Introdução à Teoria dos Números

Projeto Supervisionado (MS 777)
Professor coordenador da disciplina: Alberto Vasquez Saa
Professor orientador do projeto: Lucas Catão de Freitas Ferreira
Aluna: Viviane Ezequiel Groot
Livro base: Introdução à Teoria dos Números
Autor: José Plínio de Oliveira Santos
Conteúdo estudado: capítulos 1 e 2.

Este trabalho tem como objetivo apresentar resultados e teoremas em Teoria dos Números, que, diferentemente de outros ramos da matemática, destaca-se não pela linguagem e pela técnica que desenvolve, mas pelos tipos de problemas e teoremas que possui e pela interdisciplinaridade e imaginação que eles exigem em sua resolução. Por esta razão, a área atrai simpatizantes de todos os ramos da matemática. Sua apresentação a alunos do ensino fundamental até o ensino superior se torna uma boa alternativa para o ensino do rigor e do pensamento matemático.

Resultados base para as demonstrações em Teoria dos Números

Princípio da Boa Ordem (PBO): Todo conjunto não-vazio de inteiros positivos admite um elemento mínimo.

Teorema 1 (Princípio da Indução Finita): Seja B subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades

(i) $1 \in B$
(ii) $k+1 \in B \text{ sempre que } k \in B$

Então B contém todos os inteiros positivos.

Dem. Vamos assumir o PBO como hipótese do teorema 1. Queremos mostrar que se B satisfaz (i) e (ii) então B contém necessariamente todos os inteiros positivos. Suponha por absurdo que b não contenha todos os inteiros positivos. Seja A o conjunto dos inteiros positivos que não estão contidos em B. Pelo PBO, A possui um menor elemento, digamos n_0 e este é maior que 1, pois $1 \in$ B. Então, $n_0 - 1 \in$ B e B satisfaz (ii). Logo o sucessor de $n_0 - 1$;

n_0 deve pertencer à B, absurdo. Portanto A deve ser vazio e concluímos demonstração de que B contém todos inteiros positivos.

■

Exercício: Mostre por indução finita que $n! > 2^n, \forall n \geq 4$.

Solução: Para $n = 4$ temos que $24 = 4! > 2^4 = 16, ok!$ Suponha válido para k: $k! > 2^k$. Vamos mostrar que o resultado se verifica para $k+1$. Então:

$(k+1)! = (k+1)k! > (k+1)2^k = k2^k + 2^k \geq 2^1 2^k = 2^{k+1}$, pois $k \geq 4$ por hipótese.

■

Divisibilidade

Definição 1: Sejam a,b $\in Z$. Dizemos que a|b (a divide b) se $\exists\ c \in Z$ tal que b = ac. Se a não divide b denotamos por "|" com uma barra.

Propriedades:

(i) a,b,c inteiros, se a|b e b|c então a|c;
(ii) a,b,c,m,n inteiros, c|a e c|b então c|(am + bn);
(iii) n inteiro então: n|n; 1|n; n|0;
(iv) d,n inteiros, d|n então ad|an;
(v) a,d inteiros, ad|an e a≠0 então d|n;
(vi) d,n inteiros, d|n e n≠0 então |d|≤|n|;
(vii) d,n inteiros, d|n e n|d então |d|=|n|;
(viii) d,n inteiros, d|n e d≠0 então (n/d)|n.

Dem. (i) Como $a|b\ e\ b|c$, então existem inteiros k_1, k_2 tais que $b = ak_1$ (1), $c = bk_2$ (2). Daí, substituindo (1) em (2) temos: $c = k_2(ak_1) = a\underbrace{(k_1k_2)}_{k} = ak$. Por definição temos portanto a|c.

(ii) Como c|a e c|b, então existem inteiros k_1, k_2 tais que $a = ck_1, b = ck_2$. Multiplcando essas duas equações por m e n, respectivamente, obtemos: $am = c(mk_1); bn = c(nk_2)$. Somando-as segue que $am + bn = c\underbrace{(mk_1 + mk_2)}_{k}$, donde, temos por definição que $c|(am + bn)$.

(iii) Vamos mostrar que n|n. Escolha k=1. Então, pela defințão, existe um inteiro k tal que n=kn=1n, pela nossa escolha, ficando provada a afirmação. Mostremos agora que n|0, ou seja, escolha n=0 tal que 0=nk=n1, pela escolha anterior. Logo, n|0. Resta mostrar que 1|n. Entao, n=1k, pela própria definição temos que 1|n.

(iv) Como d|n, existe k inteiro tal que n=kd. Multiplicando a igualdade por um inteiro a, temos: na=(ad)k o que implica que ad|na.

(v) Queremos mostrar que se $ad|an, a \neq 0$ *então* $d|n$. Então existe inteiro k tal que $an = kad$. Como $a \neq 0$, então podemos dividir por a: $n = kd \overset{def.}{\Longrightarrow} d|n$.

(vi) Queremos mostrar que se d|n e n é não nulo, então $|d| \leq |n|$. Por definição, existe um inteiro k tal que n=kd. Se k=1, temos que |n|=|d|, pois n e d são inteiros. Agora, suponha que k>1. Então, $n = kd \Rightarrow |d| \leq |n|$.

(vii) Como d|n e n|d, existem inteiros k_1, k_2 tais que: $n = dk_1$ (1), $d = nk_2$ (2). Substituindo (1) em (2): $d = d(k_1k_2)$. Fazendo (2) em (1): $n = k_1k_2n$. Assim, |d|=|n|.

