DCC-UFRJ–Números Inteiros e Criptografia–Primeira Prova–2015/1

Justifique cuidadosamente todas as suas respostas.

Questão 1 (2 pontos)

Jullyana precisava usar seu celular pré-pago para entrar em contato com seu amigo Gabriel que está participando do programa Ciência sem Fronteiras no Canadá. Se o contato fosse feito através de mensagens de texto, cada uma das quais custaria 3 reais e cinquenta centavos, sobraria 1 real e 32 centavos em sua conta. Jullyana decidiu-se por uma ligação telefônica, cada minuto da qual custou 13 reais e 53 centavos, e sobrou-lhe 1 real e 17 centavos na conta do celular. Use o algoritmo euclidiano estendido para determinar a quantia mínima (em reais) que Jullyana podia ter na conta do seu celular.

121

Questão 2 (2 pontos)

121 Sabe-se que $(9,4) \in \mathcal{P}(5)$. Calcule as coordenadas de $(9,4)^4 \otimes (-9,4)^3$.

$= (9,4)^{-3}$

$= (9,4)$

Questão 3 (2 pontos)

No conjunto $\mathcal{G}$ dos pares de números racionais (x, y) *cuja segunda coordenada não é nula* definimos uma operação $\star$ pela regra $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 y_2)$.

121

(a) Determine o elemento neutro desta operação.

(b) Quais propriedades de um grupo (abeliano) esta operação satisfaz? $\mathcal{G}$ com a operação $\star$ é um grupo (abeliano)?

Questão 4 (2 pontos)

121

(a) Ache dois fatores de 1009427 pelo algoritmo de Fermat.

(b) Qual o menor número inteiro positivo n para o qual $n!$ é divisível por 253000?

Questão 5 (2 pontos)

Dado um número primo $p > 2$, defina $p^{\triangle}$ como sendo o produto de todos os primos *ímpares* positivos menores ou iguais a p. Considere a sequência de primos gerada pela seguinte regra recursiva:

$$p_1 = 5 \text{ e } p_n \text{ é o menor fator primo de } \quad p_{n-1}^{\triangle} - 2.$$

Mostre que os primos $p_1, p_2, \ldots$ gerados por esta regra são todos distintos; isto é, se $i \neq j$ então $p_i \neq p_j$.

$P_1 = 5$

$P_2 = 5 - 2 = 3$

$P_3 = 5 . 3 - 2 = 13$

$P_4 = 5 . 3 . 13 - 2 = 195 - 2 = 193$

$(P_1, P_2 \ldots . P_{m-1}) - 2$ ñ é divisível por nem um dos fatores P_i pois $P_i > 2$, logo não poderemos botar um P_i em evidência pa como um fator desse nº, então P_m não será igual a nem um dos anteriores.