Álgebra I para Licenciatura

Lista 3

Gabarito

Equações Diofantinas

1. (a) $mdc(3,5) = 1|47 \Rightarrow$ há soluções. Utilizando o algoritmo de Euclides decomponha 5 e 3 e note que:

   $$7 = 14(3) + (-7)5$$

   Portanto, são soluções particulares $x_0 = 14$ e $y_0 = -7$. Em geral $x = 14 + 5t$ e $y = -7 - 3t$ são as soluções para $y \in \mathbb{Z}$.

   (b) Similar ao item anterior. As soluções sao $x = -792 + 29t$ e $y = 1287 - 47t$ com $t \in \mathbb{Z}$.

2. (a) Como no exercício anterior, chegamos nas soluções gerais: $x = 604 + 7t$ e $y = 6342 - 18t$ com $t \in \mathbb{Z}$. Note que $x \geq 0 \Rightarrow -87 > t$ e $y \geq 0 \Rightarrow t > 352$.

   (b) Similar ao item anterior.

3.

4. Considere a equação

   $$11x + 9y = 270$$

   Resolvendo como no exercício 1, obtemos os múltiplos: $11(-2080 + 9t)$ e $9(1350 - 11t)$

5. Considere o sistema

   $$x = 37q + 9 \quad (1)$$
   $$x = 52p + 15 \quad (2)$$

   Basta resolver $52p + (-37)q = 6$ para p e q e encontrar os x que satisfazem.

6. Considere o sistema

   $$6x + 9y = 126 \quad (3)$$
   $$6y + 9x = 114 \quad (4)$$

   Manipulando o sistema acima obtemos que $(-1)x + (1)y = 4$. Basta resolvê-lo para x e y.

7. $2x+3y=p17$ pois $2x+3y$ é múltiplo de 17: $1=3+(-1)2 \Rightarrow p17 = 2(-p17)+3(p17) \Rightarrow x=-p17+3t, y=p17-2t$. Então,$3x+5y = 17(-4p+t)$.

8. Ele recebeu $100Y+X$ centavos no lugar de $100X+Y$ centavos. Gastou 68 centavos e restou o dobro do valor original. Isto é $100Y+X-68=2(100X+Y)$. O que nos leva para a seguinte equação diofantina: $(-199)X+98Y=-68$. Basta resolver para $X, Y \geq 0$ e $Y < 100$ pois é a quantidade em centavos.

9.

10. Considere $13,6 = 1,5X + 0,7Y$ e resolva $136 = 15X + 07Y$.

11. Basta resolver $252 = 18X + 3Y$ para X e Y.

12. (a)

    (b)

Números primos e Teorema Fundamental da Aritmética

13. $mmc(120, a) = 360 \Rightarrow a \leq 360$
    $mdc(450, a) = 90 \Rightarrow a = 90q$.
    Portanto $a = 90$.

14. $mdc(x,y) = 20 \Rightarrow x = 20p$ e $y = 20q$. Como $mmc(x,y) = 420$ então, $8400 = |xy| = 400|pq| \Rightarrow pq = 21 \Rightarrow x = 60, y = 140$.

15. Se $q|n$, q primo, $2 \leq q \leq n-2$. Caso $(n-1)! \equiv -1(mod\ n) \Rightarrow (n-1)! \equiv -1(mod\ q)$. Mas $(n-1)! \equiv 0(mod\ q)$, uma contradição.

16. Escreva a decomposição de a e b em fatores primos e perceba que p é o maior fator comum entre a decomposição de ambos. Logo $mdc(a^2, b) = p$ e rapidamente $mdc(a^2, b^2) = p^2$.

17.

18. Note que $p = 2k+1$ e $q = 2l+1 \Rightarrow p^2 - q^2|4$. Além disso, $p = 3a + r$ e $q = 3b + s$ com $0 < r, s < 3$ utilizando o algoritmo de Euclides e o fato de p e q serem primos. Analisando todas possibilidades de restos chegamos em $p^2 - q^2|6$. Portanto $p^2 - q^2|24$.

19. (a) $n = rs \Rightarrow 2^n - 1 = (2^s - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2s + 1)$, um número composto.

    (b) $n^4 + 4 = (2 - 2n + n^2)(2 + 2n + n^2)$.

(c) Se $N = 3n + 2$ não tem fatores tipo $3k + 2$, então todos os fatores primos tem a forma $3k+1$. Note que $(3k_1+1)(3k_2+1)\cdots(3k_n+1) = 3m + 1$, uma contradição.

(d) $n^3 - 1 = (n-1)(n^2+n+1)$.

(e)

20. (a) Note que, fazendo a divisão inteira: $100 : 7 = 14$ e $14 : 7 = 2$. Então "cabem" 7^{16} em 100!. De forma parecida, obtemos que "cabem" 2^{97} em 100!. Assim, a resposta é 14^{16}.

    (b) Similar ao item anterior.

21. Suponha que existam finitos primos da forma $3n + 2$. Seja S conjunto de primos nesse formato e escreva $\{p_1, ..., p_k\}$. Então, teremos que

$$(p_1 \cdots p_k)^2 + 1 \equiv 2(mod 3).$$

Um absurdo pois $(p_1 \cdots p_k)^2 \equiv 2(mod 3)$.

22.
$$2^{k+1} + 1 = (2+1)(2^{2k} - 2^{2k-1} + \cdots - x + 1)$$

Se m não é potência de 2, $m = (2k+1)2^l \Rightarrow 2^m + 1 = (2^l)^{2k+1} + 1$ que é divisível por $2^l + 1$.

23.

24. Veja as notas de aula.

25. Veja as notas de aula.

Congruências

26. a) Observe que

$$\begin{aligned} 11 &\equiv 4(\mod 7) \\ 18 &\equiv 4(\mod 7) \\ 2322 &\equiv 5(\mod 7) \\ 13 &\equiv 6(\mod 7) \\ 19 &\equiv 5(\mod 7) \end{aligned}$$

Assim $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv 4 \cdot 4 \cdot 5 \cdot 6 \cdot 5 \equiv 6(\mod 7)$.

b) Temos que

$$1 + 2 + \cdot 2^{19} = 2^{20} - 1$$

Por outro lado $2^{20} \equiv 0(\mod 4)$ e $-1 \equiv 3(\mod 4)$. Assim a resposta é 3.

27.

28.

29.

30.

31. Se $x \equiv y (\mod n)$, assim $n|(x-y)$. Seja $d = mdc(x,n)$ e $d' = mdc(y,n)$, assim $d|x$ e $d|n$ assim $d|y$ e $d|d'$. Semelhante $d'|d$. Assim $d = d'$.

32.

33. Como $6 \equiv (-5)(\mod 11)$ assim $6^n \equiv -5^n(\mod 11)$ para todo impar n.

34.

35.

36. a) Como $2^6 \equiv 1(\mod 7)$, assim $2^{48} \equiv 1(\mod 7)$. Assim $2^{50} \equiv 4(\mod 7)$.

    b) $41 \equiv -1(\mod 7)$ assim $41^{65} \equiv -1(\mod 7)$. Resto é 6.

    c) Resto é 0

37. b) Temos que $2^4 \equiv 7(\mod 23)$ e $7^2 \equiv 3(\mod 23)$, assim $2^11 \equiv 1(\mod 23)$.

38.

39.

40.