Extra 2: esercizi secondo foglio

Sunday, October 11, 2020 3:44 PM

img2020...

Come si ricava esplicitamente l'identità di Bézout? (1)

Vediamo due esempi.

(1) Abbiamo già visto che $MCD(1001, 345) = 1$ poiché

$$
\begin{aligned}
1001 &= 2 \cdot 345 + 311 \\
345 &= 1 \cdot 311 + 34 \\
311 &= 9 \cdot 34 + 5 \\
34 &= 6 \cdot 5 + 4 \\
5 &= 1 \cdot 4 + 1 \quad \leftarrow \text{MCD.} \\
4 &= 4 \cdot 1 + 0
\end{aligned}
$$

Procediamo a ritroso.

$1 = 1 \cdot 5 - 1 \cdot 4$ Ma $4 = 34 - 6 \cdot 5$

$= 1 \cdot 5 - (34 - 6 \cdot 5) = 7 \cdot 5 - 34$

Ma $5 = 311 - 9 \cdot 34$ quindi

$1 = 7(311 - 9 \cdot 34) - 34 = 7 \cdot 311 - 64 \cdot 34$

Ma $34 = 345 - 311$ quindi

$1 = 7 \cdot 311 - 64(345 - 311) = 71 \cdot 311 - 64 \cdot 345$

Ma $311 = 1001 - 2 \cdot 345$ quindi

$1 = 71 \cdot (1001 - 2 \cdot 345) - 64 \cdot 345 = 71 \cdot 1001 - 206 \cdot 345$

$h \quad a \quad k \quad b$

② $MCD(35,21) = 7$

$35 = 1 \cdot 21 + 14$
$21 = 1 \cdot 14 + 7$ ← MCD
$14 = 2 \cdot 7 + 0$

$7 = 21 - 14 = 21 - (35 - 21) = 2 \cdot 21 - 35$

$7 = (-1) \cdot 35 + 2 \cdot 21$ ✓

Esistono infiniti primi $\equiv 3 \mod 4$.

Dim: se ve ne sono solo una quantità finita $q_1, q_2, \dots, q_k$ calcolo

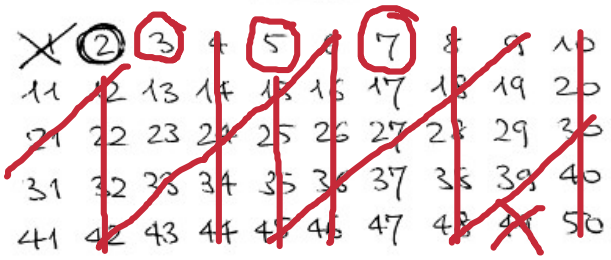
$N = 4 \cdot q_1 q_2 \cdots q_k - 1 \qquad 2 \nmid N, \ q_1, \dots, q_k \nmid N$

$\Rightarrow$ N è prodotto di primi $\equiv 1 \mod 4 \Rightarrow N \equiv 1 \mod 4$ assurdo.

Ex: Esistono infiniti primi $\equiv 5 \mod 6$ $(6k-1)$.

Hint: $6q_1 \cdots q_r - 1 \dots$

Crivello di Eratostene Come trovo i primi fino a 50?



Tolgo i multipli di p solo a partire da p^2

Se N è composto $N = ab$, allora uno dei fattori è $\leq \sqrt{N} \Rightarrow$ lo divide un primo $\leq \sqrt{N}$.

① $a^2 + b^2$ non può essere $\equiv 3 \mod 4$ $(a, b \in \mathbb{Z})$. ③

$(2n)^2 = 4n^2 \equiv 0 \mod 4 \qquad (2n+1)^2 = 4(n^2+n) + 1 \equiv 1 \mod 4$

in realtà mod 8

Se sommo due quadrati perfetti, mod 4 ottengo $0+0, 0+1, 1+0, 1+1$, quindi mai 3.

② a. Mostrare che $m \mid n$ implica $a^m-1 \mid a^n-1$. $\left(\begin{smallmatrix} a,m,n \in \mathbb{N} \\ a,m>1 \end{smallmatrix}\right)$

Ricordate che siamo in grado di calcolare il MCD a partire dalle proprietà $MCD(a,0)=a$, $MCD(a,b)=MCD(b,a)$,
$MCD(a,b)=MCD(a\pm b,b)$. ← iterando si ottiene
$MCD(a\pm qb,b)=MCD(a,b)$
e questa è la descrizione dell'algoritmo euclideo.

