1

ARITMÉTICA MODULAR

"God invented the integers;
all else is the work of man." — Kronecker

1.1 - INTRODUÇÃO


Carl Friedrich Gauss

A Teoria dos Números é a parte da matemática que estuda as propriedades dos números naturais 1, 2, 3, ... , também chamados inteiros positivos. Neste capítulo discutiremos alguns fatos básicos da chamada Teoria dos Números Clássica, em contraposição à Teoria dos Números Algébrica [Cassels 10] e à Teoria dos Números Analítica [Apostol 10]. Estes fatos básicos surgirão posteriormente em aplicações da Matemática Discreta, e daí nosso interesse neles.

Com resultados que datam de antes de Cristo, a Teoria dos Números tem duas características que a distinguem de outros ramos da matemática: i) A vasta maioria dos grandes matemáticos, em todas as épocas, investigou algum problema ligado ao assunto; ii) Muitos de seus problemas (alguns ainda sem solução) podem ser formulados com um mínimo de conhecimento prévio do assunto. Dentre os matemáticos que mais se destacaram no assunto, podemos citar Pierre de Fermat (1601-1665), Leonard Euler (1707– 1783) e Carl Friedrich Gauss (1777-1855). Uma pequena biografia destes e de outros matemáticos ilustres é apresentada no apêndice A.

A Teoria dos Números sempre foi um dos ramos da Matemática inteiramente desvinculado de qualquer cenário de aplicação fora da própria Matemática, uma característica considerada desejável para alguns matemáticos importantes do século 20, tal como G. H. Hardy [Hardy 40]. Entretanto, com o advento dos modernos computadores digitais, a situação mudou drasticamente e, desde a década de 70, inúmeras aplicações desse ramo da Matemática surgiram em diversas áreas da Engenharia Eletrônica, tais como, segurança de dados, transmissão de informação e processamento digital de sinais [Simmons 92], [McClellan 79]. Em particular, os principais sistemas de criptografia de chave pública (algoritmos de cifragem e decifragem, protocolos de troca de chave) empregam resultados oriundos da Teoria dos Números, a maioria deles desenvolvidos nos séculos 17 e 18 (!) [Stallings 07].

Este capítulo tem o objetivo de apresentar algumas noções básicas sobre o assunto, de modo a permitir ao leitor a compreensão de um dos primeiros criptossistemas de chave pública propostos na literatura, a ser discutido no Capítulo 2. Especificamente, vamos abordar a chamada aritmética modular, com ênfase na resolução de congruências lineares. Algumas aplicações simples do material apresentado são discutidas no final do capítulo.

1.2 - DIVISIBILIDADE

No que se segue supõe-se que o leitor está familiarizado com a formulação usual das proposições matemáticas. Em particular, se A e B denotam proposições quaisquer, as seguintes afirmações são equivalentes:

- A implica B ($A \Rightarrow B$).
- Se A é verdadeiro, então B é verdadeiro.
- Para que A seja verdadeiro, é necessário que B seja verdadeiro.
- B é uma condição necessária para A.
- A é uma condição suficiente para B.

Se A implica B e B implica A, então B é uma condição necessária e suficiente (CNS) para A e vice-versa. Neste caso, escreve-se $A \Leftrightarrow B$ ou A se e só se B. Como exemplo, suponha que A e B correspondem às afirmações:
A: n é par, B: n é divisível por 2. É claro, portanto, que neste caso $A \Leftrightarrow B$.

A noção de divisibilidade e suas implicações são conhecidas desde o tempo de Euclides, cerca de 350 A.C.

Definição 1: Um inteiro a é divisível por um inteiro b (escreve-se $b \mid a$), não nulo, se existe um inteiro k, tal que $a = kb$. ■

Outras denominações para a condição de divisibilidade são:
- b divide a.
- b é um divisor de a.
- b é um fator de a.
- a é um múltiplo de b. ■

Os teoremas 1 e 2 a seguir apresentam alguns resultados úteis referentes à definição 1 [Burt 10].

Teorema 1: Para quaisquer a, b, c e d inteiros, tem-se

i) $b \mid a \Rightarrow b \mid ac$, $\forall$ (para todo) c.
ii) $b \mid a$ e $c \mid d \Rightarrow bc \mid ad$.
iii) $b \mid a$ e $a \mid c \Rightarrow b \mid c$.
iv) $b \mid a$ e $b \mid c \Rightarrow b \mid (ax + cy)$, $\forall$ x, y inteiros.
v) $b \mid a$ e $a \mid b \Rightarrow a = \pm b$.
vi) $b \mid a$ com $a, b > 0 \Rightarrow b \leq a$.

vii) $b \mid a \Leftrightarrow mb \mid ma, \quad \forall\, m$ inteiro $\neq 0$. ■

A prova desse teorema segue diretamente da definição de divisibilidade e não é apresentada aqui. Observe que (iii) e (iv) podem ser estendidos.

Teorema 2: Para quaisquer a e b inteiros, com $b > 0$, existem inteiros q e r únicos, tais que $a = qb + r$, $0 \le r < b$. Se b não divide a, então $0 < r < b$. ■

O teorema 2 é conhecido como *algoritmo da divisão*. Os valores q e r são chamados, respectivamente, o quociente e o resto da divisão de a por b.

Exemplo 1.1: Para $a = 23$ e $b = 7$, o algoritmo da divisão resulta em $23 = 3.7 + 2$ ($q = 3$ e $r = 2$). Para $a = -19$ e $b = 5$, tem-se $-19 = (-4).5 + 1$ ($q = -4$ e $r = 1$). ■

Exemplo 1.2: Usando o algoritmo da divisão, mostra-se que o quadrado de qualquer número ímpar é da forma $8k+1$, k um inteiro positivo. Isto porque com $b=4$, todo inteiro a, ímpar, pode ser expresso na forma $4q+1$ ou $4q+3$, de modo que, ou se tem $a^2 = 16q^2 + 8q + 1 = 8k + 1$, ou $a^2 = 16q^2 + 24q + 9 = 8k' + 1$ ■

Exemplo 1.3: Em alguns estados, a data e o mês de nascimento são incorporados ao número da carteira nacional de habilitação (CNH), por meio da expressão $XYZ = 40(m-1) + n$, em que m e n representam o mês e a data de nascimento, respectivamente, e XYZ são os três últimos dígitos da CNH. Assim, considerando que $349 = 40.8 + 29$, o titular da CNH com esses três últimos dígitos nasceu no dia 29 de setembro. ■

Um conceito simples e muito utilizado em Teoria dos Números é o de *Máximo Divisor Comum* entre os inteiros a e b.

Definição 2 - Dados os inteiros a e b, com pelo menos um deles diferente de zero, o inteiro positivo d é dito ser o Máximo Divisor Comum entre a e b, denotado por MDC (a, b), se:
i) $d \mid a$ e $d \mid b$.
ii) Se $c \mid a$ e $c \mid b$ então $c \le d$. ■

O teorema 3 a seguir é o ponto de partida para a solução de congruências lineares, ferramenta importante na Criptografia moderna.

Teorema 3: Se $d \triangleq$ MDC (a, b), então existem inteiros x e y tais que

$$d = ax + by, \tag{1.1}$$

Ou seja, o MDC entre dois inteiros, a e b, pode ser expresso como uma combinação linear dos mesmos. ■

Prova: Seja S o conjunto de todas as combinações lineares do tipo $ax+by$, com $x, y \in \boldsymbol{Z}$. Essas combinações produzem inteiros positivos e negativos, além do zero (para $x = y = 0$). Denotando por t o menor desses inteiros positivos, então $t \mid a$ e $t \mid b$. Isso porque se t não divide a, então existem inteiros q e r satisfazendo $a = qt + r$, $0<r < t$. Ou seja,

$$r = a - qt = a - q(ax + by),$$

e assim

$$r = a(1 - qx) + b(-qy)$$

e portanto $r < t$ é da forma $ax + by$ e assim $\in$ S, o que contradiz o fato de que t é o menor elemento positivo em S. De maneira análoga, prova-se que $t \mid b$. Agora, como $d \mid a$ e $d \mid b$, pode-se escrever $a = dA$ e $b = dB$, de modo que

$$t = ax + by = dAx + dBy,$$

ou $t = d(Ax + By)$ e portanto $d \mid t$, o que implica $d \leq t$. Como d = MDC (a, b), tem-se então que d = $t = ax + by$. ■

Note que se $ax + by = 1$, então MDC(a, b) = 1. Neste caso, diz-se que a e b são relativamente primos (ou primos entre sí).

Os valores de x e y na expressão (1.1) podem ser determinados através do chamado algoritmo de Euclides, o qual é usado para determinar o valor de d.

Teorema 4 (Algoritmo de Euclides): Dados os inteiros a e b, considere a aplicação repetida do algoritmo da divisão (Teorema 2) para obter a série de equações

$$\begin{aligned}
b &= q_1 a + r_1, \quad 0 < r_1 < a,\\
a &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2,\\
r_2 &= q_4 r_3 + r_4, \quad 0 < r_4 < r_3,\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\\
r_{j-2} &= q_j r_{j-1} + r_j, \quad 0 < r_j < r_{j-1},\\
r_{j-1} &= q_{j+1} r_j \text{ (resto zero).}
\end{aligned}$$

Então o MDC(a, b) é r_j, o último resto não nulo do processo de divisão. Os valores de x e y em $d = ax + by$ podem ser obtidos pela eliminação sucessiva de r_{j-1}, r_{j-2}, ... , r_2, r_1 do conjunto de expressões acima. ■

Prova: A cadeia de expressões é produzida pela divisão sucessiva de b por a (deixa resto r_1), a por r_1 (deixa resto r_2), r_1 por r_2 (deixa resto r_3), e assim sucessivamente. Aplicando repetidamente a propriedade indicada no problema 1.4, tem-se MDC(a, b) = MDC(a, b-

$q_1 a$) = MDC(a, r_1) = MDC(r_1, a-q_2 r_1) = MDC(r_1, r_2) = MDC(r_2, r_1-q_3 r_2) = MDC(r_2, r_3) = ...= MDC(r_{j-1}, r_j) = r_j, uma vez que $r_j \mid r_{j-1}$. Não é difícil ver que a eliminação repetida dos restos de cada divisão leva a uma expressão do tipo $g = ax + by$, com x e y inteiros. ■

Exemplo 1.4: MDC(172, 20) = MDC(20, 12) = MDC(12, 8) = MDC(8, 4) = 4. ■

Para concluir esta seção são introduzidas algumas noções elementares sobre os números primos.

Definição 3 - O inteiro $p > 1$ é dito ser um número *primo* se não existe nenhum divisor de p satisfazendo $1 < d < p$. Se $n > 1$ não é primo, n é dito ser um número composto. ■

Números primos desempenham um papel fundamental na Criptografia Moderna. O criptossistema de chave pública (Criptografia de Chave Pública ou Assimétrica é tratada no Capítulo 2) de maior uso comercial hoje em dia, o criptossistema RSA, tem sua segurança baseada na dificuldade de fatorar um número composto n que é um produto de dois primos distintos p e q. Esses dois números primos são parâmetros do sistema, o que traz o problema de se encontrar números primos *grandes*, uma vez que, por razões de segurança, esses números devem ter, no mínimo, cerca de 150 dígitos decimais cada, a fim de resistir às modernas técnicas de criptoanálise empregadas com computadores de alta velocidade configurados em estruturas paralelas.

