Definition. Let a, b, n be integers, $n \neq 0$.
We say that a *is congruent to* b *modulo* n, and write $a \equiv b \pmod{n}$, if n divides $a - b$.

In other words: $a \equiv b \pmod{n}$ means that a and b leave the same remainder on division by n.

The congruence notation was first introduced by C. F. Gauss (1777–1855).

Proposition 1. *If a, a', b, b', c, n are integers, with $n \neq 0$, then:*

(1) $a \equiv a \pmod{n}$;
(2) $a \equiv b \pmod{n}$ *if and only if* $b \equiv a \pmod{n}$;
(3) $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *implies* $a \equiv c \pmod{n}$;
(4) *if* $a \equiv b \pmod{n}$ *and* $a' \equiv b' \pmod{n}$, *then* $a \pm a' \equiv b \pm b' \pmod{n}$ *and* $aa' \equiv bb' \pmod{n}$;
(5) *assume that* $c \neq 0$; *then* $a \equiv b \pmod{n}$ *if and only if* $ac \equiv bc \pmod{nc}$;
(6) *if* $ac \equiv bc \pmod{n}$ *and* $\gcd(n, c) = 1$, *then* $a \equiv b \pmod{n}$;
(7) *if* $a \equiv a' \pmod{n}$ *and* $b \equiv b' \pmod{n}$, *then* $ac \equiv b \pmod{n}$ *if and only if* $a'c \equiv b' \pmod{n}$.

Proof. For (4), note that $aa' - bb' = (a - b)a' + (a' - b')b$. □

Notes: Items (1), (2), (3) together say that 'congruence modulo n' is an equivalence relation on the set $\mathbb{Z}$. The set of equivalence classes will be denoted by $\mathbb{Z}_n$. Item (4) says that if we define addition/subtraction/multiplication on $\mathbb{Z}_n$ by means of representatives of the classes, these operations are well-defined. Item (6) allows cancellation under certain circumstances; note that, for example, $4{\cdot}3 \equiv 8{\cdot}3 \pmod{12}$, where cancellation is not possible (the example also shows that products in $\mathbb{Z}_n$ can equal 0 without any of the factors being (congruent to) 0).

Exercise 1. Find an integer x satisfying the congruence $1966x \equiv 29 \pmod{9}$.

Exercise 2. Prove that if $x \equiv y \pmod{n}$ and $a_0, a_1, \ldots, a_k$ are integers, then

$$a_k x^k + \ldots + a_1 x + a_0 \equiv a_k y^k + \ldots + a_1 y + a_0 \pmod{n}.$$

Exercise 3. Show that if $a \equiv b \pmod{n}$ and $|a| < n/2$, $|b| < n/2$, then $a = b$.

Solving linear congruences of the form $ax \equiv b \pmod{n}$ is equivalent to solving linear Diophantine equations $ax - cy = b$ in integers x, y. These were covered in Lecture 1.

Proposition 2. *Let $a, b, n \in \mathbb{Z}$, $n > 0$. Then, the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n) | b$, in which case it has d mutually incongruent solutions among non-negative integers smaller than n, where $d = \gcd(a, n)$.*

Proof. The first part follows from Proposition 4 in lecture 1. Now, if $d = \gcd(a, n)$ and $d|b$, then all integer solutions of $ax - ny = b$ have the form $x = x_0 + tn/d$ and $y = y_0 + ta/d$. Observe that the d integers $x_j = x_0 + jn/d$ for $0 \leq j \leq d - 1$ are pairwise incongruent mod n; all other values of $x = x_0 + tn/d$ will be congruent mod n to one of the d numbers x_j. □

Corollary 3. *If $m > 0$ and $\gcd(a, n) = 1$, then there exists a unique $b \in \mathbb{Z}$ modulo n such that $ab \equiv 1 \pmod{n}$.*

Such b is called the *inverse of a modulo n* and denoted $\bar{a}$ or a^{-1}.

Exercise 4. Determine all solutions of $3x \equiv 11 \pmod{2275}$.

Exercise 5. Determine the inverse of 500 modulo 2007.

Exercise 6. There is a well-known criterion for an integer m to be divisible by 9 in terms of the decimal digits of m. State it and prove it.

Exercise 7. Find the last two decimal digits of the number $123^{1234567}$.
If you know something about the Euler ϕ function, this will be manageable 'by hand'. If you don't know the Euler phi function, then the fact that

$$23^{40} = 2945190837423705167875564697729320458241471826430830401$$

should help.

Some GAP commands

To calculate (large) powers of an integer a modulo n, don't say `a^k mod n` but rather use `PowerMod(a,k,n)`. The reason is that the latter command never computes the (large) value a^k, but reduces all intermediate products modulo n. For example, the command `123456^1234567 mod 10;` takes quite some time to execute, whilst `PowerMod(123456,1234567,10);` executes instantly.

`PrimeResidues(20)` will return a list of all integers from 1 to 19 which are relatively prime to 20 (and which have therefore an inverse modulo 20). The total number of such integers is called $\phi(20)$, and can be obtained in GAP with the command `Phi(20)`.