Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 6

Congruências I

Definição 1. *Dizemos que os inteiros a e b são congrentes módulo m se eles deixam o mesmo resto quando divididos por m. Denotaremos isso por $a \equiv b \pmod{m}$.*

Por exemplo, $7 \equiv 2 \pmod{5}$, $9 \equiv 3 \pmod{6}$, $37 \equiv 7 \pmod{10}$ mas $5 \not\equiv 3 \pmod{4}$. Veja que $a \equiv b \pmod{m}$ se, e somente se, $m \mid a - b$.

Teorema 2. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

i) $a + c \equiv b + d \pmod{m}$

ii) $a - c \equiv b - d \pmod{m}$

iii) $ka \equiv kb \pmod{m}\ \forall k \in \mathbb{Z}$

iv) $ac \equiv bd \pmod{m}$

v) $a^k \equiv b^k \pmod{m}\ \forall k \in \mathbb{N}$

vi) *Se* $mdc(k, m) = d$, *então* $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{m/d}$

Demonstração. Sejam q_1 e q_2 tais que:

$$\begin{aligned} a - b &= q_1 m \\ c - d &= q_2 m \end{aligned}$$

Então, $(a + c) - (b + d) = (q_1 + q_2)m$. Logo, $a + c$ e $b + d$ deixam o mesmo resto por m e consequentemente $a + c \equiv b + d \pmod{m}$. Usando que $a - b \pmod{a})^k - b^k$ e que $m \mid a - b$, concluímos que $m \pmod{a})^k - b^k$. Os demais itens serão deixados para o leitor.

Em termos práticos, podemos realizar quase todas as operações elementares envolvendo igualdade de inteiros. Uma das diferenças cruciais é a operação de divisão como mostra o último item do teorema anterior.

Exemplo 3. *Calcule o resto de 4^{100} por 3.*

Como $4 \equiv 1 \pmod 3$, temos $4^{100} \equiv 1^{100} = 1 \pmod 3$.

Exemplo 4. *Calcule o resto de 4^{100} por 5.*

Como $4 \equiv -1 \pmod 5$, temos $4^{100} \equiv (-1)^{100} = 1 \pmod 5$.

Exemplo 5. *Calcule o resto de 4^{100} por 7.*

Você deve ter percebido que encontrar relações do tipo $a \equiv \pm 1 \pmod m$ podem simplificar bastante o cálculo de $a^k \pmod m$. Procuremos alguma relação como essa para 4 e 7. Veja que:

$$4^0 \equiv 1 \pmod 7, 4^1 \equiv 4 \pmod 7, 4^2 \equiv 2 \pmod 7, 4^3 \equiv 1 \pmod 7.$$

Assim,

$$4^{99} = (4^3)^{33} \equiv 1^{33} = 1 \pmod 7.$$

Como $4^3 \equiv 1 \pmod 7$, os restos das potências de 4 na divisão por 7 se repetem periodicamente de 3 em 3 pois $4^{3k+r} \equiv 4^{3k} \cdot 4^r \equiv 4^r \pmod 7$.

Exemplo 6. *Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?*

Inicialmente devemos perceber que existe uma relação entre os números do problema: $36 + 41 = 77$. Assim:

$$\begin{aligned} -36 &\equiv 41 \pmod{77}, \\ (-36)^{41} &\equiv 41^{41} \pmod{77}, \\ 36^{36}(1 - 36^5) &\equiv 36^{36} + 41^{41} \pmod{77}. \end{aligned}$$

Nosso próximo passo é encontrar o resto de 36^5 na divisão por 77. Como $36 \equiv 1 \pmod 7$, $36^5 \equiv 1 \pmod 7$. Além disso, $36 \equiv 3 \pmod 1$1 produzindo $36^5 \equiv 3^5 \equiv 1 \pmod 1$1. Como $mdc(7, 11) = 1$ e ambos dividem $36^5 - 1$, podemos concluir que $77 \mid 36^5 - 1$. Logo, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77.

Exemplo 7. *Prove que $p^2 - 1$ é divisível por 24 se p é um primo maior que 3.*

Se p é um primo maior que 3, $p \equiv \pm 1 \pmod 3$ e $p \equiv 1 \pmod 2$. Daí, $p^2 \equiv 1 \pmod 3$. Além disso, se $p = 2k + 1$, segue que $p^2 = 4k(k+1) + 1 \equiv 1 \pmod 8$ pois $k(k+1)$ é par. Como $mdc(8, 3) = 1$ e ambos dividem $p^2 - 1$, segue que $24 \mid p^2 - 1$.

