution.

Exercise 1.4. Prove that the following polynomials have no integer roots:
(a) $x^3 - x + 1$
(b) $x^3 + x^2 - x + 1$
(c) $x^3 + x^2 - x + 3$

However, this method doesn't always work. For example

$$f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$$

clearly has no integer roots. However, some advanced techiques will tell you that for every integer $n \geq 1$ there is a solution of $f(x) \equiv 0 \bmod(n)$, so in this case, there is no suitable choice of n.

Theorem 1.1.6. *There is no non-constant polynomial $f(x)$, with integer coefficients, such that $f(x)$ is prime for all integers x.*

Proof. Suppose that $f(x)$ is prime for all integers x, and is not constant. If we choose any integer a, then $f(a)$ is a prime$p$. For each $b \equiv a \bmod (p)$, Lemma 1.1.5 implies that $f(b) \equiv f(a) \bmod (p)$, so $f(b) \equiv 0 \bmod (p)$ and hence p divides $f(b)$. By our hypothesis, $f(b)$ is prime, so $f(b) = p$. There are infinitely many integers $b \equiv a \bmod (p)$, so the polynomial $g(x) = f(x) - p$ has infinitely many roots. However, this is impossible: having degree $d \geq 1$, $g(x)$ can have at most d roots, so such a polynomial $f(x)$ cannot exist. □

Earlier we saw that if a and b are coprime then the linear polynomial $f(x) = ax+b$ has infinitely many prime values, but it is not known whether any polynomial of degree $d \geq 2$ can have this property.

1.2 Linear Congruences

We now return to the question of division of congruence classes, postponed from earlier in this lecture. In order to assign a meaning to a quotient $[b]/[a]$ of two congruence classes $[a], [b] \in \mathbb{Z}_n$, we need to consider the solutions of the linear congruence $ax \equiv b \mod n$. Note that if x is a solution, and if $x' \equiv x$, then $ax' \equiv ax \equiv b$ and so x' is also a solution; thus the solutions (if they exist) form a union of congruence classes. Now $ax \equiv b \mod n$ if and only if $ax - b$ is a multiple of n, so x is a solution of this linear congruence if and only if there is integer y such that x and y satisfy the linear Diophantine equation $ax + ny = b$.

Theorem 1.2.1. *If $d = gcd(a, n)$, then the linear congruence*

$$ax \equiv b \mod n$$

has a solution if and only if d divides b. If d does divide b, and if x_0 is any solution, then the general solution is given by

$$x = x_0 + \frac{nt}{d}$$

where $t \in \mathbb{Z}$; in particular, the solutions form exactly d congruence classes mod(n), with representatives

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{n(d-1)}{d}$$

Proof. To prove this, note that

$$x_0 + \frac{nt}{d} \equiv x_0 + \frac{nt'}{d} \mod n$$

if and only if n divides $n(t-t')/d$, that is, if and only if d divides $t-t'$, so the congruence classes of solutions $\mod n$ are obtained by letting t range over a complete set of residues $\mod d$, such as $0, 1, \ldots, d-1$. □

Corollary 1.2.1.1. *If $gcd(a,n) = 1$ then the solutions x of the linear congruence $ax \equiv b \mod n$ form a single congruence class $mod(n)$.*

This means that if a and n are coprime then for each b there is a unique class $[x]$ such that $[a][x] = [b]$ in $\mathbb{Z}_n$; we can regard this class $[x$ as the quotient class $[b]/[a]$ obtained by dividing $[b]$ by $[a]$ in $\mathbb{Z}_n$. If $d = gcd(a,n) > 1$, however, there is either more than one such class $[x]$ (when d divides b), or there is no such class (when d does not divide b), so we cannot define a quotient class $[b]/[a]$ in this case.

Lemma 1.2.2. *1. Let m divide a, b and n, and let $a' = a/m, b' = b/m$ and $n' = n/m$; then*

$$ax \equiv b \mod n \quad \text{if and ony if} \quad a'x \equiv b' \mod n'$$

2. Let a and n be coprime, let m divide a and b, and let $a' = a/m$ and $b' = b/m$ then

$$ax \equiv b \mod n \quad \text{if and only if} \quad a'x \equiv b' \mod n$$

Proof. 1. We have $ax \equiv b \mod n$ if and only if $ax - b = qn$ for some integer q; dividing by m, we see that this is equivalent to $a'x - b' = qn'$, that is, to $a'x \equiv b' \mod n'$.

