NUMERI PRIMI E TEORMA FONDAMENTALE DELL'ARITMETICA

Teorema 1. *(Teorema fondamentale dell'Aritmetica) Sia $n \in \mathbb{Z}^*$, $n \neq \pm 1$. Allora esistono s numeri primi $p_1, \dots, p_s$ e s interi naturali $h_1, \dots, h_s$ tali che*

$$n = p_1^{h_1} \cdot \ \dots \ \cdot p_s^{h_s}.$$

Questa decomposizione è essenzialmente unica, nel senso che se $q_1, \dots, q_r$ sono numeri primi e $k_1, \dots, k_r$ sono interi positivi tali che

$$n = q_1^{k_1} \dots q_r^{k_r}$$

allora $s = r$ ed inoltre si può cambiare l'ordine dei fattori in modo che $q_1 = \pm p_1, \dots, q_s = \pm p_s$, $h_1 = k_1, \dots, h_s = k_s$.

Osservazione 1. Siano $n, m \in \mathbb{Z} - \{0, \pm 1\}$. Allora esistono $p_1, \dots, p_s$ numeri primi, $h_1, \dots, h_s, k_1, \dots, k_s \in \mathbb{N}$ tali che

$$n = p_1^{h_1} \cdots p_s^{h_s}, \quad m = p_1^{k_1} \cdots p_s^{k_s};$$

cioè i due numeri possono essere fattorizzati usando gli stessi fattori primi, eventualmente elevati a potenza 0. Per esempio,

$$945 = 2^0 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^0 \cdot 17^0, \quad 3366 = 2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \cdot 17.$$

Si può provare che

$$M.C.D.(n, m) = p_1^{min(h_1,k_1)} \cdots p_s^{min(h_s,k_s)},$$

$$m.c.m.(n, m) = p_1^{max(h_1,k_1)} \cdots p_s^{max(h_s,k_s)}.$$

Nel caso considerato:

$$M.C.D.(945, 3366) = 2^{min(0,1)} \cdot 3^{min(3,2)} \cdot 5^{min(1,0)} \cdot 7^{min(1,0)} \cdot 11^{min(0,1)} \cdot 17^{min(0,1)},$$

quindi $M.C.D.(945, 3366) = 3^2 = 18$. Inoltre

$$m.c.m.(945, 3366) = 2^{max(0,1)} \cdot 3^{max(3,2)} \cdot 5^{max(1,0)} \cdot 7^{max(1,0)} \cdot 11^{max(0,1)} \cdot 17^{max(0,1)},$$

per cui $m.c.m.(945, 3366) = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 = 353430$.

Metodi di fattorizazione

CRIVELLO DI ERATOSTENE

Per determinare i numeri primi minori o uguali di un assegnato numero naturale $n \geq 4$, si scrive una tabella con tutti i numeri fino ad n e si comincia con il cancellare i multipli di 2. Finita questa operazione, si eliminano tutti i multipli del primo numero non cancellato, ovvero 3; dopo i multipli di 5, che è il primo numero non cancellato, dopo 7, e così via e ci si può fermare al più grande numero primo q più piccolo di $\sqrt{n}$. Infatti se p è un numero primo più grande di $\sqrt{n}$ un suo multiplo tramite un numero primo più piccolo di $\sqrt{n}$ eventualmente presente nella tabella è stato già scartato e già $p^2 > n$.

Osservazione 2. Tra i fattori primi di un numero naturale n non primo (ci si può sempre riferire a un numero positivo senza ledere la generalità) $n \geq 4$ ce n'è almeno uno minore o uguale di $\sqrt{n}$. Sia infatti

$$n = p_1^{h_1} \cdot \dots \cdot p_s^{h_s}$$

la scomposizione di n in fattori primi. Se fosse

$$p_1 > \sqrt{n}, \dots, p_s > \sqrt{n},$$

allora sarebbe

$$n = p_1^{h_1} \cdot \dots \cdot p_s^{h_s} > n$$

il che è una contraddizione.

Esempio 1. Se si vuole fattorizzare il numero $n = 4187$, si considera la sua radice $\sqrt{n} \backsim 64,707$ e quindi si prendono in esame tutti i numeri primi minori di 64: essi sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.$$

Effettuando (se necessario) le divisioni con la calcolatrice si ottiene un eventuale primo fattore. Se non si trova nessun fattore, il numero è irriducibile.
In queso caso si vede che n è divisibile per 53 e precisamente $n = 53 \cdot 79$.

