22. Seja $U_n = 111\ldots1$ um número formado por n 1's. Provar que U_n primo implica n primo.

23. Mostrar que se para algum n, $m|(35n+26)$, $m|(7n+3)$ e $m > 1$, então $m = 11$.

24. Sendo $\frac{1}{a} + \frac{1}{b}$ um inteiro, onde a e b são inteiros positivos, mostrar que $a = b$. Mostrar, também, que $a = 1$ ou 2.

25. Mostrar que se $(a,b) = 1$, então $(2a+b, a+2b) = 1$ ou 3.

26. Mostrar que, sendo n um inteiro, o número $n(n+1)(n+2)(n+3)+1$ é um quadrado perfeito.

27. Determinar todos o números de 3 algarismos divisíveis por 8, 11 e 12.

28. Encontrar todos os inteiros positivos n para os quais $(n+1)|(n^2+1)$.

29. Dados a e b inteiros com $b \neq 0$, mostrar que existem inteiros q e r satisfazendo $a = qb \pm r$, $0 \leq r \leq b/2$.

30. Mostrar que se a e b são inteiros, $(a,3) = (b,3) = 1$, então $a^2 + b^2$ não é um quadrado perfeito.

31. Mostrar que para $n > 1$ os números $n^4 + 4$ e $n^4 + n^2 + 1$ são, ambos, compostos.

32. Demonstrar os ítens (a), (b) e (c) do problema 13 sem fazer uso de indução.

33. Mostrar que $(a, bc) = 1$, se, e somente se, $(a,b] = (a,c) = 1$.

34. Mostrar que se $b|c$ então $(a+c, b) = (a, b)$

35. Mostrar que se $(a,c) = 1$ então $(a, bc) = (a, b]$.

36. Mostrar que $(a, b, c) = ((a, b), c)$.

37. Dizer qual é o maior inteiro que pode ser somado ao dividendo sem alterar o quociente quando se divide 431 por 37.

38. Para cada par de inteiros "a"e "b"dado abaixo encontrar o quociente q e o resto r satisfazendo o algoritmo da divisão de Euclides.

(i) $a = 59$; $b = 6$
(ii) $a = -71$; $b = 5$
(iii) $a = -48$; $b = -7$
(iv) $a = 67$; $b = -13$

39. Mostrar que se n e m são inteiros ímpares, então $8|(n^4 + m^4 - 2)$.

40. Encontrar o menor inteiro positivo da forma $36x + 54y$ onde x e y são inteiros.

41. Utilizando o processo descrito no Teorema 1.17 expressar o número 274 nas bases 2,5,7 e 9.

42. Transformar para a base 10 os seguintes números
(a) $(2351)_7$ (b) $(1001110)_2$ (c) $(7706)_8$ (d) $(11122)_4$

43. Mostrar que se $2^n + 1$ é um primo ímpar, então n é uma potência de 2.

44. Provar que se $d = (a,b)$, então d é o número de inteiros na seqüência $a, 2a, 3a, \ldots, ba$ que são divisíveis por b.

Capítulo 2

Congruência

2.1 Congruência

Grande parte dos resultados deste capítulo foi introduzida por Gauss (1777-1855) em um trabalho publicado em 1801 (*Disquisitiones Arithmeticae*) quando tinha apenas 24 anos. Várias idéias de grande importância, que serviram de base para o desenvolvimento da teoria de números, aparecem neste trabalho. Até mesmo a notação, lá introduzida, é a que utilizamos hoje.

Definição 2.1 Se a e b são inteiros dizemos que a é *congruente* a b módulo m ($m > 0$) se $m|(a-b)$. Denotamos isto por $a \equiv b \pmod{m}$. Se $m \nmid (a-b)$ dizemos que a é *incongruente* a b módulo m e denotamos $a \not\equiv b \pmod{m}$.

Exemplo 2.1 $11 \equiv 3 \pmod{2}$ pois $2|(11-3)$. Como $5 \nmid 6$ e $6 = 17 - 11$ temos que $17 \not\equiv 11 \pmod{5}$.

Proposição 2.1 *Se a e b são inteiros, temos que $a \equiv b \pmod{m}$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b \pmod{m}$, então $m|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial pois da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m|(a-b)$ isto é, $a \equiv b \pmod{m}$. □

Proposição 2.2 *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a \pmod{m}$
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$
3. Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então $a \equiv d \pmod{m}$.

Demonstração: (1) Como $m|0$, então $m|(a-a)$, o que implica $a \equiv a \pmod{m}$. (2) Se $a \equiv b \pmod{m}$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a - k_1 m$, o que implica, pela Proposição 2.1, $b \equiv a \pmod{m}$. (3) Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d \pmod{m}$. □

Esta proposição nos diz que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois acabamos de provar que ela é reflexiva, simétrica e transitiva.

Teorema 2.1 *Se a, b, c e m são inteiros tais que $a \equiv b \pmod{m}$, então*

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$

Demonstração: (1) Como $a \equiv b \pmod{m}$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \pmod{m}$. (2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ temos que $a - c \equiv b - c \pmod{m}$. (3) Como $a - b = km$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto, $ac \equiv bc \pmod{m}$. □

Teorema 2.2 *Se a, b, c, d e m são inteiros tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$

Demonstração: (1) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = km$ e $c - d = k_1 m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d \pmod{m}$. (2) Basta subtrair membro a membro $a - b = km$ e $c - d = k_1 m$ obtendo $(a-b)-(c-d) = (a-c)-(b-d) = (k - k_1)m$ o que implica $a - c \equiv b - d \pmod{m}$. (3) Multiplicamos ambos os lados de $a - b = km$ por c e ambos os lados de $c - d = k_1 m$ por b, obtendo $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$ o que implica $ac \equiv bd \pmod{m}$. □

Teorema 2.3 *Se* a, b, c *e* m *são inteiros e* $ac \equiv bc \pmod{m}$, *então* $a \equiv b \pmod{m/d}$ *onde* $d = (c, m)$.

Demonstração: De $ac \equiv bc \pmod{m}$ temos $ac - bc = c(a-b) = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a-b) = k(m/d)$. Logo $(m/d)|(c/d)(a-b)$ e, como $(m/d, c/d) = 1$, pelo Teorema 1.6, $(m/d)|(a-b)$ o que implica $a \equiv b \pmod{m/d}$. □

Definição 2.2 Se h e k são dois inteiros com $h \equiv k \pmod{m}$, dizemos que k é um *resíduo* de h módulo m.

Definição 2.3 O conjunto dos inteiros $\{r_1, r_2, \ldots, r_s\}$ é um *sistema completo de resíduos* módulo m se
(1) $r_i \not\equiv r_j \pmod{m}$ para $i \neq j$
(2) para todo inteiro n existe um r_i tal que $n \equiv r_i \pmod{m}$.