Exemplo 8. *(OCM-2001) Achar o menor natural n tal que 2001 é a soma dos quadrados de n inteiros*

Podemos concluir da solução do problema anterior que todo todo inteiro ímpar ao quadrado deixa resto 1 por 8. Usemos isso para estimar o valor de n. Sejam $x_1, x_2, \ldots, x_n$ inteiros ímpares tais que:

$$x_1^2 + x_2^2 + \ldots x_n^2 = 2001.$$

Analisando a congruência módulo 8, obtemos:

$$\begin{aligned} x_1^2 + x_2^2 + \dots x_n^2 &= 2001 \pmod 8 \\ 1 + 1 + \dots + 1 &\equiv 1 \pmod 8 \\ n &\equiv 1 \pmod 8 \end{aligned}$$

Como 2001 não é quadrado perfeito, não podemos ter $n = 1$. O próximo candidado para n seria $1 + 8 = 9$. Se exibirmos um exemplo para $n = 9$, teremos achado o valor mínimo. Veja que:

$$2001 = 43^2 + 11^2 + 5^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2.$$

Exemplo 9. *(IMO) Seja $s(n)$ a soma dos dígitos de n. Se $N = 4444^{4444}$, $A = s(N)$ e $B = s(A)$. Quanto vale $s(B)$?*

Pelo critério de divisibilidade por 9, $N \equiv A \equiv B \pmod 9$. Inicialmente calculemos o resto de N por 9. Como $4444 \equiv 16 \equiv 7 \pmod 9$, precisamos encontrar $7^{4444} \pmod 9$. Seguindo os métodos dos primeiros exemplos, seria interessante encontrarmos um inteiro r tal que $7^r \equiv \pm 1 \pmod 9$. O menor inteiro positivo com essa propriedade é $r = 3$. Como $4444 = 1481 \cdot 3 + 1$, temos:

$$7^{4444} \equiv 7^{1481 \cdot 3 + 1} \equiv (7^3)^{1481} \cdot 7 \equiv 7 \pmod 9.$$

Nosso próximo passo é estimar o valor de $s(B)$. Como $N = 4444^{4444} < 10^{5 \cdot 4444}$, $A = s(N) \leq 5 \cdot 4444 \cdot 9 = 199980$. Além disso, $B = s(A) \leq 1 + 9 \cdot 5 = 46$ e $s(B) \leq 12$. O único inteiro menor ou igual a 12 com resto 7 por 9 é o próprio 7, daí $s(B) = 7$.

Exemplo 10. *Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer natural n.*

Duas relações que podemos extrair dos números envolvidos são: $144 - 11 = 133$ e $133 - 12 = 121$. Assim:

$$\begin{aligned} 144 &\equiv 11 \pmod{133}, \\ 12^2 &\equiv 11 \pmod{133}, \\ 12^{2n} &\equiv 11^n \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot 12 \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot (-121) + 133 \cdot 11^n \pmod{133}, \\ 12^{2n+1} &\equiv -11^{n+2} \pmod{133}. \end{aligned}$$

Exemplo 11. *Prove que $n^5 + 4n$ é divisível por 5 para todo inteiro n*

Inicialmente note que $n^5 + 4n = n(n^4 + 4)$. Se $n \equiv 0 \pmod 5$, não há o que fazer. Se $n \equiv \pm 1 \pmod 5$, $n^4 + 4 \equiv 1 + 4 = 0 \pmod 5$. Finalmente, se $n \equiv \pm 2 \pmod 5$, $n^2 \equiv 4 \equiv -1 \pmod 5$ e consequentemente $n^4 + 4 \equiv 1 + 4 = 0 \pmod 5$.

Exemplo 12. *Seja $n > 6$ um inteiro positivo tal que $n - 1$ e $n + 1$ são primos. Mostre que $n^2(n^2 + 16)$ é divisível por 720. A recíproca é verdadeira?*

Veja que n é da forma $6k$, pois $n-1$ e $n+1$ são primos maiores que 3, portanto da forma $6k-1$ e $6k+1$, respectivamente. Logo,

$$n^2(n^2+16) = 144(9k^4+4k^2).$$

Resta provar que $9k^4+4k^2$ é um múltiplo de 5. Vamos analisar a igualdade acima módulo 5.

i) Se $k \equiv 0, 2$ ou $3 \pmod 5$, temos $9k^4+4k^2 \equiv 0 \pmod 5$;

ii) Se $k \equiv 1 \pmod 5 \Rightarrow n \equiv 1 \pmod 5$, temos $n-1 \equiv 0 \pmod 5$, um absurdo;

iii) Se $k \equiv 4 \pmod 5 \Rightarrow n \equiv 4 \pmod 5$, temos $n+1 \equiv 0 \pmod 5$, novamente um absurdo.

Isso conclui a demonstração. A recíproca não é verdadeira. Basta tomar, por exemplo, $n = 90$.