2. If $ax \equiv b \mod n$, then as in (a) we have $ax - b = qn$ and hence $a'x - b' = qn/m$; in particular, m divides qn. Now m divides a, which is coprime to n, so m is also coprime to n and hence m must divide q. Thus $a'x - b' = (q/m)n$ is a multiple of n, so $a'x \equiv b' \mod n$. For the converse, if $a'x \equiv b' \mod n$ then $a'x - b' = q'n$ for some integer q', so multiplying through by m we have $ax - b = mq'n$ and hence $ax \equiv b \mod n$.

□

We now give an algorithm to solve the linear congruence $ax \equiv b \mod (n)$.

Step 1. We calculate $d = gcd(a,n)$, and see whether d divides b. If it does not, there are no solutions, so we stop. If it does, we go on to step 2.
Theorem 1.2.1 gives us the general solution, provided we can find a particular solution x_0, so from now on we concentrate on a method for finding x_0. The general strategy is to reduce $|a|$ until $a = \pm 1$, since in this case the solution $x_0 = \pm b$ is obvious.

Step 2. Since d divides a, b and n, Lemma 1 implies that we can replace the original congruence with

$$a'x \equiv b' \mod n$$

where $a' = a/d$, $b' = b/d$ and $n' = n/d$ and a' and n' are coprime.

Step 3. We can therefore use Lemma 2 to divide this new congruence through by $m = gcd(a', b')$, giving a congruence

$$a''x \equiv b'' \mod n$$

where $a''(= a'/m)$ is coprime to both $b''(= b'/m)$ and n'. If $a'' = \pm 1$ then $x_o = \pm b''$ is the required solution. Otherwise, we go on to step 4.

Step 4. Noting that

$$b'' \equiv b'' \pm n' \equiv b'' \pm 2n' \equiv \ldots \mod n',$$

we may be able to replace b'' with some congruent number $b''' = b'' + kn'$ such that $gcd(a'', b''') > 1$; by applying step 3 to the congruence $a''x \equiv b'''$ mod n' we can again reduce $|a''|$. An alternative at this stage is to multiply through by some suitably chosen constant c, giving $ca''x \equiv cb''$ mod n'; if c is chosen so that the least absolute residue a''' of ca'' satisfies $|a'''| < |a''|$, then we have reduced $|a''|$ to give a linear congruence $a'''x \equiv b'''$ mod n' with $b''' = cb''$.
A combination of the methods in step 4 will eventually reduce a to ± 1, in which case the solution x_0 can be read off; then Theorem 1.2.1 gives the general solution.

Example 1.5. Consider the congruence

$$10x \equiv 6 \mod 14$$

Step 1 gives $gcd(10, 14) = 2$, which divides 6, so solutions do exist. If x_0 is any solution, then the general solution is $x = x_0 + (14/2)t = x_0 + 7t$, where $t \in \mathbb{Z}$; these form the congruence classes $[x_0]$ and $[x_0 + 7]$ in $\mathbb{Z}_{14}$ To find x_0 we use step 2: we divide the original congruence through by $gcd(10, 14) = 2$ to give

$$5x \equiv 10 \mod 7$$

and then divide by 5 (which is coprime to 7) to give

$$x \equiv 2 \mod 7$$

Thus $x_0 = 2$ is a solution, so the general solution has the form

$$x = 2 + 7t \quad (t \in \mathbb{Z}).$$

1.3 Simultaneous Linear Congruences

We will now consider the solutions of simultaneous congruences. In the 1st century AD, the Chinese mathematician Sun-Tsu considered problems like 'find a number which leaves remainders $2, 3, 2$ when divided by $3, 5, 7$ respectively. Equivalently, he wanted to find x such that the congruences

$$x \equiv 2 \text{ mod } (3), x \equiv 3 \text{ mod } (5), x \equiv 2 \text{ mod } (7)$$

Theorem 1.3.1. *Let $n_1, n_2, \cdots, n_k$ be positive integers, with $gcd(n_i, n_j) = 1$ whenever $i \neq j$, and let $a_1, a_2, \cdots, a_k$ be any integers. Then the solutions of the simultaneous congruences*

$$x \equiv a_1 \text{ mod } (n_1), x \equiv a_2 \text{ mod } (n_2), \cdots, x \equiv a_k \text{ mod } (n_k)$$

form a single congruence class mod (n), where $n = n_1 n_2 \cdots n_k$.

