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

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

Dimostrazione. Da $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ segue $n \mid (a-b)$ e $n \mid (c-d)$. 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 $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, allora $n \mid (a-b)$ e $n \mid (c-d)$ e quindi $n \mid (a-b)c$ e $n \mid (c-d)b$. Pertanto $n \mid (a-b)c + (c-d)b$, cioé $n \mid ac - bd$, ovvero $ac \equiv bd \pmod{n}$, e (2) risulta verificata.
Per provare (3) si procede per induzione completa su k. Per $k = 1$, certamente $a^1 \equiv b^1 \pmod{n}$ è verificato poiché $a^1 = a$, $b^1 = b$. Sia $k \in \mathbb{N}$, $k > 1$. Si suppone che sia $a^k \equiv b^k \pmod{n}$ e si deve provare che $a^{k+1} \equiv b^{k+1} \pmod{n}$. Per ipotesi di induzione si ha $a^k \equiv b^k \pmod{n}$; inoltre, per ipotesi, $a \equiv b \pmod{n}$. Allora, usando (2), $a^k a \equiv b^k b \pmod{n}$ e, ricordando che per ogni numero intero x, risulta $x^{k+1} = x^k \cdot x$, si ha $a^{k+1} \equiv b^{k+1} \pmod{n}$.

Teorema 1. *Sia $n \in \mathbb{N}^*$, $n \neq 1$. Allora $\forall a \in \mathbb{N}, \exists | r_0, \ldots, r_h \in \mathbb{N}$ tali che*

$$a = r_h n^h + r_{h-1} n^{h-1} + \cdots + r_1 n + r_0. \tag{1}$$

Dimostrazione. (cenno) Si eseguono le seguenti divisioni:

$$\begin{array}{rcll} a &=& q_0\, n + r_0, & r_0 < n \\ q_0 &=& q_1\, n + r_1, & r_1 < n \\ q_1 &=& q_2\, n + r_2. & r_2 < n \\ \vdots && & \\ q_{h-2} &=& q_{h-1}\, n + r_{h-1} & r_{h-1} < n \\ q_{h-1} &=& 0\, n + r_h & r_h < n \end{array}$$

Poichè si tratta di numeri naturali, si ha $q_0 > q_1 > \ldots$, per cui, ad un certo punto il quoziente di una divisione si deve azzerare.
Si ha, quindi:

$$a = q_0 n + r_0 = (q_1 n + r_1)n + r_0 = q_1 n^2 + r_1 n + r_0$$

$$= (q_2 n + r_2)n^2 + r_1 n + r_0 = q_2 n^3 + r_2 n^2 + r_1 n + r_0$$

$$= \cdots = r_h n^h + r_{h-1} n^{h-1} + \cdots + r_1 n + r_0.$$

Osservazione 1. Per comoditá, invece di usare l'espressione (1), si scrive:

$$(a)_n = r_h r_{h-1} \ldots r_1 r_0.$$

che si dice *scrittura del numero a in base n.*

Osservazione 2. Sia $n \in \mathbb{N}^*$, $n \neq 1$. Poiché risulta:

$$\begin{array}{rcl} n &=& 1\, n + 0 \\ 1 &=& 0\, n + 1, \end{array}$$

si ha $(n)_{10} = (10)_n$

Esempio 1. Si vuole scrivere 11 in base 2. Si effettuano le divisioni, come suggerisce il Teorema 1

$$\begin{aligned} 11 &= 5 \cdot \mathbf{2} + 1 \\ 5 &= 2 \cdot \mathbf{2} + 1 \\ 2 &= 1 \cdot \mathbf{2} + 0 \\ 1 &= 0 \cdot \mathbf{2} + 1. \end{aligned}$$