(viii) Como $d|n\ e\ d \neq 0$, então existe inteiro k tal que $n = kd$. Temos que n é divisível por d, então $\frac{n}{d} \in Z$. Escolha $k = \frac{n}{d}$, donde temos o seguinte resultado: $n = kd = \frac{n}{d}\ d$, ou seja, $n = \left(\frac{n}{d}\right) d \Leftrightarrow \frac{n}{d}|n$.

■

Teorema 2 (Teorema Fundamental da Aritmética- TFA): Todo inteiro maior do que 1 pode ser escrito de modo único, a menos de ordem, como um produto de fatores primos.

Dem. Se n é primo, acabou. Suponha então que n é composto. Seja p_1 , $p_1 > 1$ o menor dos divisores primos positivos de n. Se p_1 não fosse primo, existiria um p, $1 < p < p_1$ com p|n, contradizendo a escolha de p_1. Logo, n = $p_1 n_1$. Se n_1 é primo, a prova está completa. Caso contrário, tomamos p_2 como menos fator de n_1. Pelo argumento anterior, p_2 é primo e temos que n = $p_1 p_2 n_2$. Repetindo este procedimento, obtemos uma seqüência descreste de inteiros positivos $n_1, n_2, \dots, n_r$. Como todos são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, \dots, p_k$ não são necessariamente distintos, n terá, em geral, a forma:

$$n = p_1^{a1} p_2^{a2} \dots p_k^{ak}.$$

Mostremos a unicidade por indução em n. Para n = 2 a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é:

$n = p_1 p_2 \dots p_s$ e $n = q_1 q_2 \dots q_r$. Vamos provar que s = r e que cada $p_i = q_j$, para algum i e j. Como $p_1 | q_1 q_2 \dots q_r$, então ele divide algum fator q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, temos a igualdade: $p_1 = q_1$. Logo, $\frac{n}{p_1} = p_2 \dots p_s = q_2 \dots q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são identicas, isto é, s = r e, a menos de ordem, as fatorações $p_1 p_2 \dots p_s$ e $q_1 q_2 \dots q_r$ são iguais.

■

Teorema 3 (Euclides): A sequência dos números primos é infinita.

Dem. Suponha por absurdo que a sequência dos números primos seja finita. Sejam eles: $p_1, p_2, \dots, p_n$. Considere o número m:= $p_1 p_2 \dots p_n + 1$, m não é divisível por nenhum p_i , $\forall\, i = 1, 2, \dots, n$ e m é maior que todo p_i . Pelo teorema 2, ou m é primo, ou m é múltiplo de algum p_i , ou seja, existe um primo que não está na lista. Logo, a seqüência de números primos é infinita.

□

Definição 2: O mínimo múltiplo comum entre dois inteiros a e b é definido como sendo o menor inteiro positivo que divide *a* e divide *b*. Notação: [a,b].

Definição 3: Um número da forma $F_n = 2^{2^n} + 1$ é dito número de Fermat.

Teorema 4: Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.

Dem. Vamos primeiro mostrar que a seguinte relação se verifica: $F_{n-2} = F_0 F_1 \dots F_{n-1}$. A prova é por indução em n. Se n=1 se verifica, isto é,$F_0 = F_1 - 2$. Suponha válido para n e mostremos que também vale para n+1.

$$\begin{aligned} F_0 F_1 \dots F_n &= (F_0 F_1 \dots F_{-1}) F_n = (F_n - 2) F_n = \left(2^{2^n} + 1 - 2\right)\left(2^{2^n} + 1\right) = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= 2^{2^{n+1}} - 1 = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2 \end{aligned}$$

Supondo $n < m$ temos, pela relação acima que $F_0 F_1 \dots F_n \dots F_{m-1} = F_m - 2$ o que implica que $F_m - F_0 \dots F_n \dots F_{m-1} = 2$. Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é ímpar, d não pode ser 2 e portanto, $(F_n , F_m) = 1$.

Disso, podemos concluir que existem infinitos números primos, pois sendo infinita a seqüência dos números de Fermat e não possuindo fatores primos em comum, isto não poderia ocorrer caso este conjunto fosse finito.

■

Problema: Mostrar que se $a^n - 1$ for primo com $n > 1$ e $a > 1$, então $a = 2$ e n também é primo.

Resolução: observe que $a^n - 1 = (a-1)(a^{n-1} + \cdots + 1)$ $(*)$, onde $(a-1)(a^{n-1} + \cdots + 1) > 1$, então concluímos que $a - 1 = 1$, pois por hipótese temos que $a^n - 1$ é primo, implicando que um dos fatores do segundo membro de $(*)$ deve ser igual á 1. Assim, $a = 2$.

Suponha por absurdo que n não é primo, ou seja, podemos escrever $n = kb; k, b \in Z$. Daí, como $a = 2$, temos:

$(2^n - 1) = (2^{kb} - 1) = (2^k - 1)(2^{k(b-1)} + \cdots + 2^b + 1)$, contradizendo o fato de n ser primo – pois fatoramos um número que por hipótese é primo. Logo, n é primo.

Teorema 5 (Teorema de Eudoxius): Dados *a, b* inteiros com $b \neq 0$ então a é múltiplo de b ou encontra-se entre dois múltiplos consecutivos de *b*. Isto é, correspondendo a cada par de inteiros a e $b \neq 0$, existe um inteiro q tal que, $qb \leq q < (qb+1)$, para $b > 0$, ou $qb \leq a < (q-1)b$, para $b < 0$.