Exemplo 2.2 $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.

Exemplo 2.3 Para m ímpar o conjunto abaixo é um sistema completo de resíduos módulo m.

$$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$$

Teorema 2.4 *Se* k *inteiros* $r_1, r_2, \ldots, r_k$ *formam um sistema completo de resíduos módulo* m *então* $k = m$.

Demonstração: Primeiramente demonstramos que os inteiros $t_0, t_1, \ldots, t_{m-1}$, com $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Pelo Teorema 1.2 sabemos que, para cada n, existe um único par de inteiros q e s, tal que $n = mq + s$, $0 \leq s < m$. Logo $n \equiv s \pmod{m}$, sendo s um dos t_i. Como $|t_i - t_j| \leq m - 1$, temos que $t_i \not\equiv t_j \pmod{m}$ para $i \neq j$. Portanto, o conjunto $\{t_0, t_1, \ldots, t_{m-1}\}$ é um sistema completo de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente um dos t_i, o que nos garante $k \leq m$. Como o conjunto $\{r_1, r_2, \ldots, r_k\}$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e portanto $m \leq k$. Desta forma $k = m$. □

Teorema 2.5 *Se* $r_1, r_2, \ldots, r_m$ *é um sistema completo de resíduos módulo* m *e* a *e* b *são inteiros com* $(a, m) = 1$, *então*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração: Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1+b, ar_2+b, \ldots, ar_m+b$, são incongruentes módulo m. Para isto vamos supor que $ar_i + b \equiv ar_j + b \pmod{m}$. Logo, pelo Teorema 2.1, temos $ar_i \equiv ar_j \pmod{m}$. Mas, como $(a, m) = 1$, o Teorema 2.3 nos diz que $r_i \equiv r_j \pmod{m}$. O fato de $r_i \equiv r_j \pmod{m}$ implica $i = j$, uma vez que, $r_1, r_2, \ldots, r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração. □

Proposição 2.3 *Se* a, b, k *e* m *são inteiros com* $k > 0$ *e* $a \equiv b \pmod{m}$, *então* $a^k \equiv b^k \pmod{m}$.

Demonstração: Isto segue, imediatamente, da identidade:

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}).$$

Teorema 2.6 *Se* $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ *onde* $a, b, m_1, m_2, \ldots, m_k$ *são inteiros com* m_i *positivos,* $i = 1, 2, \ldots, k$, *então*

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$$

onde $[m_1, m_2, \ldots, m_k]$ *é o mínimo múltiplo comum de* $m_1, m_2, \ldots, m_k$.

Demonstração: Seja p_n o maior primo que aparece nas fatorações de m_1, m_2, $\ldots$, m_k. Cada m_i, $i = 1, 2, \ldots, k$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} \cdot p_2^{\alpha_{2i}} \cdots p_n^{\alpha_{ni}},$$

(alguns α_{ji} podem ser nulos).

Como $m_i|(a-b), i = 1, 2, \ldots, k$ temos que $p_j^{\alpha_{ji}}|(a-b), i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max_{1 \leq i \leq k} \{\alpha_{ji}\}$ teremos que

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} | (a-b).$$

Mas,

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k]$$

o que implica $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$. □

2.2 Congruência Linear

Chamamos de *congruência linear* em uma variável a uma congruência da forma $ax \equiv b \pmod{m}$ onde x é uma incógnita.

É fácil de se verificar que se x_0 é uma solução, i.e., $ax_0 \equiv b \pmod m$ e $x_1 \equiv x_0 \pmod m$ então x_1 também é solução. Isto é óbvio pois se $x_1 \equiv x_0 \pmod m$ então $ax_1 \equiv ax_0 \equiv b \pmod m$.

O que acabamos de verificar é que se um membro de uma classe de equivalência é solução então todo membro desta classe é solução. Destas observações surge uma questão natural: no caso de existir alguma solução, quantas soluções incongruentes existem?

Antes de respondermos a esta importante questão, necessitamos provar um teorema que nos dá informações sobre a existência de soluções para uma equação diofantina linear.

Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada *equação diofantina linear*. (o nome vem do matemático grego Diofanto).

Teorema 2.7 *Sejam a e b inteiros positivos e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k$$

onde k é um inteiro.

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d|a$ e $d|b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, pois, que $d|c$. Pelo Teorema 1.3 existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d. \tag{2.1}$$

Como $d|c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos, ambos os membros de (2.1) por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k$$

são soluções, uma vez que

$$\begin{aligned} ax + by &= a(x_0 + (b/d)k) + b(y_0 - (a/d)k) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \end{aligned}$$

$$= ax_0 + by_0 = c.$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, i.e., $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

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

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$ temos, pelo corolário da Proposição 1.4,

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{2.2}$$

Logo, pelo Teorema 1.6, $(b/d)|(x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja $x = x_0 + (b/d)k$. Substituindo-se este valor de x na equação (2.2) temos $y = y_0 - (a/d)k$, o que conclui a demonstração. □

Com este teorema à mão podemos, agora, dizer quantas são as soluções incongruentes (caso exista alguma) que a congruência linear $ax \equiv b \pmod m$ possui.

Teorema 2.8 *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \pmod m$ não possui nenhuma solução e quando $d|b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Pela Proposição 2.1 sabemos que o inteiro x é solução de $ax \equiv b \pmod m$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax - my = b$. Do teorema anterior sabemos que esta equação não possui nenhuma solução caso $d \nmid b$, e que se $d|b$ ela possui infinitas soluções dadas por $x = x_0 - (m/d)k$ e $y = y_0 - (a/d)k$ onde (x_0, y_0) é uma solução particular de $ax - my = b$. Logo a congruência $ax \equiv b \pmod m$ possui infinitas soluções dadas por $x = x_0 - \left(\frac{m}{d}\right)k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \pmod m$. Isto implica $(m/d)k_1 \equiv (m/d)k_2 \pmod m$, e como $(m/d)|m$, temos $(m/d, m) = m/d$, o que nos permite o cancelamento de m/d resultando, pelo Teorema 2.3,

$k_1 \equiv k_2 (\mathrm{mod}\ d)$. Observe que m foi substituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Definição 2.4 Dizemos que uma solução x_0 de $ax \equiv b (\mathrm{mod}\ m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Definição 2.5 Uma solução $\overline{a}$ de $ax \equiv 1 (\mathrm{mod}\ m)$ é chamada de um *inverso* de a módulo m.