Proof. Let $c_i = n/n_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ for each $i = 1, \cdots, k$. Since each of its factors $n_j (j \neq i)$ is coprime to n_i, so is c_i, Corollary 1.2.1.1 therefore implies that for each i, the congruence $c_i x \equiv 1$ mod (n_i) has a single congruence class $[d_i]$ of solutions mod (n_i). We now claim that the integer

$$x_0 = a_1 c_1 d_1 + \cdots + a_k c_k d_k$$

simultaneously satisfies the given congruences, that is, $x_0 \equiv a_i$ mod (n_i) for each i. To see this, note that each c_j (other than c_i) is divisible by n_i, so $a_j c_j d_j \equiv 0$ and hence $x_0 \equiv a_i c_i d_i$ mod (n_i); now $c_i d_i \equiv 1$, by choice of d_i , so $x_0 \equiv a_i$ as required. Thus $x_0$is a solution of the simultaneous congruences, and it immediately follows that the entire congruence class $[x_0]$ of x_0 mod (n) consists of solutions.
To see that this class is unique, suppose that x is any solution; then $x \equiv a_i \equiv x_0$ mod (n_i) for all i, so each n_i divides $x - x_0$. Since $n_1, \cdots, n_k$ are mutually coprime, their product n also divides $x - x_0$, so $x \equiv x_0$ mod (n). □

Note that the proof of the Chinese Remainder Theorem does not merely show that there is a solution for the simultaneous congruences; it also gives us a formula for a particular solution x_0, and hence for the general solution $x = x_0 + nt (t \in \mathbb{Z})$.

Example 1.6.

$$x \equiv 2 \bmod (3), x \equiv 3 \bmod (5), x \equiv 2 \bmod (7)$$

We can also use the Chinese Remainder Theorem as the basis for a second method for solving simultaneous linear congruences, which is less direct but often more efficient. We start by finding a solution $x = x_1$ of one of the congruences. It is usually best to start with the congruence involving the largest modulus, so we could start with $x \equiv 2 \bmod (7)$, which has $x_1 = 2$ as an obvious solution. The remaining solutions of this congruence are found by adding or subtracting multiples of 7, and among these we can find an integer $x_2 = x_1 + 7t$ which also satisfies the second congruence $x \equiv 3 \bmod (5)$: trying $x_1, x_1 \pm 7, x_1 \pm 14, \cdots$ in turn, we soon find $x_2 = 2 - 14 = -12$. This satisfies $x \equiv 2 \mod (7)$ and $x \equiv 3 \mod (5)$, and by the Chinese Remainder Theorem, the general solution of this pair of congruences has the form $x_2 + 35t = -12 + 35t (t \in \mathbb{Z})$. Trying $x_2, x_2 \pm 35, x_2 \pm 70, \cdots$ in turn, we soon find a solution $x_3 = -12 + 35t$ which also satisfies the third congruence $x \equiv 2 \mod (3)$, namely $x_3 = -12 + 35 = 23$. This satisfies all three congruences, so by the Chinese Remainder Theorem their general solution consists of the congruence class $[23] \mod (105)$.

Exercise 1.5.
Solve the simultaneous congruences

$$x \equiv 1 \bmod (4), x \equiv 2 \bmod (3), x \equiv 3 \bmod (5)$$

Exercise 1.6.
Solve the simultaneous congruences

$$3x \equiv 6 \bmod (12), 2x \equiv 5 \bmod (7), 3x \equiv 1 \bmod (5)$$

Exercise 1.7.
Solve the linear congruences

$$13x \equiv 71 \bmod (380)$$

1.4 Simultaneous non-linear congruences

It is sometimes possible to solve simultaneous congruences by the Chinese Remainder Theorem, even when the congruences are not all linear.

