MC538 - Análise de Algoritmos II
MC548 - Projeto e Análise de Algoritmos II
Semestre 2003-1 - Turma A
Prova 3 - 17/jun/2003

Nome

RA	**Assinatura**

Notas

A prova é individual e sem consulta.
Não são permitidos computadores ou calculadoras.
Não separe as folhas deste caderno de prova.
Não é permitido o uso de outro rascunho além destas folhas.
Escreva seu nome completo, e assine a tinta.
Valem apenas as respostas nos espaços indicados.

1. Dados $a = 27$ e $b = 21$, o algoritmo estendido de Euclides devolve

   $d =$ ☐ $x =$ ☐ $y =$ ☐

2. Encontre todas as soluçoes da equação $21x \equiv 6 \pmod{27}$.

3. Quais são os elementos de $\mathbb{Z}_{14}^{+}$?

4. Quais são os elementos de $\mathbb{Z}_{14}^{*}$?

5. Qual é o inverso multiplicativo de 5 módulo 14?

6. Qual é o valor de $\phi(40)$?

7. Encontre dois subgrupos distintos de $\mathbb{Z}_{11}^{*}$, cada qual com pelo menos dois elementos.

8. Liste as potências de 3 módulo 11:

9. Calcule o logaritmo discreto de 5 na base 3 módulo 11 ($\mathrm{ind}_{11,3}\, 5$ na notação do Cormen)?

10. Qual o valor de $7^{20} \bmod 50$? (Mostre as contas.)

11. Encontre uma raiz quadrada não trivial da unidade no grupo $\mathbb{Z}_{24}^*$.

12. A questão abaixo se refere ao algoritmo RSA para ciframento com chave pública. Para facilitar as contas, vamos usar um módulo n de apenas **quatro** algarismos.

    (a) Escolha valores adequados dos fatores p e q, entre 40 e 50:

    (b) Escolha uma chave pública e adequada, e determine a chave secreta correspondente d.

13. Mostre que 22 não é um número primo, pelo teste de Miller-Rabin. Ou seja, encontre uma testemunha a que faz o teste falhar, e mostre os cálculos efetuados pelo algoritmo de Miller-Rabin para essa testemunha.