Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 8
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1. Dados $a \in Z$ e $n \in N$ com $n > 0$, chamamos de forma reduzida de a (mod n) o único $b \in \{0, 1, 2, . . . , n - 1\}$ que satisfaz $b \equiv a \pmod n$. Calcule a forma reduzida de cada item abaixo:

* c. −(1234567890^99999!) (mod 2)

  −(1234567890^99999!)≡b (mod 2)
  Tendo em mente que a divisão de um número por 2 nos retornará resto zero ou resto um, caso ele seja par ou ímpar respectivamente. Como −(1234567890^99999!) é um número par, logo temos que:
  −(1234567890^99999!)≡ 0 (mod 2)

* h. 2^130 (mod 263) (Use o fato que 2^131 ≡ 1 (mod 263))

  Sabendo que 264 ≡ 1 (mod 263) por transitividade temos que $2^{131} \equiv 264$ mod (263).
  Como 263 e 2 são coprimos podemos dividir ambos:
  $(2^{131}/2) \equiv (264/2)$ mod (263).
  Logo:
  2^130 ≡ 132 (mod 263)

Questão 3. Determine o resto da divisão de:

* c. 39^50! por 2251 (Use o fato que 39^1125 ≡ 1 (mod 2251)).

  Como 45*25 = 1125, podemos dizer que:
  39^50! = (39^(45*25))^50*...*46* 44 * ….* 26* 25* … *1

  Assim, sabendo que 39^1125 ≡ 1 (mod 2251)
  (39^(45*25))^(50*...) ≡ (1)^(50*...) ≡ 1 (mod 2251)

  Logo nosso resto é 1

* g. 2^987657 + 5^15 por 65. (Dica: lembre-se que 2^6 ≡ 64 ≡ −1 (mod 65).)

  Analisando a congruência das potências de 5:
  5≡5 (mod 65)
  $5^2 \equiv 25$ (mod 65)
  $5^3 \equiv 60$ (mod 65)
  5^4 ≡ 40 (mod 65)
  5^5 ≡ 5 (mod 65)

  Voltando para o problema, temos que achar o resto de:

$2^{987657} + 5^{15}$ por 65

Como sabemos que $2^6 \equiv 64 \equiv -1 \pmod{65}$, quando dividimos 987657 por 6, vemos que nossa divisão nos dá resto 3, assim para facilitar nossa conta e usarmos o que sabemos sobre a potência de 2, vamos dizer que:

$2^{987654} * 2^3 + 5^{15}$

Por algebrismo temos que:

$(2^6)^{164609} * 2^3 + (5^5)^3 \equiv (-1)(8) + 5^3 \equiv -8 + 60 \equiv 52 \pmod{65}$

Logo nosso resto é 52

*Questão 4. Prove por indução que, para todo inteiro $n \geq 1$, temos $n^3 \equiv n \pmod{6}$.

Caso base:
$P(1) = 1^3 \equiv 1 \pmod{6}$

Passo indutivo:
P(k)
/\
\/
$n^3 \equiv n \pmod{6}$
/\
\/
$6|k^3-k$
/\
\/
$6|(k^3-k) +3(k^2 + k)$
/\
\/
$6|k^3+3k^2 + 3k - k$
/\
\/
$6|k^3+3k^2 + 3k + 1 - k - 1$
/\
\/
$6|(k+1)^3-(k+1)$
/\
\/
$(k+1)^3 \equiv (k+1) \pmod{6}$
/\
\/
P(k+1)

*Questão 6. São oito horas da manhã. Que horas serão daqui a 243^213! horas?

Temos que:
$243 \equiv 3 \pmod{24}$
$243^2 \equiv 9 \pmod{24}$
$243^3 \equiv 3 \pmod{24}$
$243^4 \equiv 9 \pmod{24}$

Perceba que encontramos um padrão, onde 243 elevado a um número par é congruente a 9, e se for um número ímpar, será congruente a 3

Como 213! é um número, visto que em sua constituição possui diversas multiplicações de números pares. Logo:

$243^{213!} \equiv 9 \pmod{24}$

Como temos resto 9, então somamos com 8 horas: Serão então 17:00 daqui a 243^213! horas.

*Questão 9. Seja um fator primo de 1200! + 1. <u>1200</u> tem inverso em Zp? Se existir, qual é o seu inverso em Zp?