Muitas conjecturas interessantes existem sobre os números primos, algumas já propostas há bastante tempo, tais como a conjectura de Goldbach (1690-1764), apresentada em uma carta de Christian Golbach a Leonhard Euler em 1742 [Saut 08]. Famílias especiais de números primos também são de especial interesse, tais como os chamados primos de Mersenne, dentre os quais se encontram os maiores primos conhecidos até o momento [PriMersenne 11]. Um inteiro da forma

$$M_n = 2^n - 1$$

é chamado número de Mersenne, por causa do Monge francês Marin Mersenne (1588 - 1644), que fez uma conjectura parcialmente incorreta, porém, provocativa sobre sua primalidade. Os números de Mersenne que são primos são chamados primos de Mersenne. A conjectura afirmava que M_p é primo para p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e composto para todos os outros primos $p < 257$. A definição sobre a veracidade dessa conjectura levou cerca de 300 anos, e apenas em 1947 é que o exame da primalidade de M_p para os 55 primos na faixa $p \leq 257$ foi concluído. Uma lista de todos os primos de Mersenne conhecidos até hoje pode ser encontrada em [PriMersenne 11].

O maior número primo conhecido até o momento (agosto 2011) é $M_{43112609}$, um primo de Mersenne com 12978189 dígitos, descoberto em 23 de agosto de 2008 [Primaior 11]. As Tabelas 1.1 e 1.2 mostram, respecticamente, os oito primeiros primos de Mersenne (incluindo a correspondente decomposição de M_n -1 em fatores primos) e os dez maiores números primos conhecidos até hoje (agosto 2011). Observe que nove desses primos são primos de Mersenne. Isto ocorre porque os números de Mersenne representam o tipo de número cuja primalidade é a mais fácil de ser verificada em um computador digital. De fato, os maiores números primos encontrados tem sido, quase sempre, primos de Mersenne. A razão específica para isso é que a prova da primalidade de números N grandes (digamos,

com mais de 1000 dígitos), se baseia na fatoração de N+1 ou N-1, e para os números de Mersenne a fatoração de N+1 é trivial pois $M_n + 1 = 2^n$ [Primachar 11], [Riesel 94].

A busca por números primos grandes sofreu um tremendo impacto com a criação do projeto GIMPS (do ingles *Great Internet Mersenne Prime Search*), lançado por George Woltman em 1996 [GIMPS 11]. Desde então, no período 1996-2008, o projeto foi responsável pela determinação dos ultimos 11 maiores números primos conhecidos [Caldwell 11]. O programa disponibilizado pelo GIMPS é de livre acesso e milhares de usuários no planeta tem substituído seus "descansos de tela" pelo uso mais produtivo do tempo ocioso de máquina, contribuindo assim na busca por números primos *grandes*.

É possível provar que, se $a^n - 1$ é primo (a>0, $n \geq 2$), então a = 2 e n é primo, ou seja, os únicos números primos dessa forma são os primos de Mersenne. Esses números primos são atraentes para aplicações em Engenharia envolvendo aritmética modular, devido ao fato de que os corpos finitos em que a operação de multiplicação é mais simples são os corpos GF(p) (do inglês *Galois Field*, em homenagem ao matemático francês Evariste Galois (1811-1832)), em que p é um primo de Mersenne. Mais especificamente, se os inteiros são representados como números binários de m-bits, uma vez que $2^m \equiv 1 (mod\ 2^m - 1)$, a complexidade da execução das operações é igual à complexidade da aritmética complemento de 1 [Blahut 2010].

Outra família especial de interesse é a dos chamados primos de Fermat. Um inteiro da forma

$$F_n = 2^{2^n} + 1,$$

$n \geq 0$, é chamado número de Fermat, por causa do matemático francês Pierre de Fermat (1601-1665), que conjecturou que os números dessa forma eram primos. Os números de Fermat que são primos são chamados primos de Fermat. Sabe-se que, se $2^m + 1$ é um número primo, então m é uma potência de dois. No entanto, o inverso não é verdade, uma vez que, por exemplo, $2^{32} + 1$ não é primo. Os únicos primos de Fermat conhecidos até hoje são F_0, F_1, F_2, F_3 e F_4, respectivamente, 3, 5, 17, 257 e 65537 [Burton 2010].

Tabela 1.1 – *Os primeiros oito números primos de Mersenne*

n	$M_n = 2^n - 1$	$M_n - 1 = 2\,(2^{n-1} - 1)$
2	**3**	**2**
3	**7**	**2 · 3**
5	**31**	**2 · 3 · 5**
7	**127**	**2 · 3^2 · 7**
13	**8191**	**2 · 3^2 · 5 · 7 · 13**
17	**131071**	**2 · 3 · 5 · 17 · 257**
19	**524287**	**2 · 3^3 · 7 · 19 · 73**
31	**2147483647**	**2 · 3^2 · 7 · 11 · 31 · 151 · 331**

Tabela 1.2 – *Os 10 maiores números primos conhecidos.*

Posição	Primo	Digitos	Quando
1º	$2^{43112609}-1$	12978189	2008
2°	$2^{42643801}-1$	12837064	2009
3º	$2^{37156667}-1$	11185272	2008
4º	$2^{32582657}-1$	9808358	2006
5º	$2^{30402457}-1$	9152052	2005
6º	$2^{25964951}-1$	7816230	2005
7º	$2^{24036583}-1$	7235733	2004
8º	$2^{20996011}-1$	6320430	2003
9º	$2^{13466917}-1$	4053946	2001
10º	$19249 \cdot 2^{13018586}+1$	3918990	2007

Primos de Mersenne e de Fermat tem aplicações, por exemplo, em Processamento Digital de Sinais, quando são usados na concepção das chamadas transformadas numéricas de Fourier e de Hartley. Essas transformadas permitem a implementação de filtragem digital com baixa complexidade computacional e sem erros de arredondamento ou truncagem, o chamado ruído computacional, que acontece quando a aritmética usual dos números reais é usada com processadores de precisão finita [Pol 71], [Camp 98], [Camp 01], [Blahut 10].

Outro cenário de aplicação é o de Codificação de Canal, em que novos códigos de bloco lineares p-ários foram construídos a partir da autoestrutura de transformadas definidas sobre corpos finitos [Camp 09], [Camp 11].

De especial importância em Teoria dos Números tem-se o chamado teorema da fatoração única, usualmente denominado teorema fundamental da aritmética.

Teorema 5 (Teorema Fundamental da Aritmética): A fatoração de qualquer inteiro $n>1$, como um produto de fatores primos, é única [Burt 10].

É importante mencionar que a propriedade de fatoração única não é algo trivial quanto parece sugerir a fatoração dos números inteiros na aritmética usual. Alguns sistemas simples não possuem a propriedade da fatoração única, como é o caso dos inteiros positivos pares {2, 4, 6, 8, ...} juntamente com a operação de multiplicação usual. Neste caso, o inteiro 60 pode ser fatorado de dois modos distintos, a saber, $60 = 2x30 = 6x10$. Observe que, neste sistema, os números 2, 6, 10 e 30 são todos primos.

Outro resultado importante acerca dos números primos é mostrado no Teorema 6 a seguir.

Teorema 6 (Euclides): A série dos números primos é infinita.

Prova: Considere r primos $p_1, p_2, ..., p_r$ e forme o inteiro $n = 1 + p_1, p_2, ..., p_r$. Claramente, p_i não divide n. Assim, qualquer primo p divisor de n é um primo distinto de

p_i. Como n ou é primo ou tem fatores primos, conclui-se que existe um primo distinto dos p_i. ■

1.3 - CONGRUÊNCIAS LINEARES

A aritmética modular (ou dos resíduos), foi introduzida por C. F. Gauss em 1801, no seu livro Disquisitiones Arithmeticae [Gauss 01]. Algumas das mais importantes técnicas de criptografia de chave pública são baseadas nesse tipo de aritmética.

Definição 4: Dados os inteiros a, b e $n \neq 0$, a é dito ser congruente com b módulo n se n divide a diferença a-b, isto é, se a-$b = kn$, para algum inteiro k. Neste caso, escreve-se $a \equiv b \pmod{n}$ (lê-se "a é congruente com b, módulo n").

Para fixar ideias, considere $n = 7$. Então $3 \equiv 24 \pmod 7$, $-31 \equiv 11 \pmod 7$, etc. Note também que dois inteiros são congruentes módulo 2 se ambos são pares ou ímpares.

Dado um inteiro a, sejam q e r, respectivamente, o quociente e o resto da divisão de a por um inteiro n, isto é, $a = qn + r$, $0 \leq r < n$. Então, por definição, $a \equiv r \pmod n$. Desde que existem n escolhas para r, então cada inteiro é congruente, módulo n, a exatamente um dos valores 0, 1, 2, ..., n-1. Em particular, $a \equiv 0 \pmod n$ se e só se $n \mid a$. O conjunto $Z_n = \{0, 1, ..., n\text{-}1\}$ dos inteiros módulo n é dito ser um conjunto completo de resíduos módulo n. Em geral, uma coleção de n inteiros $r_1, r_2, ... r_n$ é um conjunto (ou sistema) completo de resíduos se todo inteiro a é congruente módulo n a um e apenas um dos r_i.

Congruências tem muitas propriedades interessantes, algumas semelhantes àquelas apresentadas por igualdades.

1.3.1 - Algumas Propriedades das Congruências Lineares

No que se segue $n>1$ é um inteiro fixo, denominado módulo, e a, b, c e d são inteiros arbitrários.

i) $a \equiv a \pmod n$.
ii) $a \equiv b \pmod n$, $b \equiv a \pmod n$ e $a\text{-}b \equiv 0 \pmod n$ são declarações equivalentes.
iii) Se $a \equiv b \pmod n$ e $b \equiv c \pmod n$, então $a \equiv c \pmod n$.
iv) Se $a \equiv b \pmod n$ e $c \equiv d \pmod n$, então $a + c \equiv b + d \pmod n$ e $ac \equiv bd \pmod n$.
v) Se $a \equiv b \pmod n$, então $a + c \equiv b + c \pmod n$ e $ac \equiv bc \pmod n$.
vi) Se $a \equiv b \pmod n$ e $d \mid n$, $d > 0$, então $a \equiv b \pmod d$.
vii) Se $a \equiv b \pmod n$, então $ac \equiv bc \pmod{nc}$ para $c > 0$.
viii) Se $a \equiv b \pmod n$, então $a^k \equiv b^k \pmod n$, para qualquer inteiro positivo k.
ix) Se $ca \equiv cb \pmod n$, então $a \equiv b \pmod{n/d}$, em que $d \triangleq \text{MDC}(c, n)$.
x) $a \equiv b \pmod{pq}$ se e só se $a \equiv b \pmod p$ e $a \equiv b \pmod q$, em que p e q são primos distintos. Esta propriedade pode ser generalizada para inteiros positivos arbitrários, n_1 e n_2 (no lugar de p e q), conforme indicado no problema 1.14.

Estas propriedades são muito úteis na resolução de congruências lineares. Especificamente, uma congruência linear é uma expressão da forma $ax \equiv c \pmod{n}$, em que a, c e n são inteiros dados e $x \in Z_n$ é o valor a determinar. Por definição,

$$ax \equiv c \pmod{n} \Rightarrow n \mid (ax\text{-}c),$$

ou seja,

$$ax - ny = c \tag{1.2}$$

para algum inteiro y. Assim, o problema de se encontrar os inteiros satisfazendo à congruência linear $ax \equiv c \pmod{n}$, é equivalente àquele de se obter todas as soluções da equação diofantina (ou diofântica) (1.2). Uma equação é dita diofantina, em homenagem a Diophantus de Alexandria (~250 D.C.), quando só se permitem soluções inteiras para a mesma. Provavelmente, a equação diofantina mais famosa é aquela relacionada ao último teorema de Fermat,

$$x^n + y^n = z^n,$$

Em que $n > 2$, inteiro, e x, y, z são inteiros não nulos a determinar [Singh 2005].