Teorema 6 (Algoritmo da Divisão): Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que:

$$a = qb + r \qquad (1)$$

$com\ 0 \leq r < b\ \ e\ r = 0 \Leftrightarrow b|a$.

Obs.: q é dito quociente e r resto da divisão de a por b.

Dem. Pelo teorema de Eudoxius, como b > 0, existe um q satisfazendo: $qb \leq q < (q+1)b$ $\Rightarrow 0 \leq a - qb\ e\ a - qb < b$. Defina $r = a - qb$, pois assim garantimos a existência de q e r, que são únicos.

Para provar a unicidade, suponha que exista outro par q_1, r_1 satisfazendo: $a = q_1 b + r_1\ com\ 0 \leq r_1 < b$. Assim, temos $(qb + r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r$, ou seja, $b|(r_1 - r)$. Observe que $r_1 < b\ e\ r < b \Rightarrow |r_1 - r| < b$, absurdo. Logo, temos que $q_1 = q, r_1 = r, com\ b > 0$. Portanto $q\ e\ r$ são únicos satisfazendo (1).

■

Teorema 7: Existem infinitos números primos da forma 6k+5.

Dem. Pelo teorema anterior, quando dividimos um número qualquer por 6, temos os possíveis restos: 0,1,2,3,4,5; ou seja, podemos escrever um inteiro da seguinte forma: 6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5.

Se p é primo e diferente de 3, então p é da forma 6k+1 ou 6k+5. Vamos supor por absurdo que exista uma quantidade finita de números primos da forma 6k+5. Seja então $p_0 = 5, p_1, p_2, \ldots, p_r$ estes números e considere $P = 6p_1 \ldots p_r + 5$ e pela propriedade (ii) de divisibilidade temos que P não é divisível por nenhum $p_i, \forall i \in \{0,1,\ldots,r\}$. Afirmamos que P possui um fator primo da forma 6k+5, pois se fosse da forma 6k+1 implicaria que o produto dos números dessa forma continua 6k+1. Então, ou P é primo ou P possui fator primo da forma 6k+5. Assim, provamos a existência de infinitos números primos da forma 6k+5.

■

Teorema 8: Se a e b são inteiros e $a = qb + r, onde\ q\ e\ r$ são inteiros, então (a,b) = (b,r).

Dem. Por $a = qb + r$, podemos concluir que todo divisor de b e r é divisor de a, pela propriedade (ii) de divisibilidade. Escrevendo $r = a - qb$ temos que todo divisor de a e b é um divisor de r. Logo, o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r. Portanto, temos a igualdade (a,b) = (b,r).

■

Teorema 9 (Algoritmo de Euclides): Sejam $r_0 = a\ e\ r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algortimo da divisão for aplicado sucessivamente para obter-se

$$r_j = q_{j+1}r_{j+1} + r_{j+2}\ com\ 0 \leq r_{j+2} < r_{j+1}; j \in \{0,1,\dots,n-1\}\ e\ r_{n+1} = 0$$

$então\ (a,b) =\ r_n$, onde r_n é o último resto não nulo.

Dem. Pelo teorema 6, temos: $a = bq + r\ com\ 0 \leq r < b$

$$r_1 = q_2r_2 + r_3\ com\ 0 \leq r_3 < r_2$$

$$r_2 = q_3r_3 + r_4\ com\ 0 \leq r_4 < r_3$$

$$\dots$$

$$r_{n-2} = q_{n-1}r_{n-1} + r_n\ com\ 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_nr_n + 0.$$

Logo, concluímos pelo teorema anterior, que a última dessas equações, o máximo divisor comum de $r_n\ e\ r_{n-1}$ é r_n. A penúltima, (r_{n-1}, r_{n-2}). Repetindo este processo vamos obter a sequência:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \cdots = (r_1, r_2) = (r_0, r_1) = (a, b).$$

Portanto, o máximo divisor comum entre a e b é o último resto não nulo da sequência de divisões.

■

Definição 4: O máximo divisor comum de dois inteiros a e b é o maior inteiro que divide a e b, denotado por (a,b).

Definição 4.1: Dois números a e b são ditos co-primos ou primos relativos se $(a,b) = 1$.

Exercício: Encontre inteiros x e y tais que: $43x + 128y = 1$.

Solução: Note que $(128,43) = (43,42) = 1$. Então, podemos escrever:

$$143 = (2)43 + 42$$
$$43 = (1)42 + 1, donde$$
$$1 = 43 - 42 = 43 - (143 - 2.43)$$
$$1 = (3)43 + (-1)128 \Rightarrow x = 3\ e\ y = -1$$

Lema 1: Se $a|bc$ e $(a,b) = 1$, então $a|c$.

Dem. Como $a|bc$, pelo item (ii) de divisibilidade $\exists\ m, n \in Z$ tais que $an + bm = 1 \Leftrightarrow n(ac) + m(bc) = c$. Temos que $a|ac\ e\ por\ hipótese\ a|bc$, então pelo item (ii) de divisibilidade $a|c$.

■

Lema 2: Se $c > 0\ e\ a, b \in Z$ são divisíveis por c, então $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$. Em particular, $\left(\frac{a}{c}, \frac{b}{c}\right) = 1$.