Example 1.7.
Consider the simultaneous congruences

$$x^2 \equiv 1 \mod (3) \text{ and } x \equiv 2 \mod (4).$$

By inspection of the three congruence classes mod (3), we see that the first of these (which is not linear) is equivalent to $x \equiv 1$ or $2 \mod (3)$, so the pair of congruences are equivalent to

$$x \equiv 1 \text{ or } x \equiv 2 \mod (3), \text{ and } x \equiv 2 \mod (4).$$

We now have two pairs of simultaneous linear congruences, and each pair can be solved by using the Chinese Remainder Theorem. The first pair has general solution $x \equiv -2 \mod (12)$, while the second pair has general solution $x \equiv 2 \mod (12)$, so our original pair of congruences has general solution $x \equiv \pm 2 \mod (12)$.

Exercise 1.8.
Solve the simultaneous congruences

$$x^2 + 2x + 2 \equiv 0 \mod (5) \text{ and } 7x \equiv 3 \mod (11).$$

The Chinese Remainder Theorem is useful for solving polynomial congruences when the modulus is composite.

Theorem 1.4.1. *Let $n = n_1 \cdots n_k$ where the integers n_i are mutually co-prime, and let $f(x)$ be a polynomial with integer coefficients. Suppose that for each $i = 1, \cdots, k$ there are N_i congruence classes $x \in \mathbb{Z}_{n_i}$ such that $f(x) \equiv 0 \mod (n_i)$. Then there are $N = N_1 \cdots N_k$ classes $x \in \mathbb{Z}_n$ such that $f(x) \equiv 0 \mod (n)$.*

Proof. Since the moduli n_i are mutually coprime, we have $f(x) \equiv 0 \mod (n)$ if and only if $f(x) \equiv 0 \mod (n_i)$ for all i. Thus each class of solutions $x \in \mathbb{Z}_n$ of $f(x) \equiv 0 \mod (n)$ determines a class of solutions $x = x_i \in \mathbb{Z}_{n_i}$ of $f(x_i) \equiv 0 \mod (n_i)$ for each i. Conversely, if for each i we have a class of solutions $x_i \in \mathbb{Z}_{n_i}$ of $f(x_i) \equiv 0 \mod (n_i)$, then by the Chinese Remainder Theorem there is a unique class $x \in \mathbb{Z}_n$ satisfying $x \equiv x_i \mod (n_i)$ for all i, and this class satisfies $f(x) \equiv 0 \mod (n)$. Thus there is a one-to-one correspondence between classes $x \in \mathbb{Z}_n$ satisfying $f(x) \equiv 0 \mod (n)$, and k-tuples of classes $x_i \in \mathbb{Z}_{n_i}$ satisfying $f(x_i) \equiv 0 \mod (n_i)$ for all i. For each i there are N_i choices for the class $x_i \in \mathbb{Z}_{n_i}$, so there are $N_1 \cdots N_k$ such k-tuples and hence this is the number of classes $x \in \mathbb{Z}_n$ satisfying $f(x) \equiv 0 \mod (n)$. □

Example 1.8.
Putting $f(x) = x^2 - 1$, let us find the number N of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \mod (n)$. We first count solutions of $x^2 \equiv 1 \mod (p^e)$, where p is prime. If p is odd, then there are just two classes of solutions: clearly the classes $x \equiv \pm 1$ both satisfy $x^2 \equiv 1$, and conversely if $x^2 \equiv 1$ then p^e divides $x^2 - 1 = (x-1)(x+1)$ and hence (since $p > 2$) it divides $x - 1$ or $x + 1$, giving $x \equiv \pm 1$. If $p^e = 2$ or 4 then there are easily seen to be one or two classes of solutions, but if $p^e = 2^e \geq 8$ then a similar argument shows that there are four, given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$: for any solution x, one of the factors $x \pm 1$ must be congruent to 2 mod (4), so the other factor must be divisible by 2^{e-1} . Now in general let n have prime-power factorisation $n_1 \cdots n_k$, where $n_i = p_i^{e_i}$ and each $e_i \geq 1$. We have just seen that for each odd p_i there are $N_i = 2$ classes in $\mathbb{Z}_{n_i}$ of solutions of $x_2 \in 1 \mod (n_i)$, whereas if $p_i = 2$, we may have $N_i = 1, 2$ or 4, depending on e_i By Theorem 1.4.1 there are $N = N_1 \cdots N_k$ classes in $\mathbb{Z}_n$ of solutions of $x2 \equiv 1 \mod (n)$, found by solving the simultaneous congruences $x_2 \equiv 1 \mod (n_i)$. Substituting the values we have obtained for N_i, we therefore have