Allora si ha:

$$\begin{aligned} (11)_{10} &= 5 \cdot \mathbf{2} + 1 = (2 \cdot \mathbf{2} + 1)\mathbf{2} + 1 = 2 \cdot \mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ &= (1 \cdot \mathbf{2} + 0)\mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ &= 1 \cdot \mathbf{2}^3 + 0 \cdot \mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ &= (1011)_2 \end{aligned}$$

CRITERI DI DIVISIBILITÀ

Osservazione 3. Siano $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $n \neq 1$, con $a \equiv b \pmod{n}$. Allora

$$n \mid a \Leftrightarrow n \mid b.$$

Dimostrazione. Se $n \mid a$, poichè per ipotesi $a \equiv b \pmod{n}$, risulta $n \mid a - b$ e quindi $n \mid a - (a - b)$, cioè $n \mid b$. L'altra implicazione è del tutto analoga: se $n \mid b$, poichè dall'ipotesi segue $n \mid a - b$, si ha $n \mid b + (a - b)$, cioè $n \mid a$.

Sia $a \in \mathbb{N}^*$. Se $a = r_h r_{h-1} \dots r_1 r_0$ (ovviamente in base 10), allora si può scrivere:

$$a = r_h 10^h + r_{h-1} 10^{h-1} \dots r_1 10 + r_0. \tag{2}$$

Criteri di divisibilità per 10, per 5, per 2

È noto che a è divisibile per 2 se e solo se l'ultima cifra r_0 è pari, è divisibile per 5 se e solo se r_0 è uguale a 5 oppure a 0, è divisibile per 10 se e solo se r_0 è 0. Questo si dimostra usando l'Osservazione 3: (2) può essere scritta come $a = 10(r_h 10^{h-1} + r_{h-1} 10^{h-2} \dots r_1) + r_0$ e quindi:

$$a - r_0 = 10(r_h 10^{h-1} + r_{h-1} 10^{h-2} \dots r_1),$$

e quindi $10 \mid a - r_0$ per cui anche $5 \mid a - r_0$ e $2 \mid a - r_0$. Allora $a \equiv r_0 \pmod{10}$, $a \equiv r_0 \pmod{5}$, $a \equiv r_0 \pmod{2}$ e quindi, per l'Osservazione 3:

$$\begin{aligned} 10 \mid a &\Leftrightarrow 10 \mid r_0, \\ 5 \mid a &\Leftrightarrow 5 \mid r_0, \\ 2 \mid a &\Leftrightarrow 2 \mid r_0 \end{aligned}$$

Criteri di divisibilità per 3, per 9

Poichè $10 \equiv 1 \pmod{3}$, per (3) del Lemma 1, risulta $10^k \equiv 1^k \equiv 1 \pmod{3}$, per ogni $k \in \{1, \dots, h\}$, e quindi

$$a \equiv r_h + r_{h-1} + \dots + r_0 \pmod{3},$$

da cui, per l'Osservazione 3 si ricava il noto criterio di divisibilità per 3:

$$3 \mid a \Leftrightarrow 3 \mid r_h + r_{h-1} + \dots + r_0.$$

Analogamente si ottiene il criterio di divisibilità per 9, osservando che $10 \equiv 1 \pmod{9}$.

Criterio di divisibilità per 11

Si osserva che $10 \equiv -1 \pmod{11}$ e quindi

$$10^k \equiv (-1)^k \pmod{11},$$

cioè $10^k \equiv 1 \pmod{11}$ se k è pari $10^k \equiv -1 \pmod{11}$ se k è dispari. Allora usando ancora l'Osservazione 3 si ha

$$a \equiv r_h(-1)^h + r_{h-1}(-1)^{h-1} + \cdots + r_1(-1) + r_0(-1)^0 \pmod{11},$$

cioè

$$11 \mid a \Leftrightarrow 11 \mid r_h(-1)^h + r_{h-1}(-1)^{h-1} + \cdots + r_1(-1) + r_0(-1)^0.$$

Esempio 2. Risulta che $11 \mid 939115309$, perchè $9 - 3 + 9 - 1 + 1 - 5 + 3 - 0 + 9 = 22$ che è un multiplo di 11.

