Problemas Sortidos de Teoria dos Números – Edição II – Live (alguns disponíveis no sabor Combinatória)

Guilherme Zeus Moura
zeusdanmou@gmail.com

1. (IMC 2020, 6) Ache todos os primos p tais que existe um único $a \in \{0, 1, 2, \ldots, p-1\}$ para o qual $a^3 - 3a + 1 \equiv 0 \pmod{p}$.

Rascunho.
Casos Pequenos: Para $p = 2$, é irredutível. Para 3, tem uma raíz única. Para 5, é irredutível, Para 7, é irredutível. Para 11, é irredutível. Para 13, é irredutível. Para 17, tem 3 raízes distintas.

Considere $P(x) = x^3 - 3x + 1$. No mundo $\mathbb{Z}_p[x]$, isto é, considerando os polinômios de coeficientes inteiros $\pmod{p}$, podemos dividir o polinômio P unicamente em um produto de polinômios irredutíveis, isto é, polinômios que não podem ser fatorados. Existem 3 casos:

- P é irredutível em $\mathbb{Z}_p[x]$.
- $P(x) = (x - \alpha) \cdot Q(x)$, com Q irredutível em $\mathbb{Z}_p[x]$.
- $P(x) = (x - \alpha) \cdot (x - \beta) \cdot (x - \gamma)$.

Teorema 1. Se α é raiz de P, então $(x - \alpha)$ divide $P(x)$.

Pergunta 1. Quais são as raízes reais de $P(x) = x^3 - 3x + 1$?
Pergunta 2. Expresse $\cos(3\theta)$ em função de $\cos\theta$.
Resposta da Pergunta 2.

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$$
$$2\cos(3\theta) = (2\cos\theta)^3 - 3(2\cos\theta)$$

Resposta da Pergunta 1. Logo, se x está no intervalo $[-2, 2]$, podemos escrever $x = 2\cos\theta$, com $\theta \in [0°, 180°]$ e temos

$$\begin{aligned} & x^3 - 3x + 1 = 0 \\ \iff & (2\cos\theta)^3 - 3(\cos\theta) + 1 = 0 \\ \iff & 2\cos(3\theta) = -1 \\ \iff & \cos(3\theta) = \frac{-1}{2} \\ \iff & 3\theta \in \{120°, 240°, 480°\} \\ \iff & \theta \in \{40°, 80°, 160°\} \end{aligned}$$

Então, $2\cos(40°)$, $2\cos(80°)$ e $2\cos(160°)$ são raízes de P e, como P tem grau 3, são todas as raízes.
Observe as relações

$$\begin{aligned} 2\cos(80°) &= (2\cos(40°))^2 - 2 \\ 2\cos(160°) &= (2\cos(80°))^2 - 2 \\ 2\cos(40°) &= (2\cos(160°))^2 - 2 \end{aligned}$$

Em resumo, nos reais, se a é raíz de $P(x)$, então $a^2 - 2$ também é raiz de $P(x)$.
Será que isso também vale no mundo $\pmod{p}$? (Verifiquem!)
A solução completa está na próxima página. (Note que isso é só um rascunho...)
Parte da beleza desse problema é ver essa relação interessante entre as raízes de um polinômio em $\mathbb{R}$ e em $\mathbb{Z}_p$. Infelizmente[1] esse problema só nos dá um gostinho dessa relação e a gente fica sem entender direito o *porquê* dessa relação existir, mesmo que a gente entenda que ela existe.[2]

[1] Ou felizmente, talvez? Um pouco de mistério a longo prazo pode manter vocês engajados no estudo da matemática.
[2] Quando eu entender o *motivo* por traz disso tudo, eu conto pra vocês. Ou se vocês descobrirem primeiro, contem pra mim!

Início da Solução.