Segue, agora, do Teorema 2.8 que se $(a, m) = 1$ então a possui um único inverso módulo m. A proposição seguinte nos diz quando um inteiro a é o seu próprio inverso módulo p, onde p é um número primo.

Proposição 2.4 *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 (\mathrm{mod}\ p)$ ou $a \equiv -1 (\mathrm{mod}\ p)$.*

Demonstração: Se a é o seu próprio inverso, então $a^2 \equiv 1 (\mathrm{mod}\ p)$, o que significa que $p|(a^2 - 1)$. Mas se $p|(a-1)(a+1)$, sendo p primo, $p|(a-1)$ ou $p|(a+1)$, o que implica $a \equiv 1 (\mathrm{mod}\ p)$ ou $a \equiv -1 (\mathrm{mod}\ p)$. A recíproca é imediata pois, se $a \equiv 1 (\mathrm{mod}\ p)$ ou $a \equiv -1 (\mathrm{mod}\ p)$, então $p|(a-1)$ ou $p|(a+1)$. Portanto $p|(a-1)(a+1)$ o que significa $a^2 \equiv 1 (\mathrm{mod}\ p)$, o que conclui a demonstração. □

2.3 Os Teoremas de Euler, Fermat e Wilson

Antes de demonstrarmos o Teorema de Wilson, que diz que para p primo $(p-1)! \equiv -1 (\mathrm{mod}\ p)$, fornecemos um exemplo, tomando $p = 13$, com a finalidade de apresentarmos a idéia utilizada na demonstração.

Dentre os números 1,2,3,...,12 somente os números 1 e 12 são os seus próprios inversos módulo 13. Isto segue da Proposição 2.4, pois $1 \equiv 1 (\mathrm{mod}\ 13)$ e $12 \equiv -1 (\mathrm{mod}\ 13)$ e nenhum dos números $2, 3, \ldots, 11$ é congruente a 1 ou -1 módulo 13. Mas, como os números $2, 3, 4, \ldots, 11$ são todos relativamente primos com 13, cada um deles possui, pelo Teorema 2.8, um único inverso módulo 13. Eles podem, portanto, ser agrupados em 5 pares $(5 = (13-3)/2)$ que são os seguintes:

$$\begin{aligned} 2 \times 7 &\equiv 1 (\mathrm{mod}\ 13) \\ 3 \times 9 &\equiv 1 (\mathrm{mod}\ 13) \\ 4 \times 10 &\equiv 1 (\mathrm{mod}\ 13) \\ 5 \times 8 &\equiv 1 (\mathrm{mod}\ 13) \\ 6 \times 11 &\equiv 1 (\mathrm{mod}\ 13) \end{aligned}$$

Pelo Teorema 2.2(3) podemos multiplicar estas congruências, membro a membro, obtendo

$$2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \equiv 1 (\mathrm{mod}\ 13)$$

Se multiplicarmos os dois lados por 12 teremos

$$2 \times 3 \times 4 \ldots 11 \times 12 \equiv 12 (\mathrm{mod}\ 13)$$

e, portanto, como $12 \equiv -1 (\mathrm{mod}\ 13)$ temos, finalmente, $(13-1)! \equiv -1 (\mathrm{mod}\ 13)$.

Teorema 2.9 (Teorema de Wilson) *Se p é primo, então $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.*

Primeira Demonstração: Como $(2-1)! \equiv 1 \equiv -1 (\mathrm{mod}\ 2)$ o resultado é válido para $p = 2$. Pelo Teorema 2.8, a congruência $ax \equiv 1 (\mathrm{mod}\ p)$ tem uma única solução para todo a no conjunto $\{1, 2, 3, \ldots, p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $(p-3)/2$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos, pelo Teorema 2.2 (3) $2 \times 3 \times 4 \times 5 \times \ldots (p-2) \equiv 1 (\mathrm{mod}\ p)$. Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times \ldots (p-2)(p-1) \equiv (p-1) (\mathrm{mod}\ p)$$

isto é $(p-1)! \equiv -1 (\mathrm{mod}\ p)$ uma vez que $p - 1 \equiv -1 (\mathrm{mod}\ p)$. □

Segunda Demonstração: Esta segunda demonstração foi apresentada por Stern e ilustra o uso de análise em Teoria dos Números. A primeira segue, essencialmente, Gauss.

Consideramos a expansão de Maclaurin da função

$$\ln\left(\frac{1}{1-x}\right),$$

isto é,

$$\ln \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots; \qquad -1 \leq x < 1.$$

Logo

$$e^{x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots} = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \tag{2.3}$$

O lado esquerdo desta igualdade pode ser escrito como

$$e^x e^{\frac{x^2}{2}} e^{\frac{x^3}{3}} \cdots = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots\right).$$

$$\left(1+\frac{x^2/2}{1!}+\frac{(x^2/2)^2}{2!}+\cdots\right)\cdots$$
$$\left(1+\frac{x^p/p}{1!}+\frac{(x^p/p)^2}{2!}+\cdots\right)\cdots$$
$$=1+\frac{x}{1!}+x^2\left(\frac{1}{2!}+\frac{1}{2}\right)+x^3\left(\frac{1}{3!}+\frac{1}{1!}\,\frac{1/2}{1!}+\frac{1/3}{1!}\right)+\cdots$$
$$+x^p\left(\frac{1}{p!}+\frac{1}{(p-2)!}\,\frac{1/2}{1!}+\cdots+\frac{1/p}{1!}\right)+\cdots$$

Por (2.3) sabemos que o coeficiente de x^p é igual a 1 o qual, pela expressão acima é da forma $\frac{1}{p!}+\frac{r}{s}+\frac{1}{p}$ onde r/s é a soma de um número finito de racionais que não possuem o fator p no denominador. Logo se $(r,s)=1, p\nmid s$.

Sendo $\frac{1}{p!}+\frac{r}{s}+\frac{1}{p}=1$ temos que

$$1-\frac{r}{s}=\frac{1}{p!}+\frac{1}{p}=\frac{(1+(p-1)!)}{p!}$$

e, portanto,

$$(s-r)\,(p-1)!=\frac{s(1+(p-1)!)}{p}.$$

Como $(s-r)\,(p-1)!$ é um inteiro e $p\nmid s$, então $p|(1+(p-1)!)$. □

O teorema seguinte nos diz que se um número satisfaz a relação do teorema de Wilson, ele deve ser primo.

