

Criteri di divisibilit  per 2,3,5,9,11

Un numero $n \in \mathbb{Z}_{\geq 0}$ che ha $r + 1$ cifre se scritto in base 10 si scrive come

$$n = a_r \dots a_0 = \sum_{i=0}^r a_i 10^i.$$

Il numero n   divisibile per un intero $m > 1$ se e solo se $n(\bmod m) = 0(\bmod m)$. Si ha che

$$n(\bmod m) = \left[\sum_{i=0}^r a_i 10^i \right](\bmod m) = \sum_{i=0}^r (a_i 10^i)(\bmod m) = \sum_{i=0}^r [a_i(\bmod m)] \cdot [10^i(\bmod m)].$$

Per $m = 2$ oppure 5 si ha che $10^i(\bmod m) = 0(\bmod m)$ per ogni $i \geq 0$.

Per $m = 3$ oppure 9 si ha che $10^i(\bmod m) = 1(\bmod m)$ per ogni $i \geq 0$.

Per $m = 11$ si ha che $10^i(\bmod m) = -1(\bmod m)$ per ogni $i \geq 0$ dispari e invece $10^i(\bmod m) = 1(\bmod m)$ per ogni $i \geq 0$ pari.

Deduciamo che $n(\bmod 2) = a_0(\bmod 2)$ e analogamente $n(\bmod 5) = a_0(\bmod 5)$. Quindi n   divisibile per 2 (risp. per 5) se e solo se $a_0 = 0, 2, 4, 6, 8$ (risp. $a_0 = 0, 5$).

Inoltre n   divisibile per 3 (risp. per 9) se e solo se la somma delle cifre di n (i.e. $\sum_{i=0}^r a_i$)   divisibile per 3 (risp. per 9).

Infine n   divisibile per 11 se e solo se la somma alternata delle cifre di n (i.e. $\sum_{i=0}^r (-1)^i a_i$)   divisibile per 11.

Se $n \in \mathbb{Z}_{<0}$ ed m   un intero, $m > 1$ allora $n(\bmod m) = 0(\bmod m)$ se e solo se $-n(\bmod m) = 0(\bmod m)$ quindi ci possiamo ricondurre al caso $n \in \mathbb{Z}_{\geq 0}$.

Crivello di Eratostene

Sia n un numero intero positivo. Ci sono diversi modi per determinare e scrivere una lista dei numeri primi minori o uguali ad n . Un algoritmo molto semplice   il crivello di Eratostene. Per una descrizione del crivello di Eratostene si veda

[http : //en.wikipedia.org/wiki/Sieve_of_Eratosthenes](http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes)

Nota bene: in questo algoritmo   sufficiente escludere i multipli dei numeri primi $p \leq \sqrt{n}$ (si noti che se n   il quadrato di un numero primo occorre testare tutti i primi fino a $\sqrt{n}$ compreso). Questo fatto   una conseguenza della seguente osservazione.

Osservazione 1. *Se un numero intero positivo n   composto allora esiste un numero primo $p \leq \sqrt{n}$ tale che p divide n .*

Dimostrazione. Se n   composto allora $n = a \cdot b$ dove a e b sono due interi positivi. Almeno uno tra a e b   minore o uguale a $\sqrt{n}$. Supponiamo che si abbia $b \leq \sqrt{n}$. Allora possiamo prendere come primo p un qualunque divisore primo di b . $\square$

Da questo fatto segue anche:

Osservazione 2. *Nota la tavola dei numeri primi fino a $\sqrt{n}$ possiamo verificare se n   primo nel seguente modo: basta verificare che n non   un multiplo di p per ogni primo $p \leq \sqrt{n}$.*

Polinomi a coefficienti interi

Sia n un numero intero positivo e sia f un polinomio a coefficienti interi tale che $f(a) = n$ per un certo intero a . Supponiamo che il polinomio f si fattorizzi come prodotto di due polinomi a coefficienti interi g_1 e g_2 . Allora $n = f(a) = g_1(a) \cdot g_2(a)$. Dato che $g_1(a)$ e $g_2(a)$ sono due numeri interi la fattorizzazione del polinomio f puo' aiutarci a trovare la fattorizzazione del numero n . Diamo adesso la fattorizzazione di alcuni polinomi a coefficienti in $\mathbb{Z}$.

$$x^d - 1 = (x - 1)(x^{d-1} + x^{d-2} + \dots + 1) \text{ per ogni } d \geq 1;$$

$$x^d + 1 = (x + 1)(x^{d-1} - x^{d-2} + x^{d-3} - x^{d-4} \dots + 1) \text{ per ogni } d \geq 1 \text{ dispari.}$$

Invece ad esempio $x^2 + 1$ non si fattorizza come prodotto di polinomi a coefficienti in $\mathbb{Z}$.

