1. Numeri primi.

Proposizone 1. *(Divisione con resto). Siano $n, m \in \mathbf{Z}$ con $m \neq 0$. Allora esistono unici $q, r \in \mathbf{Z}$ con*

$$n = qm + r, \qquad \text{con } 0 \leq r < |m|.$$

Dimostrazione. Dimostriamo prima l'unicità di q e r. Supponiamo che $n = qm + r$ e $n = q'm + r'$ per $q, q', r, r' \in \mathbf{Z}$ con $0 \leq r, r' < |m|$, allora sottraendo le due equazioni troviamo che

$$(q - q')m = r' - r.$$

Il numero a sinistra è un multiplo di m, mentre il numero a destra è un intero di valore assoluto $< |m|$. L'unico multiplo di m di valore assoluto $< |m|$ è zero. Questo implica che $m(q - q') = r' - r = 0$ e quindi $q = q'$ e $r = r'$ come richiesto.

Dimostriamo l'esistenza prima quando $m > 0$. Per $x \in \mathbf{R}$ scriviamo $[x]$ per il più grande intero $k \in \mathbf{Z}$ che soddisfa $k \leq x$. Si ha che $0 \leq x - [x] < 1$. Sia $q = [n/m]$ e sia $r = n - qm$. Si ha quindi che $n = qm + r$. Moltiplicando la disuguaglianza $0 \leq n/m - [n/m] < 1$ per m, si trova che $0 \leq r < m$ come richiesto.

Il risultato per $m < 0$ segue dal fatto che $n = qm + r$ implica che $n = (-q)(-m) + r$. Questo conclude la dimostrazione.

Proposizone 2. *(Bézout) Siano $n, m \in \mathbf{Z}$ e sia $d = \mathrm{mcd}(n, m)$. Allora esistono $a, b \in \mathbf{Z}$ con*

$$an + bm = d.$$

Dimostrazione. Se $n = m = 0$ abbiamo che $\mathrm{mcd}(n, m) = 0$ e l'affermazione è chiara. Se uno tra n, m è diverso da 0 consideriamo il seguente sottoinsieme di $\mathbf{Z}$.

$$I = \{an + bm : a, b \in \mathbf{Z}\}.$$

Poiché uno tra n, m è diverso da 0, l'insieme I contiene numeri positivi. Sia e il più piccolo numero positivo contenuto in I.

Affermiamo che $e = d = \mathrm{mcd}(n, m)$. Ogni divisor comune di n, m divide ogni elemento di I. In particolare, $d = \mathrm{mcd}(n, m)$ divide e. Per vedere che $d = e$, dividiamo n per e con resto r. Abbiamo quindi che $n = qe + r$ con $0 \leq r < e$. Poiché $e = an + bm$ per certi $a, b \in \mathbf{Z}$, troviamo che

$$r = n - qe = (1 - qa)n - (qb)m$$

è un elemento di I. Per la minimalità di e abbiamo quindi che $r = 0$. Questo implica che e divide n. Nello stesso modo si fa vedere che e divide m. Allora e è un divisore comune di n e m e si ha quindi che $e \leq d = \mathrm{mcd}(n, m)$. Poiché d divide e, abbiamo che $d = e$ come richiesto.

Proposizione 3. *Siano $n, m \in \mathbf{Z}$ e sia p un numero primo. Allora p divide nm se e solo se p divide almeno uno di m, n.*

Dimostrazione. Se p divide uno di n, m allora divide anche il prodotto nm. Viceversa, se p non divide n, il mcd di n e p deve essere uguale a 1. Per Bézout esistono quindi $a, b \in \mathbf{Z}$ con $an + bp = 1$. Similmente, se p non divide m esistono $c, d \in \mathbf{Z}$ con $cm + dp = 1$. Questo implica che

$$1 = (an + bp)(cm + dp) = (ac)nm + p(and + bcm + bdp)$$

e non è possibile che p divida nm, come richiesto.

Teorema 4. *Ogni numero naturale è un prodotto di numeri primi.*

Dimostrazione. Sia $n \in \mathbf{Z}_{>0}$. Il numero $n = 1$ non è divisibile per nessun primo e quindi il prodotto è vuoto. Possiamo quindi suppore che $n > 1$. Dimostriamo prima l'esistenza di una fattorizzazione di n come prodotto di numeri primi. Se n è un numero primo, allora il prodotto consiste di se stesso. Se n non è primo, allora $n = a \cdot b$ con $1 < a, b < n$. Per induzione sia a che b sono uguali ad un prodotto di numeri primi. Il numero n è quindi uguale al prodotto di questi due prodotti.