Teorema 2.10 *Se n é um inteiro tal que $(n-1)!\equiv -1(\mathrm{mod}\ n)$, então n é primo.*

Demonstração: A prova é por contradição. Vamos supor que $(n-1)!\equiv -1(\mathrm{mod}\ n)$, isto é, $n|((n-1)!+1)$ e que n não seja primo, ou seja, $n=rs, 1<r<n$ e $1<s<n$. Nestas condições $r|(n-1)!$ e, sendo r um divisor de n, $r|(n-1)!+1$ e, portanto, r deve dividir a diferença $(n-1)!+1-(n-1)!=1$, o que é absurdo, uma vez que $r>1$. Logo, um n satisfazendo $(n-1)!\equiv -1(\mathrm{mod}\ n)$ deve ser primo. □

O próximo teorema nos diz que se p é primo e $p\nmid a$, então $p|(a^{p-1}-1)$. Vamos primeiramente provar isto num caso particular com a finalidade de ilustrar a idéia usada na demonstração.

Sejam $p=11$ e $a=5$. Logo temos:

$$\begin{aligned}
1\times 5 &\equiv 5(\mathrm{mod}\ 11)\\
2\times 5 &\equiv 10(\mathrm{mod}\ 11)\\
3\times 5 &\equiv 4(\mathrm{mod}\ 11)\\
4\times 5 &\equiv 9(\mathrm{mod}\ 11)\\
5\times 5 &\equiv 3(\mathrm{mod}\ 11)\\
6\times 5 &\equiv 8(\mathrm{mod}\ 11)\\
7\times 5 &\equiv 2(\mathrm{mod}\ 11)\\
8\times 5 &\equiv 7(\mathrm{mod}\ 11)\\
9\times 5 &\equiv 1(\mathrm{mod}\ 11)\\
10\times 5 &\equiv 6(\mathrm{mod}\ 11)
\end{aligned}$$

Observe que 11 não divide nenhum dos produtos $j\times 5, 1\le j\le 10$ que estão na coluna da esquerda nas congruências acima. Observe, também, que todos eles são incongruentes módulo 11, pois se $5j\equiv 5k(\mathrm{mod}\ 11)$, devemos ter $j\equiv k(\mathrm{mod}\ 11)$ com $1\le j\le 10$ e $1\le k\le 10$, e, portanto, $j=k$. Logo, como nenhum é congruente a zero módulo 11 e todos são incongruentes módulo 11, eles devem ser congruentes a diferentes números dentre $1,2,3,\ldots,10$. Observe que todos estes números aparecem, sem repetições, na coluna da direita nas congruências acima. Agora podemos multiplicar, membro a membro, estas congruências para obter

$$(1\times 5)(2\times 5)\cdots(10\times 5)\equiv 5\times 10\times 4\times 9\times 3\times 8\times 2\times 7\times 1\times 6(\mathrm{mod}\ 11)$$

e, portanto, $5^{10}10!\equiv 10!(\mathrm{mod}\ 11)$. Mas, como $(10!,11)=1$ temos, pelo Teorema 2.3, que

$$5^{10}\equiv 1(\mathrm{mod}\ 11),$$

o que mostra a validade do teorema neste caso particular em que $a=5$ e $p=11$. Com este exemplo em mente será fácil provar o teorema.

Teorema 2.11 (Pequeno Teorema de Fermat) *Seja p primo. Se $p\nmid a$ então $a^{p-1}\equiv 1(\mathrm{mod}\ p)$.*

Demonstração: Sabemos que o conjunto formado pelos p números $0,1,2,\ldots,p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0,1,2,\ldots,p-1\}$. Vamos, agora, considerar os números $a,2a,3a,\ldots,(p-1)a$. Como $(a,p)=1$, nenhum destes números $ia, 1\le i\le p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p.

Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak(\text{mod } p)$ implica $j \equiv k(\text{mod } p)$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)\cdots(p-1)a \equiv 1.2.3\cdots(p-1)(\text{mod } p)$$

ou seja $a^{p-1}(p-1)! \equiv (p-1)!(\text{mod } p)$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1(\text{mod } p),$$

o que conclui a demonstração. □

Corolário 2.1 *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a(\text{mod } p)$.*

Demonstração: Temos que analisar dois casos, se $p|a$ e se $p \not| a$. Se $p|a$, então $p|(a(a^{p-1}-1))$ e, portanto $a^p \equiv a(\text{mod } p)$. Se $p \not| a$, pelo Teorema 2.11 $p|(a^{p-1}-1)$ e, portanto, $p|(a^p - a)$. Logo, em ambos os casos, $a^p \equiv a(\text{mod } p)$. □

Definição 2.6 Se n é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.

Definição 2.7 Um *sistema reduzido de resíduos* módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j(\text{mod } m)$.

Exemplo 2.4 O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, portanto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. A fim de se obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.

Teorema 2.12 *Seja a um inteiro positivo tal que $(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Demonstração: Como na seqüência $ar_1, ar_2, \ldots, ar_{\phi(m)}$ temos $\phi(m)$ elementos, devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m. Como $(a, m) = 1$ e $(r_i, m) = 1$, temos (veja Problema 1.33 no final do cap. 1), $(ar_i, m) = 1$. Logo, nos resta mostrar que

$ar_i \not\equiv ar_j(\text{mod } m)$ se $i \neq j$. Mas, como $(a, m) = 1$, de $ar_i \equiv ar_j(\text{mod } m)$ temos $r_i \equiv r_j(\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$, é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □ Vamos, agora, mostrar a validade do Teorema de Euler num caso especial para ilustrar a idéia que usaremos na demonstração. Sejam $m = 8$ e $a = 5$. Sabemos que o conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. Consideremos o conjunto formado por 5×1,5×3,5×5 e 5×7. Pelo Teorema 2.12 este conjunto também constitui um sistema reduzido de resíduos módulo 8. Isto significa que cada um dos elementos 5×1, 5×3, 5×5 e 5×7 é congruente módulo 8 a exatamente um dos elementos 1,3,5 e 7. Temos, na realidade que

$$\begin{aligned} 5 \times 1 &\equiv 5(\text{mod } 8) \\ 5 \times 3 &\equiv 7(\text{mod } 8) \\ 5 \times 5 &\equiv 1(\text{mod } 8) \\ 5 \times 7 &\equiv 3(\text{mod } 8). \end{aligned}$$

Multiplicando-se, membro a membro, estas congruências obtemos

$$5^4(1 \times 3 \times 5 \times 7) \equiv (1 \times 3 \times 5 \times 7)(\text{mod } 8).$$

Como $(1 \times 3 \times 5 \times 7, 8) = 1$ podemos cancelar o fator $(1 \times 3 \times 5 \times 7)$ obtendo

$$5^4 \equiv 1(\text{mod } 8).$$

Observe que $4 = \phi(8)$, ou seja, provamos que $5^{\phi(8)} \equiv 1(\text{mod } 8)$.