Problemas Propostos

Problema 13. *Determine o resto de* $2^{20}-1$ *na divisão por 41.*

Problema 14. *Qual o resto de* $1^{2000}+2^{2000}+\ldots+2000^{2000}$ *na divisão por 7?*

Problema 15. *Qual o resto na divisão de* $2^{70}+3^{70}$ *por 13?*

Problema 16. *Qual o resto de* 3^{200} *por* 100*?*

Problema 17. *(Estônia 2000) Determine todos os possíveis restos da divisão do quadrado de um número primo com o 120 por 120.*

Problema 18. *Qual o último dígito de* 777^{777}*?*

Exemplo 19. *Prove que* $2222^{5555}+5555^{2222}$ *é divisível por 7.*

Problema 20. *Prove que o número* n^3+2n *é divisível por 3 para todo natural* n*.*

Problema 21. *Prove que* n^2+1 *não é divisível por 3 para nenhum* n *inteiro.*

Problema 22. *Prove que* n^3+2 *não é divisível por 9 para nenhum* n *inteiro.*

Problema 23. *Prove que* p^2-q^2 *é divisível por 24 se* p *e* q *são primos maiores que 3.*

Problema 24. *Prove que se* $2n+1$ *e* $3n+1$ *são ambos quadrados perfeitos, então* n *é divisível por 40.*

Problema 25. *Se* n *é ímpar, prove que* $7|2^{2n+1}+3^{n+2}$*.*

Problema 26. *Seja* $d(n)$ *a soma dos dígitos de* n*. Suponha que* $n+d(n)+d(d(n)) = 1995$*. Quais os possíveis restos da divisão de* n *por* 9*?*

Problema 27. *Prove que não existem inteiros positivos* $x_1, x_2, \ldots, x_{14}$ *tais que:*

$$x_1^4+x_2^4+\ldots+x_{14}^4 = 1599.$$

Problema 28. *Escreva uma única congruência que é equivalente ao par de congruências* $x \equiv 1 \pmod 4$ *e* $x \equiv 2 \pmod 3$.

Problema 29. *Prove que* $20^{15} - 1$ *é divisível por* $11 \cdot 31 \cdot 61$

Problema 30. *(Alemanha 1997) Determine todos os primos* p *para os quais o sistema*

$$p + 1 = 2x^2$$
$$p^2 + 1 = 2y^2$$

tem uma solução nos inteiros x, y.

Problema 31. *Mostre que se* n *divide um número de Fibonacci então ele dividirá uma infinidade.*

Dicas e Soluções

13. Veja que

$$\begin{aligned} 2^5 = 32 &\equiv -9 \pmod{41} \Rightarrow \\ 2^{10} \equiv 81 &\equiv -1 \pmod{42} \Rightarrow \\ 2^{20} &\equiv 1 \pmod{41}. \end{aligned}$$

Assim, o resto procurado é zero.

14. Como $i^{2000} \equiv (i + 7k)^{2000} \pmod 7$, podemos simplificar o problema calculando primeiramente o valor de:

$$1^{2000} + 2^{2000} + 3^{2000} + 4^{2000} + 5^{2000} + 6^{2000} + 7^{2000} \pmod 7.$$

Outra observação importante que simplificará o cálculo é perceber que $2^3 \equiv 1 \pmod 7$. Assim,

$$2^{3k} \equiv 1 \pmod 7, 2^{3k+1} \equiv 2 \pmod 7, \text{ e } 2^{3k+2} \equiv 4 \pmod 7.$$

Usando isso e o fato de que 2000 é par, temos:

$$\begin{aligned} 1^{2000} + 2^{2000} + 3^{2000} + 4^{2000} + 5^{2000} + 6^{2000} + 7^{2000} &\equiv \\ 1^{2000} + 2^{2000} + (-4)^{2000} + 4^{2000} + (-2)^{2000} + (-1)^{2000} + 0^{2000} &\equiv \\ &\equiv 1 + 4 + 2 + 2 + 4 + 1 + 0 \\ &\equiv 0 \pmod 7. \end{aligned}$$

Dentre os primeiros 2000 naturais consecutivos, podemos formar 285 grupos de 7 números consecutivos cuja soma é múltipla de 7, em virtude da soma anterior. Os cinco números restantes possuem como resto na divisão por 7 o número:

$$\begin{aligned} 1996^{2000} + 1997^{2000} + 1998^{2000} + 1999^{2000} + 2000^{2000} &\equiv 1 + 4 + 2 + 2 + 4 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Assim, o resto da soma na divisão por 7 é 6.

