1. Determinare tutti i numeri primi $100 \leq p \leq 120$.

Sol. :) :) :)

2. (i) Dimostrare che se $n \geq 2$ non è primo, allora esiste un primo p che divide n e tale che $p^2 \leq n$.
   (ii) Sfruttare il risultato (i) per dimostrare che 467 è primo (basta verificare che non ha divisori minori o uguali a 19).

Sol. (i) Se n non è primo è prodotto di almeno due fattori m, k maggiori di 1 (primi o composti). Se entrambi fossero maggiori di $\sqrt{n}$, avremmo $n = m \cdot k > \sqrt{n}^2 = n$. Assurdo. In particolare almeno un fattore primo di n è minore o uguale a $\sqrt{n}$.
(b) :) :) :)

3. Dimostrare che il numero 123456789 non è primo.

Sol. :) :) :)

4. Fattorizzare i seguenti numeri in fattori primi.

(a) 91;	(d) $15^2 - 2^2$;	(g) $2^{11} - 1$;
(b) 210;	(e) 10!;	(h) 10001;
(c) 6^6;	(f) $2^{10} - 1$;	(i) 100000003.

Sol. :) :) :)

5. Calcolare il massimo comun divisore fra le seguenti coppie di numeri: $\mathrm{mcd}(623, 413)$, $\mathrm{mcd}(1014, 273)$, $\mathrm{mcd}(1122, 105)$, $\mathrm{mcd}(2244, 418)$.

Sol. Mediante l'algoritmo di Euclide troviamo

$$623 = 413 \cdot 1 + 210, \quad 413 = 210 \cdot 1 + 203, \quad 210 = 203 \cdot 1 + 7, \quad 203 = 7 \cdot 29 + 0.$$

Quindi $\mathrm{mcd}(623, 413) = 7$.

$$1014 = 273 \cdot 3 + 195, \quad 273 = 195 \cdot 1 + 78, \quad 195 = 78 \cdot 2 + 39, \quad 78 = 39 \cdot 2 + 0.$$

Quindi $\mathrm{mcd}(1014, 273) = 39$.

In modo simile troviamo $\mathrm{mcd}(1122, 105) = 3$, $\mathrm{mcd}(2244, 418) = 22$.

6. Definiamo sui numeri naturali $\mathbf{N} = \{1, 2, 3 \ldots\}$ la relazione "aRb se $\mathrm{mcd}(a, b) > 1$". Determinare se la relazione è riflessiva, simmetrica o transitiva.

Sol. La relazione non è riflessiva: $mcd(n, n) = n$. Per $n = 1$ tale massimo comun divisore non è maggiore di 1 come richiesto.
La relazione è simmetrica: se $mcd(n, m) > 1$, allora anche $mcd(m, n) = mcd(n, m) > 1$.
La relazione non è transitiva: per esempio $mcd(3, 15) = 3 > 1$, $mcd(15, 5) = 5 > 1$, mentre $mcd(3, 5) = 1$.

7. Siano $a = da'$ e $b = db'$ interi con $\mathrm{mcd}(a, b) = d$. Dimostrare che $\mathrm{mcd}(a', b') = 1$.

Sol. È chiaro che $mcd(a, b) = d \cdot mcd(a', b') = d$.

8. Siano n, m due numeri naturali. Siano $\mathrm{mcd}(n,m)$ e $\mathrm{mcm}(n,m)$ il massimo comun divisore e il minimo comune multiplo fra n ed m. Dimostrare che $\mathrm{mcm}(n,m)\cdot\mathrm{mcd}(n,m)=nm$.

Sol. Siano $n = p_1^{k_1}\dots p_\alpha^{k_\alpha} l_1^{b_1}\dots l_t^{b_t}$ ed $m = p_1^{a_1}\dots p_\alpha^{a_\alpha} q_1^{h_1}\dots q_\beta^{h_\beta}$ le decomposizioni di n ed m in fattori primi. Il massimo comun divisore $mcd(n,m)$ è dato dal fattore comune $p_1^{min(k_1,a_1)}\dots p_\alpha^{min(k_\alpha,a_\alpha)}$. Il minimo comune multiplo è dato dal prodotto di $n\cdot m$ diviso per il fattore comune (che altrimenti verrebbe contato due volte)

$$mcm(n,m)=\frac{n\cdot m}{mcd(n,m)}=p_1^{max(k_1,a_1)}\dots p_\alpha^{max(k_\alpha,a_\alpha)} l_1^{b_1}\dots l_t^{b_t} q_1^{h_1}\dots q_\beta^{h_\beta},$$

da cui $mcm(n,m)\cdot mcd(n,m)=nm$, come richiesto.