$$N = \begin{cases} 2^{k+1} & n \equiv 0 \mod (8) \\ 2^{k-1} & n \equiv 2 \mod (4) \\ 2^k & \text{otherwise} \end{cases}$$

where k is the number of distinct primes dividing n. For instance, if $n = 60 = 22.3.5$ then $k = 3$ and there are $2k = 8$ classes of solutions, namely $x \equiv \pm 1, \pm 11, \pm 19, \pm 29 \mod (60)$.

Exercise 1.9.
How many classes of solutions are there for each of the following congruences?

1. $x^2 - 1 \equiv 0 \mod (168)$
2. $x^2 + 1 \equiv 0 \mod (70)$
3. $x^2 + x + 1 \equiv 0 \mod (91)$
4. $x^3 + 1 \equiv 0 \mod (140)$

1.5 Extension of Chinese Remainder Theorem

Our final result, known to Yih-Hing in the 7th century AD, generalises the Chinese Remainder Theorem to the case where the moduli are not necessarily coprime. First we consider a simple illustration:
Let us consider under what circumstances any pair of simultaneous congruences

$$x \equiv a_1 \mod 9 \quad \text{and} \quad x \equiv a_2 \mod 6$$

have a solution. The greatest common divisor of the moduli 9 and 6 is 3, and the two congruences imply that

$$x \equiv a_1 \mod 3 \quad \text{and} \quad x \equiv a_2 \mod 3$$

so if a solution exists then $a_1 \equiv a_2 \mod 3$, that is, 3 divides $a_1 - a_2$ Conversely, suppose that 3 divides $a_1 - a_2$, so $a_1 = a_2 + 3c$ for some integer c. Then the general solution of the first congruence $x \equiv a_1 \mod 9$ has the form

$$x = a_1 + 9s = a_2 + 3c + 9s = a_2 + 3(c + 3s) \quad \text{where} \quad s \in \mathbb{Z}$$

while the general solution of the second congruence $x \equiv a_2 \mod 6$ is

$$x = a_2 + 6t \quad \text{where} \quad t \in \mathbb{Z}$$

This means that an integer $x = a_1 + 9s$ will satisfy both congruences provided $c + 3s = 2t$ for some t, that is, provided $s \equiv c \mod 2$. Thus the pair of congruences have a solution if and only if $3|(a_1 - a_2)$, in which case the general solution is

$$x = a_1 + 9(c + 2u) = a_1 + 9c + 18u \quad \text{where} \quad u \in \mathbb{Z}$$

forming a single congruence class $[a_1 + 9c] \mod 18$.

The final modulus, 18, is the least common multiple $[9, 6] = lcm(9, 6)$ of the moduli 9 and 6. A similar argument (which you should try for yourself) shows that in general, a pair of simultaneous congruences

$$x \equiv a_1 \mod n_1 \quad \text{and} \quad x \equiv a_2 \mod n_2$$

have a solution if and only if $gcd(n_1, n_2)$ divides $a_1 - a_2$, in which case the general solution is a single congruence class mod $lcm(n_1, n2)$. Yih-Hing's result extends this to any finite set of linear congruences, showing that they have a solution if and only if each pair of them have a solution:

Theorem 1.5.1. *Let $n_1, \ldots, n_k$ be positive integers, and let $a_1, \ldots, a_k$ be any integers. Then the simultaneous congruences*

$$x \equiv a_1 \mod n_1, \ldots, x \equiv a_k \mod n_k$$

have a solution x if and only if $gcd(n_i, n_j)$ divides $a_i - a_j$ whenever $i \neq j$. When this condition is satisfied, the general solution forms a single congruence class mod (n), where n is the least common multiple of $n_1, \ldots, n_k$.

Proof. If a solution x exists, then $x \equiv a_i \mod n_i$ and hence $n_i|(x - a_i)$ for each i. For each pair $i \neq j$ let $n_{ij} = gcd(n_i, n_j)$, so n_{ij} divides both n_i and n_j; it therefore divides $x - a_i$ and $x - a_j$, so it divides $(x - a_j) - (x - a_i) = a_i - a_j$, as required.

