1. ...

$9 \mid 123456789$ since $1 + 2 + \ldots 9 = 45$ and $4 + 5 = 9$.
$11 \not| 123456789$ since $11 \not| 1 - 2 + \cdots + 9 = 5$.
476271 is no prime, since $4 + 7 + 6 + 2 + 7 + 1 = 27$ is divisible by 3.

2. *Division criteria for 4 and 8 .*

(i) 4: The powers of 10 modulo 4 are $1 \equiv 1, 10 \equiv 2, 100 \equiv 2^2 = 4 \equiv 0$, and all the rest 0. So the decimal numbers $a_n a_{n-1} \ldots a_1 a_0$ and $a_1 a_0$ and the number $2a_1 + a_0$ are simultaneously div by 4. Ex: $222222 \equiv 22$ is not, neither is $2 \cdot 2 + 2 = 4$ but $600560 \equiv 60$ is , also $2 \cdot 6 + 0$ is. Finally: : 3416 is, since 16 is.

(ii) 8 The powers of 10 modulo 8 are $1 \equiv 1, 10 \equiv 2, 100 \equiv 2^2 = 4, 1000 \equiv 2^3 = 8 \equiv 0$ and all the rest 0. So the decimal numbers $a_n a_{n-1} \ldots a_1 a_0$ and $a_2 a_1 a_0$ and $4 \cdot a_2 + 2 \cdot a_1 + a_0$ are simultaneously div by 8. Exx. $222222 \equiv 222$ not, since $4{\cdot}2{+}2{\cdot}2{+}2 = 8{+}4{+}6$ is not, but $600560 \equiv 560$ is, since $4{\cdot}5{+}2{\cdot}6{+}0 = 20 + 12 = 32$ is div by 8 (you can recycle tehe test: $0 \cdot 2 + 3 \cdot 2 + 2 = 8$ is div. Finally 3416 is, since 416 is, becaus $4 \cdot 4 + 2 \cdot 1 + 6 = 16 + 2 + 6 = 24$ is div by 8.

3. *Algebra— Lagrange...*

By definition $\varphi(n) = \#\mathbb{Z}_n^*$ kertaluku, so by Lagrange $N = \text{ord } a \in \mathbb{Z}_n^*$divides $\varphi(n)$, ie. $\varphi(n) = Nk$ for some $k \in \mathbb{N}$. By definition of ord: $a^N = 1 \in \mathbb{Z}_n^*$, so

$$a^{\varphi(n)} = a^{Nk} = (a^N)^k = 1^k = 1 \in \mathbb{Z}_n^*. \quad \Box$$

4. ...

(a) $3x \equiv 5 \pmod 7$.
$(3, 7) = 1$, so there is only one (class of) solution, and it can be found by multiplying with the inverse (mod 7) of 3, which is on 5. (I tried the alternatives 2,3,4,5,6, and noticed that $3 \cdot 2 = 6 = -1$, joten $3 \cdot 2 \cdot 3 \cdot 2 = 1$ eli $1 = 3{\cdot}(2{\cdot}3{\cdot}2) = 3{\cdot}12 = 3{\cdot}5$, and yes: $3{\cdot}5 = 15 = 1$.) So $x = 5^2 = 25 = 4 \in \mathbb{Z}_7$.

(b) $6x \equiv 5 \pmod{12}$.
Since $(6, 12) = 6 \not| 5$, there are no solutions (thm 2.27).

(c) $943x \equiv 381 \pmod{2576}$
Since $(943, 2576) = 23$ (<-Euclid on the calculator — or Excel) and $23 \not| 381$, there is no solution.

(d) $1375x \equiv 242 \pmod{5625}$ Since $(1375, 5625) = 11$ and $242 = 22 \cdot 11$, there are 11 solutions.

5. *Solve* $6x \equiv 4 \pmod{10}$.

Since $(6, 10) = 2$ and $2 \mid 4$, there are 2 solutions. Three methods to find them:

(1) trial and error: $6 \cdot 0 = 0 \not\equiv 4 \pmod{10}$
$6 \cdot 1 = 6 \not\equiv 4 \pmod{10}$
$6 \cdot 2 = 12 \equiv 2 \not\equiv 4 \pmod{10}$

$6 \cdot 3 = 18 \not\equiv 4 \pmod{10}$
$6 \cdot 4 = 24 \equiv 4 \pmod{10}$ OK!
$6 \cdot 5 = 30 \not\equiv 4 \pmod{10}$
$6 \cdot 6 = 36 \not\equiv 4 \pmod{10}$
$6 \cdot 7 = 42 \not\equiv 4 \pmod{10}$
$6 \cdot 8 = 48 \not\equiv 4 \pmod{10}$
$6 \cdot 9 = 54 \equiv 4 \pmod{10}$ OK!
really: $9 = 4 + 10/2$, like the theory predicts.