A forma mais simples dessas equações é a que está sendo tratada no momento, ou seja, a equação diofantina linear, em duas variáveis,

$$ax + by = c,$$

em que a, b e c são inteiros dados. A questão que se põe é a da existência de soluções e de sua determinação explícita.

Teorema 7: A equação diofantina $ax + by = c$ tem solução se e só se $d = \text{MDC}(a, b) \mid c$. Além disso, se (x_0 , y_0) é qualquer solução particular da equação, então todas as outras soluções são dadas por

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t, \tag{1.3}$$

t inteiro.

Prova: Do teorema 3**,** sabe-se que existem inteiros x e y tais que $d = ax + by$. Se $d \mid c$, então existe k inteiro satisfazendo $c = kd$, de modo que $c = akx + bky$, e (kx, ky) é solução da equação. Por outro lado, se (x_0 , y_0) é uma solução da equação, então $ax_0 + by_0 = c$. Se $d = \text{MDC}(a, b)$, existem inteiros r e s tais que $a = dr$ e $b = ds$, com $\text{MDC}(r, s) = 1$. Portanto $drx_0 + dsy_0 = c$, o que implica $d \mid c$.

Se (x, y) denota uma outra solução qualquer da equação, então é possível escrever

$$ax + by = ax_0 + by_0 = c,$$

ou, eliminando o fator comum d,

$$r(x - x_0) = s(y_0 - y),$$

de modo que, como r e s são relativamente primos, então $s \mid (x - x_0)$ e $r \mid (y_0 - y)$, o que leva diretamente a $x = x_0 + st$ e $y = y_0 - rt$ para t inteiro e (1.3) segue. ■

Aplicando o resultado acima diretamente à congruência linear $ax \equiv c \pmod{n}$, é fácil ver que a mesma só admite solução se e só se d = MDC(a, n) | c e, se x_0 é uma solução particular da congruência, as soluções incongruentes módulo n são da forma $x = x_0 + (n/d)t$, em que $t = 0, 1, ..., d-1$. Assim, o número de soluções incongruentes, módulo n, é igual a d. Uma consequência imediata desse resultado é que se MDC(a, n) = 1, então a congruência tem uma única solução módulo n.

Um caso de interesse especial ocorre quando $c = 1$. A congruência torna-se $ax \equiv 1 \pmod{n}$, e x é dito ser o inverso multiplicativo, módulo n, de a (denota-se $x = a^{-1} \pmod{n}$). Os resultados acima mostram que uma CNS para que o inteiro a tenha inverso multiplicativo módulo n é que MDC(a, n) = 1. Claramente, se o inverso existe, então ele é único.

Exemplo 1.5: A Tabela 1.3 a seguir mostra os inversos multiplicativos dos inteiros módulo 11, ou seja, os inteiros x tais que $ax \equiv 1 \pmod{11}$. Observe que os elementos a=1 e a =10 satisfazem à condição $a = a^{-1}$.

Tabela 1.3. Inversos multiplicativos módulo 11.

a	1	2	3	4	5	6	7	8	9	10
$a^{-1} \pmod{11}$	1	6	4	3	9	2	8	7	5	10

■

Os conceitos apresentados até agora são suficientes para construir o que foi um dos primeiros criptossistemas de chave pública propostos pela comunidade científica, o chamado criptossistema da mochila (*knapsack*), discutido no Capítulo 2. Embora tendo sido quebrado desde 1984, esse sistema é muito útil para ilustrar os principais elementos presentes num criptossistema de chave pública, além de ter outras aplicações na área de segurança de dados.

Exemplo 1.6: Resolva a congruência linear $8x \equiv 12 \pmod{20}$.

Solução: Resolver a congruência significa encontrar todas as soluções incongruentes módulo n. Como MDC(8, 20) = 4 e 4|20, então a congrência tem exatamente 4 soluções incongruentes módulo 20. Considerando a solução particular $x_0 = 4$ (que pode ser encontrada por meio da equação diofantina $8x+20y = 12$), a solução geral tem a forma

$$x = x_0 + (n/d)t \pmod{20} = 4 + 5t \pmod{20},$$

que leva às soluções incongruentes (mod 20) x = 4, 9, 14 e 19. Note que podemos também cancelar o fator comum c = 4 na congruência dada, e então resolver a congruência

$$2x \equiv 3 \pmod{20/\text{MDC}(4, 20)}$$

ou

$$2x \equiv 3 \pmod{5}.$$

1.4 - ALGUMAS APLICAÇÕES

1.4.1 - O Cadastro de Pessoa Física

O cadastro de pessoa física (CPF) de um contribuinte é composto por onze algarismos, em que os dois últimos são dígitos de paridade, chamados dígitos verificadores, criados a partir dos nove primeiros. O cálculo dos dois dígitos verificadores é feito em duas etapas, uma para cada dígito, utilizando-se aritmética módulo 11. Denotando por DV1 e DV2 o primeiro e o segundo dígito verificador, respectivamente, tem-se

i) Computando DV1: se P_1 denota o vetor ponderador (10, 9, 8, 7, 6, 5, 4, 3, 2), então

$$\text{DV1}=\begin{cases}0, \text{ se } \ v\cdot P_1(mod\ 11)<2,\\ 11-v\cdot P_1(mod\ 11),\ caso\ contrário,\end{cases}$$

em que $v\cdot P_1$ denota o produto escalar entre o vetor v, formado pelos nove primeiros dígitos do CPF e o vetor ponderador P_1.

ii) Computando DV2: se P_2 denota o vetor ponderador (11, 10, 9, 8, 7, 6, 5, 4, 3, 2), então

$$\text{DV2}=\begin{cases}0, \text{ se } \ v'\cdot P_2(mod\ 11)<2,\\ 11-v'\cdot P_2(mod\ 11),\ caso\ contrário,\end{cases}$$

em que v' denota o vetor, de dez componentes, formado pela justaposição dos nove primeiros dígitos do CPF com o primeiro dígito verificador. Para ilustrar o procedimento considere a criação de um CPF a partir dos nove dígitos componentes do vetor $v=(1\ 2\ 0\ 4\ 5\ 0\ 7\ 8\ 1)$. As Tabelas 1.4 e 1.5 a seguir, mostram os cálculos para a determinação dos dígitos verificadores DV1 e DV2, respectivamente.

Tabela 1.4. Cálculo do primeiro dígito verificador

v	1 2 0 4 5 0 7 8 1
Vetor ponderador P_1	10 9 8 7 6 5 4 3 2
Produto escalar	10 + 18 + 0 + 28 + 30 + 0 + 28 + 24 + 2 =140 ≡ 8 (*mod* 11)
DV1	3

Tabela 1.5. Cálculo do segundo dígito verificador

v'	1 2 0 4 5 0 7 8 1 3
Vetor ponderador P_2	11 10 9 8 7 6 5 4 3 2
Produto escalar	11 + 20 + 0 + 32 + 35 + 0 + 35 + 32 + 3 + 6 = 174 ≡ 9(*mod* 11)
DV2	2

Portanto, o CPF em questão é 120450781-32. ■

1.4.2 - O Código de Barras UPC

Muitos sistemas de identificação empregam códigos numéricos baseados em aritmética modular. Esses sistemas são largamente usados em livros, placas de carro, talões de cheque, produtos em um supermercado, etc. Um exemplo de um sistema desse tipo é o bem conhecido código de barras UPC (do inglês, Universal Product Code), que associa a um produto um número de 12 dígitos $\boldsymbol{a} = (a_1, a_2, a_3, ..., a_{12})$, em que a_{12} é um dígito verificador, calculado de modo que o produto escalar $\boldsymbol{a} \bullet \boldsymbol{v} \equiv 0 \pmod{10}$, em que $\boldsymbol{v} = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ é chamado vetor ponderador. Esse sistema detecta todos os erros de digitação envolvendo um único dígito. Isto ocorre porque se o código $\boldsymbol{a}$ é digitado erroneamente, com um erro na posição i, $1 \le i \le 12$, como $\boldsymbol{a}' = (a_1, a_2, a_3, ... a_i+k, ..., a_{12})$, $1 \le k \le 9$, então o sistema computa

$$\boldsymbol{a}' \bullet \boldsymbol{v} = 3a_1 + a_2 + 3a_3 + ... + 3(a_i+k) + ...+ a_{12} = \boldsymbol{a} \bullet \boldsymbol{v} + 3k \equiv 3k \pmod{10}.$$

Estamos supondo, sem perda de generalidade, que o erro ocorreu numa posição ímpar. Neste caso, se $k \neq 0$, então $3k \ (mod\ 10) \neq 0$ e o erro é detectado. Por outro lado, se o erro ocorreu numa posição par, resulta em $\boldsymbol{a}' \bullet \boldsymbol{v} \equiv k \ (mod\ 10)$ de modo que, como anteriormente, se $k \neq 0$, o erro é detectado.

O esquema de detecção de erros empregado pelo sistema UPC é capaz de detectar a maioria dos erros que envolvem a transposição de dígitos adjacentes, um dos tipos de erro mais frequentes nesse cenário (veja o problema 1.36).

Outras aplicações desse sistema são o padrão ISBN (do inglês *International Standard Book Number*) de identificação de livros, números de identificação de passagens aéreas, de cheques e de ordens de pagamento postal [Gallian 02].

1.5 - O TEOREMA CHINÊS DO RESTO

A solução de um sistema de congruências lineares requer o teorema chinês dos restos.

Teorema 8: Sejam $n_1, \ n_2, \ ....., \ n_r$ inteiros positivos tais que MDC($n_i, \ n_j$) =1, para i ≠ j. Então o sistema de congruências lineares

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &..... \\ x &\equiv a_r \pmod{n_r}, \end{aligned}$$

tem uma única solução módulo n, dada por $x = \sum_{i=1}^{r} a_i N_i x_i \pmod{n}$, em que $n = \prod_{i=1}^{r} n_i$, $N_i = (n/n_i)$ e x_i é solução da congruência $N_i x_i \equiv 1 \pmod{n_i}$. ■

Prova: Como $N_i \equiv 0 \pmod{n_j}$ para $i \neq j$, então a solução proposta no enunciado satisfaz $x \equiv a_i N_i x_i \pmod{n_i} \equiv a_i \pmod{n_i}$ e a mesma atende ao sistema de congruências lineares dado. Agora, se x e x' satisfazem

$$x \equiv a_i \equiv x' \pmod{n_i}, \quad i = 1, 2, \ldots\ldots, r,$$

então $n_i \mid (x - x')$. Como MDC(n_i, n_j) =1, então $n = (n_1\, n_2 \ldots\ldots n_r) \mid (x - x')$. Portanto $x \equiv x' \pmod{n}$ e a solução é única. ■

Exemplo 1.7: O inteiro x, $0 \leq x < 120$, que satisfaz simultaneamente às congruências $x \equiv 2(mod\ 3),\ x \equiv 5(mod\ 8)\ e\ x \equiv 4\ (mod\ 5)$, pode ser computado por meio de

$$x = (a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3)(mod\ n),$$

em que $n = 120,\ a_1 = 2,\ a_2 = 5,\ a_3 = 4,\ N_1 = 40,\ N_2 = 15\ e\ N_3 = 24;\ \ x_1,\ x_2\ e\ x_3$ são, respectivamente, soluções das congruências

$$40x_1 \equiv 1(mod\ 3),$$
$$15x_2 \equiv 1(mod\ 8),$$
$$24x_3 \equiv 1(mod\ 5).$$

O resultado é $x = 989\ (mod\ 120) = 29$. ■

Exemplo 1.8: Determine, por meio do teorema chinês dos restos, os dois menores inteiros positivos que satisfazem à congruência $13x \equiv 17(mod\ 42)$.