Dem. Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são números inteiros. Então pela propriedade (ii) de divisibilidade existem m,n inteiros tais que se $d = \left(\frac{a}{c}, \frac{b}{c}\right) \xRightarrow{prop.(ii)divisibilidade} \frac{1}{c}(a, b)$.

Temos que c é divisor de a e de b. Tome $c = d = (a, b)$, ou seja, o máximo divisor comum. Então, dividindo a e b por seu divisor comum, c, chegamos em $\left(\frac{a}{c}, \frac{b}{c}\right) = 1$.

■

Teorema 10: Sejam $a\ e\ b$ inteiros co-primos. Então, se d é $divisor\ positivo\ de\ ab$, existe um único par de divisores positivos $d_1 de\ a,\ d_2\ de\ b\ tais\ que\ d = d_1 d_2$. Reciprocamente, se $d_1\ e\ \ d_2$ são divisores positivos de $a\ e\ b$, respectivamente, então $d = d_1 d_2$ é um divisor positivo de ab.

Dem. Vamos consideraras fatorações de $a\ e\ b$ dadas por: $a = p_1^{a1} \dots p_n^{an}$ e $b = q_1^{b1} \dots q_m^{bm}$. Como $(a, b) = 1$, os conjuntos $\{p_1, \dots p_n\}\ e\ \{q_1, \dots, q_m\}$ são disjuntos. Assim temos que a fatoração de $ab = p_1^{a1} p_2^{a2} \dots p_n^{an} q_1^{b1} \dots q_m^{bm}$. Se d é divisor positivo de ab, então temos que $d = p_1^{k1} \dots p_n^{kn} q_1^{l1} \dots q_m^{lm}$ com $0 \leq ki \leq ai\ e\ 0 \leq lj \leq bj, \forall i \in \{1, \dots, n\}\ e\ \forall j \in \{1, \dots, m\}$.

Defina então $d_1 = p_1^{a1} \dots p_n^{an}\ e\ d_2 = q_1^{b1} \dots q_m^{bm}$. É fácil ver que $(d_1, d_2) = 1$, pois $d = d_1 d_2$.

Reciprocamente, consideremos $d_1\ e\ d_2$ divisores de $a\ e\ b$, respectivamente. Assim, $d_1 = p_1^{k1} \dots p_n^{kn}, 0 \leq ki \leq ai, \forall i$ e $d_2 = q_1^{l1} \dots q_m^{lm}, 0 \leq lj \leq bj, \forall j$. Então, o número $d = d_1 d_2$ é divisor de ab.

■

Teorema 11: Se n é primo, então n possui, necessariamente, um fator primo menor ou igual à $\sqrt{n}$.

Dem. Como n é composto, então $n = n_1 n_2$, $onde$ $1 < n_1 < n, 1 < n_2 < n$. Sem perda de generalidade vamos supor que $n_1 \leq n_2 \Rightarrow n_1 \leq \sqrt{n}$, pois caso contrário, teríamos $n = n_1 n_2 > \sqrt{n}\sqrt{n} = n$, absurdo. Pelo TFA, n_1 possui algum fator primo $p \leq \sqrt{n}$. Como p é fator primo de n_1 também é fator primo de n, completando a demonstração.

■

Exercício: Mostre que se m,n são inteiros ímpares então $8|(n^4 + m^4 - 2)$.

Solução: Como m e n são ímpares, vamos representá-los por $n = 2n - 1\ e\ m = 2m - 1$. Assim, $n^4 = (2n - 1)^4 = 16n^4 + 16n^2 + 1 + 2(4n^2 - 4n - 16n^3)$ e $m^4 = (2m - 1)^4 = 16m^4 + 16m^2 + 1 + 2(4m^2 - 4m - 16m^3)$. Então, $n^4 + m^4 - 2 = 2(2n^4 + 2n^2 + 2m^4 + 2m^2 - 4n^3 + n^2 - n + m^2 - m - 4m^3)$.

$\therefore 8|(n^4 + m^4 - 2)$.

■

Congruências

Definição 5: Dizemos que a é côngruo à b modulo m: $a \equiv b\ mod\ m, m > 0,\ a, b\ \in Z$ se $m|(a - b)$. Dizemos que a é incongruente à b se m não divide (a - b).

Propriedades:

(i) $a, b, c, m\ \in Z, a \equiv b\ mod\ m$ se e somente se existe $k \in Z$ tal que $a = km + b$;
(ii) $a \equiv a\ mod\ m$;

(iii) $se\ a \equiv b\ mod\ m\ , então\ b \equiv a\ mod\ m;$

(iv) $se\ a \equiv b\ mod\ m\ e\ b \equiv c\ mod\ m, então\ a \equiv c\ mod\ m;$

(v) $a + c \equiv b + c\ mod\ m;$

(vi) $a - c \equiv b - c\ mod\ m;$

(vii) $ac \equiv bc\ mod\ m.$

(viii) $k \in N,\ a \equiv b\ mod\ m,\ então\ a^k \equiv b^k\ mod\ m.$

Dem. (i): Como $a \equiv b\ mod\ m$, por definição temos que $m|(a-b) \Leftrightarrow \exists\ k \in Z\ tal\ que\ a - b = km$ $\Leftrightarrow a = km + b.$

(ii): Como $m|0 \Leftrightarrow m|(a-a)$, temos por definição que $a \equiv a\ mod\ m.$

(iii): Se $a \equiv b\ mod\ m$, então existe $k_1 \in Z$ tal que $a = mk_1 + b$. Logo, $b = a - mk_1 \underset{(i)}{\Rightarrow} b \equiv a\ mod\ m.$