Teorema 2.13 (Euler) *Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1(\text{mod } m).$$

Demonstração: No Teorema 2.12 mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $(a, m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Isto significa que ar_i é congruente a exatamente um dos, r_j $1 \leq j \leq \phi(m)$, e portanto o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1.ar_2\cdots ar_{\phi(m)} \equiv r_1.r_2.\ldots.r_{\phi(m)}(\text{mod } m)$$

ou seja

$$a^{\phi(m)}r_1.r_2\ldots r_{\phi(m)} \equiv r_1.r_2\ldots r_{\phi(m)}(\text{mod } m).$$

Como

$$(\prod_{i=1}^{\phi(m)} r_i, m) = 1$$

podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$. □

Como para p primo, $\phi(p) = p - 1$, o teorema acima é uma generalização do Teorema 2.11.

2.4 O Teorema do Resto Chinês

O nome dado ao teorema seguinte se deve ao fato de que este resultado já era conhecido, na antigüidade, pelos matemáticos chineses.

Teorema 2.14 (O Teorema do Resto Chinês) *Se* $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para* $i \neq j$ *e* c_i *inteiro, então o sistema*

$$\begin{aligned} a_1 x &\equiv c_1 (\mathrm{mod}\ m_1) \\ a_2 x &\equiv c_2 (\mathrm{mod}\ m_2) \\ a_3 x &\equiv c_3 (\mathrm{mod}\ m_3) \\ &\vdots \\ a_r x &\equiv c_r (\mathrm{mod}\ m_r) \end{aligned}$$

possui solução e a solução é única módulo m, *onde* $m = m_1 \cdot m_2 \cdots m_r$.

Demonstração: Do fato de $(a_i, m_i) = 1$, o Teorema 2.8 nos diz que $a_i x \equiv c_i (\mathrm{mod}\ m_i)$ possui uma única solução que denotamos por b_i. Se definirmos $y_i = m/m_i$ onde, $m = m_1 \cdot m_2 \cdots m_r$, teremos $(y_i, m_i) = 1$, uma vez que $(m_i, m_j) = 1$ para $i \neq j$. Novamente, o Teorema 2.8 nos garante que cada uma das congruências $y_i x \equiv 1 (\mathrm{mod}\ m_i)$ possui uma única solução que denotamos por $\overline{y}_i$. Logo, $y_i \overline{y}_i \equiv 1 (\mathrm{mod}\ m_i)$, $i = 1, 2, \ldots, r$. Afirmamos que o número x dado por

$$x = b_1 y_1 \overline{y}_1 + b_2 y_2 \overline{y}_2 + \cdots + b_r y_r \overline{y}_r$$

é uma solução simultânea para o nosso sistema de congruências. De fato

$$\begin{aligned} a_i x &= a_i b_1 y_1 \overline{y}_1 + a_i b_2 y_2 \overline{y}_2 + \cdots + a_i b_i y_i \overline{y}_i + \cdots + a_i b_r y_r \overline{y}_r \\ &\equiv a_i b_i y_i \overline{y}_i (\mathrm{mod}\ m_i) \equiv a_i b_i \equiv c_i (\mathrm{mod}\ m_i) \end{aligned}$$

uma vez que y_j é divisível por m_i para $i \neq j$, $y_i \overline{y}_i \equiv 1 (\mathrm{mod}\ m_i)$ e b_i é solução de $a_i x \equiv c_i (\mathrm{mod}\ m_i)$.

Provamos, a seguir, que esta solução é única módulo m. Se $\overline{x}$ é uma outra solução para o nosso sistema, então $a_i \overline{x} \equiv c_i \equiv a_i x (\mathrm{mod}\ m_i)$ e, sendo $(a_i, m_i) = 1$ obtemos $\overline{x} \equiv x (\mathrm{mod}\ m_i)$. Logo $m_i | (\overline{x} - x)$, $i = 1, 2, \ldots, r$. Mas, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1 . m_2 . \ \ldots . m_r .$$

Portanto, pelo Teorema 2.6, $m_1 . m_2 . \ \ldots . m_r | (\overline{x} - x)$, ou seja $\overline{x} \equiv x (\mathrm{mod}\ m)$, o que conclui a demonstração. □

Mostramos, a seguir, um teste de divisibilidade, comum, para 7, 11 e 13.

Observando que $7 \times 11 \times 13 = 1001$ e que $10^3 = 1000 \equiv -1 \ (\mathrm{mod}\ 1001)$ temos

$$\begin{aligned} (a_k a_{k-1} a_{k-2} \ldots a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0 = \\ &= (10^2 a_2 + 10 a_1 + a_0) + +10^3 (10^2 a_5 + 10 a_4 + a_3) + \\ &\quad + (10^3)^2 (10^2 a_8 + 10 a_7 + a_6) + \cdots \\ &\equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots (\mathrm{mod}\ 1001) \end{aligned}$$

Isto nos diz que um inteiro é congruente, módulo 1001, ao inteiro formado por sucessivamente, somando-se e subtraindo-se inteiros de três digitos formados por sucessivos blocos de três digitos, onde os digitos são agrupados começando-se pela direita.

Exemplo 2.5. Testar se os números 465647 e 2210000 são divisíveis por 7,11 ou 13.

Para o número 465647 temos: $647 - 465 = 182$.

Como $7 | 182, 11 \not| 182$ e $13 | 182$ concluimos que 465647 é divisível por 7 e 13 mas não por 11.

Para o número 2210000 temos: $000 - 210 + 2 = -208$.

Como $7 \not| 208, 11 \not| 208$ e $13 | 208$ concluimos que 2210000 é divisível por 13 mas não é divisível por 7 e nem por 11.

2.5 Problemas Resolvidos

Problema 2.1 Usando o Teorema de Wilson, encontrar o menor resíduo positivo de: a) $6 \times 7 \times 8 \times 9$ módulo 5 b) $8 \times 9 \times 10 \times 11 \times 12 \times 13$ módulo 7.

Solução: a) Para acharmos o menor resíduo positivo de $6 \times 7 \times 8 \times 9$, utilizamos o fato, elementar, de que $6 \equiv 1 (\mathrm{mod}\ 5), 7 \equiv 2 (\mathrm{mod}\ 5)$, $8 \equiv 3 (\mathrm{mod}\ 5)$ e $9 \equiv 4 (\mathrm{mod}\ 5)$. Logo,

$$6 \times 7 \times 8 \times 9 \equiv 1 \times 2 \times 3 \times 4 (\mathrm{mod}\ 5)$$

e, pelo Teorema de Wilson sendo $4! \equiv -1 (\mathrm{mod}\ 5)$, temos

$$6 \times 7 \times 8 \times 9 \equiv -1 \equiv 4 (\mathrm{mod}\ 5).$$

b)·O menor resíduo positivo de $8{\times}9{\times}10{\times}11{\times}12{\times}13$ módulo 7 pode ser encontrado de forma análoga, isto é,

$$8 \times 9 \times 10 \times 11 \times 12 \times 13 \equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 (\mathrm{mod}\ 7)$$

e, como $6! \equiv -1 \equiv 6 (\mathrm{mod}\ 7)$, temos que $8 \times 9 \times 10 \times 11 \times 12 \times 13 \equiv 6 (\mathrm{mod}\ 7)$.

