Ciclo 6 – Encontro 1

APLICAÇÕES DE CONGRUÊNCIAS, ARITMÉTICA MODULAR

Nível 3
PO: Márcio Reis
11º Programa de Iniciação Científica Jr.

A aritmética dos restos

- Apostila 1: INICIAÇÃO À ARITMÉTICA, de Abramo Hefez.

  Seções 4.5 e 4.6:

  Algumas aplicações;

  Aritmética modular.

Um critério de divisibilidade por 6

Observe inicialmente que

$$10 \equiv 4 \bmod 6,$$

$$10^2 \equiv 4^2 \equiv 4 \bmod 6,$$

$$10^3 \equiv 10^2 \times 10 \equiv 4 \times 4 \equiv 4 \bmod 6,$$

$$10^4 \equiv 10^3 \times 10 \equiv 4 \times 4 \equiv 4 \bmod 6.$$

Você tem ainda alguma dúvida de que $10^i \equiv 4 \bmod 6$, para todo número natural $i > 0$?

Um critério de divisibilidade por 6

Assim, se um número natural n é escrito no sistema decimal como $n_r \dots n_1 n_0$, temos que

$$n = n_0 + 10n_1 + 10^2 n_2 + \cdots + 10^r n_r \equiv n_0 + 4n_1 + 4n_2 + \cdots + 4n_r \bmod 6.$$

Com isto, temos que o resto da divisão de n por 6 é igual ao resto da divisão de $n_0 + 4n_1 + 4n_2 + \cdots + 4n_r$ por 6.

Logo, provamos que:

Um número $n = n_r \dots n_1 n_0$ *é divisível por* 6 *se e somente se* $n_0 + 4n_1 + 4n_2 + \cdots + 4n_r$ *é divisível por* 6.

Um critério de divisibilidade por 7, 11 e 13

Note que $7 \times 11 \times 13 = 1\,001$. Logo,

$$1\,000 \equiv -1 \bmod 7, \quad 1\,000 \equiv -1 \bmod 11 \quad \text{e} \quad 1\,000 \equiv -1 \bmod 13.$$

Assim, módulo 7, 11 e 13, temos que

$$10^3 \equiv -1,$$

$$10^6 \equiv (-1)^2 \equiv 1,$$

$$10^9 \equiv (-1)^3 \equiv -1,$$

$$10^{12} \equiv (-1)^4 \equiv 1,$$

etc.

Um critério de divisibilidade por 7, 11 e 13

Escrevendo um número n na representação decimal como $n_r \dots n_2 n_1 n_0$, temos, módulo 7, 11 ou 13, que

$$\begin{aligned} n &= n_2 n_1 n_0 + n_5 n_4 n_3 \times 10^3 + n_8 n_7 n_6 \times 10^6 + \cdots \\ &\equiv n_2 n_1 n_0 - n_5 n_4 n_3 + n_8 n_7 n_6 - \cdots . \end{aligned}$$

Assim, o resto da divisão de n por 7,11 ou 13 é igual ao resto da divisão de $n_2 n_1 n_0 - n_5 n_4 n_3 + n_8 n_7 n_6 - \cdots$ por 7, 11 ou 13, respectivamente.

Um critério de divisibilidade por 7, 11 e 13

Desse modo, obtemos o seguinte critério de divisibilidade por 7, 11 ou 13:

O número $n_r \ldots n_2 n_1 n_0$ *é divisível por* 7, 11 *ou* 13 *se, e somente se, o número* $n_2 n_1 n_0 - n_5 n_4 n_3 + n_8 n_7 n_6 - \cdots$ *é divisível por* 7, 11 *ou* 13, *respectivamente.*

Os restos da divisão das potências de 2 por 7

Observe que

$$2^1 \equiv 2 \bmod 7,$$

$$2^2 \equiv 4 \bmod 7,$$

$$2^3 \equiv 1 \bmod 7.$$

Dado um número inteiro n, pelo algoritmo da divisão, podemos escrevê-lo na forma $n = 3q + r$, onde $r = 0, 1$ ou 2.

Os restos da divisão das potências de 2 por 7

Assim,

$$2^n = 2^{3q+r} = (2^3)^q \times 2^r \equiv 2^r \bmod 7.$$

Por exemplo, se $n = 132 = 3 \times 44$, então $2^{132} \equiv 1 \bmod 7$, pois $r = 0$.