(iv): Como $a \equiv b\ mod\ m\ e\ b \equiv c\ mod\ m, então, por\ definição\ temos\ \exists k_1, k_2 \in Z$ tal que $a = mk_1 + b\ e\ b = mk_2 + c$. Assim, $a = mk_1 + mk_2 + c \xRightarrow{k=k_1+k_2} a = mk + c \overset{def.}{\Longrightarrow} a \equiv c\ mod\ m.$

(v): $a \equiv b\ mod\ m \overset{\exists k \in Z}{\Longleftrightarrow} a = mk + b \Leftrightarrow a + c = mk + (b + c) \overset{def.}{\Longleftrightarrow} a + c \equiv b + c\ mod\ m.$

(vi): Como $a \equiv b\ mod\ m$, então $\exists k \in Z$ tal que $a - b = mk \Leftrightarrow (a - c) - (b - c) = mk \Leftrightarrow a - c \equiv b - c\ mod\ m.$

(vii): Como $a \equiv b\ mod\ m$, então $\exists k \in Z$ tal que $a - b = mk \Leftrightarrow ac - bc = mkc \overset{def.}{\Longrightarrow} m|(ac - bc)$ $\Leftrightarrow ac \equiv bc\ mod\ m.$

(viii): Como $a \equiv b\ mod\ m\ \Rightarrow m|(a-b), mas\ (a-b) = \frac{(a^k - b^k)}{(a^{k-1} + a^{k-2}b + \cdots + b^{k-2}a + b^{k-1})}$. Então $\exists c > 0 \in Z$ tal que $m = (a - b)c \Leftrightarrow \frac{(a^k - b^k)}{(a^{k-1} + a^{k-2}b + \cdots + b^{k-2}a + b^{k-1})} c$. Seja $k \coloneqq (a^{k-1} + \cdots + b^{k-1})$; então temos: $mk = (a^k - b^k)c \Leftrightarrow m\frac{k}{c}|(a^k - b^k) \overset{def.}{\Longrightarrow} a^k \equiv b^k\ mod\ m.$

■

Exercício: Mostrar que $47|(2^{23} - 1)$.

Solução: Mostrar $47|(2^{23} - 1)$ equivale a mostrar que $2^{23} \equiv 1\ mod\ 47$.

Teorema 12: Sejam $a, b, c, d, m \in Z\ tais\ que\ a \equiv b\ mod\ m\ e\ c \equiv d\ mod\ m. Então$:

(i) $a + c \equiv b + d\ mod\ m;$

(ii) $a - c \equiv b - d\ mod\ m;$

(iii) $ac \equiv bd\ mod\ m.$

Dem. (i): Como $a \equiv b\ mod\ m\ e\ c \equiv d\ mod\ m, \exists k, k_1 \in Z\ tais\ que\ a = mk + b\ e\ c = mk_1 + d.$ Somando membro a membro obtemos: $a + c = m(k + k_1) + (b + d) \Rightarrow a + c \equiv b + d\ mod\ m.$

(ii): Vamos subtrair membro a membro das equações: $a - b = mk\ e\ c - d = mk_1$. Então, obtemos: $(a - b) - (c - d) = m(k - k_1) \Rightarrow a - b \equiv c - d\ mod\ m.$

(iii): Do item anterior já temos que $a - b = mk \Leftrightarrow ac - bc = mkc \Rightarrow m|(ab - bc) \Rightarrow ab \equiv bc \; mod \; m$.

■

Definição 6: Se $h, k \in Z, com \; h \equiv k \; mod \; m$, dizemos que k é um resíduo de h módulo m.

Definição 7: O conjunto $\{r_1, r_2, \dots, r_s\}$ é um sistema completo de resíduos módulo m se:

(i) $r_i \not\equiv r_j \; mod \; m \; para \; i \neq j$;

(ii) $\forall \; n, \exists \; r_i \; tal \; que \; n \equiv r_i \; mod \; m$.

Teorema 13: Se k inteiros $r_1, r_2, \dots, r_k$ formam um sistema completo de resíduos módulo m; então $k = m$.

Dem. Vamos mostrar primeiro que $t_0, t_1, \dots, t_{m-1} \; com \; t_i = i$ formam um sistema completo de resíduos módulo m. Pelo algoritmo da divisão sabemos que para cada n existe um único par de inteiros q e s, tal que $n = qm + s, 0 \leq s < q$. Logo, $n \equiv s \; mod \; m$, sendo s um dos t_i. Como $|t_i - t_j| \leq m - 1, temos \; que \; t_i \not\equiv t_j \; mod \; m; para \; i \neq j$. Portanto, o conjunto $\{t_0, t_1, \dots, t_{m-1}\}$ é um sistema completo de resíduos módulo m.

Disso, concluímos que cada r_i é congruente a exatamente um dos t_i, o que nos garante $k \leq m$. O conjunto $\{r_1, r_2, \dots, r_k\}$, por hipótese forma um sistema completo de resíduos módulo m; cada t_i é congruente a exatamente um dos r_i e, portanto $m \leq k$. Assim, $m = k$.

■

Teorema 14: Se $\{r_1, \dots, r_m\}$ é um sistema completo de resíduos módulo m; $a, b \in Z \; com \; (a, m) = 1, então$: $ar_1 + b, ar_2 + b, \dots, ar_m + b$ também é um sistema completo de resíduos módulo m.