Problema 2.2 Usando o Pequeno Teorema de Fermat , encontrar o resto da divisão de 2^{100000} por 17.

Solução: Pelo Teorema de Fermat temos $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ quando p é primo e $p \not| a$. Logo, como 17 é primo e $17 \not| 2$, temos $2^{16} \equiv 1 (\mathrm{mod}\ 17)$. Mas $100000 = 6250 \times 16$ e, portanto,

$$2^{100000} = (2^{16})^{6250} \equiv 1^{6250} \equiv 1 (\mathrm{mod}\ 17).$$

Logo, o resto da divisão por 17 de 2^{100000} é 1.

Problema 2.3 Encontrar o dígito das unidades de 3^{100} quando expresso na base 7.

Solução: Isto equivale a encontrar o menor resíduo positivo de 3^{100} módulo 7. Como 7 é primo e $7 \not| 3$, temos $3^6 \equiv 1 (\mathrm{mod}\ 7)$. Sendo $100 = 6 \times 16 + 4$, temos: $3^{96} = (3^6)^{16} \equiv (1)^{16} \equiv 1 (\mathrm{mod}\ 7)$. Agora, $3^2 = 9 \equiv 2 (\mathrm{mod}\ 7)$ e, portanto, $3^4 \equiv 4 (\mathrm{mod}\ 7)$. Assim $3^{100} = 3^{96} \times 3^4 \equiv 1 \times 4 \equiv 4 (\mathrm{mod}\ 7)$.

Problema 2.4 Mostrar que se p é um primo ímpar, então

$$2(p-3)! \equiv -1 (\mathrm{mod}\ p).$$

Solução: Sendo p primo, temos, pelo Teorema de Wilson que

$$(p-1)! \equiv -1 (\mathrm{mod}\ p)$$

mas, $(p-1)! = (p-1)(p-2)(p-3)!$ e, como $p-1 \equiv -1 (\mathrm{mod}\ p)$ e $p-2 \equiv -2 (\mathrm{mod}\ p)$ para $p \neq 2$, temos $(p-1)(p-2)(p-3)! \equiv (-1)(-2)(p-3)! \equiv 2(p-3)! \equiv -1 (\mathrm{mod}\ p)$.

Problema 2.5 Mostrar que se p e q são primos distintos, então

$$p^{q-1} + q^{p-1} \equiv 1 (\mathrm{mod}\ pq).$$

Solução: Devemos mostrar que $q|(p^{q-1} + q^{p-1} - 1)$ e que $p|(p^{q-1} + q^{p-1} - 1)$. Como $(q,p) = 1$ temos, pelo Teorema 2.11, que $q^{p-1} \equiv 1 (\mathrm{mod}\ p)$ e que $p^{q-1} \equiv 1 (\mathrm{mod}\ q)$. Logo, $p|(q^{p-1} - 1)$ e $q|(p^{q-1} - 1)$. Portanto, como $p|p^{q-1}$ e $q|q^{p-1}$, temos que $p|(p^{q-1} + q^{p-1} - 1)$ e que $q|(p^{q-1} + q^{p-1} - 1)$, o que conclui a demonstração.

Problema 2.6 Mostre que p é o menor primo que divide $(p-1)! + 1$.

Solução: Pelo Teorema de Wilson $p|((p-1)! + 1)$. Logo, como qualquer primo menor que p divide $(p-1)!$, nenhum deles pode dividir $(p-1)! + 1$ pois, neste caso, deveria dividir 1. Portanto, p é o menor primo tendo esta propriedade.

Problema 2.7 Mostrar que 2,3,5,7 e 13 são divisores de $n^{13} - n$ para todo n.

Solução: Como $n^{13} - n = n(n^{12} - 1)$ e

$$\begin{aligned} n^{12} - 1 &= (n-1)(n^{11} + n^{10} + \cdots + n + 1) \\ n^{12} - 1 &= (n^2 - 1)(n^{10} + n^8 + \cdots + n^2 + 1) \\ n^{12} - 1 &= (n^4 - 1)(n^8 + n^4 + 1) \\ n^{12} - 1 &= (n^6 - 1)(n^6 + 1) \end{aligned}$$

temos que $n, (n-1), (n^2-1), (n^4-1), (n^6-1)$ e $(n^{12}-1)$ são divisores de $n^{13} - n$. Logo, $2|(n^{13} - n)$ pois $n(n-1)$ é divisível por 2 e caso n não seja divisível por 3,5,7 e 13 teremos que

$$\begin{array}{lllll} 3|(n^{13}-n) & \text{pois} & n^2 \equiv 1 (\mathrm{mod}\ 3) & & \text{(Euler)} \\ 5|(n^{13}-n) & \text{pois} & n^4 \equiv 1 (\mathrm{mod}\ 5) & & \text{(Euler)} \\ 7|(n^{13}-n) & \text{pois} & n^6 \equiv 1 (\mathrm{mod}\ 7) & & \text{(Euler)} \\ 13|(n^{13}-n) & \text{pois} & n^{12} \equiv 1 (\mathrm{mod}\ 13) & & \text{(Euler).} \end{array}$$

Problema 2.8 *Mostre que* $13|2^{70} + 3^{70}$.

Solução: Como $2^{12} \equiv 1 (\mathrm{mod}\ 13)$, temos que $2^{60} \equiv 1 (\mathrm{mod}\ 13)$. Mas $2^5 \equiv 6 (\mathrm{mod}\ 13)$ e, portanto, $2^{10} \equiv 36 \equiv -3 (\mathrm{mod}\ 13)$. Logo, $2^{60}.2^{10} \equiv -3 (\mathrm{mod}\ 13)$. Sabemos que $3^3 \equiv 1 (\mathrm{mod}\ 13)$, donde $3^{69} \equiv 1 (\mathrm{mod}\ 13)$. Como $3 \equiv 3 (\mathrm{mod}\ 13)$ temos que $3^{70} \equiv 3 (\mathrm{mod}\ 13)$. Logo somando-se, membro a membro, $2^{70} \equiv -3 (\mathrm{mod}\ 13)$ com $3^{70} \equiv 3 (\mathrm{mod}\ 13)$ obtemos $2^{70} + 3^{70} \equiv 0 (\mathrm{mod}\ 13)$, o que conclui a demonstração.