Let x_0 be any solution; then an integer x is a solution if and only if $x \equiv x_0 \mod n_i$ for each i, that is, $x - x_0$ is divisible by each n_i, or equivalently by their least common multiple $n = lcm(n_1, \ldots, n_k)$. Thus the general solution consists of a single congruence class $[xo] \mod n$.
To complete the proof, we have to show that if n_{ij} divides $a_i - a_j$ for each pair $i \neq j$, then a solution exists. The strategy is to replace the given set of congruences with an equivalent set of congruences having mutually coprime moduli, and then to apply the Chinese Remainder Theorem to show that this new set has a solution. First replace each congruence $x \equiv a_i \mod n_i$ with an equivalent finite set of congruences $x \equiv a_i \mod (p^e)$, where p^e ranges over all the prime powers in the factorisation of n_i. This gives us a set of congruences, equivalent to the first set, in which all the moduli are prime powers. These moduli are not necessarily coprime, since some primes p may divide n_i for several i. For a given prime p let us choose i so that n_i is divisible by the highest power of p, and let this power be p^e. If $p^f|n_j$, so that $f \leq e$, then p^f divides n_{ij} and hence (by our hypothesis) divides $a_i - a_j$; thus $a_i \equiv a_j \mod p^f$, so the congruence $x \equiv a_i \mod p^e$, if true, will imply $x \equiv a_i \mod p^f$ and hence $x \equiv a_j \mod p^f$. This means that we can discard all the congruences $x \equiv a_j \mod p^f$ for this prime p from our set, with the exception of the single congruence $x \equiv a_i \mod p^e$ involving the highest power of p, since this last congruence implies the others. If we do this for each prime p, we are then left with a finite set of congruences of the form $x \equiv a_i \mod p^e$ involving distinct primes p; since these moduli p^e are mutually coprime, the Chinese Remainder Theorem implies that the congruences have a common solution, which is automatically a solution of the original set of congruences. □

Example 1.9. Consider the congruences

$$x \equiv 11 \mod 36, \quad x \equiv 7 \mod 40, \quad x \equiv 32 \mod 75$$

Here $n_1 = 36$, $n_2 = 40$ and $n_3 = 75$, so we have

$$n_{12} = gcd(36, 40) = 4, \quad n_{13} = gcd(36, 75) = 3 \quad \text{and} \quad n_{23} = gcd(40, 75) = 5.$$

Since

$$a_1 - a_2 = 4, \quad a_1 - a_3 = -21 \quad \text{and} \quad a_2 - a_3 = -25,$$

the conditions $n_{ij}|(a_i - a_j)$ are all satisfied, so there are solutions, forming a single congruence class mod (n) where $n = lcm(36, 40, 75) = 1800$. To find the general solution, we follow the procedure described in the last paragraph of 1.5.1. Factorising each n_i, we replace the first congruence with

$$x \equiv 11 \mod 2^2 \quad \text{and} \quad x \equiv 11 \mod 3^2,$$

the second with,

$$x \equiv 7 \mod 2^3 \quad \text{and} \quad x \equiv 7 \mod 5,$$

and the third with

$$x \equiv 32 \mod 3 \quad \text{and} \quad x \equiv 32 \mod 5^2,$$

This gives us a set of six congruences, in which the moduli are powers of the primes $p = 2, 3$ and 5. From these, we select one congruence involving the highest power of each prime: for $p = 2$ we must choose $x \equiv 7 \mod 2^3$ (which implies $x \equiv 11 \mod 2^2$), for $p = 3$ we must choose $x \equiv 11 \mod 3^2$ (which implies $x \equiv 32 \mod 3$, and for $p = 5$ we must choose $x \equiv 32 \mod 5^2$ (which implies $x \equiv 7 \mod 5$). These three congruences, which can be simplified to

$$x \equiv 7 \mod 8, \quad x \equiv 2 \mod 9, \quad x \equiv 7 \mod 25$$

have mutually coprime moduli, and you can check that our earlier methods, based on the Chinese Remainder Theorem, now give the general solution $x \equiv 407 \mod 1800$.