

METODI DI FATTOORIZZAZIONE

CRIVELLO DI ERATOSTENE.

Si scrivono tutti i numeri da 1 fino a n

$$n = 60$$

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |

$$\sqrt{60} \approx 7,745$$

Le eliminazioni dei multipli di $\leq n$ eseguono fino al più grande numero naturale $\leq \sqrt{n}$: nel caso in esame 7.

Verifica: Siano $q_1, \dots, q_a = q$ i numeri primi minori o uguali di \sqrt{n} ; tutti i multipli di q_1, \dots, q_n sono stati già eliminati. Se $a > q$ e se a non è primo, allora a è il prodotto di alcuni dei numeri

piùni precedenti, cioè di alcuni dei $q_1 \cdots q_n$ e quindi a è già stato eliminato. Se a è un numero primo allora i prodotti $q_1 \cdot a, q_2 \cdot a, \dots, q_n \cdot a$ sono strettamente già eliminati oppure sono maggiori di n ; d'altra parte il prodotto di a per un altro numero primo p maggiore di \sqrt{n} è più grande di n , perché:

$$a > \sqrt{n}, \quad p > \sqrt{n}$$

$$\text{e quindi } a \cdot p > \sqrt{n} \cdot \sqrt{n} = n.$$

In conclusione, eliminando man mano i multipli dei numeri non cancellati e facendo questo operazione fino a \sqrt{n} restano non cancellati tutti e soli i numeri primi minori o uguali di n .

Per fattorizzare un numero intero m , possiamo cercare tutti i numeri primi che precedono m : in realtà possiamo cercare i fattori primi minori e quelli di $n = \sqrt{m}$. Infatti se il numero m non è primo, sicuramente esiste un fattore primo di m minore o uguale di \sqrt{m} . Se infatti i fattori di m fossero tutti maggiori di \sqrt{m} , per esempio

$$m = p_1 \cdot p_2 \cdots \cdot p_k \quad (\text{eventualmente ripetuti})$$

$$m = p_1 \cdot p_2 \cdots \cdot p_k > \underbrace{\sqrt{m} \cdot \sqrt{m} \cdots \cdot \sqrt{m}}_{k\text{-volte}} \geq \sqrt{m} \cdot \sqrt{m} = m$$

$\Rightarrow m > m$ contraddizione.

Per fondare un numero intero m bisogna effettuare le divisioni di m per ogni primo $p \leq \sqrt{m}$. Se il numero non è primo, sicuramente si trova un fattore fra questi; al contrario, se non c'è alcun fattore fino a \sqrt{m} allora m è primo.

Esempio $m = 33.061$

$$\sqrt{m} \approx 181$$

Numeri primi fino a 181

$$\underbrace{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \dots}$$

Scriveteli tutti per esercizio.

Si effettuano le divisioni fino a che non si ottiene resto 0.

$$33.061 = 7 \cdot 4720 + 1$$

m non è divisibile per 7.

$$\cancel{+3} - \cancel{3} + 0 - 4 + 1 = -3$$

11×-3 per cui m non è
divisibile per 11.

eseguendo le divisioni, si vede che m non è divisibile
per 13 e neanche per 17.

$$m = 33.061 = 19 \cdot 1.739$$

1.739 per chi' è divisibile?

$$\sqrt{1.739} \approx 41,703$$

dividere per tutti i numeri primi minori o uguali di 41.
Effettuando le divisioni 19, 23, 29, 31 si ottengono
resti non nulli, mentre 1.739 è divisibile per 37
e si ha

$$1.739 = 37 - 47$$

$$+6 - 1 + 3 = 8$$

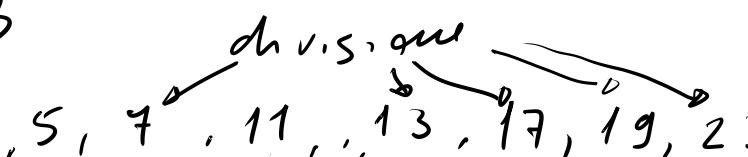
La conclusione $m = 19 \cdot 37 \cdot 47$.

