21-128 Congruences

Definitions of congruence

Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, the expression '$a \equiv b \bmod n$' can be interpreted in many (equivalent) ways. It means...

(a) a and b leave the same remainder when divided by n.

(b) There exist $q_1, q_2, r \in \mathbb{Z}$ such that $a = q_1 n + r$ and $b = q_2 n + r$.

(c) $a = b + kn$ for some $k \in \mathbb{Z}$.

(d) n divides $a - b$, that is $\frac{a-b}{n}$ is an integer.

(e) a and b differ by a multiple of n.

Congruence behaves like equality

Congruence modulo n 'behaves like equality' in some special ways. First, is an equivalence relation, meaning that it is:

- **reflexive:** given $a \in \mathbb{Z}$, we have $a \equiv a \bmod n$;
- **symmetric:** given $a, b \in \mathbb{Z}$, if $a \equiv b \bmod n$ then $b \equiv a \bmod n$;
- **transitive:** given $a, b, c \in \mathbb{Z}$, if $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.

Second, it respects addition, subtraction and multiplication, meaning that if $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, then

- $a + b \equiv a' + b' \bmod n$;
- $a - b \equiv a' - b' \bmod n$;
- $ab \equiv a'b' \bmod n$.

A bunch of other useful properties follow from this. For example, by induction, it follows that congruence respects *all* sums and products: if $a_1, \dots, a_r, a'_1, \dots, a'_r$ are integers and $a_i \equiv a'_i$ for all $1 \le i \le r$, then

$$\sum_{i=1}^{r} a_i \equiv \sum_{i=1}^{r} a'_i \bmod n \quad \text{and} \quad \prod_{i=1}^{r} a_i \equiv \prod_{i=1}^{r} a'_i \bmod n$$

Some more consequences are:

- If $a, b, c \in \mathbb{Z}$ and $a \equiv b \bmod n$, then

$$ca \equiv cb \bmod n \quad \text{and} \quad a + c \equiv b + c \bmod n \quad \text{and} \quad a - c \equiv b - c \bmod n$$

  So we can 'multiply both sides' and 'add to both sides', and so on, just like with equality.

- If $a, b \in \mathbb{Z}$ with $a \equiv b \bmod n$, then $a^k \equiv b^k \bmod n$ for all $k \in \mathbb{N}$.

All these nice properties of congruence means that we can rearrange congruences just like we rearrange equations provided all we do is add, subtract and multiply.

Congruence doesn't behave like equality

Aside from the arithmetic properties discussed above, congruence has many *dissimilarities* with equality. This usually catches people out the first time they see it: all the nice properties of congruence lull you into a false sense of security!

Here are some examples of where things go wrong:

- **Division.** Although we can add, subtract and multiply, division doesn't work. Indeed:
  - If $q \notin \mathbb{Z}$ then it makes no sense to mention q in a congruence. For example, it makes no sense to say $2x \equiv 1 \bmod 3 \Rightarrow x \equiv \frac{1}{2} \bmod 3$.
  - Cancellation is also often impossible. It is not the case, for instance, that $2x \equiv 2y \bmod 4 \Rightarrow x \equiv y \bmod 4$—to see this, try letting $x = 0$ and $y = 2$.
  - ... however, cancellation does work in the case where the number being cancelled and the modulus are relatively prime: that is, if a and n are relatively prime then it is true that $ax \equiv ay \bmod n \Rightarrow x \equiv y \bmod n$. This cancellation comes from multiplication by a multiplicative inverse for a (see next section below), **not** from division by a.

- **Algebra.** One of the most used rules in algebra is that if $ab = 0$ then $a = 0$ or $b = 0$. This is why we can use factorisation to solve polynomial equations: if $(x-1)(x-2) = 0$ then $x - 1 = 0$ or $x - 2 = 0$, so $x = 1$ or $x = 2$. In general, this doesn't work for congruences. For example, the following steps are valid:

$$x^2 \equiv 1 \bmod 8 \quad \Rightarrow \quad x^2 - 1 \equiv 0 \bmod 8 \quad \Rightarrow \quad (x-1)(x+1) \equiv 0 \bmod 8$$

  but it doesn't follow that $x \equiv 1 \bmod 8$ or $x \equiv -1 \bmod 8$; indeed, $x = 1, 3, 5, 7$ all satisfy $x^2 \equiv 1 \bmod 8$.

- **Applying functions.** A very useful property of functions is that if $x = y$ then $f(x) = f(y)$—this is part of what it means for a function to be well-defined. Unfortunately, it is not in general true that $x \equiv y \bmod n \Rightarrow f(x) \equiv f(y) \bmod n$. (We say such a function 'respects congruence modulo n'.) For example:
  - The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2^x$ for all $x \in \mathbb{Z}$ doesn't respect congruence modulo 5. Indeed,
  $$1 \equiv 6 \bmod n \quad \text{but} \quad 2^1 = 2 \not\equiv 4 \equiv 64 = 2^6 \bmod n$$
  In general, it is almost never true that $x \equiv y \bmod n \Rightarrow a^x \equiv a^y \bmod n$—see the section on Fermat's little theorem and Euler's theorem below.
  - If a function doesn't take integer values then there is no hope of it being a valid thing to use in congruences. For example, square roots, logarithms, trigonometric functions, and the like, all behave badly (in fact, they don't behave at all) around congruences.

