Matrícula: Nome:

1. Mostre que se p é primo e $p \not| a$, então a^{p-2} é inverso de a mod p.

2. Suponha que alguém use $(n, e) = (111, 31)$ como chave pública no RSA. Qual sua chave secreta?

3. Resolva as seguintes congruências:
   a) $2x \equiv 5 (\text{mod } 17)$
   a) $19x \equiv 4 (\text{mod } 141)$

4. Mostre como usar funções geradoras para determinar o número de maneiras de devolver R$150

   A) em notas de R$5, R$10, R$20 e R$50
   B) em notas de R$5, R$10, R$20 e R$50 usando pelo menos uma de cada

5. Uma fila de n cadeiras de um estádio deve ser pintada nas cores verde, amarelo e branco, sendo que não pode haver duas cadeiras seguidas pintadas de branco.

   A) Escreva uma relação de recorrência para o número de maneiras de pintar as n cadeiras.
   B) Quais são as condições iniciais?
   C) De quantas maneiras 7 cadeiras podem ser pintadas?

Formulário:

Pequeno teorema de Fermat:
se p primo e a não é múltiplo de p, então $a^{p-1} \equiv 1 (\text{mod } p)$

RSA: $n = pq$, $\phi = (p-1)(q-1)$, $de \equiv 1 (\text{mod } \phi)$