Esempio: $m = 613$

$$\sqrt{m} \approx 24,758$$

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

m non è divisibile per 2, 3, 5, 7, 11, 13, 17, 19, 23



Quando per l'orologio di Eratostene il numero è primo.

METODO DI FATTOORIZZAZIONE DI FERMAT.

Osserv. Sia $n \in \mathbb{N}$, $n \neq 0, 1$, a dispari.

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

Dim. Ipotesi $\exists a, b \in \mathbb{N}$ tali che $n = a \cdot b$
tali $\exists x, y \in \mathbb{N}$ tali che $n = x^2 - y^2$.

Siamo $x = \frac{a+b}{2}$ $y = \frac{a-b}{2}$

$$\begin{aligned} x^2 - y^2 &= \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} - \frac{a^2 - 2ab + b^2}{4} = \\ &= \frac{\cancel{a^2} + 2ab + \cancel{b^2} - \cancel{a^2} + 2ab - \cancel{b^2}}{4} = \frac{4ab}{4} = ab = n \end{aligned}$$

$$\exists x, y \in \mathbb{N} \text{ tali che } n = x^2 - y^2$$

Viceversa: Ipotesi: $\exists x, y \in \mathbb{N}$ tali che $n = x^2 - y^2$
tali i $\exists a, b \in \mathbb{N}$ tali che $n = a \cdot b$

$$n = x^2 - y^2 = (x-y)(x+y) \quad \text{Allora basta porre } a = x-y, b = x+y$$

e risulta $n = a \cdot b$.

Allora n si scomponga se e solo se esistono $x, y \in \mathbb{N}$ tali che $n = x^2 - y^2$, ovvero $x^2 - n = y^2$;

n si scomponibile se esiste $x \in \mathbb{N}$ tale che $x^2 - n$ sia un quadrato (perfetto).

Algoritmo: Si prende t il più piccolo numero intero maggiore o uguale di \sqrt{n}

$t^2 - n$ se è un quadrato OK, se non
è un quadrato si calcola

$$(t+1)^2 - n$$

$$(t+2)^2 - n$$

$$(t+3)^2 - n$$

$$\vdots$$

$$(t+h)^2 - n = y^2$$

$$x = t + h$$

$$x^2 - n = y^2$$

$$x^2 - y^2 = n$$

$$(x-y)(x+y) = n.$$

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

Esempio $n = 343$ $\sqrt{n} \approx 18,57$ $t = 19$

$$19^2 - 343 = 361 - 343 = 18 \quad \text{non è un quadrato}$$

$$20^2 - 343 = 400 - 343 = 57 \quad " " " "$$

$$21^2 - 343 = 441 - 343 = 98 \quad " " " "$$

$$22^2 - 343 = 484 - 343 = 161 \quad " " " "$$

$$23^2 - 343 = 529 - 343 = 186 \quad " " " "$$

$$24^2 - 343 = 576 - 343 = 233 \quad " " " "$$

$$25^2 - 343 = 625 - 343 = 282 \quad " " " "$$

$$26^2 - 343 = 676 - 343 = 333 \quad " " " "$$

$$27^2 - 343 = 729 - 343 = 386 \quad " " " "$$

$$28^2 - 343 = 784 - 343 = 441 = 21^2$$

$$343 = 28^2 - 21^2 = (28 + 21)(28 - 21) = \\ = 49 \cdot 7 = 7^3.$$

TEOREMA DI EULERO FERMAT.

LEMMA. Siano $x, y \in \mathbb{Z}$, $p \in \mathbb{N}$, p primo.

Allora si prova che

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Senza dimostrazione.

Pirrola Teorema di Fermat.

Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ primo. Allora

$$a^p \equiv a \pmod{p}$$

Dim 1° caso $a > 0$: si procede per induzione completa su a .

