Teoria de Números Computacional

—— folha 5			
Determine (a) $\operatorname{ord}_5 2$	(b) ord ₁₃ 10	(c) $ord_{10}3$	(d) $ord_{10}7$
Calcule (a) $\operatorname{ord}_{11}3$	(b) ord ₁₇ 2	(c) $ord_{21}10$	(d) $ord_{25}9$
Sejam $F_n =$	$2^{2^n} + 1$ o n -ésin	no número de F	ermat e p um factor primo de F_n .
•			
(a) 5 é um (b) 2 é um	a raiz primitiva a raiz primitiva	de 6; de 11.	
•	•		m dos seguintes naturais: (e) 14 (f) 18
Mostre que	12 não tem raíze	es primitivas.	
Mostre que	20 não tem raíze	es primitivas.	
Mostre que	se $(a,n) = 1$ ent	$\tilde{a}o \operatorname{ord}_n a^{-1} = o$	$\mathrm{rd}_n a$.
Mostre que s módulo p .	se a, b são raízes	primitivas módu	alo $p \neq 2$ primo então ab não é raiz primitiv
Calcule, mó	dulo 7,		
(a) ind_52			
(c) $\operatorname{ind}_5 0$ (d) $\operatorname{ind}_5 3^4$			
Resolva a co	_	rática $6x^{12} \equiv 1$	1 mod 17. Para tal, resolva cada uma da
• * *			
	Calcule (a) $ord_{11}3$ Sejam $F_n =$ (a) Mostre (b) Mostre (c) Mostre (d) 5 é um (e) 2 é um (f) 2 é um (g) 4 Mostre que (a) ind ₅ 2 (b) ind ₅ 3 (c) ind ₅ 6 (d) ind ₅ 3 Resolva a calíneas segu (a) Sabeno	Calcule (a) ord_52 (b) $\operatorname{ord}_{13}10$ Calcule (a) $\operatorname{ord}_{11}3$ (b) $\operatorname{ord}_{17}2$ Sejam $F_n = 2^{2^n} + 1$ o n -ésin (a) Mostre que $\operatorname{ord}_{F_n}2 \mid 2^n$ (b) Mostre que $\operatorname{ord}_{p}2 = 2^n$ (c) Mostre que p é necessa Mostre que (a) 5 é uma raiz primitiva (b) 2 é uma raiz primitiva (a) 4 (b) 5 (c) 10 Mostre que 12 não tem raíze Mostre que 20 não tem raíze Mostre que se $(a, n) = 1$ ent Mostre que se a, b são raízes módulo a Calcule, módulo 7, (a) a (b) a Calcule, módulo 7, (a) a (b) a Resolva a congruência quad alíneas seguintes: (a) Sabendo que a a a a a a a a	Calcule (a) ord_52 (b) $\operatorname{ord}_{13}10$ (c) $\operatorname{ord}_{10}3$ Calcule (a) $\operatorname{ord}_{11}3$ (b) $\operatorname{ord}_{17}2$ (c) $\operatorname{ord}_{21}10$ Sejam $F_n = 2^{2^n} + 1$ o n -ésimo número de Formalia (a) Mostre que $\operatorname{ord}_{F_n}2 \mid 2^{n+1}$. (b) Mostre que $\operatorname{ord}_{p}2 = 2^{n+1}$. (c) Mostre que p é necessariamente da formalia (a) 5 é uma raiz primitiva de 6; (b) 2 é uma raiz primitiva módulo cada un (a) 4 (b) 5 (c) 10 (d) 13 (d) 13 (e) 4 (d) 13 (e) 5 (e) 10 (d) 13 (e) 6 (d) ind_53 Resolva a congruência quadrática $\operatorname{6}x^{12} \equiv 1$

- (c) Construa a tabela dos índices de 3 módulo 17.
- (d) Mostre que $6x^{12} \equiv 11 \mod 17$ se e só se $15 + 12 \operatorname{ind}_3 x \equiv 7 \mod 16$
- (e) Resolva a congruência $15 + 12y \equiv 7 \mod 16$
- (f) Deduza que $ind_3x \equiv 2, 6, 10, 14 \mod 16$
- 12. Resolva a congruência $7^x \equiv 6 \mod 17$, sabendo que ind $3^7 = 11$ e que ind $3^6 = 15$.
- 13. Escorde o teste de primalidade de Lucas. Use-o para mostrar que 2003 é primo, com x = 5.
- 14. Usando a chave pública (p, r, b) = (2551, 6, 33) de um sistema de chave pública Elgamal, cifre a mensagem 133. Sabendo que a = 13 é a chave privada, decifre (421, 95).
- 15. Usando a chave pública (p, r, b) = (370113067, 3, 161485623) de um sistema de chave pública Elgamal, cifre a mensagem 138616298. Decifre (267037772, 234691095), sabendo que a chave privada é 164943214.
- 16. Calcule
 - (a) $\left(\frac{3}{11}\right)$
 - (b) $\left(\frac{8}{11}\right)$
 - (c) $\left(\frac{24}{11}\right)$
 - (d) $\left(\frac{9}{11}\right)$
 - (e) $\left(\frac{72}{11}\right)$
 - (f) $\left(\frac{21}{235}\right)$
 - (g) Sabendo que $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2 1}{8}}$, calcule $\left(\frac{101}{159}\right)$.
- 17. Mostre se existem soluções para as congruências
 - $x^2 \equiv 90 \mod 101$
 - (b) $x^2 \equiv 123 \mod 401$
 - (c) $x^2 \equiv 43 \mod 179$
 - (d) $x^2 \equiv 1093 \mod 65537$