Supponiamo adesso che $n > 1$ sia un prodotto di numeri primi in due modi:

$$n = \prod_p p = \prod_q q$$

Sia p un primo che appare nel prodotto a sinistra. Allora p divide il prodotto di primi $\prod_q q$. Per la proposizione precedente, p divide uno dei fattori q. Poichè q è primo, questo implica che $p = q$ per un primo q che appare nel prodotto a destra. Chiamiamo r il primo che i due prodotti hanno in comune. Dividiamo per r e troviamo che

$$\frac{n}{r} = \prod_{p \neq r} p = \prod_{q \neq r} q$$

Abbiamo che $\frac{n}{r} < n$. Per induzione i due prodotti per $\frac{n}{r}$ sono quindi uguali. Ma allora anche i due prodotti per n erano uguali. Basta moltiplicare per r.

2. Congruenze.

Proposizione 5. *Sia $n \in \mathbf{Z}_{>0}$ e siano $a, b \in \mathbf{Z}$. Se $\mathrm{mcd}(a, n) = 1$, allora l'equazione*

$$aX \equiv b \pmod{n}$$

ha una unica soluzione modulo n. In altre parole, esiste $x_0 \in \mathbf{Z}$ tale che le soluzioni hanno la forma $x_0 + kn$ per qualche $k \in \mathbf{Z}$.

Dimostrazione. Per Bézout esistono $c, d \in \mathbf{Z}$ con $ac + dn = 1$ e quindi $ac \equiv 1 \pmod{n}$. Multiplichiamo l'equazione per$c$:

$$X \equiv caX \equiv cb \pmod{n}.$$

Il risultato segue con $x_0 = cb$.

Teorema 6. *(Teorema cinese del resto) Siano $a, b, n, m \in \mathbf{Z}$. Supponiamo che $n, m > 0$ e che $\mathrm{mcd}(n, m) = 1$. Allora il sistema di congruenze*

$$\begin{cases} X \equiv a \pmod{n}; \\ X \equiv b \pmod{m}. \end{cases}$$

ha una unica soluzione modulo nm.

Dimostrazione. La prima equazione dice che $X = a + nZ$ per un certo intero Z. Sostituiamo questo nella seconda equazione. Troviamo che

$$nZ \equiv b - a \pmod{m}.$$

Per la Proposizione 5, questa equazione ha una unica soluzione modulo m. In altre parole, esiste $z_0 \in \mathbf{Z}$ tale che $Z = z_0 + km$ per un certo $k \in Z$. Questo implica che $X = nZ + a = (nz_0 + a) + knm$ per un certo $k \in \mathbf{Z}$, come richiesto.

Proposizione 7. *Sia $n \in \mathbf{Z}_{>0}$ e siano $a, b \in \mathbf{Z}$. Allora l'equazione*

$$aX \equiv b \pmod{n}$$

ammette una soluzione in $\mathbf{Z}$ se e solo se $d = \mathrm{mcd}(a, n)$ divide b. In questo caso la soluzione è unica modulo n/d. In altre parole, esiste $x_0 \in \mathbf{Z}$ tale che le soluzioni hanno la forma $x_0 + k\frac{n}{d}$ per qualche $k \in \mathbf{Z}$.

Dimostrazione. L'equazione ammette una soluzione se e solo se esistono $x, k \in \mathbf{Z}$ tali che

$$ax = b + kn.$$

Se esiste una soluzione, ogni divisor comune di a e n, in particolare $d = \mathrm{mcd}(a, n)$ divide quindi b.

Viceversa, se $d = \mathrm{mcd}(a, n)$ divide b, allora dividiamo l'equazione per d e otteniamo

$$\tfrac{a}{d}x = \tfrac{b}{d} + k\tfrac{n}{d}$$

ossia

$$\tfrac{a}{d}X \equiv \tfrac{b}{d} \pmod{\tfrac{n}{d}}.$$

Poiché $\mathrm{mcd}(\frac{a}{d}, \frac{n}{d}) = 1$, si può applicare la Proposizione 5 e il risultato segue.

Proposizione 8. *Siano $a, b, n, m \in \mathbf{Z}$. Supponiamo che $n, m > 0$. Allora il sistema di congruenze*

$$\begin{cases} X \equiv a \pmod{n}; \\ X \equiv b \pmod{m}. \end{cases}$$

ammette una soluzione in $\mathbf{Z}$ se e solo se $d = \mathrm{mcd}(n, m)$ divide $a - b$. In questo caso la soluzione è unica modulo $\frac{nm}{d}$.

Dimostrazione. La prima equazione dice che $X = a + Zn$ per un certo $Z \in \mathbf{Z}$. Sostituiamo questo nella seconda equazione e troviamo che

$$nZ \equiv b - a \pmod{m}.$$

Per la Proposizione 7, esiste una soluzione $z_0 \in \mathbf{Z}$ se e solo se $\mathrm{mcd}(n, m)$ divide $b - a$. La soluzione è unica modulo n/d. Questo implica che si ha che $X = nZ + a = (nz_0 + a) + k\frac{nm}{d}$ per un certo $k \in \mathbf{Z}$, come richiesto.