METODI DI FATTORIZZAZIONE

CRIVELLO DI ERATOSTENE

Sia $n \in \mathbb{N}$, $n \geq 4$ (si può sempre studiare la scomposizione dei numeri interi riferendosi ai numeri positivi, senza ledere la generalità dei ragionamenti). Per determinare i numeri primi minori o uguali di n, si scrive una tabella con tutti i numeri fino ad n e si inizia con il cancellare tutti 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 tutti i multipli di 7 e così via. È importante osservare che il procedimento si ferma al più grande numero primo q più piccolo di $\sqrt{n}$. Siano $q_1, \ldots, q_h = q$ i numeri primi minori o uguali di $\sqrt{n}$. Se p è un numero primo $p > \sqrt{n}$ un suo multiplo tramite uno dei numeri primi $q_1, \ldots, q_h = q$ minori o uguali di $\sqrt{n}$ (cioè $q_1 p, \ldots, q_h p$) eventualmente presente nella tabella è stato già scartato; inoltre, se $a \in \mathbb{N}$, con $q \leq a \leq p$, risulta

$$n = \sqrt{n}\,\sqrt{n} < ap$$

e quindi aq è fuori della tabella. I numeri che restano non cancellati nella tabella sono i numeri primi minori o uguali di n.

Osservazione 4. Tra i fattori primi di un numero naturale n non primo $n \geq 4$ ce n'è almeno uno minore o uguale di $\sqrt{n}$. Sia infatti

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

la scomposizione di n in fattori primi. Se fosse

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

allora sarebbe

$$n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s} > \sqrt{n}^{h_1} \cdot \ldots \cdot \sqrt{n}^{h_s} \geq n$$

il che è una contraddizione.

Esempio 3. Si vuole trovare l'eventuale scomposizione in fattori primi del 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, che 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, per l'Osservazione 4, il numero è certamente primo.
In queso caso si vede che n è divisibile per 53 e precisamente $n = 53 \cdot 79$.

Esempio 4. Si vuole trovare l'eventuale scomposizione in fattori primi del numero $n = 613$. Si considera la sua radice $\sqrt{n} \backsim 24,758$ e quindi si prendono in esame tutti i numeri primi minori di 24, che sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

Effettuando le divisioni necessarie con la calcolatrice, si vede che il numero non è divisibile per alcuno dei numeri primi minori di 24, per cui, per l'Osservazione 4, 613 è certamente un numero primo.

METODO DI FATTORIZZAZIONE DI FERMAT

Proposizione 1. *Sia $n \in \mathbb{N}^*$, $n \neq 1$, n dispari (se n fosse pari, si potrebbe dividere per 2 anche più volte, fino ad ottenenere un numero dispari). Sussiste la seguente equivalenza:*

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

Dimostrazione. Se $n = ab$, allora a e b sono due numeri dispari, per cui la loro somma, come la loro differenza, è pari. Quindi $\frac{a+b}{2} \in \mathbb{N}$, e, se per esempio si suppone che sia $a \geq b$, anche $\frac{a-b}{2} \in \mathbb{N}$. Si vede facilmente che

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

per cui $\exists\ x = \frac{a+b}{2},\ y = \frac{a-b}{2} \in \mathbb{N}$ tali che $n = x^2 - y^2$.
Il viceversa è ovvio, perchè se esistono $x, y \in \mathbb{N}$ tali che $n = x^2 - y^2 = (x + y) \cdot (x - y)$, certamente è $x \geq y$ per cui $a = x + y \in \mathbb{N},\ b = x - y \in \mathbb{N}$ e si ha $n = ab$.

Osservazione 5. 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 1, 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 5. $n = 1183$, $\sqrt{n} \backsim 34,39$, $t = 35$ allora si ha:

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

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