9. Per i seguenti numeri n e m, determinare $a,b\in\mathbf{Z}$ tali che $an+bm=\mathrm{mcd}(n,m)$.

(a) $n=4$ e $m=30$;	(c) $n=103$ e $m=101$;	(e) $n=221$ e $m=169$;
(b) $n=14$ e $m=40$;	(d) $n=91$ e $m=0$;	(g) $n=10001$ e $m=9999$.

Sol. Gli interi $a,b\in\mathbf{Z}$ tali che $an+bm=\mathrm{mcd}(n,m)$ si trovano con "l'algoritmo di Euclide esteso" (vedi nota1, pag.5). Osservare che a,b non sono unici. Come mai??

$(-7)\cdot4+1\cdot30=2,\quad 3\cdot14+(-1)\cdot40=2,\quad (-50)\cdot103+51\cdot101=1,\quad 1\cdot91+0\cdot0=91$

$(-3)\cdot221+4\cdot169=14,\qquad (-4999)\cdot10001+5000\cdot9999=1$

10. (a) Stabilire se esistono $s,t\in\mathbf{Z}$ tali che $24s+18t=20$;
(b) Stabilire se esistono $s,t\in\mathbf{Z}$ tali che $24s+18t=-12$;
(c) Stabilire se esistono $s,t\in\mathbf{Z}$ tali che $24s+18t=3$.

Sol. Un'equazione diofantea $as+bt=c$ ha soluzioni *intere* $s,t\in\mathbf{Z}$ se e solo se $mcd(a,b)$ divide c.
(a) Non ha soluzioni: $mcd(24,18)=6$ che non divide 20.
(b) Ha soluzioni: $mcd(24,18)=6$ che divide -12.
(c) Non ha soluzioni: $mcd(24,18)=6$ che non divide 3.

11. Determinare se la seguente equazione diofantea ha soluzioni:

$$2000000007X+1000000000Y=3.$$

Sol. Questa equazioni ha soluzioni intere in quanto $mcd(2000000007,1000000000)=1$ che divide 3.

12. Dare una descrizione esplicita delle classi di congruenza modulo 3 e delle classi di congruenza modulo 5 in $\mathbf{Z}$.

Sol. Le classi di congruenza modulo 3 sono tre:

$$\bar{0}=\{0,\ \pm3,\ \pm6,\ \pm9,\ \dots\},\qquad \text{multipli interi di } 3;$$

$$\bar{1}=\{1\pm3,\ 1\pm6,\ 1\pm9,\ \dots\},\quad \text{numeri che differiscono da 1 per multipli interi di } 3;$$

$$\bar{2}=\{2\pm3,\ 2\pm6,\ 2\pm9,\ \dots\},\quad \text{numeri che differiscono da 2 per multipli interi di } 3;$$

Le classi di congruenza modulo 5 sono cinque:

$$\bar{0}=\{0,\ \pm5,\ \pm10,\ \pm15,\ \dots\},\qquad \text{multipli interi di } 5;$$

$$\bar{1} = \{1 \pm 5,\ 1 \pm 10,\ 1 \pm 15,\ \ldots\}, \quad \text{numeri che differiscono da 1 per multipli interi di } 5;$$

$$\bar{2} = \{2 \pm 5,\ 2 \pm 10,\ 2 \pm 15,\ \ldots\}, \quad \text{numeri che differiscono da 2 per multipli interi di } 5;$$

$$\bar{3} = \{3 \pm 5,\ 2 \pm 10,\ 2 \pm 15,\ \ldots\}, \quad \text{numeri che differiscono da 3 per multipli interi di } 5;$$

$$\bar{4} = \{4 \pm 5,\ 2 \pm 10,\ 2 \pm 15,\ \ldots\}, \quad \text{numeri che differiscono da 4 per multipli interi di } 5.$$