Sulla ϕ di Eulero

Proposizione 3. Sia n un numero naturale, allora $\sum_{d|n} \phi(d) = n$ dove d varia tra i divisori di n (sono quindi inclusi 1 ed n).

Dimostrazione. Se $n = 1$ allora $n = \phi(1) = 1$ e l'affermazione e' vera. Dimostriamo ora l'affermazione per $n = p^a$ dove p e' un qualsiasi numero primo ed a e' intero, $a \geq 0$. Useremo l'induzione su a . Il caso iniziale $a = 0$ e' gia' stato verificato. Calcoliamo

$$\begin{aligned} \sum_{d|n} \phi(d) &= \phi(1) + \phi(p) + \dots + \phi(p^a) = \\ &= 1 + (p-1) + (p-1) \cdot p + \dots + (p-1)p^{a-1} = p + (p-1) \cdot p + \dots + (p-1)p^{a-1} = \\ &= p \cdot (1 + (p-1) + (p-1) \cdot p + \dots + (p-1)p^{a-2}) = p \cdot (\phi(1) + \phi(p) + \dots + \phi(p^{a-1})) \end{aligned}$$

che per ipotesi induttiva si scrive come

$$p \cdot p^{a-1} = p^a.$$

Adesso mostriamo l'affermazione se n e' composto per induzione su n . Come caso iniziale prendiamo come prima $n = 1$. Scriviamo $n = p^a \cdot n_0$ dove p e' un primo e p non divide n_0 . Scriviamo l'insieme dei divisori di n come unione dei seguenti insiemi:

$$\{d_0 | n_0\} \cup \{p \cdot d_0 \text{ con } d_0 | n_0\} \cup \dots \cup \{p^a \cdot d_0 \text{ con } d_0 | n_0\}$$

Allora scriviamo

$$\begin{aligned} \sum_{d|n} \phi(d) &= \sum_{d_0 | n_0} [\phi(d_0) + \phi(p \cdot d_0) + \dots + \phi(p^a \cdot d_0)] = \\ &= \sum_{d_0 | n_0} [\phi(d_0) + \phi(p) \cdot \phi(d_0) + \dots + \phi(p^a) \cdot \phi(d_0)] = \\ &= \sum_{d_0 | n_0} \phi(d_0) \cdot [1 + \phi(p) + \dots + \phi(p^a)] = \\ &= \left[\sum_{d_0 | n_0} \phi(d_0) \right] \cdot [\phi(1) + \phi(p) + \dots + \phi(p^a)]. \end{aligned}$$

Per ipotesi induttiva questa espressione e'

$$n_0 \cdot p^a = n.$$

Questo dimostra il passo induttivo e conclude la dimostrazione. □

1 Sul teorema di Wilson

Vogliamo calcolare la classe di resto di $(n-1)!$ modulo n dove n e' un intero maggiore di 1.

Se n non e' potenza di un primo possiamo scrivere $n = a \cdot b$ con a e b interi coprimi diversi da 1. Allora $a \leq n-1$, $b \leq n-1$ dunque $a \mid (n-1)!$ e $b \mid (n-1)!$. Dato che a e b sono coprimi allora $a \cdot b$ divide $(n-1)!$. Allora n divide $(n-1)!$ quindi la classe di resto di $(n-1)!$ modulo n e' la classe di resto dello 0 cioe' $0(\text{mod } n)$.

Sia $n = p^a$ con $a \geq 3$. Allora p^{a-1} e p sono fattori di $(n-1)!$ quindi p^a divide $(n-1)!$ e allora la classe di resto di $(n-1)!$ modulo n e' $0(\text{mod } n)$.

Sia $n = p^2$ e p diverso da 2. Allora p e $2p$ sono fattori di $(n-1)!$ quindi p^2 divide $(n-1)!$ e allora la classe di resto di $(n-1)!$ modulo n e' $0(\text{mod } n)$. Se $n = 2^2 = 4$ allora $3! = 2(\text{mod } 4)$.