Ora: $MCD(a^m-1, a^0-1)=a^m-1$.
$MCD(a^m-1, a^n-1)=MCD(a^n-1, a^m-1)$
$MCD(a^m-1, a^n-1)=MCD(a^{m\pm n}-1, a^n-1)$

Se $d \mid a^m-1, a^n-1$, allora divide anche $a^m-1-a^{m-n}(a^n-1)=$
$=a^{m-n}-1$.

Pertanto $MCD(a^m-1, a^n-1)=a^{MCD(m,n)}-1$.

In particolare, a^m-1 divide $a^n-1 \iff MCD(a^m-1, a^n-1)=a^m-1$
$\iff a^m-1=a^{MCD(m,n)}-1 \iff m=MCD(m,n) \iff m$ divide n.

b. Se n è composto (diciamo $n=ab$, $a,b>1$) allora
$2^n-1=2^{ab}-1$ ammette 2^b-1 come fattore, e $2^b-1<2^n-1$.
Di conseguenza, 2^n-1 non può essere primo (ho un fattore proprio).
Equivalentemente, a^n-1 primo $\Rightarrow n$ primo.

c. a^n-1 è multiplo di $a-1$; se $a>2$ e $n>1$, questo è un fattore proprio di a^n-1. Pertanto se a^n-1, $a,n>1$, è primo allora $a=2$ e per quanto detto in b., n è primo.

I numeri primi della forma 2^p-1, p primo, si chiamano ④ primi di Mersenne (non sono tantissimi).

③ $a,n>1$. Che possiamo concludere se a^n+1 è primo?

Se a è dispari, a^m+1 è pari ($e>2$) e non può essere primo.
Pertanto a è sicuramente pari.

Voglio mostrare che n non può avere divisori dispari ($\neq 1$).

In effetti $x^3+1=(x+1)(x^2-x+1)$
$x^5+1=(x+1)(x^4-x^3+x^2-x+1)$.

In generale, $x^{\text{dispari}}+1$ ammette $x+1$ come divisore.

Se $n = dh$ con d dispari (>1) allora

$a^n + 1 = a^{dh} + 1 = (a^h)^d + 1$ è multiplo di $a^h + 1 < a^n + 1$

e non può essere primo.

Ma se n non ha divisori dispari $\neq 1$, l'unico primo che lo divide è 2, e quindi n è una potenza di 2.

NB: I numeri primi della forma $2^{2^n} + 1$ si chiamano primi di Fermat (si pensa siano in numero finito. Quelli noti sono 3, 5, 17, 257, 65537, cioè $n = 1, 2, 3, 4, 5$)

④ a. $7n^{34} - n^{21} + 22n^5 + 4n^4 - 21n$ è multiplo di 11.

Intanto è $\equiv 7n^{34} - n^{21} + 4n^4 + n$ PTF: $n \equiv n^{11} \mod 11$.

$n^2 = n \cdot n \equiv n \cdot n^{11} \mod 11$. In generale $n^d \equiv n^{d+10} \equiv \dots \equiv n^{d+10k} \mod 11$ se $d \geq 1$.

n^{12}

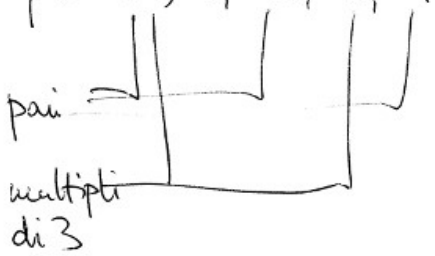
$7n^{34} - n^{21} + 4n^4 + n \equiv 7n^4 - n + 4n^4 + n \equiv 11n^4 \equiv 0 \mod 11$.

b. Allo stesso modo $n^d \equiv n^{d+6k} \mod 7$ se $d > 0$ quindi

$n^{55} + 2n^{50} + 3n^{45} + 4n^3 + 5n^2 + 6n \equiv n + 2n^2 + 3n^3 + 4n^3 + 5n^2 + 6n = 7(n^3 + n^2 + n) \equiv 0 \mod 7$

⑤ a. i primi ≥ 5 sono congrui a $\pm 1 \mod 6$. ⑤

$p \equiv 0, 1, 2, 3, 4, 5 \mod 6$



Rimangono 1 e $5 \equiv -1 \mod 6$.

b. Premessa: PTF $a^p \equiv a \mod p$.