Solução: A congruência dada é equivalente ao sistema de congruências

$$13x \equiv 17(mod\ 2),$$
$$13x \equiv 17(mod\ 3),$$
$$13x \equiv 17(mod\ 7),$$

que pode ser reescrito na forma

$$x \equiv 1(mod\ 2),$$
$$x \equiv 2(mod\ 3),$$
$$6x \equiv 3(mod\ 7).$$

Eliminando o fator 6 na última congruência (para isso basta multiplicar ambos os lados da congruência pelo inverso multiplicativo de 6, módulo 7, que é igual a 6), resulta em $x \equiv 4(mod\ 7)$. Resolvendo, pelo teorema chinês dos restos, o sistema de congruências resultante, chega-se a $x \equiv 11(mod\ 42)$. Então, os inteiros pedidos são 11 e 53. ■

O teorema chinês do resto, assim denominado por ser um resultado já conhecido na antiguidade (no século 1) pelos matemáticos chineses, tem aplicações em Criptografia, na subárea denominada compartilhamento de segredo (*secret sharing*) [Iftene 07], em Codificação de Canal [Goldreich 00] e em Processamento Digital de Sinais, na concepção

de algorimos rápidos para a computação de transformadas discretas como a de Fourier. Tais algoritmos são denominados genericamente de algoritmos FFT (do inglês *Fast Fourier Transform*) [Blahut 10].

PROBLEMAS

1.1) Prove que $\sum_{i=0}^{n} C_n^i = 2^n$.

1.2) Prove, por indução, que para todo n inteiro positivo,
a) $1+3+5+.....+(2n-1)=n^2$.
b) $1^3+2^3+3^3+.....+n^3=[\frac{n(n+1)}{2}]^2$.

1.3) Prove que o quadrado de um número inteiro quando dividido por 4 deixa resto 0 ou 1.

1.4) Prove que MDC(a, b) = MDC(a, ax+b).

1.5) Se g = MDC(a, b), encontre inteiros x e y satisfazendo $g = ax + by$, quando: i) a = 1819, b = 3587. ii) a = 243, b = 198. iii) a = 729, b = 1245.

1.6) Encontre x e y inteiros satisfazendo: a) $43x + 64y = 1$. b) $243x + 198y = 18$.

1.7) Prove que se $a^n - 1$ é primo (a>0, $n \geq 2$), então a = 2 e n é primo.

1.8) Os inteiros da forma $F_n = 2^{2^n} + 1,\ n \geq 0$, são chamados números de Fermat. Se F_n é primo, então é dito ser um primo de Fermat. Calcule F_n para n = 0, 1, 2, 3, 4 e verifique sua primalidade. F_n é primo para todo n ? F_p tem aplicações semelhantes a M_p.

1.9) Considere a classe de inteiros pares positivos E = {2, 4, 6, 8,....}, juntamente com a operação de multiplicação usual. Dê exemplos de números primos e números compostos em E. O teorema 4 é verdadeiro para esse sistema? Por quê?

1.10) Prove que:
a) O quadrado de qualquer inteiro é da forma 3k ou 3k+1.
b) O quadrado de qualquer inteiro ímpar é da forma 8k+1.

1.11) Prove que MDC(a, b) x MMC(a, b) = ab.

1.12) Prove que se $d \mid n$, então $(2^d-1) \mid (2^n-1)$.

1.13) Prove que a série dos números primos é infinita.

1.14) Prove que se $a \equiv b \pmod{p}$ e $a \equiv b \pmod{q}$, então $a \equiv b \pmod{pq}$, em que p e q são primos distintos. Generalize para inteiros quaisquer n_1 e n_2 (no lugar de p e q).

1.15) Divida 200 em duas parcelas tais que uma é divisível por 7 e outra por 11.

1.16) Determine o resto da divisão por 7 de: a) 2^{50}. b) 41^{65}.

1.17) Encontre as soluções incongruentes de: a) $6x \equiv 15 \pmod{21}$. b) $10x \equiv 4 \pmod{16}$.

1.18) Considere um criptossistema de chave secreta em que um símbolo de texto claro, cuja posição no alfabeto é x, é cifrado no símbolo cuja posição é $f(x) = kx \pmod{n}$, em que $n = 27$ e a posição 26 corresponde ao espaço em branco. Sabendo que o símbolo de texto claro D corresponde ao símbolo de texto cifrado M, decifre o criptograma HZERHU.

1.19) Se os inteiros a e b são escolhidos aleatoriamente nos conjuntos {1,....,14} e {0,....,14}, respectivamente, qual é a probabilidade que a congruência linear $ax \equiv b \pmod{15}$ tenha: i) Pelo menos uma solução. ii) Exatamente uma solução?

1.20) Encontre o menor inteiro $a > 2$ tal que $2 \mid a$, $3 \mid (a + 1)$, $4 \mid (a + 2)$ e $5 \mid (a + 3)$.

1.21) Determine o menor inteiro positivo x satisfazendo às congruências: $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{3}$ e $x \equiv 5 \pmod{7}$.

1.22) Prove que as congruências $x \equiv a \pmod{n}$ e $x \equiv b \pmod{m}$ admitem uma solução simultânea se, e somente se, $\text{MDC}(n,m) \mid (a-b)$. Se a solução existir, mostre que ela é única módulo mmc(n, m).

1.23) Após a divisão, em partes iguais, de uma herança de x moedas de ouro entre 10 herdeiros, restaram 3 moedas. Descobriu-se então que um dos participantes não tinha direito à herança e, após uma nova divisão em partes iguais, restou uma única moeda. O impasse foi resolvido quando dois herdeiros decidiram se retirar do grupo e então uma divisão exata pôde ser feita. Qual o número mínimo de moedas da herança?

1.24) Encontre as soluções incongruentes, módulo 210, do sistema de congruências: $2x \equiv 3 \pmod{5}$, $4x \equiv 2 \pmod{6}$, $3x \equiv 2 \pmod{7}$.

1.25) Prove que se $x \equiv a \pmod{n}$, então $x \equiv a \pmod{2n}$ ou $x \equiv (a + n) \pmod{2n}$.

1.26) Prove que se $ca \equiv cb \pmod{n}$, então $a \equiv b \pmod{(n/d)}$, em que $d \triangleq \text{MDC}(c, n)$.

1.27) Se n é o produto de dois números primos distintos, quantas soluções tem a congruência $x^2 \equiv a \pmod{n}$? Por quê?

1.28) Resolva, sem usar busca exaustiva, as congruências: i) $x^2 \equiv 9 \pmod{28}$. ii) $x^2 \equiv 44 \pmod{70}$.

1.29) Use o teorema chinês do resto para resolver a congruência $19x \equiv 1 \pmod{140}$.

1.30) Resolva a congruência quadrática $x^2 \equiv 8x \pmod{35}$.

1.31) Encontre todas as soluções da congruência linear $3x - 7y \equiv 11 \pmod{13}$.

1.32) Insira os números 0, 1, 2, ..., n-1 nos arranjos indicados a seguir. O inteiro i, $0 \leq i \leq n-1$, deve ocupar no arranjo a posição (i_1, i_2), em que $i_1 = i \ (mod\ n_1)$, $i_2 = i \ (mod\ n_2)$ e $n = n_2 n_1$.

a) $n_1 = 3,\ n_2 = 2$:

	0	1	2
0			
1			

b) $n_1 = 4,\ n_2 = 3$:

	0	1	2	3
0				
1				
2				

c) $n_1 = 8,\ n_2 = 2$:

	0	1	2	3	4	5	6	7
0								
1								

d) $n_1 = 7,\ n_2 = 3$:

	0	1	2	3	4	5	6
0							
1							
2							

1.33) Usando o sistema da questão anterior, é possível inserir todos os inteiros da sequência 0, 1, 2, ..., 429, 430, 431, em um arranjo de dimensões 16 x 27? É certo que dois inteiros da lista acima nunca vão ocupar a mesma posição no arranjo? Por quê?

1.34) Dado qualquer inteiro positivo k, prove que existem k inteiros consecutivos, todos divisíveis por um quadrado perfeito maior que 1. Ilustre sua prova para o caso k =3.

1.35) No sistema UPC descrito na seção 1.4.2, considere que o vetor ponderador é da forma $\boldsymbol{v}$ = (w, 1, w, 1, w, 1, w, 1, w, 1, w, 1). Que outros valores podem ser usados para w, além daquele indicado anteriormente (w=3)?

1.36) Um erro muito comum no cenário descrito na seção 1.4.2 é a transposição de dois dígitos adjacentes. Existem erros desse tipo que não possam ser detectados por esse código de barras? Quais?

1.37) Para proteger a transmissão de números de telefone de oito dígitos, dois dígitos de paridade, $a_9 \, e \, a_{10}$, são anexados, de modo que o número transmitido $N = (a_1 \, a_2 .....a_8 \, a_9 \, a_{10})$ satisfaz $\sum_{i=1}^{10} a_i \equiv 0 \, (mod \, 11)$ e $N \bullet v \equiv 0 \, (mod \, 11)$, em que $\bullet$ denota produto escalar e $v = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10)$. Em qual telefone será recebido o número 2126851056?

1.38) Algumas companhias aéreas usam aritmética modular para calcular dígitos de paridade em números de identificação de suas passagens. Considere um esquema em que apenas um dígito de paridade (a_{10}) é acrescentado a um número com nove dígitos $N = a_1 a_2 ....a_9$, em que $a_{10} = N (\mathrm{mod}\, 7)$. Esse esquema é capaz de detectar qualquer erro de digitação envolvendo apenas um único dígito? Por quê?

1.39) Aritmética modular é frequentemente usada para acrescentar um dígito extra a números de identificação, com o objetivo de descobrir erros de digitação ou falsificações. Um exemplo é o ISBN (*International Standard Book Number*), usado para identificação de livros. O ISBN é um número de 10 algarismos $N = (a_1, a_2, ...a_9, a_{10})$ em que a_{10} é um dígito de paridade, calculado de modo que $(a_1, a_2, ...a_9, a_{10}) \bullet$ (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)(mod 11) = 0. Quando o valor calculado de a_{10} é 10, ele é substituído pelo símbolo X.

a) O ISBN 0618122141 é válido?

b) O ISBN 0669039254 é o resultado da transposição de dois dígitos adjacentes, não envolvendo o primeiro ou o último dígito. Determine o ISBN correto.

1.40) Quantos números tem a maior sequência de inteiros positivos compostos? Por quê?

1.41) O serviço postal americano do norte usa ordens de pagamento identificadas por 11 dígitos, em que o décimo primeiro algarismo é um dígito de paridade, calculado por $a_{11} = N (\mathrm{mod}\, 9)$, com $N = a_1 a_2 ....a_9 a_{10}$. Esse esquema é capaz de detectar qualquer erro de digitação envolvendo apenas um único dígito? Por quê? A ordem de pagamento de número $OP = 39559881642$ é válida? É possível computar a_{11} fazendo uma única operação numa máquina de calcular que realiza apenas as quatro operações (+, -, /, $*$)? É necessário calcular a divisão $(N/9)$ para encontrar a_{11}?