13. Senza fare la moltiplicazione, determinare il resto della divisione per 10 e per 5 dei seguenti numeri

$$12345678 \times 90123, \qquad 9085679 \times 120001, \qquad 4876515329871674 \times 765976.$$

Sol. La classe resto $\bar{x}$ di un intero x modulo 10 è per definizione resto della divisione di x per 10 e coincide con l'ultima cifra della sua rappresentazione decimale. Per la Prop.0.15(i),(ii) (vedi nota1, pag.7) abbiamo

$$\overline{12345678 \times 90123} = \overline{12345678} \times \overline{90123} = \bar{8} \times \bar{3} = \overline{24} = \bar{4} \quad \text{mod } 10;$$

$$\overline{9085679 \times 120001} = \overline{9085679} \times \overline{120001} = \bar{9} \times \bar{1} = \bar{9} \quad \text{mod } 10;$$

$$\overline{4876515329871674 \times 765976} = \overline{4876515329871674} \times \overline{765976} = \bar{4} \times \bar{6} = \overline{24} = \bar{4} \quad \text{mod } 10.$$

La classe resto $\bar{x}$ di un intero x modulo 5 è per definizione resto della divisione di x per 5 e coincide con la classe resto modulo 5 dell'ultima cifra della sua rappresentazione decimale. Per la Prop.0.15(i),(ii) (vedi nota1, pag.7) abbiamo

$$\overline{12345678 \times 90123} = \overline{12345678} \times \overline{90123} = \bar{3} \times \bar{3} = \bar{9} = \bar{4} \quad \text{mod } 5;$$

$$\overline{9085679 \times 120001} = \overline{9085679} \times \overline{120001} = \bar{4} \times \bar{1} = \bar{4} \quad \text{mod } 5;$$

$$\overline{4876515329871674 \times 765976} = \overline{4876515329871674} \times \overline{765976} = \bar{4} \times \bar{1} = \bar{4} \quad \text{mod } 5.$$

14. Verificare che $2468 \times 13579 \equiv -3 \pmod{25}$.

Sol. La classe resto $\bar{x}$ di un intero x modulo 25 è per definizione resto della divisione di x per 25 e coincide con la classe resto modulo 25 delle ultime due cifre della sua rappresentazione decimale. Come nell'esercizio precedente abbiamo

$$\overline{2468 \times 13579} = \overline{2468} \times \overline{13579} = \overline{18} \times \bar{4} = \overline{72} = \overline{22} = \overline{-3} \quad \text{mod } 25.$$

15. Determinare tutte le soluzioni intere $x \in \mathbf{Z}$ delle seguenti congruenze
 (a) $x \equiv 3 \pmod{11}$; (b) $3x \equiv 1 \pmod{5}$; (c) $9x \equiv 0 \pmod{30}$.

Sol. (a) Soluzione generale: $x = 3 + k11$, al variare di $k \in \mathbf{Z}$; ad esempio $x = 3,\ 3+11,\ 3-11,\ 3+22,\ 3-22$, etc...;
(b) Poiché $mcd(3,5) = 1$ divide 1, la congruenza ha soluzioni. La soluzione generale (cioè la famiglia di tutte le soluzioni intere della congruenza) è data da $x = x_0 + 5k$, al variare di $k \in \mathbf{Z}$, e dove x_0 è una soluzione particolare della congruenza stessa. Per determinare una soluzione particolare x_0, ricordiamo che $mcd(3,5) = 1$ implica che esistono interi $x_0,\ y_0$ tali che

$$3x_0 + 5y_0 = 1$$

Ad esempio $x_0 = -3$ e $y_0 = 2$ (se non si vedono ad occhio, x_0 e y_0 possono essere determinati con l'algoritmo di Euclide esteso). Conclusione: la soluzione generale della congruenza è data da $x = -3 + 5k$, al variare di $k \in \mathbf{Z}$.
P.S.: C'è un'unica soluzione particolare $x_0 \in \{0, 1, 2, 3, 4\}$. In questo caso è $x_0 = 2$.
(c) Poiché la congruenza è omogenea ha soluzioni. Osserviamo che la congruenza $9x \equiv 0 \pmod{30}$ è equivalente alla congruenza

$$3x \equiv 0 \pmod{10},$$

ottenuta dividendo tutti i coefficienti per $mcd(9, 30) = 3$. La soluzione generale della congruenza è data da $x = 10k$, al variare di $k \in \mathbf{Z}$.