Se $p \nmid a$, cioè se $MCD(a,p) = 1$, posso dire che

$p \mid a^p - a = a(a^{p-1} - 1)$. Poiché $MCD(p,a) = 1$, allora

p divide $a^{p-1} - 1$, cioè $a^{p-1} \equiv 1 \mod p$.

$a^{2p-2} + a^{p-1} + p - 2 \equiv (a^{p-1})^2 + a^{p-1} - 2 \equiv 1^2 + 1 - 2 \equiv 0 \mod p$.

c. $(10^{p-2} + 10^{p-1} + \dots + 10 + 1)(10 - 1) = 10^{p-1} - 1$. NB: $10 = 2 \cdot 5$.

Se $p > 5$, allora $MCD(p, 10) = 1$ e quindi $10^{p-1} \equiv 1 \mod p$.

Allora p divide $10^1 - 1 = (10-1)\cdot(10 + \dots + 10 + 1)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \ 9$

Ma $MCD(p, 9) = 1$, quindi p divide $10^{p-2} + \dots + 10 + 1$

poiché $p > 5$ non è 3

⑥ Devo mostrare che $5^n + 7^n$ è multiplo di 12 $\iff$ n è ~~pari~~ dispari

Faccio i conti modulo 12,

$5^n + 7^n \equiv 5^n + (-5)^n = 5^n \cdot (1 + (-1)^n)$.

~~Se~~ Se 12 $\mid 5^n(1+(-1)^n)$, poiché $MCD(12,5) = 1 \Rightarrow MCD(12, 5^n) = 1$

allora 12 divide $1 + (-1)^n$. Questo è 2 se n è pari e 0 se n è dispari.

⑦ a. $MCD(ab, a+b)$ divide $MCD(a^2, b^2)$. ⑥

È sufficiente mostrare che se d divide ab e $a+b$, allora divide sia a^2 che b^2.

$a^2 = a(a+b) - ab$ $\qquad$ $b^2 = b(a+b) - ab$ ✓

b. $MCD(3a+4, 4a+5) = 1$.

Se d divide $4a+5$ e $3a+4$, divide anche la differenza

$4a+5 - (3a+4) = a+1$.

Ma allora d divide anche $3a+4 - 3(a+1) = 1$.

Quindi $d = \pm 1$.

Criteri di divisibilità 12345678 è divisibile per 3?

$= 1\cdot 10^7 + 2\cdot 10^6 + 3\cdot 10^5 + 4\cdot 10^4 + 5\cdot 10^3 + 6\cdot 10^2 + 7\cdot 10 + 8 \equiv ?$ mod 3.

$10 \equiv 1$ mod $3 \Rightarrow 10^n \equiv 1$ mod 3

$\equiv 1+2+3+4+5+6+7+8 = 36 \equiv 3+6 = 9 \equiv 0$ mod 3.

mod 9 è la stessa cosa: $10 \equiv 1$ mod 9.

---

mod 2 $10 \equiv 0$ mod $2 \iff 10^n \equiv 0$ mod 2 se $n > 0$.

Quindi $\sum 10^n \cdot a_n \equiv a_0$ mod 2 ← decide tutto l'ultima cifra

mod 5 stessa cosa

mod 4 $10^0 \equiv 1$, $10^1 \equiv 2$, $10^n \equiv 0$ mod 4 se $n \geq 2$.

Quindi $\sum 10^n \cdot a_n \equiv 2a_1 + a_0 \mod 4$ ← decidono le ultime due cifre

mod 11 | $10^0 \equiv 1$, $10^1 \equiv 10 \equiv -1$, $10^n \equiv (-1)^n$ ⟨ 1 se n pari ; −1 se n dispari

$\sum 10^n \cdot a_n \equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) \mod 11$.

mod 7 | $10^0 \equiv 1$, $10^1 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1$ poi si ripetono

1 2 3 4 5 6 7 8 $\equiv 3 + 2 + 15 + 16 + 30 + 12 + 21 + 8 = 107 \equiv 9 \equiv 2 \mod 7$

3 1 5 4 6 2 3 1 (2 5 1)