Elementos de Teoria dos Números (2020.3) - Prova 1

Prof. Ricardo Bortolotti

1. Prove por indução que 19 divide $2^{2^{6k+2}} + 3$ para $k = 0, 1, 2, \ldots$.

   Solução: $k = 0$: $2^{2^2} + 3 = 2^4 + 3 = 16 + 3 = 19$ obviamente é múltiplo de 19.

   Passo indutivo: Se vale para $k = n$, temos $2^{2^{6n+2}} \equiv -3 \pmod{19}$. Então

   $$2^{2^{6(n+1)+2}} + 3 = 2^{2^6 \cdot 2^{6n+2}} + 3 = (2^{2^{6n+2}})^{64} + 3 \equiv (-3)^{64} + 3 \pmod{19}$$

   Vamos olhar as potências de -3 módulo 19 e ver que $(-3)^{64} \equiv -3 \pmod{19}$.

   Pelo Pequeno Teorema de Fermat: $(-3)^{18} \equiv 1 \pmod{19}$, então

   $$(-3)^{64} \equiv (-3)^{3 \cdot 18 + 10} \equiv ((-3)^{18})^3 \cdot 3^{10} \equiv 3^{10} \pmod{19}.$$

   Olhando o valor de 3^{10}:

   $(-3)^2 \equiv 9 \pmod{19}$,
   $(-3)^4 \equiv 81 \equiv 5 \pmod{19}$,
   $(-3)^8 \equiv 25 \equiv 6 \pmod{19}$,
   $(-3)^{10} \equiv (-3)^8 \cdot (-3)^2 \equiv 6 \cdot 9 = 54 \equiv 16 \equiv -3 \pmod{19}$.

   Concluímos que $(-3)^{64} + 3 \equiv -3 + 3 \equiv 0 \pmod{19} \Rightarrow 19$ divide $2^{2^{6(n+1)+2}} + 3$.

2. Prove que se $(a, b) = 1$, então existe um sistema completo de resíduos módulo a formado por números congruentes a 1 módulo b.

   Solução: Vimos em aula que se $\{r_1, \cdots, r_k\}$ é um sistema completo de resíduos módulo m e $(a, m) = 1$, então $\{ar_1 + c, \cdots, ar_k + c\}$ também é sistema completo de resíduos módulo m.

   Aplicamos este resultado para o sitema completo de resíduos módulo a $\{0, 1, \cdots, a-1\}$ multiplicando por b e somando 1: $\{1, b+1, 2b+1, \cdots, (a-1)b+1\}$ é sistema completo de resíduos módulo a formado por números congruentes a 1 módulo b.

3. Existem infinitos inteiros compostos da forma $10^n + 3$?

   Solução: Sim. Tem várias maneiras de demonstrar, uma é notar que $10^n + 3$ é múltiplo de 13 para infinitos n's (escolhi o 13 por ser fator primo do caso $n = 1$).

   Pelo Pequeno Teorema de Fermat: $10^{12} \equiv 1 \pmod{13}$, logo $10^{12k+1} \equiv (10^{12})^k \cdot 10 \equiv 1 \cdot 10 \equiv 10 \pmod{13}$.

   Então $10^{12k+1} + 3 \equiv 13 \equiv 0 \pmod{13}$, portanto é sempre múltiplo de 13, logo é composto.

4. Existem infinitos primos p tais que $\dfrac{p^3+8^{p-1}-1}{5^p+7}$ é inteiro?

   Solução: Não. Para $p>3$ primo a expressão já não é mais um inteiro. Olhando módulo 3, vamos ver que o denominador é sempre múltiplo de 3 e o numerador não é múltiplo de 3 (se $p>3$).

   Como p é ímpar: $5^p+7 \equiv (-1)^p+7 \equiv -1+7 \equiv 0 \pmod 3$, logo 3 divide o denominador. Da mesma forma: $p^3+8^{p-1}-1 \equiv p^3+(-1)^{p-1}-1 \equiv p^3+1-1 \equiv p^3 \pmod 3$, o que não é múltiplo de 3.

5. Encontre todos os inteiros $n>1$ tais que $1^n+2^n+\cdots+(n-1)^n$ é múltiplo de n.

   Solução: A solução são todos os n's ímpares.

   Se n é ímpar: note que $(n-x)^n \equiv (-x)^n \equiv -x^n \pmod n$, logo $x^n+(n-x)^n \equiv 0 \pmod n$. Usando isso temos:

$$\begin{aligned} 1^n+2^n+\cdots+(n-1)^n &\equiv 1^n+(n-1)^n+2^n+(n-2)^n+\cdots+(\frac{n-1}{2})^n+(\frac{n+1}{2})^n \pmod n \\ &\equiv 0+0+\cdots+0 \equiv 0 \pmod n \end{aligned}$$

   Se n é par. Primeiro supomos que n não é múltiplo de 4: $n=2s$, s ímpar, então $1^n+2^n+...+(n-1)^n$ é a soma de $\frac{n}{2}$ termos ímpares e $\frac{n}{2}$ termos pares, que é ímpar e não é múltiplo de n.

   Em geral, escrevemos $n=2^k s$, s ímpar, e refazemos o argumento acima módulo 2^k. Temos $(2m)^n \equiv 0 \pmod{2^k}$ pois o fator 2 aparece ao menos 2^k vezes na potência. Pelo Teorema de Euler: $(2m+1)^{2^{k-1}} \equiv 1 \pmod{2^k}$, logo $(2m+1)^n \equiv 1 \pmod{2^k}$. Então $1^n+2^n+\cdots(n-1)^n \equiv 0+1+0+1+\cdots+0+1 \equiv 2^{k-1} \pmod{2^k}$. Logo não é múltiplo de 2^k, portanto não é múltiplo de n.