15. Inicialmente é interessante buscarmos alguma relação entre os números envolvidos no problema. Como $13 = 4 + 9$, podemos escrever:

$$\begin{aligned} 9 &\equiv -4 \pmod{13} \Rightarrow \\ 9^{35} &\equiv (-4)^{35} \pmod{13} \Rightarrow \\ 3^{70} + 2^{70} &\equiv 0 \pmod{13}. \end{aligned}$$

17. Use a fatoração $120 = 3 \cdot 5 \cdot 2^3$ e analise a congruência módulo 3, 5 e 8 separadamente.

18. Se n não é múltiplo de 3, sabemos que $n^2 \equiv 1 \pmod 3$. Assim $n^2 + 2 \equiv 0 \pmod 3$. Se n é múltiplo de 3, $n \equiv 0 \pmod 3$. Em qualquer caso, $n(n^2 + 2) \equiv 0 \pmod 3$.

19. Basta repetir a análise do problema anterior

20. Podemos montar uma tabela de congruências na divisão por 9:

n	0	1	2	3	4	5	6	7	8
n^3	0	1	8	0	1	8	0	1	8

Como nenhum cubo perfeito diexa resto 7 na divisão por 9, $n^3 + 2 \not\equiv 0 \pmod 9$.

23. Proceda como no exemplo 7.

25.

$$\begin{aligned} 2^{2n+1} + 3^{n+2} &\equiv 4^n \cdot 2 + 3^n \cdot 9 \\ &\equiv (-3)^n \cdot 2 + 3^n \cdot 2 \\ &\equiv 0 \pmod 7. \end{aligned}$$

26. Seja r o resto na divisão por 9 de n. Pelo critério de divisibilidade por 9, temos:

$$n + d(n) + d(d(n)) \equiv 3r \equiv 1995 \pmod 9.$$

Assim, $r \equiv 2 \pmod 3$ (Pela propriedade *vi* do teorema 2). Além disso,

$$\begin{aligned} n &\leq 1995 \Rightarrow \\ d(n) &\leq 27 = d(1989) \Rightarrow \\ d(d(n)) &\leq 10 = d(19). \end{aligned}$$

Consequentemente, $n \geq 1995 - d(n) - d(d(n)) \geq 1958$. Basta procurarmos nos conjunto $\{1958, 1959, \ldots, 1995\}$ os inteiros que deixam resto 2 por 3 e que satisfazem a equação do problema. Nesse conjunto, apena o inteiro 1967 cumpre essas condições.

27. Estudando a congruência módulo 16, podemos mostrar que $x^4 \equiv 0$ ou $1 \pmod 16$. Assim, a soma

$$x_1^4 + x_2^4 + \ldots + x_{14}^4$$

é congruente a um dos números do conjunto $\{0, 1, \ldots, 14\}$ m odulo 16 enquanto que $1599 \equiv 15 \pmod{16}$. Um absurdo.

28. $x \equiv 5 \pmod{12}$.

30. Suponha sem perda de generalidade que $x, y \geq 0$. Como $p+1$ é par, $p \neq 2$. Além disso,
$$2x^2 \equiv 1 \equiv 2y^2 \pmod{p}$$
e consequentente, usando que p é ímpar, $x \equiv \pm y \pmod{p}$. Como $x < y < p$, temos
$$p^2 + 1 = 2(p-x)^2 = 2p^2 - 4px + p + 1,$$
de modo que $p = 4x - 1, 2x^2 = 4x$. Podemos concluir que x é 0 ou 2 e que a única possibilidade para p é $p = 7$.

31. Em virtude da fórmula recursiva da sequência de Fibonacci, é possível mostrarmos que os restos de seus termos na divisão por qualquer número formam uma sequência periódica.

Referências

[1] E. Carneiro, O. Campos and F. Paiva, Olimpíadas Cearenses de Matemática 1981-2005 (Níveis Júnior e Senior), Ed. Realce, 2005.

[2] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[3] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[4] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.

Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 6

Congruências II

Na aula de hoje, aprenderemos um dos teoremas mais importantes do curso: o "pequeno"teorema de Fermat. Começaremos relembrando um resultado da aula passada:

Lema 1. *Se* $ka \equiv kb \pmod{m}$ *e* $mdc(m, k) = 1$*, então* $a \equiv b \pmod{m}$*.*

Demonstração. Como $m \mid k(a - b)$ e $mdc(m, k) = 1$, segue que $m \mid a - b$.