Multiplicative inverses

So we can't do division in modular arithmetic. But we *almost* can, at least, when a number is relatively prime to the modulus. The feature of division that makes it useful in solving equations is cancellation: if $2x = 4$ then $x = 2$. This works because $2 \times \frac{1}{2} = 1$ and $4 \times \frac{1}{2} = 2$, so

$$2x = 4 \quad \Rightarrow \quad \frac{1}{2} \times 2x = \frac{1}{2} \times 4 \quad \Rightarrow \quad x = 2$$

What made this work is we found a number b such that $2b = 1$. In modular arithmetic we can do the same trick: if we can find $b \in \mathbb{Z}$ such that $2b \equiv 1 \bmod 11$, for instance, then

$$2x \equiv 4 \bmod 11 \quad \Rightarrow \quad 2bx \equiv 4b \bmod 11 \quad \Rightarrow \quad x \equiv 4b \bmod 11$$

Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, a multiplicative inverse for a modulo n is an integer b such that $ab \equiv 1 \bmod n$. Then

multiplication by b has the same effect as division by a

but it is important to emphasise that we are multiplying by an integer, not dividing by a.

An integer a has a multiplicative inverse modulo n if and only if any of the following equivalent conditions hold:

- There exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$;
- a and n are relatively prime;
- The equation $ax + ny = 1$ has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$;
- $a^k \equiv 1 \bmod n$ for some $k \in \mathbb{N}$.

Solving single congruences

By the foregoing remarks on multiplicative inverses, if a and n are relatively prime then we can always solve the equation $ax \equiv c \bmod n$. Indeed, if this is so then there is some $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$, and then

- If $ax \equiv c \bmod n$ then $abx \equiv bc \bmod n$, so $x \equiv bc \bmod n$;
- If $x \equiv bc \bmod n$ then $ax \equiv abc \bmod n$, so $ax \equiv c \bmod n$.

So we have an equivalence: $ax \equiv c \bmod n$ if and only if $x \equiv bc \bmod n$.

Thus, if a and n are relatively prime, then:

- A solution $x_0 \in \mathbb{Z}$ to the congruence $ax \equiv c \bmod n$ exists (for instance we can let $x_0 = bc$, where b is a multiplicative inverse for a modulo n); and
- All other solutions x satisfy $x = x_0 + kn$ for some $k \in \mathbb{Z}$.

If a and n are arbitrary (i.e. *not* necessarily relatively prime), there is an added complication; in this case:

- A solution x_0 to the congruence $ax \equiv c \bmod n$ exists if and only if $\gcd(a,n) \mid c$; and
- All other solutions x satisfy $x = x_0 + k\frac{n}{\gcd(a,n)}$.

Here is an algorithm for solving a congruence of the form $ax \equiv c \bmod n$:

Step 1. Let $d = \gcd(a,n)$. If $d \nmid c$ then no solution exists, so stop; otherwise, proceed to step 2.

Step 2. Find $u, v \in \mathbb{Z}$ such that $au + nv = d$ using the extended Euclidean algorithm. It follows that $au \equiv d \bmod n$.

Step 3. Let $x_0 = u \cdot \frac{c}{d}$. Then $ax_0 \equiv c \bmod n$, so x_0 is a solution.

Step 4. All other solutions are now of the form $x_0 + k \cdot \frac{n}{d}$ for some $k \in \mathbb{Z}$.

Another approach is to apply the following result: if $a, c \in \mathbb{Z}$, $n \in \mathbb{N}$ and $d \in \mathbb{Z}$ with $d \mid a$, $d \mid c$ and $d \mid n$, then

$$ax \equiv c \bmod n \quad \Leftrightarrow \quad \frac{a}{d}x \equiv \frac{c}{d} \bmod \frac{n}{d}$$

So by dividing by the greatest common divisor of a and n, we reduce to the relatively prime case. (This relies on the fact that if $d = \gcd(a, n)$ then $\frac{a}{d}$ and $\frac{n}{d}$ are relatively prime!)

The new algorithm based on this approach is as follows:

Step 1. Let $d = \gcd(a, n)$. If $d \nmid c$ then no solution exists, so stop; otherwise, proceed to step 2.

Step 2. The numbers $\frac{a}{d}$ and $\frac{n}{d}$ are relatively prime; find a multiplicative inverse b for $\frac{a}{d}$ modulo $\frac{n}{d}$.

Step 3. Let $x_0 = b \cdot \frac{c}{d}$. Then $ax_0 \equiv \frac{c}{d} \bmod \frac{n}{d}$, so x_0 is a solution.

Step 4. All other solutions are now of the form $x_0 + k \cdot \frac{n}{d}$ for some $k \in \mathbb{Z}$.