Dem. Vamos considerar o resultado do teorema anterior. Então será suficiente provarmos que dois inteiros quaisquer do conjunto $ar_1 + b, ar_2 + b, \dots, ar_m + b$ são incongruentes módulo m. Então, suponha por absurdo que $ar_i + b \equiv ar_j + b \; mod \; m, \; pela \; propriedade \; (v) de \; congruência$. Então, $ar_i \equiv ar_j \; mod \; m \xRightarrow{(a,m)=1} r_i \equiv r_j \; mod \; m \Rightarrow i = j$, pois $\{r_1, \dots, r_m\}$ forma um sistema completo de resíduos módulo m.

■

Teorema 15: Se $a \equiv b \; mod \; m_1, a \equiv b \; mod \; m_2, \dots, a \equiv b \; mod \; m_k, com \; a, b, m_i > 0 \in Z, \; \forall i \in \{1,2, \dots, k\}. Então, a \equiv b \; mod[mmc(m_1, m_2, \dots, m_k)]$.

Dem. Seja p_n o maior primo que aparece nas fatorações dos m_i, onde cada m_i é escrito da forma $m_i = p_1^{a1i} p_2^{a2i} \dots p_n^{ani}$.

$m_i|(a - b) \Rightarrow p_j^{aji}|(a - b) \; \forall i. Tome \; a_j = \max_{1 \leq j \leq k}\{a_{ji}\}$, onde vamos ter que $p_1^{a1} p_2^{a2} \dots p_n^{an} \Big| (a - b)$

$\Rightarrow mmc(m_1, m_2, \dots, m_k) \Big| (a - b) \Rightarrow a \equiv b \; mod \; [mmc(m_1, m_2, \dots, m_k)]$.

■

Congruência Linear

Definição 8: É chamada de congruência linear em uma variável à congruência da forma $ax \equiv b \mod m$, onde x é uma incógnita.

Teorema 16: Sejam a e b inteiros e $d = (a,b)$. Se d não divide c, então a equação $ax + by = c$ não possui solução inteira. Se d|c, então ela possui infinitas soluções e se $x = x_0, y = y_0$ é uma solução particular, então todas as soluções são dadas por

$$x = x_0 + \left(\frac{b}{d}\right)k$$
$$y = y_0 - \left(\frac{a}{d}\right)k$$

$onde\ k$ é $um\ inteiro$.

Dem. Se $d \nmid c$, então a equação $ax + by = c$ (1) não possui solução, pois como $d|a\ e\ d|b$ deveria existir um c tal que $c = ax + by, x, y \in Z$, ou seja, c é um combinação linear de a e b.

Suponhamos então que $d|c$. Então, pela propriedade (ii) de divisibilidade, existem inteiros m_0, n_0 tal que $an_0 + bm_0 = d$ (2); e existe um k inteiro tal que $c = dk$. Então, multiplicando (2) por k, obtemos: $a(kn_0) + b(km_0) = dk = c$, ou seja, o par definido por $(x_0, y_0) \coloneqq (kn_0, km_0)$ é uma solução para a equação $ax + by = c$. Vamos verificar que $x = x_0 + \left(\frac{b}{d}\right)k, y = y_0 - \left(\frac{a}{d}\right)k$ são soluções de (1). Então, substituindo x e y em (1) temos:

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)k\right) + b\left(y_0 - \left(\frac{a}{d}\right)k\right)$$
$$= ax_0 + ak\left(\frac{b}{d}\right) + by_0 - bk\left(\frac{a}{d}\right)$$
$$= ax_0 + by_0 = c$$

Logo, (x_0, y_0) é uma solução particular, podendo dela gerar infinitas soluções. Vamos mostrar agora que toda solução de (1) é da forma $x = x_0 + \left(\frac{b}{d}\right)k, y = y_0 - \left(\frac{a}{d}\right)k.$ Então suponha que (x, y) sejá solução de (1), ou seja, $ax + by = c$. Como (x_0, y_0) é solução particular, temos também que $ax_0 + by_0 = c$. Subtraindo membro a membro das duas últimas equações chegamos na seguinte igualdade:

$$ax - ax_0 + by - by_0 = 0 \Leftrightarrow$$
$$a(x - x_0) = b(y - y_0)$$

Como $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, pelo lema 1. Então, dividindo ambos os lados por d, chegamos em:

$\frac{a}{d}(x - x_0) = \frac{b}{d}(y - y_0)$ e pelo lema 1, $\left(\frac{b}{d}\right)|(x - x_0) \xRightarrow{\exists k \in Z} (x - x_0) = k\left(\frac{b}{d}\right) \Leftrightarrow x = x_0 + k\left(\frac{b}{d}\right)$ (3)

Agora, substituindo (3) em $\frac{a}{d}(x - x_0) = \frac{b}{d}(y - y_0)$, obtemos:

$$\frac{a}{d}\left(x_0 + k\left(\frac{b}{d}\right) - x_0\right) = \frac{b}{d}(y - y_0) \Leftrightarrow$$
$$\frac{a}{d}\frac{b}{d}k = \frac{b}{d}y_0 - \frac{b}{d}y \Leftrightarrow$$
$$y_0 - \frac{a}{d}k = y\ (4)$$

As igualdades (3) e (4) é o que queríamos demonstrar.