Teorema 2. *(Teorema de Fermat) Seja* p *um primo. Se* p *não divide* a *então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Além disso, para todo inteiro a*,* $a^p \equiv a \pmod{p}$

Demonstração. Considere o conjunto de inteiros $B = \{a, 2a, 3a, \ldots, (p-1)a\}$ onde a é um inteiro satisfazendo $mdc(a, p) = 1$. Nenhum deles é divisível por p e quaisquer dois deles são incongruentes módulo p, em virtude do lema anterior. Assim, o conjunto dos restos dos elementos de B coincide com o conjunto dos restos não nulos na divisão por p, a saber, $\{1, 2, 3, \ldots, p-1\}$. Portanto,

$$\begin{aligned} a \cdot 2a \cdot 3a \ldots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots (p-1) \pmod{p}, \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p}. \end{aligned}$$

Podemos cancelar o termo $(p-1)!$ em ambos os lados pois $mdc((p-1)!, p) = 1$, concluindo assim a demonstração do teorema.

Exemplo 3. *Prove que* $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15}$ *é um inteiro para todo inteiro* n*.*

Primeiramente note que $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15} = \dfrac{3n^5 + 5n^3 + 7n}{15}$. Como $mdc(3, 5) = 1$, basta mostrarmos que o numerador é mútiplo de 3 e 5. Pelo teorema de Fermat:

$$\begin{aligned} 3n^5 + 5n^3 + 7n &\equiv 5n^3 + 7n \equiv 5n + 7n = 12n \equiv 0 \pmod{3}, \\ 3n^5 + 5n^3 + 7n &\equiv 3n^5 + 7n \equiv 3n + 7n = 10n \equiv 0 \pmod{5}. \end{aligned}$$

Problema 4. *Mostre que* $n^7 \equiv n \pmod{42}, \forall n \in \mathbb{N}$

Pelo teorema de Fermat,

$$\begin{aligned}
n^7 &\equiv n \pmod{7}\\
n^7 &\equiv (n^3)^2 \cdot n \equiv n^2 \cdot n = n^3 \equiv n \pmod{3}\\
n^7 &\equiv (n^2)^3 \cdot n \equiv n^3 \cdot n = (n^2)^2 \equiv n^2 \equiv n \pmod{2}
\end{aligned}$$

Como $2, 3$ e 7 são primos entre si, $n^7 \equiv n \pmod{2 \cdot 3 \cdot 7 = 42}$.

Exemplo 5. *(Bulgária 95) Encontre o número de inteiros* $n > 1$ *para os quais o número* $a^{25} - a$ *é divisível por* n *para cada inteiro* a.

Se n satisfaz o enunciado, p^2(p primo) não pode dividí-lo, pois $p^{25} - p$ não é divisível por p^2. Assim, n é múltiplo de primos diferentes. Os fatores primos de n são fatores de $2^{25} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. Entretanto, n não é divisível por 17 e 241 pois $3^{25} \equiv -3 \pmod{17}$ e $3^{25} \equiv 32 \pmod{241}$. Seguindo o exemplo anterior, podemos usar o teorema de Fermat para mostrar que $a^{25} \equiv a \pmod{p}$ para $p \in \{2, 3, 5, 7, 13\}$. Portanto, n deve ser igual a um dos divisores de $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ diferente de 1. A quantidade de tais divisores é $2^5 - 1 = 31$.

Exemplo 6. *Prove que para cada primo* p*, a diferença*

$$111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99 - 123456789$$

(onde cada digito está escrito exatamente p *vezes) é múltiplo de* p.

Uma boa maneira de associar os números do problema com o teorema de Fermat é perceber que:

$$\underbrace{111\ldots11}_{p\ uns} = \frac{10^p - 1}{9}.$$

Assim, podemos escrever o número $S = 111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99$ como:

$$\begin{aligned}
S &= \frac{10^p - 1}{9} \cdot 10^{8p} + 2 \cdot \frac{10^p - 1}{9} \cdot 10^{7p} + \ldots 9 \cdot \frac{10^p - 1}{9}\\
9S &= (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + \ldots 9 \cdot (10^p - 1)
\end{aligned}$$

Para $p = 2$ ou $p = 3$, o resultado do enunciado segue dos critérios de divisibilidade por 2 e 3. Podemos então nos concentrar no caso $p > 3$. Nesse caso, é suficiente mostrarmos que $9(S - 123456789)$ é divisível por p pois $mdc(p, 9) = 1$. Pelo teorema de Fermat:

$$\begin{aligned}
9S &= (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + \ldots 9 \cdot (10^p - 1)\\
&\equiv (10 - 1) \cdot 10^8 + 2 \cdot (10 - 1) \cdot 10^7 + \ldots 9 + \cdot (10 - 1) \pmod{p}\\
&\equiv 9 \cdot 123456789 \pmod{p}.
\end{aligned}$$

Exemplo 7. *Dado um primo p, prove que existem infinitos naturais n tais que p divide $2^n - n$.*

Se $p = 2$, n pode ser qualquer número par. Suponha que $p > 2$. Considere $(p-1)^{2k}$, pelo teorema de Fermat temos:

$$2^{(p-1)^{2k}} \equiv (2^{p-1})^{(p-1)^{2k-1}} \equiv 1^{(p-1)^{2k-1}} = 1 \equiv (p-1)^{2k} \pmod p.$$

Assim, para qualquer k, $n = (p-1)^{2k}$ satisfaz o problema.

