ALGEBRA I: ESERCIZI DI ARITMETICA

(1) Siano $a, m, n \in \mathbb{N}$ con $a > 1$. Mostrare che se $\mathrm{MCD}(m, n) = d$, allora $\mathrm{MCD}(a^m - 1, a^n - 1) = a^d - 1$.
(2) Con le stesse ipotesi, mostrare che $a^m - 1$ divide $a^n - 1$ se e solo se m divide n.
(3) Mostrare che se $2^n - 1$ è primo, allora n è primo.[1]
(4) Siano $a > 1, n > 1$ numeri naturale. Mostrare che se $a^n - 1$ è primo, allora $a = 2$ e n è primo.
(5) Con le stesse ipotesi, mostrare che se $a^n + 1$ è primo, allora a è pari e n è una potenza di 2.
(6) Mostrare che $2^{2^n} + 1$ è primo se $n = 0, 1, 2, 3, 4$. Trovarne una fattorizzazione quando $n = 5$.[2]
(7) I numeri di Fibonacci sono definiti per ricorrenza da
   - $F_0 = 0, F_1 = 1$;
   - $F_n = F_{n-1} + F_{n-2}$ se $n > 1$.

   Calcolare $\mathrm{MCD}(F_{10}, F_9)$ eseguendo l'algoritmo euclideo.
(8) Mostrare per induzione che se l'algoritmo euclideo per calcolo di $\mathrm{MCD}(a, b)$, dove $a \geq b$, richiede almeno[3] n divisioni euclidee, allora $a \geq F_{n+1}$ e $b \geq F_n$.
(9) L'algoritmo euclideo può essere eseguito accettando anche resti negativi, se di valore assoluto inferiore, osservando che se $a > b > 0$ e $a = bq + r$, con $|r| \leq b/2$, allora $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, |r|)$.
   Eseguire questa variante dell'algoritmo per il calcolo di $\mathrm{MCD}(M_9, M_8)$ dove i numeri M_n sono definiti per ricorrenza da
   - $M_0 = 0, M_1 = 1$;
   - $M_n = 2M_{n-1} + M_{n-2}$ se $n > 1$.
(10) Mostrare per induzione che se l'utilizzo di questa variante per il calcolo di $\mathrm{MCD}(a, b)$, dove $a \geq 2b > 0$ richiede n divisioni, allora[4] $a \geq M_{n+1}$ e $b \geq M_n$. In particolare, se il calcolo di $\mathrm{MCD}(a, b)$, dove $a > b$ richiede n divisioni, allora $b \geq M_n$ e $a \geq M_n + M_{n-1}$.
(11) Se p è un numero primo, allora $(p-1)! \equiv -1 \mod p$.
   Sugg.: nel prodotto $[1][2] \dots [p-1]$ *in* $\mathbb{Z}/(p)$*, semplificate ogni classe con la sua inversa tutte le volte che potete.*
(12) Se $p \equiv 1 \mod 4$ è un numero primo, allora

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p.$$

(13) Calcolare l'identità di Bézout per $3 = \mathrm{MCD}(54321, 12345)$.
(14) Sia $N > 0$. Mostrare che $\mathrm{MCD}(N^2 - N + 1, N + 1)$ è 1 oppure 3.
(15) Trovare tutte le soluzioni $x \in \mathbb{Z}$ della congruenza lineare $112x \equiv 223 \mod 335$.
(16) Trovare tutte le soluzioni $x \in \mathbb{Z}$ della congruenza lineare $112x \equiv 222 \mod 346$.
(17) Calcolare l'inverso, se esiste, di $[123]$ in $\mathbb{Z}/(2345)$.
(18) Trovare tutte le soluzioni $x \in \mathbb{Z}$ del sistema di congruenze

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}$$

(19) Trovare tutte le soluzioni $x \in \mathbb{Z}$ del sistema di congruenze

$$\begin{cases} 2x \equiv 1 \mod 5 \\ 4x \equiv 1 \mod 7 \\ 7x \equiv 1 \mod 11 \end{cases}$$

(20) Trovare tutte le soluzioni $x \in \mathbb{Z}$ del sistema di congruenze

$$\begin{cases} x \equiv 2 \mod 4 \\ x \equiv 4 \mod 6 \\ x \equiv 6 \mod 8 \end{cases}$$

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it

[1] I primi di questa forma sono detti *primi di Mersenne*.
[2] I primi di questa forma sono detti *primi di Fermat*. Non ne sono noti per $n > 4$.
[3] F_n cresce asintoticamente come $((1 + \sqrt{5})/2)^n/\sqrt{5}$. Il numero di divisioni richieste per calcolare $\mathrm{MCD}(a, b)$ è quindi approssimativamente $4,78$ volte il numero delle cifre di b in base 10.
[4] M_n cresce asintoticamente come $(1 + \sqrt{2})^n/(2\sqrt{2})$. Il numero di divisioni richieste per calcolare $\mathrm{MCD}(a, b)$ è quindi approssimativamente $2,61$ volte il numero delle cifre di b in base 10. Questa variante è quasi due volte più rapida!