6. Prove que se $p>3$ é primo então $p^2 \equiv 1 \pmod{24}$

   Solução: Como $24=2^2\cdot 3$, vamos ver que p^2-1 é múltiplo de 3 e de 4.

   Como p é ímpar, então $p=2k+1$, logo $p^2-1=4k^2+4k+1-1 \equiv 0 \pmod 4$.

   Como p não é múltiplo de 3, temos 2 opções: Se $p \equiv 1 \pmod 3 \Rightarrow p^2-1 \equiv 1-1 \equiv 0 \pmod 3$, neste caso 3 divide p^2-1. Se $p \equiv 2 \pmod 3 \Rightarrow p^2-1 \equiv 4-1 \equiv 0 \pmod 3$, neste caso 3 divide p^2-1. Logo concluimos o resultado.

7. Prove que todo primo diferente de 2 e 5 é múltiplo de infinitos números da forma $1, 11, 111, 1111, \ldots$.

   Solução 1: Note que tais números são da forma $\frac{10^n-1}{9}$. Vamos separar os casos $p=3$ e $p>5$. Para $p=3$, pelo critério de divisibilidade por 3, todos os números formados por $3k$ 1's são múltiplo de 3. Para $p>5$, para ser múltiplo de p, basta que 10^n-1 seja múltiplo de p. Como $10^{p-1} \equiv 1 \pmod p$, segue que $10^{(p-1)k} \equiv 1 \pmod p$, logo 10^n-1 é múltiplo de p para todo $n=(p-1)k$.

Solução 2 (Teoria Combinatória dos Números): Para provar que existem infinitos, provamos que para cada $k \geq 1$ existe um múltiplo de p na forma acima com pelo menos k 1's. Considerando os números $1, 11\cdots111, \cdots$ onde cada um tem $k+1$ 1's a mais que o anterior, pelo princípio da casa dos pombos, dois deles são congruentes entre si módulo p. Tomando a diferença deles, obtemos um múltiplo de p da forma $111\cdots11110000\cdots0000$ com pelo menos k 1's e, dividindo por uma potência de 10 para cancelar os zeros, obtemos um múltiplo de p da forma desejada.

8. Prove que para todo inteiro positivo n existe um inteiro positivo x tal que cada um dos termos $x+1, x^x+1, x^{x^x}+1, \ldots$ é múltiplo de n.

   Solução: Para $x+1$ ser múltiplo de n, tomamos $x \equiv -1 \pmod{n}$. Para o segundo termo: $x^x \equiv (-1)^x \pmod{n}$, e vai ser congruente a -1 se x for ímpar (essa mesma ideia se aplica a todos os termos seguintes).

   Então se n é par, basta tomar $x = n-1$ (que é ímpar) e todos os termos $x^{x^{\cdots^x}}+1$ serão congruentes a $(-1)^{\text{ímpar}}+1 \equiv -1+1 \equiv 0 \pmod{n}$.

   Se n é ímpar, basta tomar $x = 2n-1$ (que é ímpar) e, da mesma forma, todos os termos $x^{x^{\cdots^x}}+1$ serão congruentes a $(-1)^{\text{ímpar}}+1 \equiv -1+1 \equiv 0 \pmod{n}$.

9. Determine todos os primos da forma 10^n+1.

   Comentário: Essa questão foi mal formulada, portanto **está cancelada**. É possível provar, como feito em um exercício das listas, que n tem que ser da forma 2^k, mas é um problema em aberto a infinitude de primos de tal forma.

10. Encontre todos os inteiros n tais que $\Phi(n) = 8$.

    Solução: As soluções são $15, 16, 20, 24$ e 30. Fatorando: se $n = 2^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, então

    $$\Phi(n) = 2^{a_1-1}p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1) = 2^3.$$

    Como 2^3 apenas tem o fator primo 2, os primos ímpares p_j devem ter expoentes a_j-1 nulos, logo $a_j - 1 = 0 \Rightarrow a_j = 1$ para $j \geq 2$. Vamos separar em casos conforme o expoente do 2:

    1) $a_1 - 1 = 3$ implica que todos os outros primos não aparecem na fatoração. Temos $n = 2^4 = 16$.

    2) $a_1 - 1 = 2$ implica $(p_2-1)\cdots(p_k-1) = 2$. Então só tem um fator primo, que satisfaz $p_2 - 1 = 2$, isto é, $p_2 = 3$. Temos $n = 2^3 \cdot 3 = 24$.

    3) $a_1 - 1 = 1$ implica $(p_2-1)\cdots(p_k-1) = 2^2$, então só tem um fator primo, que satisfaz $p_2 - 1 = 4$, isto é, $p_2 = 5$. Temos $n = 2^2 \cdot 5 = 20$.

    4) n é par e $a_1 - 1 = 0$ implica $(p_2-1)\cdots(p_k-1) = 2^3 = 8$. Então pode acontecer 2 casos: $p_2 - 1 = 8$ ou $p_2 - 1 = 2$ e $p_3 - 1 = 4$, em um $p_2 = 9$ não é primo, no outro $p_2 = 3$ e $p_3 = 5$, no qual temos $n = 2 \cdot 3 \cdot 5 = 30$.

    5) O número é ímpar. Pode acontecer o mesmo do item anterior, mas sem o fator 2. Temos $n = 3 \cdot 5 = 15$.