REFERÊNCIAS

[Apostol 10] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer Undergraduate Texts in Mathematics, 2010.

[Burt 10] D. M. Burton, *Elementary Number Theory*, McGraw-Hill, 7a. edição, 2010.

[Blahut 10] R. E. Blahut, *Fast Algorithms for Signal Processing*, Cambridge University Press, 2010.

[Caldwell 11] C. K. Caldwell, *The Largest Known Prime by Year: A Brief History* http://primes.utm.edu/notes/by_year.html, acesso em 26/08/2011.

[Camp 98] R. M. Campello de Souza, H. M. de Oliveira e A. N. Kauffman, Trigonometry in Finite Fields and a New Hartley Transform, *Proceedings of the 1998 International Symposium on Information Theory*, p. 293, Cambridge, MA, Aug. 1998.

[Camp 01] R. M. Campello de Souza, H. M. de Oliveira, L. B. E. Palma e M. M. Campello de Souza, Hartley Number Theoretic Transforms, *Proceedings of the 2001 International Symposium on Information Theory*, p. 247, Washington, June 2001.

[Camp 09] R. M. Campello de Souza, E. S. V. Freire and H. M. de Oliveira, Fourier Codes, *Proceedings of the Tenth International Symposium on Communication Theory and Applications, ISCTA'09*, pp. 370-375, Ambleside, Lake District, UK, 2009.

[Camp 11] R. M. Campello de Souza, R. M. C. de Britto e H. M. de Oliveira, Códigos de Hartley, aceito para apresentação no *XXIX Simpósio Brasileiro de Telecomunicações – SBrT 2011*, Curitiba, 02-05 de outubro de 2011.

[Cassels 10] J. W. S. Cassels, A. Fröhlich (Editores), *Algebraic Number Theory*, 2a. edição, London Mathematical Society, 2010.

[Gallian 02] J. A. Gallian, Contemporary Abstract Algebra, Houghton Mifflin Company, 2002.

[Goldreich 00] O. Goldreich, D. Ron and M. Sudan, Chinese Remaindering with Errors, *IEEE Transactions on Information Theory*, Vol. 46, No. 4, pp. 1330-1338, July 2000.

[Gauss 01] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer Verlag, 1986 (a edição original é de 1801).

[GIMPS 11] *Great Internet Mersenne Prime Search (GIMPS) - Finding World Record Primes Since 1996*, http://www.mersenne.org/default.php, acesso em 26/08/2011.

[Hardy 40] G. H. Hardy and C. P. Snow, *A mathematician´s Apology*, Canto, 2001 (reimpressão da edição original, publicada pela Cambridge University Press em 1940).

[Iftene 07] S. Iftene, General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting, *Electronic Notes in Theoretical Computer Science (ENTCS)*, vol. 186, pp. 67–84, July 2007.

[McClellan 79] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*, Prentice-Hall, 1979.

[Merk 78] R. Merkle e M. Hellman, Hiding Information and Signatures in Trapdoor Knapsacks, *IEEE Transactions on Information Theory*, Vol. IT-24(5), pp. 525-530, Sept. 1978.

[Papa 94] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1995.

[Pol 71] J. M. Pollard, The Fast Fourier Transform in a Finite Field, *Mathematics of Computation*, vol. 25, No. 114, pp. 365-374, April 1971.

[Primachar] *Finding primes & proving primality* http://primes.utm.edu/prove/, acesso em 26/08/2011.

[PriMersenne 11] *Mersenne Primes: History, Theorems and Lists*, disponível em http://primes.utm.edu/mersenne/index.html, acesso em 26/08/2011.

[Primaior 11] *The Largest Known Primes*, disponível em http://primes.utm.edu/largest.html, acesso em 18/08/2011.

[Riesel 94] H. Riesel, *Prime Numbers and Computer Methods for Factorization (Progress in Mathematics)*, 2a. edição, Birkhäuser, 1994.

[Saut 08] M. du Sautoy, *A Música dos Números Primos – A história de um problema não resolvido na matemática*, Zahar, 2008.

[Simmons 92] G. J. Simmons (editor), *Contemporary Cryptology The Science of Information Integrity*, IEEE press, 1992.

[Singh 05] S. Singh, *O Último Teorema de Fermat – A história da busca épica para resolver o maior problema de matemática de todos os tempos*, Record, 2004.

[Stallings 07] W. Stallings, *Criptografia e Segurança de Redes*, Pearson Prentice-Hall, 2007.

2

O PEQUENO TEOREMA DE FERMAT

"And perhaps posterity will thank me for having shown it that the ancients did not know everything." — Fermat

2.1 – INTRODUÇÃO


Pierre de Fermat

O matemático francês Pierre de Fermat (17 de Agosto de 1601- 12 de Janeiro de 1665) é considerado o pai da Teoria dos Números. Fermat era formado em direito e atuava como juiz na cidade de Toulouse, onde ocupava o cargo de ouvidor-geral. Com o passar do tempo ele se tornou um magistrado muito conceituado, tendo chegado à posição de conselheiro do rei no Parlamento de Toulouse. Seu interesse por matemática iniciou após os 30 anos de idade, como um passatempo. Na época, matemática era sinônimo de estudos envolvendo os números inteiros e o juiz Fermat não querendo ter seu nome associado ao que poderia ser considerado apenas como uma brincadeira inconsequente, simplesmente não publicava os resultados que obtinha como fruto de suas investigações. Nas palavras do próprio Fermat, *"mesmo que o meu trabalho seja julgado merecedor de publicação, não quero que o meu nome apareça nele*" [Singh 97]. O acesso aos trabalhos de Fermat se deu por meio dos comentários que ele escrevia nas margens dos livros que usava e das cartas que enviava para outros matemáticos.

Fermat esteve profundamente envolvido na fundação de outras áreas da matemática, tais como o Cálculo Infinitesimal, a Geometria Analítica e o Cálculo das Probabilidades. Influenciado pela leitura de uma cópia da *Arithmetica* de Diofanto, traduzida do grego por Claude de Bachet (1591-1639), Fermat conheceu as propriedades e as relações entre os números inteiros, que o atraíram e fascinaram, levando-o a iniciar o desenvolvimento do que hoje chamamos de Teoria dos Números.

Neste capítulo, duas contribuições importantes de Fermat à Teoria dos Números são examinadas, a saber, o chamado pequeno teorema de Fermat e seu método de fatoração de inteiros. Além disso, é apresentado também o teorema de Wilson e uma aplicação sua à solução de um tipo especial de congruência quadrática. Tal congruência relaciona-se à existência da unidade imaginária j em uma aritmética módulo p, em que p é um primo ímpar. Estes resultados foram usados na definição de uma nova transformada

digital, a transformada de Hartley de corpo finito [Camp 98, 99] e na concepção de novos sistemas de multiplexação, de acesso múltiplo e de espalhamento espectral [Oliveira 99, 2000].

2.2 - O PEQUENO TEOREMA

O projeto de alguns dos mais importantes modernos criptossistemas de chave pública requer o uso de números primos com mais de 150 dígitos decimais. O chamado pequeno teorema de Fermat é uma ferramenta útil que auxilia na busca de tais números.

Teorema 2.1 (O pequeno teorema de Fermat): Se p é um número primo que não divide o inteiro a, então

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

Prova: Considere os p-1 múltiplos de a,

$$a, 2a, 3a, ..., (p\text{-}1)a;$$

esses múltiplos são incongruentes módulo p, pois se

$$ra \equiv sa \pmod{p},$$

em que $1 \le r, s \le p$-1, então, como MDC(a, p) =1, o fator comum a pode ser cancelado, resultando em

$$r \equiv s \pmod{p},$$

o que só é possível se $r = s$. Dessa forma os múltiplos de a são congruentes, em alguma ordem, aos inteiros 1, 2, 3, ..., p-1, ou seja,

$$a \equiv b_1 \pmod{p},$$

$$2a \equiv b_2 \pmod{p},$$

$$3a \equiv b_3 \pmod{p},$$

$$\vdots$$

$$(p\text{-}1)a \equiv b_{p\text{-}1} \pmod{p},$$

em que os inteiros b_1, b_2, b_3, …, $b_{p\text{-}1}$ representam alguma ordenação de todos os p-1 elementos de Z_p^*, o conjunto dos inteiros módulo p sem o elemento zero. Multiplicando membro a membro estas p-1 congruências, obtém-se

$$a.2a.3a....(p-1)a \equiv 1.2.3....(p-1) \pmod{p},$$

ou

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p};$$

como MDC((*p*-1)!, *p*) = 1, pode-se cancelar o fator (*p*-1)! chegando-se ao resultado desejado. ■

Uma decorrência imediata do Teorema 1 é dada pelo corolário 1 a seguir.

Corolário 2.1: Se *p* é primo, então $a^p \equiv a \pmod{p}$ para qualquer inteiro *a*.

Prova: Se $p \mid a$, o resultado é imediato, pois a congruência dada resume-se simplesmente à $a^p \equiv a \equiv 0 \pmod{p}$. Caso contrário, isto é, se MDC(*a*, *p*) = 1, pode-se usar o pequeno teorema de Fermat para escrever $a^{p-1} \equiv 1 \pmod{p}$. Multiplicando-se ambos os membros por *a*, o resultado é obtido. ■

Exemplo 1: Para qualquer inteiro a mostre que $a^9 \equiv a(mod\ 30)$.
Solução: A congruência dada é equivalente ao sistema

$$\begin{cases} a^9 \equiv a(mod\ 2), \\ a^9 \equiv a(mod\ 3), \\ a^9 \equiv a(mod\ 5). \end{cases}$$

Agora usamos o corolário 1 para cada uma das congruências:
i) Para $p = 2$, temos $a^2 \equiv a(mod\ 2)$; elevando ao expoente 4, vem $a^8 \equiv a^4 \equiv a^2 \equiv a(mod\ 2)$. Multiplicando por a obtém-se o resultado desejado.
ii) Para $p = 3$, temos $a^3 \equiv a(mod\ 3)$; elevando ao expoente 3, vem $a^9 \equiv a^3 \equiv a(mod\ 3)$.
iii) Para $p = 5$, temos $a^5 \equiv a(mod\ 5)$; Multiplicando por a^4 obtém-se $a^9 \equiv a^5 \equiv a(mod\ 5)$.
Portanto, como as três congruências são verdadeiras, está provado que $a^9 \equiv a(mod\ 30)$ para qualquer inteiro *a*. ■

2.2.1 – Um auxílio na busca por números primos grandes

Alguns dos modernos sistemas de criptografia de chave pública requerem a utilização de números primos com uma quantidade de dígitos decimais que pode variar entre 150 a 300. Um exemplo bem conhecido dessa situação é o criptossistema RSA, que emprega aritmética módulo *n*, em que *n* é o produto de dois números primos, distintos, dessa ordem.

O pequeno teorema de Fermat pode ser usado como um auxílio na busca de números primos grandes, pois de acordo com o mesmo, a condição $a^{N-1} \equiv 1 \pmod{N}$ é uma condição necessária para que *N* seja primo. Portanto, um teste de composição simples pode ser aplicado ao inteiro *N*, da seguinte forma:

i) Escolhe-se um inteiro *a* (chamado a base) satisfazendo MDC(*a*, *N*) =1.

ii) Calcula-se o valor de $f = a^{N-1} \pmod{N}$. Se $f \neq 1$, então o inteiro *N* é composto. Caso contrário ($f = 1$), *N pode ser* primo, e então

iii) Escolhe-se um inteiro *b* (outra base) satisfazendo MDC(*b*, *N*) =1 e repete-se o passo *i*).