■

Teorema 17: $Sejam\ a, b, m > 0\ inteiros\ e\ (a, m) = d. Se\ d\ não\ divide\ b, então\ a\ congruencia\ ax \equiv b\ mod\ m\ não\ possui\ solução\ e\ se\ d|b, possui\ exatamente\ d\ soluções\ incongruentes\ módulo\ m.$

Dem. Pela propriedade (i) de congruência, sabemos que o número inteiro x é solução de

$ax \equiv b\ mod\ m \Leftrightarrow \exists y\ inteiro\ tal\ que\ ax = b + my \Leftrightarrow ax - my = b$. Pelo teorema anterior esta equação terá infinitas soluções se d|b e serão da forma $x = x_0 + \frac{b}{d}k\ e\ y = y_0 - \frac{a}{d}k$, onde (x_0, y_0) é uma solução particular para $ax - my = b$. Logo, a congruência $ax \equiv b\ mod\ m$ possui infinitas soluções dadas por $x = x_0 - \frac{m}{d}k$. Queremos saber o número de soluções incongruentes, então vamos descobrir sob quais condições $x_1 = x_0 - \frac{m}{d}k_1\ e\ x_2 = x_0 - \frac{m}{d}k_2$ são congruentes módulo m.

Então, se $x_1\ e\ x_2$ são congruentes temos $x_0 - \frac{m}{d}k_1 \equiv x_0 - \frac{m}{d}k_2\ mod\ m \Rightarrow$

$$\frac{m}{d}k_1 \equiv \frac{m}{d}k_2\ mod\ m\ , como\ \left(\frac{m}{d}\right)|m\ e\ \left(\frac{m}{d}, m\right) = \frac{m}{d}$$

$$então, k_1 \equiv k_2\ mod\ m$$

Logo, as soluções incongruentes são obtidas tomando-se $x = x_0 - \frac{m}{d}k$, para k percorrendo o sistema completo de resíduos módulo d.

■

Definição 9: Dizemos que uma solução $x_0\ de\ ax \equiv b\ mod\ m$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Definição 10: Uma solução $\bar{a}\ de\ ax \equiv 1\ mod\ m$ é chamada de um inverso de a módulo m.

Lema 3: Seja p primo. O numero positivo a é o seu próprio inverso módulo p se e somente se $a \equiv 1\ mod\ p\ ou\ a \equiv -1\ mod\ p$.

Dem. ($\Rightarrow$) Se a é o seu próprio inverso, então $a^2 \equiv 1\ mod\ p \Rightarrow p|(a^2 - 1)$. Como p é primo, temos que $p|(a + 1)\ ou\ p|(a - 1), ou\ seja;\ \ a \equiv -1\ mod\ p\ ou\ \ a \equiv 1\ mod\ p.$

($\Leftarrow$) Se $a \equiv 1\ mod\ p\ ou\ a \equiv -1\ mod\ p\ \Rightarrow p|(a - 1)\ ou\ p|(a + 1) \Rightarrow p|(a - 1)(a + 1), ou\ seja,$ $p|(a^2 - 1) \Rightarrow a^2 \equiv 1\ mod\ p.$

■

Teorema 18 (Teorema de Wilson): $Se\ p$ *é* $primo, então\ (p - 1)! \equiv -1\ mod\ p.$

Dem. Se $p = 2, o\ resultado$ é $válido$: $(2 - 1)! \equiv -1\ mod\ 2$. Pelo teorema 17, $ax \equiv 1\ mod\ p\ possui\ uma\ única\ solução\ \forall a \in \{1,2,3, \dots, p - 1\}$. Destes elementos apenas 1 e p - 1 são seus próprios inversos módulo *p*. Podemos agrupar os números 2,3,4,...,*p* -2 em (p - 3)/2 pares cujo produto seja congruente a 1 módulo *p*. Multiplicando essas congruências membro a membro, temos pelo teorema 12: $2.3 \dots (p - 2) \equiv 1\ mod\ p\ \Leftrightarrow 2.3 \dots (p - 2)(p - 1) \equiv 1.(p - 1)\ mod\ p$, ou seja $(p - 1)! \equiv -1\ mod\ p,\ uma\ vez\ que\ p - 1 \equiv -1\ mod\ p.$

■

Definição 11: Se n é um inteiro positivo, a função ϕ de Euler, denotada por ϕ(n) é definida como sendo os inteiros positivos $a \leq n$ tais que $(a, n) = 1$.

Teorema 19: Seja a um inteiro positivo tal que $(a,m) = 1$. Se $r_1, \dots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, \dots, ar_{\phi(m)}$ é também um sistema reduzido de resíduos módulo m.

Dem. Como na seqüência $ar_1, \dots, ar_{\phi(m)}$ temos $\phi(m)$elementos, vamos mostrar que todos eles são co-primos com m e, dois a dois incongruentes módulo m.

Temos $(a,m) = 1\ e\ (r_i,m) = 1$ implicando que $(ar_i,m) = 1$. Vamos agora mostrar que $ar_i \not\equiv ar_j,\ se\ i \neq j$. Mas, $(a,m) = 1\ e\ ar_i \equiv ar_j\ mod\ m \Rightarrow r_i \equiv r_j\ mod\ m \Rightarrow i = j$, uma vez que $r_1, \dots, r_{\phi(m)}$ é um sistema reduzido de residuos módulo m.