Passo base

$$a = 0 \quad 0^{p-1} \equiv 0 \pmod{p} \quad \text{vera}$$

Passo induktivo : $a^p \equiv a \pmod{p}$ ipotesi d'induzione

$$(a+1)^p \equiv a+1 \pmod{p} \quad \text{fesi!}$$

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

Lemma

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

$$a^p \equiv a \pmod{p}$$

↑
ipotesi d'induzione

$$1 \equiv 1 \pmod{p}$$

$$(a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}) \Rightarrow a+c \equiv b+d \pmod{n}$$

$$a^p + 1 \equiv a + 1 \pmod{p}$$

$$(a+1)^p \equiv \underline{a^p + 1} \pmod{p} \quad \wedge \quad \underline{a^p + 1} \equiv a+1 \pmod{p}$$

per le proprietà delle congruenze (mod p) avremo che $(a+1)^p \equiv a+1 \pmod{p}$.

allora il teorema vale per $a \geq 0$.

2° caso $a < 0$ allora $-a > 0$

per il 1° caso $(-a)^p \equiv -a \pmod{p}$
 $-a \equiv -a \pmod{p}$

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

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

Lemma

$$\frac{(-a)^p + a^p}{(-a)^p + a^p} \equiv \frac{-a + a^p}{-a + a^p} \pmod{p}$$

$$\frac{-a + a^p}{-a + a^p} \equiv 0 \pmod{p}$$

per la
fornitività: $a^p - a \equiv 0 \pmod{p}$

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

(*)

Esempio: Calcolare il resto della divisione del numero

21.501^{4121} per 7 senza eseguire la divisione

$$21.501 = 7 \cdot 3.071 + 4 \quad \text{e quindi}$$

$$21.501 \equiv 4 \pmod{7}$$

purché $21.501 - 4 = 7 \cdot 3.071 \Rightarrow 7 \nmid 21.501 - 4 \Rightarrow$

$$21.501 \equiv 4 \pmod{7}.$$

$$21.501^{4121} \equiv 4^{4121} \pmod{7}$$

(*) Corollario del Piccolo Teorema di Fermat:

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

Allora

$$a^{p-1} \equiv 1 \pmod{p}$$

Dim. $a^p \equiv a \pmod{p} \Rightarrow p \mid a^p - a \Rightarrow p \mid a/a^{p-1} - 1$

$(p \text{ primo} \wedge p \nmid a) \Rightarrow p \mid a^{p-1} - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$$\text{Per il corollario } 4^{7-1} \equiv 1 \pmod{7}$$

$$4^6 \equiv 1 \pmod{7}$$

$$(16)^3 = 4.096$$

$$4.096 - 1 = 4.095$$

$$4.095 : 7 = 585$$

$$4.121 = 6 \cdot 686 + 5$$

$$4^{4.121} = 4^{6 \cdot 686 + 5} = (4^6)^{686} \cdot 4^5 \equiv 1^{686} \cdot 4^5 = 4^5 \pmod{7}$$

$$21.501^{4.121} \equiv 4^5 \equiv 4 \pmod{7}$$

$$4^5 = 1.024$$

$$1.024 = 7 \cdot 146 + 2 \equiv 2 \pmod{7}$$

$$21.501^{4.121} \equiv 2 \pmod{7}$$

e quindi il resto è 2.

Funzione di Eulero

$$\varphi : \mathbb{N} - \{0, 1\} \longrightarrow \mathbb{N}$$

$\forall x \in \mathbb{N} - \{0, 1\}$ $\varphi(x)$ = numero dei numeri
precedenti x e primi con x .

Esempi: $\varphi(2) = 1$ $M.C.D.(2, 1) = 1$

$$\varphi(3) = 2 \quad 1, 2 \quad M.C.D.(3, 1) = 1$$
$$M.C.D.(3, 2) = 1$$

$$\varphi(4) = 2 \quad 1, 3$$

$$\varphi(5) = 4 \quad 1, 2, 3, 4$$

$$\varphi(6) = 2 \quad 1, 5$$

Se p è un numero primo, allora $\varphi(p) = p - 1$.

Prop. La funzione di Eulero è moltiplicativa: cioè se $x = a \cdot b$, $a, b \neq 1$, $M.C.D.(a, b) = 1$, allora

$$\varphi(x) = \varphi(a) \cdot \varphi(b)$$

Esempio $\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$$

1, 2, 4, 7, 8, 11, 13, 14 sono gli 8 numeri precedenti 15 e primi con 15.

$$\varphi(45) = \varphi(5 \cdot 9) = \varphi(5) \cdot \varphi(9) = 4 \cdot 6 = 24$$

$\varphi(9)$? 1, 2, 4, 5, 7, 8 $\varphi(9) = 6$

Prop. Se p è un numero primo, allora $\varphi(p) = p - 1$.