Quando o valor de *f* em (*ii*) é igual a 1, diz-se que *N* passou no teste de composição de Fermat na base a. Claro, números primos sempre passam no teste. Quando um número composto passa no teste de Fermat para uma certa base, diz-se que o mesmo é um *pseudoprimo* de Fermat na dada base.

Exemplo 2: $N = 341$ é um pseudoprimo (o menor) de Fermat na base $a = 2$, pois $2^{340} \equiv 1 \pmod{341}$. Porém, um teste com a base $b = 3$, resulta em $3^{340} \pmod{341} \neq 1$, revelando que 341 é um número composto. De fato, $341 = 11 \times 31$. ■

O teste de Fermat é usado como parte de uma estratégia para a determinação de números primos grandes. Dentre possíveis inteiros *N* candidatos a números primos, muitos terão sua natureza composta facilmente identificada quando forem submetidos à sucessivas aplicações do teste, em várias bases, e poderão, então, ser descartados. Os inteiros que passaram nos testes, poderão então ter sua primalidade determinada por meio de um teste de primalidade [AKS 00], [Weisstein 11].

2.2.2 – Pseudoprimos absolutos

Existem números cuja natureza composta não pode ser determinada por um teste de composição de Fermat. Tais números, que são chamados *pseudoprimos absolutos* ou números de Carmichael, são pseudoprimos de Fermat para todas as bases. Foi o matemático Robert Daniel Carmichael (March 1, 1879 – May 2, 1967) que verificou, em 1910, que o inteiro $N = 561$ passava em um teste de composição de Fermat em qualquer base. Foi o nascimento e o batismo dos números de Carmichael.

Definição 2.1: Um número de Carmichael é um inteiro da forma $N = p_1 p_2 \ldots p_r$, em que os p_i são primos distintos tais que $(p_i - 1) | (N - 1)$. ■

Proposição 2.1: Um número de Carmichael é um pseudoprimo de Fermat em qualquer base.

Prova: Considere a base a tal que $\text{MDC}(a, N) = 1$. Então, pelo PTF, podemos escrever

$$a^{p_i - 1} \equiv 1 (mod p_i),\ i = 1, 2, \ldots, r. \qquad (1)$$

Como $(N - 1) = k_i (p_i - 1)$ para algum inteiro k_i, $i = 1, 2, \ldots, r$, ao elevarmos a congruência (1) ao expoente k_i, obtemos

$$a^{N-1} \equiv 1 (mod p_i),\ i = 1, 2, \ldots, r. \qquad (2)$$

Como os p_i são primos distintos, a equação (2) é equivalente à

$$a^{N-1} \equiv 1 (mod (p_1 p_2 \ldots p_r)),\ i = 1, 2, \ldots r, \qquad (3)$$

de modo que $a^{N-1} \equiv 1 (mod N)$ e o inteiro *N* passa no teste de composição de Fermat na base *a*. ■

Exemplo 3: O inteiro $N = 561$ é um número de Carmichael (o menor deles), porque fatora como o produto de três primos distintos, 561 = 3.11.17, que satisfazem 3 – 1 = 2 e 2 | 560, 11 – 1 = 10 e 10 | 560 e 17 – 1 = 16 e 16 | 560. ■

A Tabela 2.1 a seguir mostra todos os números de Carmichael menores do que 100000. Como se pode observar, os números de Carmichael tendem a ocorrer de forma cada vez mais espaçada. Por exemplo, existem *apenas* 2163 que são menores que 25000000000 (ou $25x10^9$) e 246683 menores que 10000000000000000 (ou 10^{16}) [Caldwell 2011]. Entretanto, essa tendência à *rarefação* não significa que não existem mais números de Carmichael a partir de certo limite. De fato, em 1994, os matemáticos W. R. Alford, A. Granville e C. Pomerance provaram que existem infinitos números de Carmichael [Alford. 94].

Tabela 2.1 - Os 16 números de Carmichael menores do que 100000.

561 = 3.11.17
1105 = 5.13.17
1729 = 7.13.19
2465 = 5.17.29
2821 = 7.13.31
6601 = 7.23.41
8911 = 7.19.67
10585 = 5.29.73
15841 = 7.31.73
29341 = 13.37.61
41041 = 7.11.13.41
46657 = 13.37.97
52633 = 7.73.103
62745 = 3.5.47.89
63973 = 7.13.19.37
75361 = 11.13.17.31

2.2.3 – O criptossistema Pohlig-Hellman

Em 1978, Pohlig e Hellman propuseram um novo criptossistema de chave secreta baseado na computação de exponenciais módulo p [Pohl 78]. Denotando por M e C a mensagem a ser cifrada e o correspondente criptograma, respectivamente, o algoritmo de cifragem nesse criptossistema consiste em computar C por meio da exponencial modular

$$C = M^e (mod\ p),$$

em que e, M e C são todos números inteiros $\in Z_p$. Para decifrar o criptograma C e encontrar a mensagem M é suficiente computar

$$M = C^d (mod\ p),$$

em que o inteiro d é solução da congruência linear $ed \equiv 1(mod\ (p-1))$. Se p é conhecido então a mensagem pode ser decifrada, de modo que esse é um criprossistema

de chave secreta e os inteiros e e p são secretos, sendo do conhecimento apenas dos usuários que desejam trocar informação de forma sigilosa.

O criptossistema de Pohlig-Hellman pertence à classe das chamadas cifras exponenciais. Um dos mais importantes esquemas desse tipo, em uso comercial hoje em dia (setembro 2011), é o criptossistema RSA, que é discutido no capítulo 3. Os dois sistemas são muito parecidos, porém o RSA emprega como módulo um inteiro n que é o produto de dois primos distintos. Essa *pequena* mudança fez uma grande diferença e o RSA é um dos mais bem sucedidos criptossistemas de chave pública [Stallings 07].

2.3 - O TEOREMA DE WILSON

Foi o estudante de matemática inglês John Wilson (1741-1793) quem primeiro encontrou o resultado apresentado nesta seção. Não conseguindo provar o mesmo, Wilson solicitou ajuda de seu orientador (Edward Waring), que também não obteve sucesso. Uma prova completa para o resultado foi dada finalmente por Lagrange, em 1773. O teorema de Wilson, como ficou conhecido, é uma ferramenta útil que auxilia na solução de alguns tipos de congruências quadráticas.

Teorema 2.2 (O Teorema de Wilson): O inteiro p é um número primo se e só se

$$(p-1)! \equiv -1 \pmod{p}.$$

Prova: *i*) Considere a congruência linear $ax \equiv 1\ (mod\ p)$, em que p é número primo e $1 \leq a \leq p-1$. Os únicos valores de a para os quais temos $x = a$ são $a = 1$ e $a = p-1$, uma vez que, nesse caso, a congruência torna-se $a^2 \equiv 1\ (mod\ p)$, ou seja $(a-1)(a+1) \equiv 0\ (mod\ p)$, de modo que ou $(a-1) \equiv 0\ (mod\ p)$ ou $(a+1) \equiv 0\ (mod\ p)$, o que leva ao resultado mencionado. Portanto, considerando os demais valores de a, (a saber, $a = 2, 3, \ldots, p-2$, são $p-3$ valores), podemos grupá-los em duplas (a_1, a_2), em que $(a_1 \neq a_2)$, satisfazendo à congruência, isto é, $a_1 a_2 \equiv 1(mod\ p)$. Existirão $(p-3)/2$ tais congruências (veja o Exemplo 3); multiplicando-se membro a membro estas congruências, obtemos $2.3 \ldots (p-2) \equiv 1(mod\ p)$, ou seja, $(p-2)! \equiv 1(mod\ p)$ e o resultado segue.

ii) Por outro lado, considere que $(n-1)! \equiv -1(mod\ n)$, ou seja, $n|((n-1)!+1)$. Se n é composto, então existe um inteiro d, $1 < d < n$, tal que $d|n$. Como $d|(n-1)!$, isso implica que $d|1$, o que não é possível. Portanto n é primo e a prova está completa. ■

Exemplo 3: Com $p = 11$, seguindo-se os mesmos passos da prova do teorema de Wilson, obtemos as 4 congruências

$$2.6 \equiv 1(mod\ 11),$$
$$3.4 \equiv 1(mod\ 11),$$
$$5.9 \equiv 1(mod\ 11),$$
$$7.8 \equiv 1(mod\ 11).$$

Multiplicando-as, chega-se à $10! \equiv -1(mod\ 11)$, o teorema de Wilson para $p = 11$. ■

2.3.1 – Uma certa congruência quadrática

Uma congruência quadrática é uma expressão da forma

$$ax^2 + bx + c \equiv 0(mod\ n), \qquad (4)$$

em que n é um inteiro positivo maior do que 1 e $a, b, c \in Z_n$. A solução geral desse tipo de congruência não é objetivo desse texto e o leitor interessado pode consultar [Burt 10]. Aqui estamos interessados na congruência quadrática

$$x^2 + 1 \equiv 0(mod\ p), \qquad (5)$$

em que p é um primo ímpar (a solução para o caso em que $p = 2$ é trivial, $x = 1$). A congruência (5) é a versão, em uma aritmética módulo p, da equação $x^2 + 1 = 0$, que não tem solução no corpo dos reais. De fato, sua solução é $x = \pm\sqrt{-1} \triangleq \pm j$, a chamada unidade imaginária do corpo dos números complexos. Uma situação análoga ocorre em (5), em que chamamos, por analogia, de reais os elementos de Z_p. Para que seja possível definir o elemento $j(mod\ p)$, é preciso que a congruência não tenha solução em Z_p. A condição para que isso ocorra é estabelecida no teorema 2.3.

Teorema 2.3: A congruência $x^2 + 1 \equiv 0(mod\ p)$, em que p é um primo ímpar, tem solução se e só se $p \equiv 1(mod\ 4)$.