(2) Euler: Divide $(6, 10)(= 2)$ away and consider $3x \equiv 2 \pmod 5$.
$\varphi(5) = 4$, so $x \equiv 3^{varphi(10)-1} = 3^3 = 9 \equiv 4$. The other solution (9) is found by adding $10/2 = 5$.

(3) Euclid: Divide again $(6, 10)(= 2)$ away and consider $3x \equiv 2 \pmod 5$. Use Eukleideen algoritmillato find y and z s. th. $3y + 5z = 1$:

$$5 = 3 + 2, \quad 3 = 2 + 1, \text{ siis}$$

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 1 \cdot 5, \text{ joten kelpaa } y = 2,\ x = -1.$$

which gives $3y \equiv 1 \pmod 5$ ie $3 \cdot 2 \equiv 1 \pmod 5$, which implies $3 \cdot 2 \cdot 2 \equiv 2 \pmod 5$, so $x = 4$ is a solution. The other solution (9) is again found by adding $10/2 = 5$.

Notice: solving the **lin cdongruendce** $ax \equiv 1 \pmod n$ **is equivalent to finding the inverse** $a^{-1} \in \mathbb{Z}_n$ **.** (denoted by a' in the course text.)

6. ...

$$\begin{cases} x \equiv 1 & \pmod 2 \\ x \equiv 2 & \pmod 3 \\ x \equiv 0 & \pmod 7 \end{cases}$$

Full explanation of solution an´d theory: 2, 3 and 7 primes, in poarticular pairwise relative primes. OK! The solution will be found as a number $x = 1 \cdot y + 2 \cdot z + 0 \cdot w$, where y, z, w satissfy the easier congruence systems (to be solved first) : $\begin{cases} y \equiv 1 \pmod 2 \\ y \equiv 0 \pmod 3 \\ y \equiv 0 \pmod 7 \end{cases}$, $\begin{cases} z \equiv 0 \pmod 2 \\ z \equiv 1 \pmod 3 \\ z \equiv 0 \pmod 7 \end{cases}$ and $\begin{cases} w \equiv 0 \pmod 2 \\ w \equiv 0 \pmod 3 \\ w \equiv 1 \pmod 7 \end{cases}$

Let

$$n_1 = 2,\ n_2 = 3,\ n_3 = 7,\ N = n_1 n_2 n_3 = 42,$$

and

$$N_1 = N/n_1 = n_2 n_3 = 21,\ N_2 = N/n_2 = n_1 n_3 = 14, \text{ and } N_3 = N/n_3 = n_1 n_2 = 6.$$

By tye theorrym the soltuion is unique $\pmod N$, jso we aearch for one solution $x \in \mathbb{Z}$. The system of congruences $\begin{cases} y \equiv 1 \pmod 2 \\ y \equiv 0 \pmod 3 \\ y \equiv 0 \pmod 7 \end{cases}$ asks for a **number** y, divisible by 3 and 7 , so of the form $y = N_1 k = 21k$ for which $y \equiv 1 \pmod 2$. We must solve $y = 21k \equiv 1 \pmod 2$ ie find the inverse $k = N_1'$ of $21 = N_1$ in $\mathbb{Z}_2$. Of couirse $k = 1$, since $N_1 = 21 \equiv 1 \pmod 2$. So $y = 21 \cdot 1 = 21$, which is readily seen to satisfy the congruences in question.

Simiolarly, from $\begin{cases} z \equiv 0 \pmod 2 \\ z \equiv 1 \pmod 3 \\ z \equiv 0 \pmod 7 \end{cases}$, we find $z = 14N_2'$, where $14N_2' \equiv 1 \pmod 3$, so one can take $N_2' = 2$, giving $z = 28$ which solves the appropriate three congruences.

The 3. set of congruences can be left unsolved, since the coefficient in x is zero. So $x = y + 2x + 0w = 21 + 2 \cdot 28 = 77$. Since $N = 42$, $77 - 42 = 35$ is the smallest positive solution. I checked it.

