Choice i) Introduction? P6578708 (6)

2) The simplest congruences are linear, 2.
of the form $ax - b \equiv 0 \pmod{m}$. This has solutions if $\gcd(a, m)$ divides b, since we can write $ax - b = km$

$$ax - km = b$$
$$d\left(\frac{a}{d}x - k\frac{m}{d}\right) = b \Rightarrow d \mid b$$

where $d = \gcd(a, m)$. The congruence can then be written $\left(\frac{a}{d}\right)x \equiv \frac{b}{d} \pmod{\left(\frac{m}{d}\right)}$ ✓

and we can solve this uniquely $\pmod{m/d}$ using the Euler Fermat theorem: $a^{\phi(m)} \equiv 1 \pmod{m}$ if $\gcd(a, m) = 1$. 4.
Multiply both sides of ② by $(a/d)^{\phi(m/d)-1}$
$(a/d)^{\phi(m/d)} x \equiv (a/d)^{\phi(m/d)-1}(b/d) \pmod{(m/d)}$
or $x \equiv (a/d)^{\phi(m/d)-1}(b/d) \pmod{(m/d)}$ is a soln of ②
We now find there are d solutions of the original congruence, since if we put $x = t + r\frac{m}{d}$, $r = 0, \ldots, d-1$ into ① ✓

we have $\frac{a}{d}\left(t + r\frac{m}{d}\right) = \frac{b}{d} + k\frac{m}{d}$
$at + rm\left(\frac{a}{d}\right) = b + km \Rightarrow at \equiv b \pmod{m}$.

There is a theorem of Lagrange analogous to the well known theory for the real numbers: A polynomial of degree n has at most n solutions in $\mathbb{R}$. 2
The theorem states: If $f(x) \equiv \sum_{i=0}^{n} c_i x^i \pmod{p}$ for p prime, then f has at most n solutions if $c_n \neq 0$.
The solutions can be found by factorising $(\bmod m)$, or substituting the