Se $n = 133 = 3 \times 44 + 1$, então $2^{133} \equiv 2 \bmod 7$, pois $r = 1$.

Se $n = 134 = 3 \times 44 + 2$, então $2^{134} \equiv 4 \bmod 7$, pois $r = 2$.

A equação diofantina $x^3 - 117y^3 = 5$

Vamos mostrar que esta equação não possui soluções inteiras. De fato, suponhamos, por absurdo, que x_0, y_0 seja uma solução inteira da equação. Então

$$x_0^3 \equiv 5 \bmod 9, \tag{4.1}$$

já que $117 \equiv 0 \bmod 9$.

Mas, sendo x_0 congruente a $0, 1, 2, 3, 4, 5, 6, 7$ ou 8 módulo 9, segue por contas elementares que x_0^3 é congruente a $0, 1$ ou 8, módulo 9. Logo, a congruência (4.1) não possui solução, o que fornece uma contradição.

Os números da forma $3^{6n} - 2^{6n}$ são divisíveis por 35

Temos que

$$3^6 = 3^3 \times 3^3 \equiv (-1) \times (-1) \equiv 1 \bmod 7,$$

$$2^6 = 2^3 \times 2^3 \equiv 1 \times 1 \equiv 1 \bmod 7.$$

Por outro lado,

$$3^6 = 3^3 \times 3^3 \equiv 2 \times 2 \equiv -1 \bmod 5,$$

$$2^6 = 2^3 \times 2^3 \equiv 3 \times 3 \equiv -1 \bmod 5.$$

Os números da forma $3^{6n} - 2^{6n}$ são divisíveis por 35

Logo, $3^{6n} - 2^{6n} \equiv 0 \bmod 7$ e $3^{6n} - 2^{6n} \equiv 0 \bmod 5$.

Assim, $3^{6n} - 2^{6n}$ é divisível por 5 e por 7 e como $\text{mdc}(5, 7) = 1$, segue, do Problema 3.42, que $3^{6n} - 2^{6n}$ é divisível por 35.

Euler tinha razão, e Fermat estava enganado?

O número 4294967297 é primo ou composto?

Apostila 1: INICIAÇÃO À ARITMÉTICA, de Abramo Hefez.

- Ler Seção 4.5, item 6, páginas 94, 95 e 96.

Aritmética modular

A Aritmética Modular foi introduzida por Gauss no seu livro *Disquisitiones Aritmeticae* publicado em 1801.

Fixado um número inteiro $m > 1$, vamos associar a um número inteiro a qualquer o símbolo $\overline{a}$ representando o resto da sua divisão por m, tal qual fizemos nas Seções 3.5 e 3.6, nos casos $m = 2$ e $m = 3$.

Portanto, dados dois números a e b tem-se que $\overline{a} = \overline{b}$ se, e somente se, os restos da divisão de a e de b por m são iguais, ou seja,

$$\overline{a} = \overline{b} \text{ se, e somente se, } a \equiv b \bmod m.$$

Aritmética modular

Sendo todos os possíveis restos da divisão por m os números $0, 1, 2, \ldots, m-1$, temos qualquer $\overline{a}$ é igual a um dos seguintes: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Nas Seções 4.3 e 4.4 observamos que os restos da divisão da soma e do produto de dois números não dependem dos números em si, mas apenas dos restos da divisão desses números. Sendo assim, para achar $\overline{(a+b)}$ e $\overline{(a \times b)}$ só precisamos saber como operar aditivamente e multiplicativamente com os símbolos $\overline{a}$ e $\overline{b}$, que são justamente elementos da forma $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, a exemplo do que fizemos nas seções 3.5 e 3.6, nos casos $m = 2$ e $m = 3$.

Aritmética modular

Aritmética módulo m = 4

Para efeito de ilustração, tomemos o caso $m = 4$. Neste caso, temos apenas os símbolos $\overline{0}$, $\overline{1}$, $\overline{2}$ e $\overline{3}$ a considerar.

Pede-se ao leitor verificar as seguintes tabelas:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note que diferentemente da aritmética dos números inteiros, surge um novo fenômeno: $\overline{2} \neq \overline{0}$ e, no entanto, $\overline{2} \times \overline{2} = \overline{0}$.