Suponha que a é raiz de $P(x) \pmod p$. Isso significa que $a^3 - 3a + 1 \equiv 0$.

$$\begin{aligned} P(a^2-2) &= (a^2-2)^3 - 3(a^2-2) + 1 \\ &= a^6 - 6a^4 + 12a^2 - 8 - 3a^2 + 6 + 1 \\ &= (3a^4 - a^3) - 6a^4 + 9a^2 - 1 \\ &= -3a^4 - a^3 + 9a^2 - 1 \\ &= -3(3a^2 - a) - a^3 + 9a^2 - 1 \\ &= -a^3 + 3a - 1 \\ &= 0. \end{aligned}$$

Logo, $a^2 - 2$ também é raíz.

Voltando ao enunciado original. Suponha que a é raíz única. Como $a^2 - 2$ também é raiz, deve valer $a \equiv a^2 - 2 \pmod p \iff (a+1)(a-2) \equiv 0 \pmod p \iff a \equiv 2$ ou $a \equiv -1 \pmod p$. Como $P(2) = 1$ e $P(-1) = 3$, a única possibilidade é $a \equiv -1 \pmod p$ e $p = 3$.

@Podemos testar e verificar que $p = 3$ funciona (com $a = 2$ único).

Logo, o único primo que funciona é $p = 3$.

2. (OBM 2018, 3) Sejam k, n inteiros positivos fixados. Em uma mesa circular, são colocados n pinos numerados sucessivamente com os números $1, \ldots, n$, com 1 e n vizinhos. Sabe-se que o pino 1 é dourado e os demais são brancos. António e Maria Clara jogam um jogo, em que uma argola é colocada inicialmente em um dos pinos e a cada passo ela muda de posição. O jogo começa com Maria Clara escolhendo com pino inicial para a argola, e o primeiro passo consiste no seguinte: António escolhe um inteiro positivo d qualquer e Maria Clara desloca a argola d pinos no sentido horário ou no sentido anti-horário (as posições são consideradas módulo n, ou seja, os pinos x, y são iguais se e somente se n divide $x - y$). Após isso, a argola muda de pinos de acordo com uma das seguintes regras, a ser escolhida em cada passo por António.

Regra 1: António escolhe um inteiro positivo d qualquer e Maria Clara desloca a argola d pinos no sentido horário ou no sentido anti-horário.

Regra 2: António escolhe um sentido (horário ou anti-horário), e Maria Clara desloca a argola nesse sentido em d ou kd pinos, onde d é o tamanho do último deslocamento realizado.

António vence se, após um número finito de passos, a argola é deslocada para o pino dourado. Determine, em função de k, os valores de n para os quais António possui uma estratégia que garanta sua vitória, não importando como Maria Clara jogue.

Vamos definir $P(n, k)$ como a proposição "António garante ganhar o jogo com os números fixos n e k". Lembrando que proposições admitem os valores de *verdadeiro* ou *falso*.

Lema 1. Se $k \equiv 1 \pmod{n}$, António tem estratégia vencedora. Usando a notação, $P(n, 1)$ é verdadeiro.

Demonstração. Se $k \equiv 1 \pmod{n}$, temos que a segunda regra é andar d ou kd, como $k \equiv 1$ temos que $kd \equiv d$, ou seja basta realizar o Antonio realizar a primeira jogada com um d tal que $\text{mdc}(d, n) = 1$, e realizarmos a segunda jogada de repetidas vezes num mesmo sentido, temos que uma hora vai chegar no 1, pois $d, 2d, 3d, \cdots, (n-1)d, nd$ é equivalente mod p a $0, 1, 2, 3, \cdots, n-1$, ou seja se ele começar esse ciclo num número i ele certamente em algum momento vai somar $-i + 1$ chegando assim no pino dourado.

Lema 2. $P(n, k) \iff P(2n, k)$.

Lema 3. $P(2^\ell, k)$ é verdadeiro.

Lema 4. Se $\text{mdc}(n, k-1) = 1$, então $P(n, k) \iff n$ é potência de 2.

Observação. Este problema não está finalizado. Vamos continuar pensando nele na última aula. (E claro, se puderem/quiserem, podem pensar nesse problema sozinhos ou em horários alternativos com os outros alunos.)

Quem tem um Lema como os Lemas acima ou tem uma demonstração para um Lema não demonstrado acima, pode mandar pra mim preferencialmente no email zeusdanmou+tex@gmail.com.