Lema 8. *Se $mdc(a, m) = 1$ então existe um inteiro x tal que*

$$ax \equiv 1 \pmod m.$$

Tal x é único módulo m. Se $mdc(a, m) > 1$ então não existe tal x.

Demonstração. Pelo teorema de Bachet-Bézout, existem inteiros x e y tais que $ax+my = 1$. Analisando essa congruência módulo m, obtemos $ax \equiv 1 \pmod m$. Se y é outro inteiro que satisfaz a congruência, temos $ax \equiv ay \pmod m$. Pelo primeiro lema, $x \equiv y \pmod m$. Se $d = mdc(a, m) > 1$, não podemos ter $d \mid m$ e $m \mid ax - 1$ pois $d \nmid ax - 1$.

Teorema 9. *(Teorema de Wilson) Se p é primo, então*

$$(p-1)! \equiv -1 \pmod p$$

Demonstração. Em virtude do lema anterior, para cada $a \in \{2, 3, \dots, p-2\}$, existe um resto $x \in \{0, 1, 2, \dots, p-1\}$ tal que $ax \equiv 1 \pmod p$. Se $x = 1$ ou $x = p-1$, teríamos $a = 1$ ou $p-1$. Além disso, não podemos ter $a = x$ pois os únicos restos que satisfazem $a^2 \equiv 1 \pmod p$ são 1 e $p-1$ (Veja o problema 20). Com isso, podemos agrupar os números de $\{2, 3, \dots, p-2\}$ em pares onde o produto deixa resto 1 por p, o que nos permite concluir que o produto de todos eles também deixa resto 1 por p. Logo,

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod p.$$

Exemplo 10. *(Estônia 2000) Prove que não é possível dividir qualquer conjunto de 18 inteiros consecutivos em dois conjuntos disjuntos A e B tais que o produtos dos elementos de A seja igual ao produto dos elementos de B.*

Suponha, por absurdo, que existam tais conjuntos. Considere o primo $p = 19$. Como o produtos dos elementos de A é igual ao produtos dos elementos de B, se um dos conjuntos contém um múltiplo de 19, o outro necessariamente também conterá. Como entre 18 inteiros consecutivos não existem dois múltiplos de 19, nenhum dos conjuntos do problema contém tais números. Seja x o resto na divisão por 19 dos produtos dos elementos de A. Calculemos então o resto na divisão por 19 do produto de todos os 18 inteiros consecutivos:

$$\begin{aligned} x \cdot x &\equiv n(n+1)(n+2)(n+3)\dots(n+17) \\ &\equiv 1 \cdot 2 \cdot 3 \dots \cdot 18 \\ &\equiv -1 \pmod{19} \text{(Pelo teorema de Wilson)}. \end{aligned}$$

Como $x^2 \equiv -1 \pmod{19}$, $x^{18} \equiv (-1)^9 \equiv 1$ (mod 1)9. Isso contraria o teorema de Fermat e obtemos um absurdo.

Definição 11. *Um conjunto S é chamado de sistema completo de resíduos módulo n, denotado abreviadamente por* **scr**, *se para cada $0 \leq i \leq n-1$, existe um elemento de $s \in S$ tal que $i \equiv s \pmod{n}$. Para qualquer a, o conjunto $\{a, a+1, a+2, \ldots, a+(n-1)\}$ é um exemplo de* **scr**.

Exemplo 12. *Se $mdc(m, s) = 1$, mostre que $\{t, t+s, t+2s, \ldots t+(m-1)s\}$ é um* **scr**.

Pelo primeiro lema, se $t + is \equiv t + js \pmod{m}$, temos $is \equiv js \pmod{m}$ e $i \equiv j \pmod{m}$. Como $i, j \in \{0, 1, \ldots, m-1\}$, $i = j$. Isso nos diz que temos m inteiros que deixam restos distintos na divisão por m. Como existem exatamente m restos na divisão por m, o conjunto é um **scr**.

Exemplo 13. *Seja m um inteiro positivo par. Suponha que $\{a_1, a_1, \ldots, a_m\}$ e $\{b_1, b_2, \ldots, b_m\}$ são dois sistemas completos de resíduso módulo m. Prove que*

$$S = \{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

não é um sistema completo de resíduos.

