Números Inteiros e Criptografia — Prova Final (parte 1)
& Segunda Chamada de P1 — 2/7/2019

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. (1 ponto) Um ano N é *bissexto* (i.e., tem 366 dias) de acordo com o seguinte algoritmo:

```
se N ≢ 0 (mod 4), então N não é bissexto;
senão, se N ≢ 0 (mod 100), então N é bissexto;
       senão, se N ≢ 0 (mod 400), então N não é bissexto;
              senão, N é bissexto.
```

No clássico do *hip hop* americano "Mind Playing Tricks on Me" (1991), do grupo *Geto Boys*, uma das estrofes começa com o verso

Nesse ano, o Halloween caiu num fim de semana

Sabendo que no ano de 2019 o *Halloween* cai numa quinta-feira, e sabendo que os fatos relatados na canção ocorreram na década de 1980, diga em quais anos eles podem ter ocorrido.

Questão 2. Dado um inteiro positivo n, seja $\mu(n)$ o valor definido de acordo com os seguintes casos:

- se n tem algum fator primo com multiplicidade maior que 1, então $\mu(n) = 0$;
- se todos os fatores primos de n têm multiplicidade igual a 1, então:
  - se n tem uma quantidade *par* de fatores primos, então $\mu(n) = 1$;
  - se n tem uma quantidade *ímpar* de fatores primos, então $\mu(n) = -1$.

A função μ é conhecida como *função de Möbius*.

(a) (1 ponto) Mostre, por meio de um exemplo, que a seguinte afirmação **não é** verdadeira: "para todos inteiros positivos n e m, temos $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$".

(b) (1 ponto) Mostre que, para quaisquer inteiros positivos **coprimos** n e m, temos $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.

A prova continua no verso!

Questão 3. Na Prova 1, estudamos uma espécie de seres alienígenas com as seguintes características:

- Os seres dessa espécie são imortais;
- Cada ser dessa espécie se torna maduro para poder se reproduzir exatamente quando completa 1 ano de vida;
- Os seres dessa espécie se reproduzem assexuadamente, e cada ser começa a se reproduzir exatamente no momento em que se torna maduro, ou exatamente no momento em que acabou de se reproduzir mais recentemente;
- Cada processo de reprodução demora exatamente 1 ano entre seu início e seu final, e cada processo de reprodução individual gera 1 novo ser.

Como vimos, se uma população desses seres começa vazia no instante atual e recebe magicamente um ser recém-nascido dessa espécie daqui a exatamente 1 ano, e sendo $A(n)$ a quantidade de seres dessa população daqui a n anos, temos a seguinte relação de recorrência:

$$\begin{cases} A(0) = 0 \\ A(1) = 1 \\ A(n+2) = A(n+1) + A(n) \quad \text{para } n \geq 2. \end{cases}$$

(a) (1 ponto) Agora seja $B(n)$ a quantidade de seres nascida exatamente no ano n (ou que tenha aparecido magicamente no ano n). Mostre que temos $B(n+2) = A(n)$ para todo inteiro $n \geq 0$. Conclua que, a partir de $n = 2$, a função $B(n)$ obedece a uma relação de recorrência quase igual à de $A(n)$.

(b) ($1\frac{1}{2}$ pontos) Mostre que para todo inteiro $n \geq 0$ temos

$$A(n) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Dica: Use *indução forte*: "para provar que uma certa propriedade é válida para todo natural $n \geq 0$, prove que:

- ela é válida para 0
- para qualquer $n > 0$:
  se ela é válida para todo natural m com $0 \leq m < n$, **então** ela é válida para n".

Para o passo de indução, será útil você investigar em seu rascunho os valores de

$$\left(\frac{1+\sqrt{5}}{2} \right)^2 \qquad \text{e} \qquad \left(\frac{1-\sqrt{5}}{2} \right)^2$$

Números Inteiros e Criptografia — Prova Final (parte 2) — 4/7/2019

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 4. (1 ponto) Cada um dos números abaixo é composto e só possui fatores primos menores do que 30. Em cada caso, diga se o número é um número de Carmichael.

(a) 2465

(b) 4095

(c) 11305

Questão 5. (½ ponto) Seja $(G, *)$ um grupo finito e suponha que $a \in G$ seja tal que

$$a \neq e \quad \text{e} \quad a^{15} = e.$$

Mostre que $a^{22} \neq e$.

Questão 6. (1 ponto) Mostre que $\overline{2}$ é um gerador do grupo $(U(11), \cdot)$, mas que $\overline{3}$ não é.

Questão 7. (1 ponto) O grupo $(U(41), \cdot)$ tem algum subgrupo de ordem ...

(a) 9?

(b) 40?

(c) 80?

Questão 8. (2 pontos) Em um sistema de criptografia RSA, um usuário tem chave de encriptação pública $e = 38671$ e $n = 40363$ (sendo e o expoente para encriptação e n o módulo). Mostre que este usuário fez uma má escolha de chave: deduza qual a sua chave privada pra descriptação.

Dica: Primeiro fatore $n = 40363$, sabendo que a parte inteira de $\sqrt{40363}$ é 200.