16. Dimostrare che la congruenza $2x \equiv 3 \pmod 2$ non ha soluzioni $x \in \mathbf{Z}$.

Sol. In questo caso $mcd(2, 2) = 2$ che non divide 3. Quindi la congruenza non ha soluzioni. D'altra parte si vede anche che per ogni $k \in \mathbf{Z}$, si ha che $2x$ è pari mentre $3 + 2k$ è dispari.

17. Stabilire se per le seguenti congruenze esistono soluzioni intere $x \in \mathbf{Z}$. In caso affermativo, determinarle tutte. Determinare poi le soluzioni $x \in \mathbf{Z}$ che soddisfano $0 < x < 100$.
    (a) $5x \equiv 8 \pmod{17}$; (b) $9x \equiv 26 \pmod{30}$; (c) $9x \equiv 24 \pmod{30}$.

Sol. (a) Poiché $mcd(5, 17) = 1$ divide 8, la congruenza ha soluzioni. La soluzione generale è data da $x = x_0 + 17k$, al variare di $k \in \mathbf{Z}$, e dove x_0 è una soluzione particolare della congruenza stessa. Per determinare una soluzione particolare x_0, ricordiamo che $mcd(5, 17) = 1$ implica che esistono interi a, b tali che

$$5a + 17b = 1$$

Ad esempio $a = 7$ e $b = -2$ (se non si vedono ad occhio, a e b possono essere determinati con l'algoritmo di Euclide esteso). Ne segue che $x_0 = 7 \cdot 8 = 56$ è una soluzione particolare della congruenza e la soluzione generale è data da $x = 56 + 17k$, al variare di $k \in \mathbf{Z}$. Un modo equivalente di esprimere la soluzione generale è $x = 5 + 17k$, al variare di $k \in \mathbf{Z}$.
(b) Poiché $mcd(9, 30) = 3$ non divide 26, la congruenza non ha soluzioni intere.
(c) Poiché $mcd(9, 30) = 3$ divide 24, la congruenza ammette soluzioni intere. Inoltre è equivalente alla congruenza

$$3x \equiv 8 \bmod 10, \qquad \text{con } mcd(3, 10) = 1.$$

18. Stabilire se per i seguenti sistemi di congruenze esistono soluzioni intere $x \in \mathbf{Z}$. In caso affermativo, determinarle tutte.

(a) $\begin{cases} x \equiv 4 \pmod 8, \\ x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 9; \end{cases}$ (c) $\begin{cases} 9x \equiv 20 \pmod 8, \\ x \equiv -2 \pmod 5, \\ -8x \equiv 4 \pmod 9; \end{cases}$

(b) $\begin{cases} 5x \equiv 4 \pmod 8, \\ 3x \equiv 3 \pmod 5, \\ 2x \equiv 4 \pmod 9; \end{cases}$ (d) $\begin{cases} x \equiv 3 \pmod 8, \\ x \equiv 1 \pmod 4; \end{cases}$

Sol. (a),(b),(c) In ognuno dei tre casi le equazioni del sistema ammettono singolarmente soluzioni intere. Inoltre, poiché $mcdd(8, 5) = mcd(8, 9) = mcd(5, 9) = 1$ anche il sistema ammette soluzioni intere. Tali soluzioni saranno della forma

$$x = x_0 + M\ 5 \cdot 8 \cdot 9 = x_0 + M360,$$

dove x_0 è una soluzione particolare ed M varia in $\mathbf{Z}$.
Per il procedimento vedi esercizio 23. etc....
(d) Poiché $mcd(4,8) = 4$ non divide $1-3=-2$, il sistema non ammette soluzioni intere.

