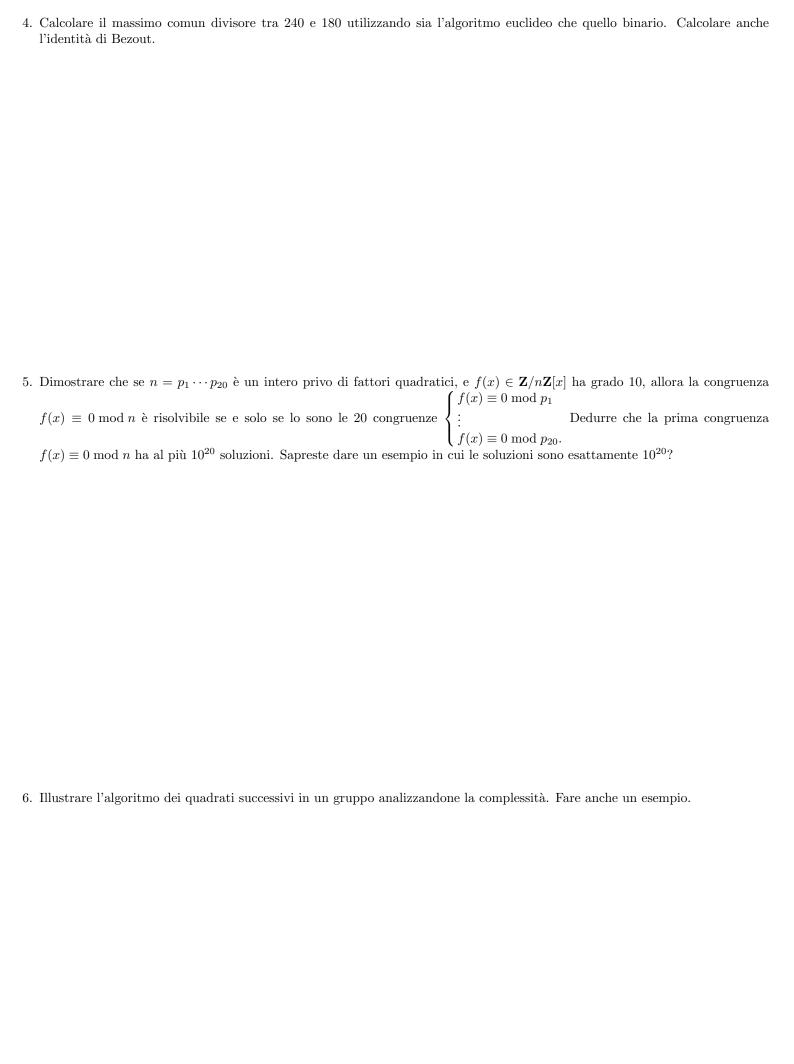
1. Se $n \in \mathbb{N}$, sia $\sigma(n)$ la somma dei divisori di n. Supponiamo che sia nota la fattorizzazione (unica) di $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Calcolare il numero di operazioni bit necessarie per calcolare $\sigma(n)$. (Suggerimento: Usare il fatto che σ è una funzione moltiplicativa e calcolare una formula per $\sigma(p^{\alpha})$)

2. Mostrare che le moltiplicazioni nell'anello quoziente $\mathbf{Z}/n\mathbf{Z}[x]/(x^d)$ si possono calcolare in $O(\log^2 n^d)$ operazioni bit mentre le addizioni in $O(\log n^d)$ operazioni bit.

3. Dato il numero binario $n = (10011100101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)



7.	Mettere in ord	line di prio	rità e spiega	re il signifi	cato di ciaso	cuna delle	seguenti ope	razioni:		
		$x \sim$	$x \wedge y$	x&y	x++	$x \backslash y$	x = y	x%y	x y	$x \ll n$
8.	Si dia la defir	nizione di p	seudo primo	o forte in h	pase 2 e si	mostri che	se $n = 2^{\alpha}$	+ 1 è pseu	do primo	forte in base 2, allora
	$2^{2^{\beta}} \equiv -1 \bmod$	n per qual	che $\beta < \alpha$.							
9.							v contiene i j	primi 100 p	oseudo-pri	mi composti in base 2 e
	il secondo i pr	imi 100 pse	eudo primi a	li Eulero co	<i>omposti</i> in b	ase 2.				

10. Implementare RSA u per decifrare).	itilizzando il	sistema	Pari e cr	eando tre	e funzion	i distinte	e (una pe	r genera	re le chia	avi, una p	er cifrare e una
NOME E COGNOME	2 1	2	3	4	5	6	7	8	9	10	TOTALE