METODO DI FATTORIZZAZIONE DI FERMAT

Osservazione 3. Si supponga di voler fattorizzare $n \in \mathbb{N}^*$, $n \neq \pm 1$. Si può ammettere che n sia dispari: se n fosse pari, si potrebbe dividere per 2 anche più volte, fino ad ottenenere un numero dispari. Si prova che:

$$(\exists a, b \in \mathbb{N} \text{ tali che } n = ab) \iff (\exists x, y \in \mathbb{N} \text{ tali che } n = x^2 - y^2).$$

Infatti se $n = ab$, allora, sviluppando i calcoli, si vede facilmente che

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

dove $\frac{a \pm b}{2} \in \mathbb{N}$, poichè n è dispari e quindi a e b sono dispari, e la loro somma, come la loro differenza,è pari. Il viceversa è ovvio, perchè $x^2 - y^2 = (x + y) \cdot (x - y)$, per cui basta porre $a = x + y$, $b = x - y$ e si ha $n = ab$. Anche quando n è primo si ha la fattorizzazione banale:

$$n = \left(\frac{n+1}{2} + \frac{n-1}{2}\right) \cdot \left(\frac{n+1}{2} - \frac{n-1}{2}\right) = n \cdot 1.$$

In virtù della Osservazione 3, cercare una fattorizzazione di n equivale a cercare x tale che $x^2 - n$ sia un quadrato (cioè y^2). Allora si usa il seguente procedimento: si determina il più piccolo intero positivo $t \geq \sqrt{n}$ e si calcolano

$$t^2 - n; \quad (t+1)^2 - n; \quad (t+2)^2 - n; \ldots\ldots$$

e così via, finché si trova un quadrato.

Esempio 2. $n = 1183$, $\sqrt{n} \backsim 34,39$, $t = 35$ allora si ha:

$$\begin{array}{rcl}
t^2 - n &=& 35^2 - 1183 = 1225 - 1183 = 42 \;\; \text{non quadrato} \\
(t+1)^2 - n &=& 36^2 - 1183 = 1296 - 1183 = 113 \quad " \quad " \\
(t+2)^2 - n &=& 37^2 - 1183 = 1369 - 1183 = 186 \quad " \quad " \\
(t+3)^2 - n &=& 38^2 - 1183 = 1444 - 1183 = 261 \quad " \quad " \\
(t+4)^2 - n &=& 39^2 - 1183 = 1521 - 1183 = 338 \quad " \quad " \\
(t+5)^2 - n &=& 40^2 - 1183 = 1600 - 1183 = 417 \quad " \quad " \\
(t+6)^2 - n &=& 41^2 - 1183 = 1681 - 1183 = 498 \quad " \quad " \\
(t+7)^2 - n &=& 42^2 - 1183 = 1764 - 1183 = 581 \quad " \quad " \\
(t+8)^2 - n &=& 43^2 - 1183 = 1849 - 1183 = 646 \quad " \quad " \\
(t+9)^2 - n &=& 44^2 - 1183 = 1936 - 1183 = 753 \quad " \quad " \\
(t+10)^2 - n &=& 45^2 - 1183 = 2052 - 1183 = 842 \quad " \quad " \\
(t+11)^2 - n &=& 46^2 - 1183 = 2116 - 1183 = 933 \quad " \quad " \\
(t+12)^2 - n &=& 47^2 - 1183 = 2209 - 1183 = 1026 \quad " \quad " \\
(t+13)^2 - n &=& 48^2 - 1183 = 2304 - 1183 = 1121 \quad " \quad " \\
(t+14)^2 - n &=& 49^2 - 1183 = 2401 - 1183 = 1218 \quad " \quad " \\
(t+15)^2 - n &=& 50^2 - 1183 = 2500 - 1183 = 1317 \quad " \quad " \\
(t+16)^2 - n &=& 51^2 - 1183 = 1601 - 1183 = 1481 \quad " \quad " \\
(t+17)^2 - n &=& 52^2 - 1183 = 2704 - 1183 = 1521 = 39^2.
\end{array}$$

Quindi: $52^2 - 1183 = 39^2$, cioè

$$1183 = 52^2 - 39^2 = (52+39)(52-39) = 91 \cdot 13$$

Bisogna scomporre 91, per esempio iterando il procedimento di Fermat: $m = 91$, $\sqrt{91} \backsim 9,53$, $k = 10$,

$$k^2 - 91 = 100 - 91 = 9 = 3^2.$$

Segue che

$$91 = 10^2 - 3^2 = (10+3)(10-3) = 13 \cdot 7.$$

Allora

$$1183 = 13^2 \cdot 7.$$

Il procedimento di Fermat è un algoritmo, ovvero ha sempre una conclusione (anche se non si sa a priori qual è il numero dei passaggi da effettuare); nel caso in cui il numero n è primo, si conclude con il quadrato $(\frac{n+1}{2})^2 - n$.

Piccolo Teorema di Fermat - Teorema di eulero

Lemma 1. *Siano* $a, b, c, d \in \mathbb{Z}$, $k, n \in \mathbb{N}$, $n \neq 0, n \neq 1$. *Si ha:*

(1) $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \Rightarrow a + c \;\equiv b + d \pmod{n}$
(2) $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \Rightarrow ac \;\equiv b \pmod{n}$
(3) $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$

Dimostrazione. Da $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n})$ segue $(n \mid (a-b) \wedge n \mid (c-d).)$ Allora $n \mid a-b+c-d$, ovvero $a \mid (a+c)-(b+d)$ e ciò vuol dire che $a+c \;\equiv b+d \pmod{n}$, per cui (1) è provata.
Poichè $(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n})$, esistono $h, k \in \mathbb{Z}$ tali che $a-b = nh$ e $c-d = nk$. Allora $(a-b)c = nhc$ e $(c-d)b = nkb$. Sommando $ac - bc + cb - db = nhc + nkb$, da cui $ac - bd = n(hc+kb)$ e pertanto $n \mid ac - bd$, ovvero $ac \;\equiv b \pmod{n}$, e (2) risulta verificata.