19. Determinare il resto delle divisioni per 3, 9, 4, 11 del numero 3548917.

Sol. Scriviamo 3548917 come

$$3548917 = 7 + 10 + 9 \cdot 10^2 + 8 \cdot 10^3 + 4 \cdot 10^5 + 5 \cdot 10^6 + 3 \cdot 10^7.$$

- Calcolando modulo 3 abbiamo

$$\overline{3548917} = \bar{7}+\overline{10}+\overline{9\cdot 10^2}+\overline{8\cdot 10^3}+\overline{4\cdot 10^4}+\overline{5\cdot 10^5}+\overline{3\cdot 10^6} = \bar{7}+\overline{10}+\bar{9}\cdot\overline{10}^2+\bar{8}\cdot\overline{10}^3+\bar{4}\cdot\overline{10}^4+\bar{5}\cdot\overline{10}^5+\bar{3}\cdot\overline{10}^6.$$

Osserviamo che $\overline{10} = \bar{1}$ modulo 3, da cui l'espressione sopra diventa

$$= \bar{1} + \bar{1} + \bar{0} + \bar{2} + \bar{1} + \bar{2} + \bar{0} = \bar{1}.$$

Conclusione: il resto della divisione per 3 del numero 3548917 è 1.
Verifica: $3548917 = 3 \cdot 1182972 + 1$.
- Calcoliamo modulo 9 tenendo conto che $\overline{10} = \bar{1}$ modulo 9. Abbiamo

$$\overline{3548917} = \bar{7}+\overline{10}+\overline{9\cdot 10^2}+\overline{8\cdot 10^3}+\overline{4\cdot 10^4}+\overline{5\cdot 10^5}+\overline{3\cdot 10^6} = \bar{7}+\bar{1}+\bar{0}+\bar{8}+\bar{4}+\bar{5}+\bar{3} = \bar{1}.$$

Conclusione: il resto della divisione per 9 del numero 3548917 è 1.
Verifica: $3548917 = 9 \cdot 394324 + 1$.
- Calcoliamo modulo 4 tenendo conto che $\overline{10}^k = \bar{0}$ modulo 4, per ogni $k \geq 2$. Questo segue dal fatto che un numero che termina con due zeri è divisibile per 100 ed in particolare diviso per 4 dà resto 0. Dunque il resto della divisione per 4 del numero 3548917 è uguale al resto della divisione per 4 di 17 ed è uguale a 1.
Verifica: $3548917 = 4 \cdot 887229 + 1$.
- Calcoliamo modulo 11 tenendo conto che $\overline{10} = \overline{-1}$ modulo 11. In particolare $\overline{10}^k = \bar{1}$, per k pari, mentre $\overline{10}^k = \overline{-1}$, per k dispari. Abbiamo

$$\overline{3548917} = \bar{7}+\overline{10}+\overline{9\cdot 10^2}+\overline{8\cdot 10^3}+\overline{4\cdot 10^4}+\overline{5\cdot 10^5}+\overline{3\cdot 10^6} = \bar{7}-\bar{1}+\bar{9}-\bar{8}+\bar{4}-\bar{5}+\bar{3} = \bar{9}.$$

Conclusione: il resto della divisione per 11 del numero 3548917 è 9.
Verifica: $3548917 = 11 \cdot 322628 + 9$.

20. Sia $x = (x_n x_{n-1} \ldots x_0)_{10}$ un numero intero positivo rappresentato in base 10. Far vedere che $x \equiv x_n + x_{n-1} + \ldots + x_0 \pmod 9$.
Usare questo risultato per dimostrare che la moltiplicazione $54321 \times 98765 = 5363013565$ è sbagliata.

Sol. Scriviamo x come

$$x = (x_n x_{n-1} \ldots x_0)_{10} = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \ldots x_n \cdot 10^n.$$

Adesso calcolando modulo 9 come nell'esercizio 19, troviamo

$$\bar{x} = \bar{x}_0 + \bar{x}_1 + \bar{x}_2 + \ldots + \bar{x}_n \text{ mod } 9.$$

Poiché modulo 9

$$\overline{54321 \times 98765} = \overline{54321} \times \overline{98765} = (\bar{5}+\bar{4}+\bar{3}+\bar{2}+\bar{1}) \times (\bar{9}+\bar{8}+\bar{7}+\bar{6}+\bar{5}) = \bar{6} \times \bar{8} = \bar{3},$$

mentre

$$\overline{5363013565} = \bar{5}+\bar{3}+\bar{6}+\bar{3}+\bar{0}+\bar{1}+\bar{3}+\bar{5}+\bar{6}+\bar{5} = \bar{1}$$

la moltiplicazione è sicuramente sbagliata.