Aritmética modular

Aritmética módulo m = 5

Analisaremos agora o caso $m = 5$. Neste caso, temos apenas os símbolos $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ e $\overline{4}$ a considerar.

Pede-se ao leitor verificar as seguintes tabelas:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note que aqui volta a valer a regra:

se $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, então $\overline{a} \times \overline{b} \neq \overline{0}$.

Exercício 1

Mostre que a equação $x^3 + 21y^2 + 5 = 0$ não tem soluções inteiras para x e y.

DICA: Suponha, por contradição, que existam x_0 e y_0 inteiros tais que

$$x_0^3 + 21y_0^2 + 5 = 0.$$

Exercício 1 - Solução

Solução: Suponha, por contradição, que existam x_0 e y_0 inteiros tais que $x_0^3 + 21y_0^2 + 5 = 0$. Então, $x_0^3 + 21y_0^2 + 5 = 0 \equiv 0 \pmod 7$ e, logo, como $21 \equiv 0 \pmod 7$ e $5 \equiv -2 \pmod 7$, tem-se $x_0^3 \equiv 2 \pmod 7$. Por outro lado, x_0 é cônguo a 0, 1, 2, 3, 4, 5 ou 6, módulo 7, e, logo, $x_0^3 \equiv 0^3 = 0 \pmod 7$ ou $x_0^3 \equiv 1^3 = 1 \pmod 7$ ou $x_0^3 \equiv 2^3 = 8 \equiv 1 \pmod 7$ ou $x_0^3 \equiv 3^3 = 3^2 \cdot 3 = 9 \cdot 3 \equiv 2 \cdot 3 = 6 \pmod 7$ ou $x_0^3 \equiv 4^3 = 4^2 \cdot 4 = 16 \cdot 4 \equiv 2 \cdot 4 = 8 \equiv 1 \pmod 7$ ou $x_0^3 \equiv 5^3 = 5^2 \cdot 5 = 25 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv 6 \pmod 7$ ou $x_0^3 \equiv 6^3 = 6^2 \cdot 6 = 36 \cdot 6 \equiv 1 \cdot 6 = 6 \pmod 7$, ou seja, x_0^3 é cônguo a 0, 1 ou 6, módulo 7, o que contradiz $x_0^3 \equiv 2 \pmod 7$.

Exercício 2

a) Mostre que todo quadrado perfeito é côngruo a 0, 1 ou 4, módulo 8.

b) Mostre que não há nenhum quadrado perfeito na sequência: 2, 22, 222, 2222, 22222, ...

c) Mostre que não há nenhum quadrado perfeito na sequência: 3, 11, 19, ..., $3 + 8n$, ...

Exercício 2

a) Mostre que todo quadrado perfeito é côngruo a 0, 1 ou 4, módulo 8.

b) Mostre que não há nenhum quadrado perfeito na sequência: 2, 22, 222, 2222, 22222, ...

c) Mostre que não há nenhum quadrado perfeito na sequência: 3, 11, 19, ..., $3 + 8n$, ...

Exercício 2a - Solução

a) Mostre que todo quadrado perfeito é côngruo a 0, 1 ou 4, módulo 8.

Solução:

a) Para resolver esse item, proceda de maneira análoga ao problema anterior quando foi mostrado que todo cubo perfeito é côngruo a 0, 1 ou 6, módulo 7.

Exercício 2b - Solução

b) Mostre que não há nenhum quadrado perfeito na sequência: 2, 22, 222, 2222, 22222, ...

Tem-se $2 \equiv 2 \pmod 8$, $22 \equiv 6 \pmod 8$, $222 = 200 + 22 \equiv 0 + 6 = 6 \pmod 8$, $2222 = 2 \cdot 1000 + 222 \equiv 2 \cdot 0 + 6 = 6 \pmod 8$, $22222 = 20 \cdot 1000 + 222 \equiv 20 \cdot 0 + 6 = 6 \pmod 8$,..., $222222 = 200 \cdot 1000 + 2222 \equiv 200 \cdot 0 + 6 = 6 \pmod 8$, e assim por diante. Assim, os números da sequência são côngruos a 2 ou 6, módulo 8, e, logo, pelo item a, não podem ser quadrados perfeitos.

Exercício 2c – Solução

c) Mostre que não há nenhum quadrado perfeito na sequência: 3, 11, 19, ..., $3 + 8n$, ...