Suponha que S seja um **scr**, então:

$$\begin{aligned}
1 + 2 + \ldots + m &\equiv (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n) \pmod{m} \\
&\equiv (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n) \\
&\equiv 2(1 + 2 + \ldots + n) \\
&\equiv 2(1 + 2 + \ldots + m)
\end{aligned}$$

Isso implica que $m \mid \dfrac{m(m+1)}{2}$, ou seja, $\dfrac{m+1}{2}$ é inteiro. Um absurdo pois m é par.

Exemplo 14. *(Polônia 1997) Prove que a sequência a_n definida por $a_1 = 1$ e*

$$a_n = a_{n-1} + a_{\left\lfloor \frac{n}{2} \right\rfloor}$$

contém infinitos termos divisíveis por 7.

Uma maneira natural para mostrarmos que existem infinitos inteiros múltiplos de 7 na sequência é verificar que o aparecimento de um múltiplo de 7 acarreta o aparecimento de outro múltiplo na sequência com um índice maior. Suponha que a_k é múltiplo de 7. Seja $a_{2k-1} = s$. Então:

$$\begin{aligned}
a_{2k-1} &= s \\
a_{2k} &= s + a_k \equiv s \pmod{7} \\
a_{2k+1} &= a_{2k} + a_k \equiv s \pmod{7}
\end{aligned}$$

Ou seja, o aparecimento de um inteiro múltiplo de 7 implica no aparecimento de 3 inteiros com o mesmo resto por 7. Exploremos essa ideia mais uma vez.

$$\begin{aligned}
a_{4k-3} &= t \\
a_{4k-2} &\equiv t + a_{2k-1} \equiv t + s \pmod 7 \\
a_{4k-1} &\equiv t + s + a_{2k-1} \equiv t + 2s \pmod 7 \\
a_{4k} &\equiv t + 2s + a_{2k} \equiv t + 3s \pmod 7 \\
a_{4k+1} &\equiv t + 3s + a_{2k} \equiv t + 4s \pmod 7 \\
a_{4k+2} &\equiv t + 4s + a_{2k+1} \equiv t + 5s \pmod 7 \\
a_{4k+3} &\equiv t + 5s + a_{2k+2} \equiv t + 6s \pmod 7
\end{aligned}$$

Se s é múltiplo de 7, já teremos conseguido outro múltiplo de 7 na sequência. Em caso contrário, o conjunto $\{t, t+s, t+2s, \ldots, t+6s\}$ é um **scr** e conterá um múltiplo de 7.

Exemplo 15. *Sejam x, y inteiros. Prove que $3x^2 + 4y^2$ e $4x^2 + 3y^2$ não podem ser ambos quadrados perfeitos.*

Comecemos com um lema bastante útil:

Lema 16. *Seja p um número primo da forma $4k + 3$. Então*

$$p \mid m^2 + n^2 \iff p \mid m \quad e \quad p \mid n.$$

Façamos inicialmente a primeira implicação. Se $p \nmid m$, então $m^{p-1} \equiv 1 \pmod p$, e daí temos as equivalências módulo p

$$\begin{aligned}
& n^2 &\equiv& -m^2 \\
\Rightarrow \quad & (nm^{p-2})^2 &\equiv& -(m^{p-1})^2 \\
& &\equiv& -1 \\
\Rightarrow \quad & (nm^{p-2})^{p-1} &\equiv& (-1)^{\frac{p-1}{2}} \\
& &\equiv& (-1)^{2k+1} \\
& &\equiv& -1,
\end{aligned}$$

o que contraria o teorema de Fermat. Assim, $p \mid m$ e $p \mid n$.

A recíproca é óbvia. Voltando ao problema, suponha que existam w, z inteiros positivos tais que

$$\begin{aligned}
3x^2 + 4y^2 &= w^2 \quad \text{e} \\
4x^2 + 3y^2 &= z^2.
\end{aligned}$$

Então $7x^2 + 7y^2 = w^2 + z^2$ $(*)$. Afirmamos que a equação $(*)$ não possui solução. Para isso, seja S o conjunto formado pelas soluções inteiras (x, y, w, z) de $(*)$, e tome $(a, b, c, d) \in S$

com $c^2 + d^2$ mínimo. Pelo lema, temos que $7|c$ e $7|d$, e daí $c = 7c'$ e $d = 7d'$. Mas então $a^2 + b^2 = 7c'^2 + 7d'^2 \Rightarrow (c', d', a, b) \in S$, com

$$a^2 + b^2 < 7(a^2 + b^2) = c^2 + d^2,$$

o que contraria a minimalidade de (a, b, c, d).

Problemas Propostos

Problema 17. *Prove que se p é primo então*

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}$$

Problema 18. *Encontre os restos da divisões de:*

a) $300^{3000} - 1$ *por 1001*

b) $7^{120} - 1$ *por 143*

Problema 19. *Encontre o resto de* $\underbrace{111\ldots11}_{p-1 \text{ uns}}$ *por p, onde p é um primo maior que* 5.

