(SF2736, Discrete maths, ht15: L3, Wed 4 Nov 2015)

(The example on page 143 in Biggs, concerning $x \equiv_9 \theta(x)$ for all $x \in \mathbb{Z}$ (where $\theta(x)$ is the sum of the base 10 digits of x) and the method of 'casting out nines', was recommended for individual study.)

Linear congruences (mod m) in $\mathbb{Z}$ = linear equations in $\mathbb{Z}_m$

$ax \equiv_m b \;\Leftrightarrow\; ax = b$ in $\mathbb{Z}_m \;\Leftrightarrow\; ax - km = b$ for some $k \in \mathbb{Z}$,
so the equation is solvable iff $d = \gcd(a, m) \mid b$ (linear Diophantine equation in x, k).
Then the general solution for x is $x = x_0 + k \cdot \frac{m}{d}$ (with $k \in \mathbb{Z}$), so there are d different solutions (mod m) and d different solutions in $\mathbb{Z}_m$.

Rules for simplifying linear congruences:

$ax \equiv ay \pmod m \;\Leftrightarrow\; x \equiv y \pmod m$ **if** $\gcd(a, m) = 1$

$ax \equiv ay \pmod{an} \;\Leftrightarrow\; x \equiv y \pmod n$

$a \nmid y \;\Rightarrow\; ax \not\equiv y \pmod{an}$.

Congruences with several moduli:

Let $m_1, \ldots, m_k \in \mathbb{N}$, $\gcd(m_i, m_j) = 1$ if $i \neq j$ and the function
$F : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$ be given by $F(a) = ([a]_{m_1}, \ldots, [a]_{m_k})$. Then

$$F(a) = F(b) \;\Leftrightarrow\; a \equiv_m b, \;\; m = m_1 \cdot \ldots \cdot m_k,$$

so the function $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$, given by

$$f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$$

is (well-defined and) **one-to-one** (= **injective**) (i.e., $a \neq b \Rightarrow f(a) \neq f(b)$).

$|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}|$, so f is also **onto** (it takes all values in $\mathbb{Z}_{m_1} \times \ldots$).

And

$$f([a]_m + [b]_m) = f([a + b]_m) = ([a + b]_{m_1}, \ldots) = f([a]_m) + f([b]_m)$$

$f([a]_m \cdot [b]_m) = f([a \cdot b]_m) = ([a \cdot b]_{m_1}, \ldots) = ([a]_{m_1} \cdot [b]_{m_1}, \ldots) = f([a]_m) \cdot f([b]_m)$
(componentwise operations in the rhs). This means that f is an **isomorphism**,

$$(\mathbb{Z}_m, +, \cdot) \approx (\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}, +, \cdot).$$

Correspondingly, for all $x, y \in \mathbb{Z}$:

$$F(x + y) = F(x) + F(y) \text{ and } F(x \cdot y) = F(x) \cdot F(y).$$

By the isomorphism,

$$f^{-1}([a_1]_{m_1}, \ldots, [a_k]_{m_k}) = [y_1 a_1 + \cdots + y_k a_k]_m,$$

where $y_i = f^{-1}(0, 0, \ldots, 1, \ldots, 0)$ (1 in pos. i), i.e., $[y_i]_{m_j} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$

The Chinese remainder theorem: If $m_1, \ldots, m_k \in \mathbb{N}$, $\gcd(m_i, m_j) = 1$ for $i \neq j$, the system

$$\begin{cases} \boldsymbol{x \equiv_{m_1} a_1} \\ \boldsymbol{x \equiv_{m_2} a_2} \\ \vdots \\ \boldsymbol{x \equiv_{m_k} a_k} \end{cases}$$

is solvable for all $a_1, \ldots, a_k \in \mathbb{Z}$ and the solutions are all x satisfying
$\boldsymbol{x \equiv_m y_1 a_1 + \cdots + y_k a_k}$ for certain $y_1, \ldots, y_k \in \mathbb{Z}$ (independent of $a_1, \ldots, a_k$).

Euler's theorem, Fermat's (little) theorem

We let U_m be the set of all invertible elements in $\mathbb{Z}_m$ and
$\phi(m) = |U_m| = |\{x \in \mathbb{Z} \mid 1 \leq x \leq m,\ \gcd(x, m) = 1\}|$.
Then $x, y \in U_m \ \Rightarrow\ xy, x^{-1} \in U_m$.
The function ϕ is called **Euler's ϕ-function**.

Theorem: $y \in U_m \Rightarrow y^{\phi(m)} = 1$ in $\mathbb{Z}_m$,
so, expressed in $\mathbb{Z}$, (**Euler's theorem**): $\mathbf{gcd(y, m) = 1 \Rightarrow y^{\phi(m)} \equiv_m 1}$.

In particular, **if p is a prime**: $y \neq 0 \Rightarrow y^{p-1} = 1$ in $\mathbb{Z}_p$,
so, expressed in $\mathbb{Z}$ (**Fermat's (little) theorem**): $\boldsymbol{p \nmid y \Rightarrow y^{p-1} \equiv_p 1}$.

It follows that $y^p = y$, all $y \in \mathbb{Z}_p$ and $y^p \equiv_p y$, all $y \in \mathbb{Z}$.