Solving systems of congruences: Chinese remainder theorem

Suppose you need to find $x \in \mathbb{Z}$ such that

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

The first congruence tells you that $x = a + km$ for some $k \in \mathbb{Z}$. Substituting into the second tells you that $a + km \equiv b \bmod n$, that is $km \equiv b - a \bmod n$. By the previous section, a solution exists if and only if $\gcd(m, n) \mid b - a$, that is if and only if $a \equiv b \bmod \gcd(m, n)$, and any two solutions are congruent modulo $\frac{mn}{\gcd(m,n)}$. Hence, when $\gcd(m, n) = 1$, a solution definitely exists, and any two solutions are congruent modulo mn.

The Chinese remainder theorem extends this result inductively in the special case when the moduli are pairwise relatively prime. Precisely: given integers $a_1, \ldots, a_r$ and natural numbers $n_1, \ldots, n_r$ such that $\gcd(n_i, n_j) = 1$ for all $1 \le i < j \le r$, the system of congruences

$$x \equiv a_i \bmod n_i \quad (1 \le i \le r)$$

has a solution $x \in \mathbb{Z}$, and any two such solutions are congruent modulo $n_1 \times n_2 \times \cdots \times n_r$.

We can combine this with what we learnt in the previous section to obtain a more general result: let $a_1, \ldots, a_r, c_1, \ldots, c_r \in \mathbb{Z}$ and $n_1, \ldots, n_r \in \mathbb{N}$, and consider the system of congruences

$$a_i x \equiv c_i \bmod n_i \quad (1 \le i \le r)$$

Let $d_i = \gcd(a_i, n_i)$ for each $1 \le i \le r$. If:

- $d_i \mid c_i$ for each $1 \le i \le r$; and
- $\gcd(\frac{n_i}{d_i}, \frac{n_j}{d_j}) = 1$ for all $1 \le i < j \le r$;

then a solution $x \in \mathbb{Z}$ exists; and any two solutions are congruent modulo $\frac{n_1}{d_1} \times \cdots \times \frac{n_r}{d_r}$.

Fermat, Euler, Wilson

Given $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$, with a and n relatively prime, it would be useful to be able to find $k \in \mathbb{Z}$ such that $a^k \equiv 1 \bmod n$—it would be even more useful if k depended only on n, not on a. Fermat's little theorem gives us such a value of k in the case when n is prime; Euler's theorem generalises this to arbitrary natural numbers.

Fermat's little theorem. Let $a \in \mathbb{Z}$ and let $p \in \mathbb{N}$ be prime. If $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

Proof strategy. Consider the list $1, 2, \ldots, p-1$. First prove that the list $a, 2a, \ldots, (p-1)a$ is the same list (modulo p), just rearranged; it then follows that

$$1 \times 2 \times \cdots \times (p-1) \equiv a \times 2a \times \cdots \times (p-1)a \equiv a^{p-1}(1 \times 2 \times \cdots \times (p-1)) \bmod p$$

Since each of $1, 2, \ldots, p-1$ is relatively prime to p, each can be cancelled from both sides. Hence $a^{p-1} \equiv 1 \bmod p$. □

Euler's theorem generalises Fermat's little theorem to remove the restriction of primality. To state it, first we need to introduce the notion of a *totient*.

Given $n \in \mathbb{N}$, the **totient** of n, denoted $\varphi(n)$, is the number of natural numbers less than n which are relatively prime to n. That is,

$$\varphi(n) = |\{k \in [n] : k \text{ and } n \text{ are relatively prime}\}|$$

For example, if $p \in \mathbb{N}$ is prime then $\varphi(p) = p - 1$, since each of the numbers $1, 2, \ldots, p-1$ is relatively prime to p.

Euler's theorem. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. If a and n are relatively prime, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Proof strategy. Let $i_1, i_2, \ldots, i_{\varphi(n)}$ be the natural numbers less than n which are relatively prime to n. First prove that the list $ai_1, ai_2, \ldots, ai_{\varphi(n)}$ is the same list (modulo n), just rearranged; it then follows that

$$i_1 \times i_2 \times \cdots \times i_{\varphi(n)} \equiv ai_1 \times ai_2 \times \cdots \times ai_{\varphi(n)} \equiv a^{\varphi(n)}(i_1 \times i_2 \times \cdots \times i_{\varphi(n)}) \bmod n$$

Since each of $i_1, i_2, \ldots, i_{\varphi(n)}$ is relatively prime to n, each can be cancelled from both sides. Hence $a^{\varphi(n)} \equiv 1 \bmod n$. □

Notice that the argument in the proof of Euler's theorem is almost identical to that of the proof of Fermat's little theorem—indeed, in the case when n is prime, the argument is exactly the same!

Wilson's theorem. Let $p \in \mathbb{N}$ be prime. Then $(p-1)! \equiv -1 \bmod p$.

Proof strategy. The numbers $1, \ldots, p-2$ come in cancelling pairs, leaving just $p-1$. □