Prova: *i*) $\exists\ solução \Rightarrow p \equiv 1(mod\ 4)$: Considere que o inteiro $x = a$ é uma solução da congruência. Do pequeno teorema de Fermat podemos escrever

$$(a^2)^{(p-1)/2} \equiv 1(mod\ p),$$

de modo que

$$(-1)^{(p-1)/2} \equiv 1(mod\ p),$$

o que implica que $(p-1)/2$ é par e portanto $p \equiv 1(mod\ 4)$.

i) $\exists\ solução \Leftarrow p \equiv 1(mod\ 4)$: nesse caso o resultado pode ser obtido com o auxílio do teorema de Wilson,

$$1.2 \ldots i \ldots (p-3)(p-2)(p-1) \equiv -1(mod\ p).$$

Como $(p-1)$ é par, o produtório nessa expressão pode ser separado em duas partes, ou seja,

$$\left[1.2.3 \ldots i \ldots \tfrac{p-1}{2}\right]\left[\tfrac{p+1}{2} \ldots (p-i) \ldots (p-3)(p-2)(p-1)\right] \equiv -1(mod\ p);$$

como $(p-i) \equiv -i(mod\ p)$, isso é o mesmo que (note que i varia de 1 a $\frac{p-1}{2}$)

$$(-1)^{\frac{p-1}{2}}((\tfrac{p-1}{2})!)^2 \equiv -1(mod\ p)$$

e, como $p \equiv 1(mod\ 4)$, chegamos a

$$((\tfrac{p-1}{2})!)^2 + 1 \equiv 0(mod\ p)$$

de modo que a congruência tem solução, a saber, $x = \left(\frac{p-1}{2}\right)!$. ■

Como consequência do teorema 2.3, quando o número primo p satisfaz $p \equiv 3(mod\ 4)$, existe a estrutura formada por números da forma $(a + jb)$, em que a e $b \in Z_p$ e j, um elemento que não $\in$ a Z_p, é raiz da congruência linear $x^2 + 1 \equiv 0(mod\ p)$. O leitor interessado, e que ainda não sabe onde se encontra o elemento j, certamente descobrirá que $j \in GF(p^2)$, uma estrutura algébrica denominada o campo de Galois de ordem (número de elementos) p^2, em homenagem ao célebre matemático francês Évariste Galois (outubro 1811 – maio 1832). A expressão campo de Galois significa a mesma coisa que corpo finito (o corpo dos reais é infinito). Em geral, um campo de Galois é denotado por $GF(q)$, sendo q uma potência de um número primo, $q = p^m$, m inteiro ≥ 1 [McEliece 87]. Por analogia com os números complexos, os elementos de $GF(p^2)$ são denominados complexos módulo p. Os primos p satisfazendo $p \equiv 3(mod\ 4)$ são denominados primos de Hartley [Kauffman 00].

Exemplo 4: $GF(7^2)$ é um corpo finito cujos elementos podem ser representados na forma complexa $(a + jb)$, em que a e $b \in Z_7$, o conjunto dos inteiros módulo 7. A aritmética (adição e multiplicação) nesse campo de Galois é a mesma dos números complexos usuais. Assim, $(2 + j5)(3 + j6) \equiv (4 + j6)(mod\ 7)$. Observe que, na aritmética módulo 7, o número complexo $(2 + j5)$ tem módulo igual a 1. ■

2.5 - O MÉTODO DE FATORAÇÃO DE FERMAT

Desde o surgimento do criptossistema RSA, as pesquisas por algoritmos eficientes para se fatorar um inteiro da forma $n = pq$ se intensificaram. A concepção de um tal algoritmo que encontrasse os fatores p e q em um tempo polinomial teria um grande impacto na área de segurança de dados, uma vez que significaria a quebra daquele criptossistema e o consequente colapso nas atividades de comércio eletrônico na internet, por exemplo.

O primeiro procedimento sistemático para se determinar todos os números primos até um certo valor N foi o chamado crivo de Eratosthenes, que data de cerca de 250 a.C. [Burt 10]. Esse crivo é essencialmente um procedimento de busca exaustiva, em que os múltiplos $2p, 3p, 4p, \ldots$, de todos os primos $p \leq \sqrt{N}$, são descartados da lista de inteiros $2, 3, 4, \ldots, N$. Os números primos são aqueles inteiros que permanecem na lista quando todos os primos até $\sqrt{N}$ forem usados. Embora a palavra *sieve*, nesse contexto, seja traduzida como crivo, um de seus significados é *peneira*. Assim, os primos são aqueles que permaneceram na peneira, após o processo de eliminação.

Para se testar a primalidade de um inteiro N é suficiente dividi-lo por todos os fatores primos até $\sqrt{N}$, ou seja, todos os primos entre 2 e $\sqrt{N}$ são testados como possíveis fatores de N. Caso nenhum tal fator seja encontrado, então N é um número primo. Claro, o processo requer uma lista dos primos existentes no intervalo especificado. Esse procedimento, assim como o crivo de Eratosthenes, embora simples de implementar, é computacionalmente ineficiente mesmo para valores moderados de N.

O primeiro avanço significativo em relação ao problema de se determinar os fatores de um número foi dado por Fermat, em 1643. O algoritmo de fatoração de Fermat, como é conhecido, é baseado na observação de que é possível encontrar dois fatores do inteiro N simplesmente encontrando-se as soluções inteiras da equação $(r^2 - s^2) = N$, pois, nesse caso, N admite a fatoração

$$N = (r + s)(r - s).$$

Por outro lado, se $N = ab$, é possível expressar N como uma diferença de quadrados resolvendo o sistema

$$r + s = a,$$
$$r - s = b,$$

para obter

$$r = \frac{a + b}{2},$$

e

$$s = \frac{a - b}{2},$$

de modo que

$$N = (\tfrac{a+b}{2})^2 - (\tfrac{a-b}{2})^2.$$

Para determinar os inteiros r e s parte-se da expressão $r^2 - N = s^2$ e testam-se valores para r até que a diferença $(r^2 - N)$ seja um quadrado perfeito. Claro, o primeiro valor de r a ser usado é o menor inteiro que torna esta diferença não negativa. O procedimento requer um número finito de passos e, no pior caso, o algoritmo termina em

$$(\tfrac{N+1}{2})^2 - N = (\tfrac{N-1}{2})^2,$$

que corresponde à fatoração trivial $N = N.1$ e indica que N é primo.

Exemplo 5: Para ilustrar seu método de fatoração, Fermat considerou a determinação dos fatores primos de $N = 2027651281$. Como $\sqrt{N} = 45029{,}449$ ..., o algoritmo inicia por $r = 45030$ e prossegue até que um quadrado perfeito seja encontrado, o que ocorre em 11 passos:

$45030^2 - 2027651281 = 2027700900 - 2027651281 = 46619,$

$45031^2 - 2027651281 = 2027790961 - 2027651281 = 139680,$

$45032^2 - 2027651281 = 2027881024 - 2027651281 = 229743,$

$45033^2 - 2027651281 = 2027971089 - 2027651281 = 319808,$

$45034^2 - 2027651281 = 2028061156 - 2027651281 = 409875,$

$45035^2 - 2027651281 = 2028151225 - 2027651281 = 499944,$

$45036^2 - 2027651281 = 2028241296 - 2027651281 = 590015,$

$45037^2 - 2027651281 = 2028331369 - 2027651281 = 680088,$

$45038^2 - 2027651281 = 2028421444 - 2027651281 = 770163,$

$45039^2 - 2027651281 = 2028511521 - 2027651281 = 860240,$

$45040^2 - 2027651281 = 2028601600 - 2027651281 = 950319$,

$45041^2 - 2027651281 = 2028691681 - 2027651281 = 1040400 = 1020^2$.

Chega-se então à fatoração $N = 2027651281 = (45041 + 1020)(45041 - 1020) = 46061 \cdot 44021$. Os fatores 46061 e 44021 são primos. ■

Os 11 passos executados no Exemplo 5 devem ser comparados com as 4580 divisões pelos primos ímpares até 44021, que são necessárias para fatorar N testando-se todos os primos entre 2 e $\sqrt{N}$ como possíveis fatores de N. Nem sempre a comparação é tão favorável assim, mas o exemplo mostra que não é necessário se conhecer todos os primos até $\sqrt{N}$ para fatorar N.

Algumas etapas do algoritmo podem ser aceleradas, tal como a computação da raiz quadrada de $(r^2 - N)$ [Riesel 94]. Os dois últimos dígitos de um quadrado perfeito são 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96. Assim, dos resultados indicados no Exemplo 5, é preciso extrair a raiz quadrada apenas dos números 499944 e 1040400.

A complexidade computacional do algoritmo de fatoração de Fermat é proibitiva para fatorar os inteiros que são empregados nos modernos criptossistemas de chave pública. De qualquer forma, é correto afirmar que o algoritmo de Fermat é tão mais eficiente quanto mais próximos estiverem os fatores de N.

PROBLEMAS

2.1) É verdade que, se p é primo, então $(a+b)^p \equiv (a^p + b^p) \pmod{p}$? Por quê?

2.2) Encontre os primos p tais que $p \mid (2^p + 1)$.

2.3) Construa uma tabela com os inteiros n e 2^n -2, onde n >1, e estabeleça uma proposição que indique em que caso n é primo. Tente provar ou disprovar sua proposição.

2.4) Considere que p e q são primos ímpares distintos tais que (p -1) | (q -1). Prove que se MDC(a, pq) = 1, então $a^{q-1} \equiv 1 \pmod{pq}$.

2.5) Se p e q são primos distintos, prove que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

2.6) Mostre que os inteiros a e a^5 tem o mesmo dígito das unidades.

2.7) Prove que, para qualquer inteiro a, tem-se $a^{21} \equiv a \pmod{15}$.

2.8) Em alguns sistemas de espalhamento espectral e de múltiplo acesso baseados em tecnologia CDMA, emprega-se aritmética módulo p, onde p é um primo de Hartley, isto é, um primo que satisfaz $p \equiv 3 \pmod{4}$. Mostre que os primos de Hartley satisfazem $(\frac{p-1}{2})! \equiv \pm 1 \pmod{p}$.

2.9) Se p e q são primos distintos prove que, para qualquer inteiro a, $pq \mid (a^{pq} - a^p - a^q + a)$.

2.10) É verdade que, para todo inteiro a , tem-se $a^3 \equiv a \pmod{6}$? Por quê?

2.11) Sendo a um inteiro qualquer, qual das afirmativas a seguir é verdadeira? Por quê?
a) $a^{21} \equiv a \pmod{15}$. b) $a^7 \equiv a \pmod{42}$. c) $a^{13} \equiv a \pmod{3.7.13}$. d) $a^9 \equiv a \pmod{30}$.

2.12) O que é um pseudoprimo de Fermat na base a?

2.13) Usando o método de Fatoração de Fermat, encontre os fatores primos de 262145.

2.14) Usando o pequeno teorema de Fermat, responda se os seguintes números são compostos: i) 97. ii) 111. iii) 75.

2.15) É verdade que $a^p \equiv a \pmod{p}$, para quaisquer inteiros a e p primo? Por quê?

2.16) Mostre que se $p \neq 2$ é primo, então $2p \mid (2^{2p-1} - 2)$.

2.17) Mostre que se n é um pseudoprimo ímpar, então o número de Mersenne $M_n = 2^n - 1$ é um pseudoprimo.

2.18) É possível determinar a natureza composta dos inteiros $M = 2821$ e $N = 15841$ por meio de um teste de composição de Fermat? Por quê?

2.19) Mostre que se $(6t+1)$, $(12t+1)$ e $(18t+1)$, em que t é um inteiro positivo, são números primos, então $N = (6t+1)(12t+1)(18t+1)$ é um número de Carmichael.

2.20) O inteiro $2222^{5555} + 5555^{2222}$ é divisível por 7? Por quê? (Sugestão: calcule o valor de 1111 (mod 7)).

2.21) Mostre que $1835^{1910} + 1986^{2061} \equiv 0(mod\ 7)$.

2.22) Use o pequeno teorema de Fermat para encontrar o dígito das unidades de 3^{101}.

2.23) Por meio do pequeno teorema de Fermat, encontre a solução (uma fórmula para o valor de x) da congruência linear $ax \equiv c(mod\ p)$, em que p é primo e $MDC(a,p) = 1$.

2.24) Use o resultado do problema anterior para resolver as congruências: a) $6x \equiv 5(mod\ 11)$. b) $3x \equiv 17(mod\ 29)$.

2.25) Se p é um primo ímpar, mostre que $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots (p-1)^{p-1} \equiv -1(mod\ p)$.

2.26) Se p é um primo ímpar, mostre que $1^p + 2^p + 3^p + \cdots (p-1)^p \equiv 0(mod\ p)$.