Para saber se um número possui inverso em Zp, o mdc entre eles deve ser igual a 1.
mdc(1200, p) = 1
Por Bezout vamos ter: $1200\alpha + p\beta = 1$

Como p é um fator primo de 1200! + 1 podemos escrever nessa forma:
1200! + 1 = p * n
1200k -pn = -1, onde k = 1199!
-1200k + pn = 1

Comparando com a nossa expressão de Bezout, temos que:
α=-k
β=n

Como o que nos interessa é α que é o inverso que procuramos:
α = -k = <u>-1199!</u>

Questão 11. Determine:
* a. o inverso de 137 módulo 2887;

Pelo algoritmo de euclides vamos encontrar o mdc(137,2887):
2887 = 137(q) + r
2887 = 137(21) + 10
137 = 10 (13) + 7
10 = 7 (1) + 3
7 = 3 (2) + 1
3 = 1 (3) + 0
Logo achamos que o mdc(137,2887) = 1
Por Bezout temos que 137α + 2887β = 1

Pelo algoritmo euclidiano estendido vamos achar:
2887(1) + 137 (0) = 2887
2887(0) + 137 (1) = 137
2887(1) + 137 (-21) = 10
2887(-13) + 137(274) = 7
2887(14) + 137(-295) = 3
2887(-41) + 137(864) = 1

Comparando com a expressão que encontramos por Bezout 864 é o inverso de 137 mod 2887

* b. x tal que 137x ≡ 544 (mod 2887), usando o item anterior.

Sabemos pela letra a) que 137*864 ≡ 1 (mod 2887), então multiplicamos 137x ≡ 544 (mod 2887) por 864, desse jeito:
137 * 864 * x ≡ 544 * 864 (mod 2887)
Como 137 * 864 ≡ 1, podemos substituir:
x ≡ 544 * 864 (mod 2887)
2887k = x - 470016
2887k + 470016 = x
Como precisamos que x seja menor que 2887, vamos achar que:
2887(-162) + 470016 = 2322
2887(-161) + 470016 = 5209
Logo vemos que x ≡ 2322 mod (2887)

Questão 13.

* a. Prove que para todo inteiro $b > 0$, se b não é divisível por 7 então $b^6 \equiv 1 \pmod 7$). (Dica: prove separadamente para cada $b \in \{1, 2, 3, 4, 5, 6\}$ e mostre que isso implica o resultado desejado. Outra dica: Na verdade, como o expoente 6 é par, mostre que basta provar separadamente para cada $b \in \{1, 2, 3\}$, mostrar que isso implica o resultado desejado para cada $b \in \{4, 5, 6\}$, e daí seguir a primeira dica.).

Temos que:
$1^6 \equiv 1 \pmod 7$
$2^6 \equiv (2^3)^2 \equiv 1^2 \equiv 1 \pmod 7$
$3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 1 \pmod 7$
$4^6 \equiv (2^2)^6 \equiv 2^{12} \equiv (2^3)^4 \equiv 1^4 \equiv 1 \pmod 7$
$5^6 \equiv (5^2)^3 \equiv 25^3 \equiv 4^3 \equiv (2^2)^3 \equiv (2^3)^2 \equiv 1^2 \equiv 1 \pmod 7$
$6^6 \equiv (2 * 3)^6 \equiv 2^6 * 3^6 \equiv 1 \pmod 7$
$7^6 \equiv 0 \pmod 7$

Vemos assim que qualquer número que não é divisível por 7 vai atender essa condição $b^6 \equiv 1 \pmod 7$, pois em algum momento será possível encontrar a congruência com alguma potência conhecida.

* b. Calcule o resto da divisão de
$1^{1!} + 2^{2!} + 3^{3!} + 4^{4!} + 5^{5!} + 6^{6!} + 7^{7!} + 8^{8!} + 9^{9!} + 10^{10!}$.
por 7. (Dica: use o item anterior.)

Pela letra a) sabemos que:
$1^{1!} \equiv 1 \pmod 7$
$2^{2!} \equiv 4 \pmod 7$
$3^{3!} \equiv 3^6 \equiv 1 \pmod 7$
$4^{4!} \equiv 2^{4!*2} \equiv (2^3)^{(4*4*1)} \equiv 1 \pmod 7$
$5^{5!} \equiv (5^{(3*2)})^{(5*4*1)} \equiv (5^6)^{(5*4*1)} \equiv 1 \pmod 7$
$6^{6!} \equiv (6^6)^{5!} \equiv 1 \pmod 7$
$7^{7!} \equiv 0 \pmod 7$
$8^{8!} \equiv (2^3)^{8!} \equiv 1 \pmod 7$
$9^{9!} \equiv (3^2)^{9!} \equiv (2)^{9!} \equiv (2^3)^{(9*...*4*2)} \equiv 1 \pmod 7$
$10^{10!} \equiv (2*5)^{10!} \equiv 2^{10!} * 5^{10!} \equiv (2^6)^{10\ldots} * (5^6)^{10\ldots} \equiv 1 \pmod 7$

Assim podemos substituir esses valores para facilitar nossa conta:
$1 + 4 + 1 + 1 + 1 + 1 + 0 + 1 + 1 + 1 \equiv b \pmod 7$
$12 \equiv b \pmod 7$
$b = 5$

Logo o resto da divisão $1^{1!} + 2^{2!} + 3^{3!} + 4^{4!} + 5^{5!} + 6^{6!} + 7^{7!} + 8^{8!} + 9^{9!} + 10^{10!}$. por 7 é igual a 5

Questão 15. Considere as relações R1 e R2 abaixo, definidas no conjunto Z dos números inteiros. Determine se são reflexivas, simétricas e/ou transitivas. Alguma das duas relações é de equivalência?