Problema 2.9 Mostrar que os números $1^2, 2^2, 3^2, \ldots, m^2, m > 2$, não formam um sistema completo de resíduos módulo m.

Solução: Basta mostrarmos que eles não são, dois a dois, incongruentes módulo m. Para isto é suficiente tomarmos dois números n e k, $n > k$, tais que

$n + k = m$, pois, desta forma

$$n^2 - k^2 = (n + k)(n - k) = m(n - k) \equiv 0 (\mathrm{mod}\ m),$$

o que implica $n^2 \equiv k^2 (\mathrm{mod}\ m)$, o que conclui a demonstração.

Problema 2.10 *Mostrar que para qualquer sistema reduzido* $r_1, r_2, \ldots, r_{p-1}$ *de resíduos módulo* p *(*p *primo), temos*

$$\prod_{i=1}^{p-1} r_i \equiv -1 (\mathrm{mod}\ p).$$

Solução: Sabemos que os números $1, 2, 3, \ldots, p-1$ formam um sistema reduzido de resíduos módulo p, para p primo. Isto significa que eles são todos primos com p e incongruentes módulo p. Logo, qualquer número relativamente primo com p é congruente módulo p a exatamente um destes números e, se dois números, primos com p, são incongrentes módulo p, eles serão congruentes a diferentes elementos deste conjunto. Portanto os números $r_1, r_2, \ldots, r_{p-1}$ são congruentes, módulo p, a diferentes elementos dentre $1, 2, \ldots, p-1$. Se multiplicarmos, membro a membro, estas congruências, teremos

$$\prod_{i=1}^{p-1} r_i \equiv 1 \times 2 \cdots (p-1) \equiv (p-1)! (\mathrm{mod}\ p)$$

e, pelo Teorema de Wilson, o resultado segue, i.e.,

$$\prod_{i=1}^{p-1} r_i \equiv -1 (\mathrm{mod}\ p).$$

Problema 2.11 Mostrar que se p é um primo ímpar, então

$$1^2 \times 3^2 \times 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} (\mathrm{mod}\ p)$$

e

$$2^2 \times 4^2 \times 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} (\mathrm{mod}\ p).$$

Solução: Mostramos apenas a primeira congruência, pois a segunda é análoga. Sabemos, pelo Teorema de Wilson, que

$$1 \times 2 \times 3 \times 4 \cdots (p-3)(p-2)(p-1) \equiv -1 (\mathrm{mod}\ p).$$

Substituímos $2, 4, 6, \ldots, (p-1)$, respectivamente, por $-(p-2), -(p-4), \ldots, -1$, obtendo

$$(-1)^{(p-1)/2} 1(p-2)3(p-4)5(p-6) \cdots 3(p-2)1 \equiv (-1) (\mathrm{mod}\ p),$$

uma vez que, de 1 até $(p-1)$ temos $(p-1)/2$ pares. Como p é ímpar, todos os fatores acima são ímpares e cada um aparece duas vezes, logo

$$(-1)^{(p-1)/2} 1^2 \times 3^2 \times 5^2 \cdots (p-2)^2 \equiv -1 (\mathrm{mod}\ p).$$

Agora basta multiplicarmos, ambos os lados, por $(-1)^{(p-1)/2}$, o que conclui a demonstração.

Problema 2.12 Resolver o sistema de congruências abaixo:

$$\begin{aligned} x &\equiv 1 (\mathrm{mod}\ 5) \\ x &\equiv 2 (\mathrm{mod}\ 7) \\ x &\equiv 3 (\mathrm{mod}\ 11) \end{aligned}$$

Solução: Utilizando a notação introduzida no Teorema 2.14 temos:

$$m_1 = 5; m_2 = 7; m_3 = 11, m = 5 \times 7 \times 11$$
$$y_1 = m/m_1 = 7 \times 11; y_2 = m/m_2 = 5 \times 11; y_3 = m/m_3 = 5 \times 7$$

Para determinar $\overline{y}_1$ resolvemos

$$\begin{aligned} &y_1 x \equiv 1 (\mathrm{mod}\ m_1), \text{ i.e.,} \\ &7 \times 11x \equiv 1 (\mathrm{mod}\ 5), \text{ ou, equivalentemente} \\ &2x \equiv 1 (\mathrm{mod}\ 5). \text{ Logo } \overline{y}_1 = 3 \end{aligned}$$

Encontramos $\overline{y}_2$ resolvendo

$$\begin{aligned} &y_2 x \equiv 1 (\mathrm{mod}\ m_2), \text{ i.e.,} \\ &5 \times 11x \equiv 1 (\mathrm{mod}\ 7), \text{ ou, equivalentemente} \\ &6x \equiv 1 (\mathrm{mod}\ 7). \text{ Logo } \overline{y}_2 = 6 \end{aligned}$$

Resolvendo $y_3 x \equiv 1 \pmod{m_3}$ obtemos $\overline{y}_3$:

$$\begin{aligned} &5 \times 7x \equiv 1 (\mathrm{mod}\ 11), \text{ i.e.,} \\ &2x \equiv 1 (\mathrm{mod}\ 11) \end{aligned}$$

e, portanto, $\overline{y}_3 = 6$.

Como, neste caso, $b_1 = 1, b_2 = 2$ e $b_3 = 3$ temos que a solução do sistema módulo $5\times7\times11$ é dada por

$$\begin{aligned} x &\equiv b_1y_1\overline{y}_1 + b_2y_2\overline{y}_2 + b_3y_3\overline{y}_3 \\ &\equiv 1\times7\times11\times3 + 2\times5\times11\times6 + 3\times5\times7\times6 \\ &\equiv 366 \pmod{385} \end{aligned}$$

Problema 2.13 Mostrar que $\sqrt[n]{k}$ é um irracional onde k não é a n-ésima potência de um inteiro.

Solução: Vamos supor que $\sqrt[n]{k}$ seja racional, isto é, que existam inteiros a e b, com $\sqrt[n]{k} = a/b$, isto é, $a^n = kb^n$. Como k não é uma n-ésima potência de um inteiro, ele deve ter algum fator primo p cuja multiplicidade não é congruente a $0(\text{mod } n)$. Como a multiplicidade de p e de todos os outros fatores primos em b^n é congruente a $0(\text{mod } n)$ concluímos que a múltiplicidade de p em kb^n não é congruente a $0(\text{mod } n)$. Mas, como a multiplicidade de p em a^n claramente é congruente a $0(\text{mod } n)$ temos uma contradição, isto é, $kb^n \neq a^n$. Desta forma $\sqrt[n]{k}$ é racional somente quando k é uma n-ésima potência de um inteiro. □

Observe que contrário às provas de casos especiais deste resultado, como o da irracionalidade de $\sqrt{2}$, neste argumento não é necessário supor que a e b sejam relativamente primos.