Como $3 + 8n \equiv 3 \pmod 8$, para todo inteiro não negativo n, então os números da sequência são côngruos a 3, módulo 8, e, logo, pelo item a, não podem ser quadrados perfeitos.

Exercício 3

Prove que, entre 52 inteiros quaisquer, existem dois cujos quadrados têm o mesmo resto na divisão por 100.

Exercício 3 - Solução

Solução: Todo número inteiro é côngruo, módulo 100, a exatamente um dos inteiros $0, 1, 2, \ldots, 99$. Assim, cada um dos 52 inteiros dados é côngruo, módulo 100, a exatamente um dos elementos de exatamente um dos 51 conjuntos: $\{0\}$, $\{50\}$, $\{1, 99\}$, $\{2, 98\}$, ..., $\{49, 51\}$. Pelo Princípio da Casa de Pombos (*se não conhecer esse Princípio, pesquise sobre ele; é bem simples!*), entre os 52 inteiros dados, existem dois deles, x e y $(x \neq y)$, tais que:

- $x \equiv 0 \equiv y \pmod{100}$ ou
- $x \equiv 50 \equiv y \pmod{100}$ ou
- para algum i, com $i = 1, 2, \ldots, 49$, tem-se $x \equiv i \pmod{100}$ ou $x \equiv 100 - i \equiv -i \pmod{100}$, e $y \equiv i \pmod{100}$ ou $y \equiv 100 - i \equiv -i \pmod{100}$.

Em qualquer um dos casos acima, tem-se $x^2 \equiv y^2 \pmod{100}$ e, logo, x^2 e y^2 têm o mesmo resto na divisão por 100.

Exercício 4

Problema 4.22. Sabendo que $2^4 = 16 \equiv -1 \bmod 17$, ache o resto da divisão de 2^{30} por 17.

Exercício 4 - Solução

4.22 Temos que $30 = 4 \times 7 + 2$, logo

$$2^{30} = (2^4)^7 \times 2^2 \equiv (-1)^7 \times 4 \equiv 3 \bmod 17.$$

Logo o resto da divisão é 3.

Exercício 5

Problema 4.25. Mostre que todo número da forma $19^{8n} - 1$ é divisível por 17.

Exercício 5 - Solução

4.25 $19 \equiv 2 \bmod 17$, logo $19^{8n} = (19^4)^{2n} \equiv (-1)^{2n} = 1 \bmod 17$. Assim, $19^{4n} - 1$ é divisível por 17.

Exercício 6

Problema 4.24. Mostre que a equação diofantina

$$x^2 + y^2 + z^2 = 8w + 7$$

não possui soluções x, y, z, w inteiros.

SUGESTÃO: Reduza a equação módulo 8 e mostre que

$$x_0^2 + y_0^2 + z_0^2 \equiv 7 \bmod 8$$

nunca ocorre.

Exercício 6 – Solução

$$x^2 + y^2 + z^2 = 8w + 7$$

$$x_o^2 + y_o^2 + z_o^2 \equiv ?\ mod\ 8$$

$$8w + 7 \equiv 7\ mod\ 8$$

$$x_o^2 + y_o^2 + z_o^2 \equiv 7\ mod\ 8$$

$$(verdadeiro\ ou\ falso?)$$

$$0^2 = 0 \equiv 0\ mod\ 8$$
$$1^2 = 1 \equiv 1\ mod\ 8$$
$$2^2 = 4 \equiv 4\ mod\ 8$$
$$3^2 = 9 \equiv 1\ mod\ 8$$
$$4^2 = 16 \equiv 0\ mod\ 8$$
$$5^2 = 25 \equiv 1\ mod\ 8$$
$$6^2 = 36 \equiv 4\ mod\ 8$$
$$\ldots$$

Estudar para o próximo encontro!

Próximo encontro: 03/12, sábado, às **8h**

Módulo: "Métodos Sofisticados de Contagem"
http://matematica.obmep.org.br/index.php/modulo/ver?modulo=16
Vídeoaulas: "Combinação Completa", "Exercícios sobre Combinação Completa – Parte 1", "Exercícios sobre Combinação Completa – Parte 2", "Exercícios sobre Combinação Completa – Parte 3", "Exercícios sobre Combinação Completa – Parte 4", "Exercícios sobre Combinação Completa – Parte 5".