Per provare (3) si procede per induzione completa. Per $k = 0$, certamente $a^0 \equiv b^0 \pmod{n}$ è verificato poichè $a^0 = b^0 = 1$ e la congruenza modulo n è riflessiva. Si suppone ora che $a \equiv b \pmod{n}$ e $a^k \equiv b^k \pmod{n}$ e si deve provare che $a^{k+1} \equiv b^{k+1} \pmod{n}$: ma basta ricordare che per ogni numero intero non nullo x, risulta $x^{k+1} = x^k \cdot x$ e usare (2).

Osservazione 4. Siano $a, b \in \mathbb{Z}$. Si osservi che, se $a \equiv b \pmod{n}$, allora, tenendo presente che $b \equiv b \pmod{n}$ e usando (2) del Lemma 1, si ha $a - b \equiv 0 \pmod{n}$.

Proposizione 1. *Siano $x, y \in \mathbb{Z}$, $p \in \mathbb{N}$, p primo. Allora*

$$(x + y)^p \equiv x^p + y^p (\bmod\ p).$$

La dimostrazione viene omessa.

Teorema 2. *(Piccolo teorema di Fermat) Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Allora*

$$a^p \equiv a \pmod{p}. \tag{1}$$

Dimostrazione. Si suppone in un primo momento che sia $a \geq 0$ e si procede per induzione completa su a. Per $a = 0$, $a^p = 0$ e (1) diviene $0 \equiv 0 \pmod{p}$, ovviamente vera. Si suppone che (1) sia vera e si prova $(a+1)^p \equiv a+1 \pmod{p}$. Per la Proposizione 1, la proprietà transitiva della congruenza modulo n e l'ipotesi di induzione risulta:

$$(a + 1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}.$$

quindi (1) è verificata quando $a \geq 0$. Se $a < 0$, allora $-a > 0$ e quindi $(-a)^p \equiv (-a) \pmod{p}$. Usando nuovamente la Proposizione 1, la proprietà transitiva della congruenza modulo n e l'ipotesi di induzione, si ha:

$$0 = (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p + (-a) \pmod{p}.$$

Pertanto $a^p + (-a) \equiv 0 \pmod{p}$ da cui, per l'Osservazione 4, $a^p \equiv a \pmod{p}$.

Corollario 1. Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Se $M.C.D.(a, p) = 1$ allora

$$a^{p-1} \equiv 1 (\bmod\ p).$$

Esercizi 1. Determinare il resto della divisione di 89741^{527} per 3.

Si osserva che

$$89741 \equiv 2 (\bmod\ 3)$$

e quindi

$$89741^{527} \equiv 2^{527} (\bmod\ 3).$$

Per il corollario, poichè $M.C.D.(2, 3) = 1$, si ha $2^{3-1} \equiv 1 (\bmod\ 3)$ (in questo caso è banale) e pertanto

$$89741^{527} \equiv 2^{527} = (2^2)^{263} \cdot 2 \equiv 1^{263} \cdot 2 = 2 (\bmod\ 3)$$

per cui il resto è 2.

2. Determinare il resto della divisione di 57432^{1142} per 9.

Si osserva che

$$57432 \equiv 3 (\bmod\ 9)$$

e quindi

$$57432^{1142} \equiv 3^{1142} \equiv (3^2)^{571} \equiv 0^{571} \equiv 0 (\bmod\ 9).$$

Definizione 1. Si dice *funzione di Eulero* l'applicazione

$$\varphi : \mathbb{N}^* \to \mathbb{N}$$

tale che $\forall n \in \mathbb{N}^*$,

$$\varphi(n) \text{=numero dei numeri minori di } n \text{ e primi con } n.$$

Osservazione 5. È ovvio che per ogni numero primo p

$$\varphi(p) = p - 1$$

Proposizione 2. La funzione di Eulero è moltiplicativa, cioè

$$\forall n, m \in \mathbb{N}^*, \ n > 1, \ m > 1 \text{ tali che } M.C.D.(n, m) = 1,$$
$$\varphi(n \cdot m) = \varphi(n)\varphi(m).$$

Proposizione 3. Sia p un numero primo. Allora

$$\varphi(p^h) = p^h - p^{h-1}.$$

Proposizione 4. Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$ la sua fattorizzazione in numeri primi. Allora

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \ldots \cdot \varphi(p_s^{h_s}).$$

Teorema 3. *(Teorema di Eulero) Siano $a \in \mathbb{Z}^*$, $n \in \mathbb{N}^*$, con $M.C.D.(a, n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1 (\texttt{mod } n).$$