7. *...solutions: .*

Since the inverses N_j' **refer to different modules** n_j, I like to represent them by $(N_j)_j^{-1}$, which is not standard.

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{12} \end{cases}$ Siis $x = 2y + 5z + 7w$,

$y = (7 \cdot 12) \cdot (7 \cdot 12)_5^{-1} = 84 \cdot (84)_5^{-1} = 84 \cdot (4)_5^{-1} = 84 \cdot 4 = 336.$

(<u>Better:</u>

$y = (7 \cdot 12) \cdot (7 \cdot 12)_5^{-1} = 84 \cdot (2 \cdot 2)_5^{-1} = 84 \cdot (4)_5^{-1} = 84 \cdot 4 = 336.$

$z = (5 \cdot 12) \cdot (5 \cdot 12)_7^{-1} = 60 \cdot (60)_7^{-1} = 60 \cdot (4)_7^{-1} = 60 \cdot 2 = 120.$

$w = (5 \cdot 7) \cdot (5 \cdot 7)_{12}^{-1} = 35 \cdot (35)_{12}^{-1} \cdot 2 = 35 \cdot (-1)_{12}^{-1} = 35 \cdot 11 = 385.$

$x = 2 \cdot 336 + 5 \cdot 120 + 7 \cdot 385 = 3967 \equiv \mathbf{187} \pmod{5 \cdot 7 \cdot 12 = 420}$

b) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$ Here a problem arises: $(6, 15) \neq 1$. Find some idea? The first congruence implies that $6 \mid x - 2$,s o $x - 2$ is divisible by both 2 and 3.

b') $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$

Similarly, the last congruence $x \equiv 7 \pmod{15}$ splits into $\begin{cases} x \equiv 7 \equiv 1 \pmod 3 \\ x \equiv 7 \equiv 2 \pmod 5 \end{cases}$

There is no solution, since a solution would be both even and odd (....very odd indeed!)

c) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{12} \end{cases}$

So $x = 2y + 5z + 8w$, where x, y and z are like in a), so $y = 336$, $z = 120$ ja $w = 385$. Just add w ti the solution of a) : $x = 187 + 385 = 572 \equiv \mathbf{152} \pmod{420}$. (Itg works.)

d) $\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 6 \pmod{10} \\ x \equiv 9 \pmod{11} \end{cases}$ So $x = 3y + 6z + 9w, \quad N = 990.$

$y = (10 \cdot 11) \cdot (10 \cdot 11)^{-1}{}_9 = 110 \cdot (1 \cdot 2)_9^{-1} = 110 \cdot (2)_9^{-1} = 110 \cdot 5 = 550.$

$z = (9 \cdot 11) \cdot (9 \cdot 11)_{10}^{-1} = 99 \cdot (-1 \cdot 1)_{10}^{-1} = 99 \cdot 9 = 891.$

$w = (9 \cdot 10) \cdot (9 \cdot 10)_{11}^{-1} = 90 \cdot (2)_{11}^{-1} = 90 \cdot 6 = 540.$

$x = 3 \cdot 550 + 6 \cdot 891 + 9 \cdot 540 = 11856 \equiv \mathbf{966} \pmod{9 \cdot 10 \cdot 11 = 990}.$

8. *Assume $p \neq q$ are primes.*

B y Fermat

$$p^{q-1} \equiv 1 \pmod{q}, \text{ joten } p^{q-1} + q^{p-1} \equiv 1 \pmod{q}.$$

$$\text{Similarly } q^{p-1} \equiv 1 \pmod{p}, \text{ joten } p^{q-1} + q^{p-1} \equiv 1 \pmod{p},$$

$$\text{so, since } (p,q) = 1, \; p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

9. *Let p be prime*

(a) $(a+b)^p \overset{Fermat}{\equiv} a+b \overset{Fermat}{\equiv} a^p + b^p \pmod{p}$.

(b) $(a+b)^p = \sum_{k=1}^{p} \binom{p}{k} a^k b^{m-k} \equiv a^p + b^p \pmod{p}$, *(Koska $p \mid \binom{p}{k}$, kun $1 < k < p$.)*

(c) *Prove Fermat's theormm by induction wrt. a. Start:* $1^p = 1 \equiv 1 \pmod{p}$

Step: $(a+1)^p \overset{2)}{\equiv} a^p + 1^p = a^p + 1 \overset{Ind.ol}{\equiv} a + 1.$