Se $n = p$ primo la classe di resto di $(p-1)!$ modulo p e' -1 . Questo risultato e' noto come Teorema di Wilson e ne diamo adesso una dimostrazione.

Dimostrazione. Abbiamo

$$(p-1)! = (p-1) \cdot (p-2) \cdot \dots \cdot 2 \cdot 1$$

quindi

$$(p-1)!(\text{mod } p) = (p-1)(\text{mod } p) \cdot (p-2)(\text{mod } p) \cdot \dots \cdot 2(\text{mod } p) \cdot 1(\text{mod } p)$$

Stiamo moltiplicando tra loro tutti gli elementi del gruppo $\mathbb{Z}_p^*$. Dato che p e' primo questo gruppo e' il sottoinsieme di $\mathbb{Z}_p$ che si ottiene rimuovendo l'elemento $0(\text{mod } p)$. L'operazione definita nel gruppo $\mathbb{Z}_p^*$ e' la moltiplicazione. Dalla definizione di gruppo ricaviamo che ogni elemento di $\mathbb{Z}_p^*$ ha un unico inverso moltiplicativo. Possiamo scrivere $\mathbb{Z}_p^*$ come unione disgiunta di sottoinsiemi $\{x, x^{-1}\}$ dove x e' un elemento di $\mathbb{Z}_p^*$ e x^{-1} e' l'inverso di x .

Se $x = 1(\text{mod } p)$ oppure $x = -1(\text{mod } p)$ l'insieme $\{x, x^{-1}\}$ e' in realta' costituito da un solo elemento o equivalentemente $x^{-1} = x$. Dimostreremo nell'Osservazione ?? che si ha $x^{-1} = x$ solo se $x = 1(\text{mod } p)$ oppure $x = -1(\text{mod } p)$.

Gli elementi di $\mathbb{Z}_p^*$ si dividono in due sottoinsiemi: gli elementi che coincidono con il proprio inverso e gli elementi che non coincidono con il proprio inverso. Facciamo il prodotto di tutti gli elementi di $\mathbb{Z}_p^*$ che non coincidono con il proprio inverso. Stiamo allora facendo il prodotto di tutti gli elementi di tutti i sottoinsiemi $\{x, x^{-1}\}$ dove x e' un elemento di $\mathbb{Z}_p^*$ tale che x e x^{-1} sono distinti. Ma il prodotto degli elementi del sottoinsieme $\{x, x^{-1}\}$ e' $x \cdot x^{-1} = 1(\text{mod } p)$ quindi il prodotto degli elementi che non coincidono con il loro inverso e' il prodotto di tanti fattori $x(\text{mod } p) \cdot x^{-1}(\text{mod } p) = 1(\text{mod } p)$ ed e' quindi in totale $1(\text{mod } p)$. Invece il prodotto degli elementi che non coincidono con il loro inverso e' il prodotto di $1(\text{mod } p)$ e di $-1(\text{mod } p)$ ed e' quindi $-1(\text{mod } p)$. Deduciamo che

$$(p-1)!(\text{mod } p) = (p-1)(\text{mod } p) \cdot (p-2)(\text{mod } p) \cdot \dots \cdot 2(\text{mod } p) \cdot 1(\text{mod } p) = -1(\text{mod } p)$$

□

Osservazione 4. Sia p un numero primo. In $\mathbb{Z}_p^*$ l'equazione $x = x^{-1}$ ha come soluzioni $1(\text{mod } p)$ e $-1(\text{mod } p)$ (queste soluzioni chiaramente coincidono se e solo se $p = 2$).

Dimostrazione. Si ha $x = x^{-1}$ se e solo se $x^2 = x \cdot x^{-1} = 1(\text{mod } p)$. Questo vuol dire che $x^2 - 1$ e' divisibile per p . Per definizione $x = a(\text{mod } p)$ dove a e' un intero con $0 < a < p$. Allora dobbiamo studiare per quali a (con a intero e $0 < a < p$) il numero $a^2 - 1$ e' divisibile per p . Abbiamo $a^2 - 1 = (a+1)(a-1)$ e p divide un prodotto se e solo se divide uno dei fattori. Allora se p divide $a - 1$ deve essere $a = 1$. Se p divide $a + 1$ deve essere $a = p - 1$. □