* a. a R1 b quando mdc(a, b) = 1.

    Reflexiva: a R a = mdc(a,a), que não se aplica ao nosso caso pois mdc (a,a) =/= 1

    Simétrica: a R b & b R a, que é verdadeira pois mdc(a,b) = mdc(b,a)

    Transitiva: a R b & b R a → a R c, que não se aplica na nossa relação visto que se fizermos:

        a = 2
        b = 3
        c = 4
        mdc(2,3) = 1
        mdc(3,4) = 1
        mdc(2,4) =2

* b. Fixe n > 0 inteiro. Então a R2 b quando mdc(a, n) = mdc(b, n).

    Reflexiva: a R a, será verdadeira visto que mdc(a,n) = mdc(a,n)

    Simétrica: a R b → b R a, também será verdadeira visto que será apenas uma visão diferente, a R b → mdc(a,n) = mdc(b,n); b R a → mdc(b,n) = mdc(a,n)

    Transitiva: a R b & b R c → a R c

    a R b → mdc(a,n) = mdc(b,n)
    b R c → mdc(b,n) = mdc(c,n)
    a R c → mdc(a,n = mdc(c,n)

    Nossa relação também será transitiva.
    Assim, temos uma relação de equivalência.

Questão 19. O objetivo desta questão (i.e., o que vamos concluir após os itens a, b e c abaixo) é mostrar que nenhum número da forma 4n+ 3 pode ser escrito como a soma dos quadrados de dois inteiros.

* a. Mostre que o quadrado de qualquer inteiro só pode ser congruente a 0 ou 1 módulo 4.

    Temos que:
    $0^2 \equiv 0 \pmod 4$
    $1^2 \equiv 1 \pmod 4$
    $2^2 \equiv 4 \equiv 0 \pmod 4$
    $3^3 \equiv 9 \equiv 1 \pmod 4$
    $4^2 \equiv 16 \equiv 0 \pmod 4$

    Temos então que se um número é par ele vai ser congruente a 0 e se for ímpar congruente a 1.

Testando isso com a definição:
$(2n)^2 \equiv 0 \text{ mod } (4)$
$4k = 4n^2$, perceba que teremos uma divisão com resto zero

$(2n+1)^2 \equiv 1 \pmod 4$
$4k = 4n^2 + 4n + 1$
$4k = 4(n^2 + n) + 1$, perceba que teremos uma divisão com resto 1

* b. Use o item anterior para mostrar que se x e y são inteiros então x^2 + y^2 só pode ser congruente a 0, 1 ou 2 módulo 4.

Vamos ter duas possibilidades de resto para x^2 e y^2, sendo elas;
$x^2 \equiv 0 \pmod 4$ ou $x^2 \equiv 1 \pmod 4$
$y^2 \equiv 0 \pmod 4$ ou $y^2 \equiv 1 \pmod 4$

Vamos testar agora essas possibilidades para x^2+y^2:
i) $x^2+y^2 \equiv 0 + 0 \equiv 0 \pmod 4$
ii)$x^2+y^2 \equiv 1 + 0 \equiv 1 \pmod 4$, perceba que teremos o mesmo resultado para $y^2 \equiv 1$ e $x^2 \equiv 0$ ou $y^2 \equiv 0$ e $x^2 \equiv 1$
iii) $x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$

* c. Use o item anterior para mostrar que um inteiro da forma 4n+ 3 não pode ser escrito como soma de dois quadrados de inteiros. Este resultado é um caso particular de um teorema comunicado por Fermat em uma carta a Roberval datada de 1640. Fermat também sabia que qualquer primo da forma 4n + 1 pode ser escrito como soma de dois quadrados de inteiros.

Temos que um inteiro m, onde ele é a soma de dois quadrados (x^2+y^2). Vamos escrever m = 4n+ 3, onde manipulando vamos chegar em:
$m = 4n+3$
$m-3 = 4n$
$4|m-3$
$m \equiv 3 \pmod 4$

Pela prova da letra b), vimos as possibilidades de congruência para a soma de dois quadrados. $x^2+y^3 \equiv 3 \pmod 3$ não é verdade visto que x^2+y^2 só será congruente a 0,1 e 2.