■

Teorema 20 (Teorema de Euler): Sejam $a, m \in Z,\ (a,m) = 1. Então,\ a^{\phi(m)} \equiv 1\ mod\ m.$

Dem. Seja $r_1, \dots, r_{\phi(m)}$ um sistema reduzido de resíduos módulo m. Então, $ar_1, \dots, ar_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Assim,

$a^{\phi(m)} r_1 \dots r_{\phi(m)} = ar_1 \dots ar_{\phi(m)} \equiv r_1 \dots r_{\phi(m)}\ mod\ m$. Como $\left(r_1 \dots r_{\phi(m)}, m\right) = 1$, então faz sentido

$a^{\phi(m)} r_1 \dots r_{\phi(m)} \equiv r_1 \dots r_{\phi(m)}\ mod\ m \Rightarrow a^{\phi(m)} \equiv 1\ mod\ m.$

■

Corolário 1 (Pequeno teorema de Fermat): Sejam $a, p \in Z, (a,p) = 1, com\ p\ primo$. Então, $a^{p-1} \equiv 1\ mod\ p.$

Dem. Como p é primo, temos que $\phi(p) = p - 1$. Aplique o teorema anterior para $\phi(p)$.

Teorema 21 (Teorema do Resto Chinês): Se $(a_i, m_i) = 1, \left(m_i, m_j\right) = 1\ para\ i \neq j\ e\ c_i\ inteiro$, então o sistema:

$$
\begin{gathered}
a_1 x \equiv c_1\ mod\ m_i \\
a_2 x \equiv c_2\ mod\ m_2 \\
\vdots \\
a_r x \equiv c_r\ mod\ m_r
\end{gathered}
$$

Possui solução e a solução é única módulo $m, onde\ m \coloneqq m_1 m_2 \dots m_r$.

Demo.: Do fato de $(a_i, m_i) = 1$, o teorema 17 nos diz que $a_i x \equiv c_i\ mod\ m_i$ possui solução única, que vamos denotar por $b_i. Defina\ y_i = \frac{m}{m_i}$ onde, $m = m_1 \dots m_r, donde\ \ vamos\ ter\ que\ (y_i, m_i) = 1$, uma vez que $\left(m_i, m_j\right) = 1\ para\ i \neq j$. Novamente, o teorema 17 nos garante que uma das congruências $y_i x \equiv 1\ mod\ m_i$ possui solução única, e vamos denotar por $\overline{y_i}$. Logo, $y_i \overline{y_i} \equiv 1\ mod\ m_i, i = 1, \dots, r$. Afirmamos que o número $x = b_1 y_i \overline{y_i} + \dots + b_r y_r \overline{y_r}$ é uma solução simultânea para o nosso sistema de congruências. De fato, $a_i x = a_i b_1 y_i \overline{y_i} + \dots + a_i b_r y_r \overline{y_r} \equiv\ a_i b_i y_i \overline{y_i}\ mod\ m_i \equiv\ a_i b_i \equiv\ c_i\ mod\ m_i$, uma vez que y_j é divisível por $m_i, para\ i \neq j, y_i \overline{y_i} \equiv 1\ mod\ m_i\ e\ b_i$ é solução de $a_i x \equiv c_i\ mod\ m_i$.

Vamos provar que esta solução é única módulo m. Se $\bar{x}$ é outra solução para o nosso sistema, então $a_i \bar{x} \equiv c_i \equiv a_i x\ mod\ m_i$ e sendo $(a_i, m_i) = 1$, obtemos $x \equiv \bar{x}\ mod\ m_i \Rightarrow m_i | (x - \bar{x}), i = 1, \dots, r$. Mas, como $\left(m_i, m_j\right) = 1$ para $i \neq j$ temos que: $[m_1, \dots, m_r] = m_1 \dots m_r$. Portanto, pelo teorema 15 $m_1 \dots m_r | (x - \bar{x}),\ \ ou\ seja, x \equiv\ \bar{x}\ mod\ m$, concluindo a demonstração.

■

Exercício: Resolver o sistema: $\begin{cases} x \equiv 1 \ mod \ 2 \\ x \equiv 2 \ mod \ 3 \\ x \equiv 5 \ mod \ 7 \end{cases}$. Pelo teorema do resto chinês, temos:

$c_1 = 1, c_2 = 2, c_3 = 5, m_1 = 2, m_2 = 3, m_3 = 7, y_1 = 21, y_2 = 14, y_3 = 6$. Vamos encontrar as soluções $b_i,\ i = 1,2,3$. Note que $b_1 = 1, b_2 = 2, b_3 = 5$ são soluções únicas das congruências do sistema dado. Agora vamos encontrar os inversos de y_1, y_2, y_3. Então, $21\overline{y_1} \equiv 1 \ mod \ 2 \Rightarrow \overline{y_1} = 1$, $14\overline{y_2} \equiv 1 \ mod \ 3 \Rightarrow \overline{y_2} = 2 \ e \ 6\overline{y_3} \equiv 1 \ mod \ 7 \Rightarrow \overline{y_3} = 6$. Afirmamos que $x = 1.21.1 + 2.14.2 + 5.6.6 = 257$, é solução única módulo 42 para o sistema de congruências.

Conclusão

O livro Introdução à Teoria dos números é um bom livro para se introduzir os conceitos de divisibilidade e congruência à alunos que nunca tiveram contato com o assunto antes. A obra ainda contribui para a iniciação do aluno ao rigor matemático com teoremas de enunciado simples e fácil compreensão, sendo agradável sua leitura. Os tópicos abordados nesse trabalho visaram a compreensão de teoremas da aritmética elementar que se tornam indispensáveis no desenvolvimento do livro.