Números Inteiros e Criptografia — Pseudoprova 2

A prova é individual e sem consulta. Responda as questões na folha de respostas, a lápis ou a caneta. Se tiver qualquer dúvida consulte o professor. Você pode usar livremente qualquer resultado visto em sala ou em listas de exercício, mas deve escrever claramente qual é o teorema/exercício/fato sendo usado. É **proibido** o uso de celular.

JUSTIFIQUE SUAS RESPOSTAS!

Questão 1. Sejam n e b inteiros positivos e suponha que n seja escrito em base b como

$$n = (b_{k-1}b_{k-2}\cdots b_2b_1b_0)_b.$$

Lembrete: isso significa que os números $b_0, \ldots, b_{k-1}$ satisfazem $0 \leq b_0, \ldots, b_{k-1} < b$ e

$$n = \sum_{i=0}^{k-1} b_i \cdot b^i.$$

(a) Mostre que n é divisível por b se, e somente se, $b_0 = 0$.

(b) (i) Seja b' um inteiro positivo tal que $b \equiv 1 \pmod{b'}$. Mostre que x é divisível por b' se, e somente se, $\sum_{i=0}^{k-1} b_i$ é divisível por b'.

(ii) No caso $b = 10$ usual, quais são os valores de b' para os quais $b \equiv 1 \pmod{b'}$? Quais são os *critérios de divisibilidade* correspondentes, que você deve ter aprendido no ensino fundamental?

(c) (i) Mostre que n é divisível por $b+1$ se, e somente se, $-b_0 + b_1 - b_2 + b_3 - b_4 + \cdots$ é divisível por $b+1$.

(ii) Sabendo que $x = (1020544352)_6$, determine a representação em base 6 do menor número maior ou igual a x que seja divisível por 7.

(d) Dizemos que n é um *palíndromo em base b* se os algarismos de n em base b são iguais quando lidos de trás pra frente ou de frente pra trás, i.e., se $n = (b_{k-1}b_{k-2}\cdots b_2b_1b_0)_b$ e também $n = (b_0b_1b_2\cdots b_{k-2}b_{k-1})_b$.

(i) Mostre que se $n = (b_{k-1}b_{k-2}\cdots b_2b_1b_0)_b$ é um palíndromo em base b e k é par, então n é divisível por $b+1$.

(ii) É sempre verdade que se $n = (b_{k-1}b_{k-2}\cdots b_2b_1b_0)_b$, k é par, e n é divisível por $b+1$, então n é um palíndromo? Se sim, prove isso. Se não, mostre um exemplo que comprove que não.

(iii) Mostre que 135792468864297531 é divisível por 11.

Questão 2. Considere a seguinte relação de recorrência:

$$\begin{cases} x_0 = 3 \\ x_{n+1} = 3^{x_n} \end{cases}$$

(a) Dado um n inteiro positivo qualquer, quem são os fatores primos de x_n? Você não precisa dizer as *multiplicidades* destes fatores primos.

(b) Calcule a forma reduzida de $x_4 \pmod{32}$.

Questão 3. Seja p primo. Mostre que a equação $x^2 = \overline{a}$ tem no máximo 2 soluções em $\mathbb{Z}_p$.

Dica: Mostre que para qualquer par de soluções distintas $x, y \in \mathbb{Z}_p$, temos $x + y \equiv 0 \pmod{p}$. O que aconteceria se $x, y, z \in \mathbb{Z}_p$ fossem três soluções distintas?

Questão 4. (a) Seja n um inteiro positivo ímpar. Mostre que não existe $\overline{a} \in \mathbb{Z}_n$ diferente de $\overline{0}$ tal que $a \equiv -a \pmod{n}$.

(b) Seja p um primo ímpar. Mostre que se $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ é tal que a equação $x^2 = \overline{a}$ tem alguma solução em $\mathbb{Z}_p$, então a equação tem pelo menos duas soluções distintas.

(c) Seja n o produto de k primos ímpares distintos. Mostre que se $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ é tal que a equação $x^2 = \overline{a}$ tem alguma solução em $\mathbb{Z}_n$, então a equação tem pelo menos 2^k soluções distintas.

Questão 5. (a) Seja $(G, *)$ um grupo finito cíclico com gerador g, e seja $a \in G$. Mostre que

$$\text{existe } x \in G \text{ tal que } x^2 = a$$
$$\text{se, e somente se,}$$
$$a = g^n \text{ para algum } n \text{ par.}$$

(b) Seja p um número primo tal que $p \equiv 3 \pmod{4}$ e seja $\overline{a} \in U(p)$. Mostre que se a equação $x^2 = \overline{a}$ tem alguma solução em $U(p)$, então

$$x \equiv \overline{a}^{\frac{p+1}{4}} \pmod{p}$$

é uma solução.

Dica: Lembre-se que $U(p)$ possui gerador e use a letra (a). Além disso, tire do bolso a seguinte igualdade em algum momento: $(p+1)\frac{n}{2} = n + (p-1)\frac{n}{2}$.

Questão 6. Sejam p, q primos ímpares distintos. Mostre que temos

$$x^{\frac{pq-p-q+3}{2}} \equiv x \pmod{pq}$$

para qualquer $x \in \mathbb{Z}_{pq}$.

Questão 7. (a) Mostre que a função de encriptação do RSA tem a seguinte *propriedade multiplicativa*: se x_0 é encriptado como x_0' e x_1 é encriptado como x_1', então $x_0 x_1$ é encriptado como $x_0' x_1'$ (o produto das mensagens encriptadas é a encriptação do produto das mensagens originais).

(b) Suponha que você tenha interceptado uma mensagem encriptada por RSA, enviada ao seu amigo Bob, cujo valor encriptado é y. Como você não sabe a chave de descriptação do Bob, você ainda não sabe qual o valor x original que foi encriptado e virou y. Mais tarde, conversando com Bob, você pode perguntar pra ele qual o valor descriptado de um único $y' \neq y$ qualquer, e ele (de boa-fé) vai te responder honestamente. Como você pode explorar essa situação para obter o valor de x? (Claro que enviar $y' = y$ pra obter x diretamente não vai funcionar, pois Bob tem boa-fé mas não é bobo, e sabe que y' foi a mensagem secreta enviada por outra pessoa.)

Questão 8. (a) Mostre que não existem números de Carmichael que sejam pares.

(b) Mostre que cada um dos números abaixo é um número de Carmichael:

$$10585 = 5 \cdot 29 \cdot 73 \qquad 75361 = 11 \cdot 13 \cdot 17 \cdot 31$$
$$1024651 = 19 \cdot 199 \cdot 271 \qquad 172947529 = 307 \cdot 613 \cdot 919$$