Prop. Se p è un numero primo, allora

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

Esempio : $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$

$$\varphi(9) = \varphi(3^2) = 3^2 - 3 = 9 - 3 = 6$$

$$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

Prop. Sia $n \in \mathbb{N}^*$, $n \neq 1$. Allora esistono p_1, \dots, p_k numeri primi ed esistono $k_1, \dots, k_n \in \mathbb{N}^*$ tali che

$$n = p_1^{k_1} \cdot \dots \cdot p_k^{k_n}$$

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1} \cdot \dots \cdot p_k^{k_n}) = \varphi(p_1^{k_1}) \cdot \dots \cdot \varphi(p_k^{k_n}) \\ &= (p_1^{k_1} - p_1^{k_1-1}) \cdot \dots \cdot (p_k^{k_n} - p_k^{k_n-1})\end{aligned}$$

Esempio : $n = 2^3 \cdot 3 \cdot 5^3 \cdot 7^2$

$$\begin{aligned}\varphi(n) &= \varphi(2^3 \cdot 3 \cdot 5^3 \cdot 7^2) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5^3) \cdot \varphi(7^2) \\ &= (2^3 - 2^2) \cdot 2 \cdot (5^3 - 5^2) \cdot (7^2 - 7) = \\ &= 4 \cdot 2 \cdot 100 \cdot 42.\end{aligned}$$

Teorema di Euler - Fermat.

Siano $a \in \mathbb{Z}^*$, $n \in \mathbb{N} - \{0, 1\}$, con $\text{H.C.D.}(a, n) = 1$.

Allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.
(senza dim.)

Corollari del piccolo T. di Fermat: caso particolare del teorema di Euler - Fermat.

$$\text{se } p \text{ primi} \Rightarrow \varphi(p) = p-1$$

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

Esercizio (appello di novembre 2021)

Calcolare l'ultima cifra del numero $18.523^{3.458}$.

Bisogna trovare il resto delle divisioni di $18.523^{3.458}$ per 10.

$$18.523 = 1.852 \cdot 10 + 3$$

$$18.523 \equiv 3 \pmod{10}$$

Si applica il Teorema di Euler - Fermat

$$3^{\varphi(10)} \equiv 1 \pmod{10}$$

$$\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$$

$$3^4 \equiv 1 \pmod{10}$$

$$3 \cdot 458 = \cancel{4} \cdot 864 + 2 \quad \left(a^{p+q} = a^p \cdot a^q \right)$$

$$18 \cdot 523^{3 \cdot 458} \equiv 3^{3 \cdot 458} \pmod{10}$$

$$3^{3 \cdot 458} = 3^{4 \cdot 864 + 2} = (3^4)^{864} \cdot 3^2 \equiv 1^{864} \cdot 3^2 \pmod{10}$$

$$18 \cdot 523^{3 \cdot 458} \equiv 3^2 \pmod{10}$$

$$18 \cdot 523^{3 \cdot 458} \equiv 9 \pmod{10}$$

il resto è 9, quindi l'ultima cifra è 9.

Esercizio. Resto della divisione di $4 \cdot 183^{381}$ per 8

$$4 \cdot 183 = 8 \cdot 522 + 7 \Rightarrow 4 \cdot 183 \equiv 7 \pmod{8}$$

$$\text{M.C.D.}(7, 8) = 1$$

$$7^{\varphi(8)} \equiv 1 \pmod{8}$$

$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$$

$$7^4 \equiv 1 \pmod{8}$$

Si divide l'esponente per $k = \ell(8)$

$$381 = 6 \cdot 95 + 1$$

$$6 \cdot 183^{381} \equiv 7^{381} \pmod{8}$$

$$7^{381} = (7^6)^{95} \cdot 7 \equiv 1^{95} \cdot 7 - 7 \pmod{8}$$

$$6 \cdot 183^{381} \equiv 7 \pmod{8}$$

il resto richiesto è 7.