21. Andare al sito `http://www.mat.uniroma2.it/~eal/psychic.swf`. Spiegare come mai la sfera magica riesce a sempre indovinare il simbolo giusto.

Sol. ;-)

22. Sia $x = (x_n x_{n-1} \ldots x_0)_{10}$ un numero intero positivo rappresentato in base 10. Far vedere che $x \equiv x_0 - x_1 + x_2 - \ldots + (-1)^n x_n \pmod{11}$.
Usare questo risultato per controllare se 1213141516171819 è divisibile per 11.

Sol. Scriviamo x come

$$x = (x_n x_{n-1} \ldots x_0)_{10} = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \ldots x_n \cdot 10^n.$$

Adesso calcolando modulo 11 come nell'esercizio 19, troviamo

$$\bar{x} = \bar{x}_0 - \bar{x}_1 + \bar{x}_2 + \ldots + (-1)^n \bar{x}_n \bmod 11.$$

Poiché modulo 11

$$\overline{1213141516171819} = \bar{9}-\bar{1}+\bar{8}-\bar{1}+\bar{7}-\bar{1}+\bar{6}-\bar{1}+\bar{5}-\bar{1}+\bar{4}-\bar{1}+\bar{3}-\bar{1}+\bar{2}-\bar{1} = \bar{3} \neq 0,$$

il numero non è divisibile per 11.

23. Sia x un numero naturale di 3 cifre (in base 10). Supponiamo che

$$\begin{cases} x \equiv 1 & \pmod{7} \\ x \equiv 2 & \pmod{11} \\ x \equiv 3 & \pmod{13}. \end{cases}$$

Determinare x.

Sol. Le tre congruenze del sistema ammettono singolarmente soluzioni intere. Poiché $mcd(7, 11) = mcd(7, 13) = mcd(11, 13) = 1$, per il Teorema Cinese del Resto anche il sistema ha soluzioni intere e tali soluzioni saranno della forma

$$x = x_0 + M\ 7 \cdot 11 \cdot 13 = x_0 + M1001,$$

dove x_0 è una soluzione particolare ed M varia in $\mathbf{Z}$. Risolviamo il sistema per sostituzione dall'alto in basso.
Sostituendo la soluzione generale della prima congruenza $x = 1 + 7k$, con $k \in \mathbf{Z}$, nella seconda troviamo l'equazione diofantea

$$1 + 7k = 2 + 11h \quad \Leftrightarrow \quad 7k - 11h = 1, \qquad k, h \in \mathbf{Z}. \tag{$*$}$$

La soluzione generale di questa equazione è data da $(k, h) = (8, 5) + (11P, 7P)$, al variare di $P \in \mathbf{Z}$. Ricavando il corrispondente valore di k e sostituendolo nell'espressione (*), troviamo che la soluzione generale del sistema formato dalle prime due congruenze è data da

$$x = 57 + 77P, \qquad P \in \mathbf{Z}. \tag{**}$$

Sostituendo (**) nella terza congruenza otteniamo l'equazione diofantea

$$57 + 77P = 3 + Q13 \quad \Leftrightarrow \quad 77P - 13Q = -54, \quad P, Q \in \mathbf{Z}.$$

La soluzione generale di questa equazione è data da $(P, Q) = (54, 324) + (13M, 77M)$, con $M \in \mathbf{Z}$. Sostituendo la corrispondente espressione di P nella (**), troviamo che la soluzione generale del sistema delle tre congruenze è data da

$$x = 57 + 77(54 + 13M) = 57 + 4158 + 1001M = 4215 + 1001M, \quad M \in \mathbf{Z}.$$

L'unica soluzione del sistema di tre cifre decimali, ossia $0 \leq x \leq 999$, è data da

$$x = 211 \qquad (\text{per } M = -4).$$

Conclusione: Un numero di tre cifre è completamente determinato dai resti delle divisioni per 7, per 11 e per 13.