2.6 Problemas Propostos

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

2. Encontrar o resto da divisão de 7^{34} por 51 e o resto da divisão de 5^{63} por 29.

3. Mostrar que se p é um ímpar e $a^2+2b^2 = 2p$, então "a"é par e "b"é ímpar.

4. Provar que para p primo $(p-1)! \equiv p-1 \pmod{1+2+3+\ldots+(p-1)}$.

5. Encontrar o máximo divisor comum de $(p-1)!-1$ e $p!$ (p primo).

6. Mostrar que para $n \geq 4$ o resto da divisão por 12 de $1!+2!+3!+\ldots+n!$ é 9.

7. Mostrar que para n inteiro $3n^2 - 1$ nunca é um quadrado.

8. Resolver as seguintes congruências.
(a) $5x \equiv 3 \pmod{24}$
(b) $3x \equiv 1 \pmod{10}$

(c) $23x \equiv 7 \pmod{19}$
(d) $7x \equiv 5 \pmod{18}$
(e) $25x \equiv 15 \pmod{120}$

9. Mostrar que $5n^3 + 7n^5 \equiv 0 \pmod{12}$ para todo inteiro n.

10. Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio com coeficientes inteiros onde $a_n > 0$ e $n \geq 1$. Mostrar que f(x) é composto para infinitos valores da variável x.

11. Mostrar que se p_1 e p_2 são primos tais que $p_2 = p_1 + 2$ e $p_1 > 3$, então $p_1 + p_2 \equiv 0 \pmod{12}$.

12. Mostrar que para a e b inteiros temos que $3|(a^2 + b^2) \Rightarrow 3|a$ e $3|b$.

13. Sejam p_1, p_2 e p_3 primos tais que $p = p_1^2 + p_2^2 + p_3^2$ é primo. Mostrar que algum dos $p_i's$ é igual a 3.

14. Mostrar que $3x^2 + 4x^2 \equiv 3 \pmod{5}$ é equivalente a $3x^2 - x^2 + 2 \equiv 0 \pmod{5}$.

15. Mostrar que $p|\binom{p^\alpha}{k}$ onde $0 < k < p^\alpha$.

16. Seja p primo e M um conjunto de p inteiros consecutivos. É possível encontrar M_1 e M_2 subconjuntos de M tais que $M_1 \cup M_2 = M, M_1 \cap M_2 = \phi, M_i \neq \phi$ de forma que

$$\prod_{i\in M_1} i = \prod_{j\in M_2} j?$$

17. Seja f(x) um polinômio com coeficientes inteiros. Mostrar que se $f(-1)$, $f(0)$ e $f(1)$ não são divisíveis por 3, então $f(n) \neq 0$ para todo inteiro n.

18. Mostrar que $3^{10} \equiv 1 \pmod{11^2}$.

19. Resolver os seguintes sistemas:

a) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 7 \end{cases}$ b) $\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 5x \equiv 7 \pmod{11} \end{cases}$ c) $\begin{cases} x \equiv 7 \pmod{11} \\ 3x \equiv 5 \pmod{13} \\ 7x \equiv 4 \pmod 5 \end{cases}$

20. Encontrar todas as soluções de cada uma das seguintes congruências lineares. (a) $5x \equiv 3 \pmod 7$
(b) $13x \equiv 14 \pmod{29}$
(c) $15x \equiv 9 \pmod{25}$
(d) $37x \equiv 16 \pmod{19}$
(e) $5x \equiv 20 \pmod{15}$

21. Mostrar que $a^7 \equiv a \pmod{21}$ para todo inteiro a.

22. Mostrar que para a e b inteiros, com $(a, b) = 1$ temos:

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

23. Provar ou dar contra-exemplo: "Se a e m são inteiros $(a, m) = 1$, então

$$m|(1 + a + a^2 + \ldots + a^{\phi(m)-1})".$$

24. Mostrar que se p e q são primos, $p \geq q \geq 5$, então $p^2 - q^2 \equiv 0 \pmod{24}$.

25. Encontrar um sistema completo de resíduos módulo 11 formado somente por múltiplos de 6.

26. Encontrar um sistema completo de resíduos módulo 7 onde todos os elementos são números primos.

27. Dado um primo p é sempre possível encontrar um sistema completo de resíduos módulo p formado só por primos? Justificar.

28. Provar que, para todo número composto $n, n \neq 4$, a congruência $(n-1)! \equiv 0 \pmod{n}$ é verdadeira.

Capítulo 3

Teoria Combinatória dos Números

3.1 Princípio da Casa dos Pombos

Embora este tópico apareça, com mais freqüência, em livros de Combinatória, ele não deixa de ser parte da Teoria dos Números. Mesmo em se tratando de algo simples, esta idéia auxilia na demonstração de muitos resultados não-triviais, como os problemas abaixo poderão mostrar.

O *Princípio da Casa dos Pombos* nos diz que para colocarmos $n+1$ pombos em n gaiolas, pelo menos uma gaiola deverá conter pelo menos dois pombos. Esta idéia tão óbvia é, na realidade, uma poderosa ferramenta na demonstração de muitos resultados bastante difíceis. O que, muitas vezes, torna o problema difícil é a construção de um conjunto ou conjuntos aos quais se possa aplicar este princípio.

Este princípio é também conhecido como "Princípio das Gavetas de Dirichlet" por ter sido por ele enunciado como: "Se $n + 1$ objetos são colocados em n gavetas, então pelo menos uma gaveta deverá conter, pelo menos, dois objetos".

Nos exemplos apresentados a seguir, utilizamos, várias vezes, resultados do Capítulo 2 sobre congruências.

Exemplo 3.1. Mostrar que, numa festa de aniversário com mais de 12 crianças, existem pelo menos duas nascidas no mesmo mês e que também existem pelo menos duas nascidas no mesmo dia da semana.

Como temos mais crianças (pombos) do que meses (gaiolas), pelo menos um "mês"deverá conter pelo menos duas "crianças". Na segunda parte, sendo o número de crianças maior do que 7, necessariamente duas ou mais terão nascido no mesmo dia da semana.

Exemplo 3.2. Mostrar que todo subconjunto de $\{1, 2, 3, \ldots, 2n\}$, contendo $n+1$ elementos, possui um par de elementos primos entre si.