Problema 20. *Prove que se n é ímpar, então* $n^5 \equiv n \pmod{240}$.

Problema 21. *Sejam p e q primos distintos. Mostre que*

i) $(a + b)^p \equiv a^p + b^p \pmod{p}$

ii) $p^q + q^p \equiv p + q \pmod{pq}$

iii) $\left\lfloor \dfrac{p^q + p^q}{pq} \right\rfloor$ *é par se* $p, q \neq 2$.

Problema 22. *Mostre que se p é primo e* $a^2 \equiv b^2 \pmod{p}$, *então* $a \equiv \pm b \pmod{p}$.

Problema 23. *Encontre os últimos três dígitos de* 7^{9999}

Problema 24. *Prove que* $20^{15} - 1$ *é divisível por* $11 \cdot 31 \cdot 61$

Problema 25. *Sejam* $\{a_1, a_2, ..., a_{101}\}$ *e* $\{b_1, b_2, ..., b_{101}\}$ *sistemas completos de resíduos módulo 101. Pode* $\{a_1b_1, a_2b_2, ..., a_{101}b_{101}\}$ *ser um sistema completo de resíduos módulo* 101*?*

Problema 26. *(Balcânica 2003) Existe um conjunto B de 4004 inteiros positivos tal que, para cada subconjunto A de B com 2003 elementos, a soma dos elementos em A não é divisível por 2003?*

Problema 27. *Para um inteiro ímpar $n > 1$, seja S o conjunto de inteiros x,$1 \leq x \leq n$, tal que ambos x e $x + 1$ são relativamente primos com n. Mostre que o produto de todos os elementos de S deixa resto* 1 *na divisão por n.*

Problema 28. *Sejam n um inteiro positivo maior que 1 e p um primo positivo tal que n divide $p-1$ e p divide n^3-1. Mostre que $4p-3$ é um quadrado perfeito.*

Dicas e Soluções

17. Pelo teorema de Fermat, $a \equiv a^p \equiv b^p \equiv b \pmod{p}$. Assim,

$$\begin{aligned} a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} &\equiv a^{p-1} + a^{p-1} + \ldots + a^{p-1} \\ &\equiv pa^{p-1} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Como $a - b \equiv 0 \pmod{p}$, temos:

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1}) \equiv 0 \pmod{p^2}$$

19. Veja que:

$$\begin{aligned} \underbrace{111\ldots11}_{p-1\ uns} &= \frac{999\ldots99}{9} \\ &= \frac{10^{p-1}-1}{9} \end{aligned}$$

Pelo teorema de Fermat, o numerador $10^{p-1}-1$ é divisível por p visto que $p \neq 5$. Além disso, usando que $p \neq 2$ e 3, segue que $\frac{10^{p-1}-1}{9}$ também é múltiplo de p.

20. Proceda como no exemplo 20.

21. i)Pelo teorema de Fermat:

$$\begin{aligned} (a+b)^p &\equiv a+b \\ &\equiv a^p + b^p \pmod{p}. \end{aligned}$$

ii) Pelo teorema de Fermat,

$$\begin{aligned} p^q + q^p &\equiv 0 + q \equiv p + q \pmod{p} \\ p^q + q^p &\equiv p + 0 \equiv p + q \pmod{q} \end{aligned}$$

22. Veja que $(a-b)(a+b) \equiv 0 \pmod{p}$ e assim $a - b \equiv 0 \pmod{p}$ ou $a + b \equiv 0 \pmod{p}$.

25. Suponha, por abusurdo, que seja possível. Sejam a_i e b_j tais que $a_i \equiv b_j \equiv 0 \pmod{101}$. Se $i \neq j$, o conjunto $\{a_1b_1, a_2b_2, ..., a_{101}b_{101}\}$ teria dois inteiros com resto

0 na divisão por p e não poderia ser um **scr**. Suponha sem perda de generalidade que $i = j = 101$, então:

$$\begin{aligned} 100! &\equiv (a_1b_1)(a_2b_2)\dots(a_{100}b_{100}) \\ &\equiv (a_1a_2\dots a_{100})(b_1b_2\dots b_{100}) \\ &\equiv (100!)(100!) \\ &\equiv (100!)^2 \pmod{101} \end{aligned}$$

Assim, $100! \equiv 1 \pmod{101}$. Isso contradiz o teorema de Wilson.

26. Sim. Um exemplo de tal conjunto é a união de um conjunto de 2002 inteiros positivos que deixem resto 0 com outro conjunto composto por 2002 inteiros que deixem resto 1 por 2003.