2.27) Quais os zeros da função $f(n) = sen[\pi\frac{(n-1)!+1}{n}]$?

2.28) Para que valores de p a aritmética módulo p de números da forma $a+jb$, onde a, $b \in$ GF(p) e $j^2 \equiv$ -1 (mod p) "imita" a aritmética dos números complexos?

2.29) Se p é primo, prove que (p-1)! ≡ p-1 (mod 1+2+3+.....+ (p-1)).

2.30) Quantas soluções incongruentes módulo n, tem a congruência $x^2 \equiv -1 (\mathrm{mod}\, n)$, quando: i) n = 1105. ii) n é um inteiro ímpar tal que $\mu(n) = (-1)^r$ (note que não é necessário resolver a congruência para responder a questão).

2.31) Seja a um inteiro tendo ordem 3 módulo p. Determine: i) O valor da soma $a^2 + a + 1 (\mathrm{mod}\, p)$. ii) A ordem de ($a$+1).

2.32) Prove que o inteiro n >1 é primo se e somente se $(n-2)! \equiv 1 (\mathrm{mod}\, n)$.

2.33) Qual o resto da divisão de: a) 2(26)! por 29. b) 255! por 257.

2.34) Se p é um primo ímpar, mostre que $3^2.5^2.7^2 \ldots (p-2)^2 \equiv (-1)^{\left(\frac{p+1}{2}\right)}(mod\ p)$.

2.35) Se p é um primo ímpar, mostre que $2^2.4^2.6^2 \ldots (p-1)^2 \equiv (-1)^{\left(\frac{p+1}{2}\right)}(mod\ p)$.

2.36) Considerando a aritmética *complexa* módulo 7, encontre $z = (a + jb)$ tal que $|z| \equiv 1(mod\ p)$. Tais elementos são chamados unimodulares. Quantos elementos unimodulares existem em $GF(7^2)$?

2.37) Mostre que todo inteiro *N* composto possui um fator primo $p \leq \sqrt{N}$.

2.38) Fatore os inteiros:

a) 768899400345071.
b) 12314613185945546501.
c) 4567654321109879870666981.
d) 5029663432778929823513947953 71.

REFERÊNCIAS

[AKS 00] M. Agrawal, N. Kayal and N. Saxena, Primes is in P, *Annals of Mathematics* **160** (2), pp. 781–793, 2004.

[Alford 94] W. R. Alford, A. Granville and C. Pomerance, There are Infinitely Many Carmichael Numbers, *Annals of Mathematics* **139**, pp. 703-722, 1994

[Burt 10] M. Burton, *Elementary Number Theory*, McGraw-Hill, 5a. edição, 2010.

[Caldwell 2011], C. K. Caldwell, *Carmichael Number, The Prime Glosssary,* http://www.utm.edu/research/primes/glossary/CarmichaelNumber.html, acesso em 18/09/2011.

[Camp 98] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, Trigonometry in Finite Fields and a New Hartley Transform, *Proceedings of the 1998 International Symposium on Information Theory*, p. 293, Cambridge, MA, Aug. 1998.

[Camp 99] R.M. Campello de Souza, H.M. de Oliveira and A.N. Kauffman, The Hartley Transform in a Finite Field, *Revista da Sociedade Brasileira de Telecomunicações*, vol. 14, No. 1, pp. 46-54, June 1999.

[Camp 00] R. M. Campello de Souza, H. M. de Oliveira, L. B. E. Palma and M. M. Campello de Souza, Hartley Number Theoretic Transforms*, Proceedings of the 2001 International Symposium on Information Theory*, p. 247, Washington, June 2001.

[Denn 82] D. E. R. Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.
[Gauss 01] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer Verlag, 1986 (a edição original é de 1801).

[Kauffman 00] A Transformada de Hartley em um Corpo Finito e Aplicações, Dissertação de Mestrado, Programa de Pós-Graduação em Engenharia Elétrica, Departamento de Eletrônica e Sistemas, UFPE.

[McEliece 87] R. J. McEliece, *Finite Fields for Computers scientists and Engineers*, Kluwer, 1987.

[Merk 78] R. Merkle and M. Hellman, Hiding Information and Signatures in Trapdoor Knapsacks, *IEEE Transactions on Information Theory*, Vol. IT-24(5), pp. 525-530, Sept. 1978.

[Oliveira 99] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, Efficient Multiplex for Band-Limited Channels, *Proceedings of the 1999 Workshop on Coding and Cryptography – WCC*'99, pp. 235-241, Paris, Jan. 1999.

[Oliveira 2000] H. M. de Oliveira and R. M. Campello de Souza, Orthogonal Multilevel Spreading Sequence design, in: *Coding, Communications and Broadcasting*, Eds. P. G. Farrell, M. Darnell and B. Honary, Research Studies Press LTD., Hertfordshire, England, pp. 291-301, 2000.

[Papa 94] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1995.

[Pohl 78] S. Pohlig and M. Hellman, An improved Algorithm for Computing Logarithms over $GF(p)$ and its Cryptographic Significance, *IEEE Transactions on Information Theory*, Vol. IT-24(1), pp. 106-110, Jan. 1978.

[Pol 71] J. M. Pollard, The Fast Fourier Transform in a Finite Field, *Mathematics of Computation*, vol. 25, No. 114, pp. 365-374, April 1971.

[Riesel 94] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics, Birkhäuser, 1994.

[Saut 08] M. du Sautoy, *A Música dos Números Primos – A história de um problema não resolvido na matemática*, Zahar, 2008.

[Singh 97] S. *Singh, Fermat's Enigma – The Epic Quest to Solve the World's Greatest Mathematical Problem*, Walker and Company, 1997 (Existe uma versão em português: *O Último Teorema de Fermat*, Record, 1998)

[Stallings 07] W. Stallings, *Criptografia e Segurança de Redes*, Pearson Prentice-Hall, 2007.

[Weisstein 11] E. W. Weisstein, *AKS Primality Test,* in: MathWorld - A Wolfram Web Resource. http://mathworld.wolfram.com/AKSPrimalityTest.html, acesso em 18/09/2011.

3

FUNÇÕES ARITMÉTICAS

3.1 - INTRODUÇÃO


Leonard Euler

O matemático suiço Leonard Euler (15 de abril de 1707- 18 de setembro de 1783) foi o segundo mais prolífico escritor de Matemática de todos os tempos. Seu trabalho completo engloba 886 livros e artigos. A Euler devemos a notação $f(x)$ das funções (1734), os símbolos e para a base dos logaritmos naturais (1727), i para a raiz quadrada de -1 (1777), π para a relação entre o comprimento de uma circunferência e seu diâmetro, e $\sum$ para os somatórios (1755). Êle introduziu, também, as funções beta e gamma e ampliou as fronteiras da geometria analítica e da trigonometria, além de dar contribuições significativas à geometria, à teoria dos números e ao cálculo. Estudou mecânica, dinâmica dos fluidos, hidráulica, acústica, eletricidade, óptica, astronomia, música, teologia, anatomia e fisiologia. Euler propôs a solução para o famoso problema das pontes de Konigsberg e foi o fundador da teoria de grafos.

Tendo passado a maior parte de sua vida profissional entre a Academia Imperial Russa de Ciências em São Petersburgo (1727 a 1741 e 1766 a 1783) e a Academia de Ciências da Prússia (1741 a 1766), sediada em Berlim, alguns anos depois de seu retorno à Rússia Euler ficou completamente cego. Isso em nada reduziu sua capacidade de trabalho e seu ímpeto produtivo continuou intenso até a sua morte em 1783.

Dentre suas contribuiçoes à teoria dos números destacam-se a função aritmética e o teorema que levam seu nome. Ambas tem aplicações importantes em criptografia moderna, tendo sido usadas na concepção de um dos mais importantes criptossistema de chave pública em uso comercial atualmente, o criptossistema RSA [Stallings 07].

Neste capítulo, além da função de Euler, estudamos também a função de Moebius, cuja aplicações em Engenharia eletrônica estão na área de processamento digital de sinais.

3.2 - FUNÇÕES ARITMÉTICAS

Como preparação para o estudo das funções de Euler e de Moebius, duas funções aritméticas simples são apresentadas, visando familiarizar o leitor com algumas noções básicas relativas a essa classe de funções.

Definição 3.1: Chama-se *função aritmética* àquela função cujo domínio é o conjunto dos números inteiros positivos. ■

Dentre as mais simples funções aritméticas estão as funções $\tau(n)$ e $\sigma(n)$.

Definição 3.2: $\tau(n)$ denota o número de divisores positivos de n e $\sigma(n)$ a soma desses divisores. Assim,

$$\tau(n) = \sum_{d|n} 1$$

e

$$\sigma(n) = \sum_{d|n} \mathrm{d}.$$

■

É fácil ver que $\tau(n) = 2$ e $\sigma(n) = (n+1)$ se e só se n é primo. Em geral, mostra-se que se $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$ é a fatoração canônica de $n > 1$, em que os p_i, $i = 1, 2, \ldots, r$, são primos distintos, então [Burt 10]

a) $\tau(n) = (k_1 + 1)(k_2 + 1)\ldots\ldots(k_r + 1)$.

b) $\sigma(n) = (\frac{p_1^{k_1+1} - 1}{p_1 - 1})(\frac{p_2^{k_2+1} - 1}{p_2 - 1})\ldots\ldots\ldots(\frac{p_r^{k_r+1} - 1}{p_r - 1})$.

Exemplo 3.1: Os divisores de $n = 60 = 2^2 \cdot 3 \cdot 5$ são da forma $d = 2^{a_1} 3^{a_2} 5^{a_3}$, em que $a_1 = 0, 1, 2$, $a_2 = 0, 1$ e $a_3 = 0, 1$. Assim d assume os valores 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 e 60. Portanto $\tau(60) = 12$ e $\sigma(60) = 168$. ■

Definição 3.3: Uma função aritmética $f(n)$, não identicamente nula, é multiplicativa se $f(mn) = f(m)f(n)$, sempre que MDC(m, n) = 1. Quando isto acontece para quaisquer inteiros m, n, então $f(n)$ é dita ser uma função completamente multiplicativa. ■

Note que se $f(n)$ é multiplicativa, então $f(n) = f(n \cdot 1) = f(n)f(1)$ e, como $f(n) \neq 0$, tem-se que $f(1) = 1$. Além disso, considerando $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}$, então $f(n)$ pode ser calculada por meio de

$$f(n) = f(p_1^{k_1} p_2^{k_2} \ldots\ldots p_r^{k_r}) = f(p_1^{k_1}) f(p_2^{k_2}) \ldots\ldots f(p_r^{k_r}) = \prod_{i=1}^{r} f(p_i^{k_i}),$$

ou seja, o valor de uma função multiplicativa para um dado argumento n pode ser obtido a partir da fatoração de n.

Um procedimento sistemático para se provar a propriedade multiplicativa de uma função, é apresentado a seguir.

Teorema 3.2: Seja $f(n)$ uma função multiplicativa e seja

$$F(n) = \sum_{d|n} f(d).$$

Então $F(n)$ também é uma função multiplicativa. A prova é deixada como um exercício para o leitor [Burt 10]. ■

Uma decorrência imediata do teorema 3.2 é que as funções $\tau(n)$ e $\sigma(n)$ são funções multiplicativas. Um modo de mostrar isto é observar que estas funções são casos particulares da função

$$\sigma_k(n) = \sum_{d|n} d^k.$$

De fato, $\tau(n) = \sigma_0(n)$ e $\sigma(n) = \sigma_1(n)$ (veja a definição 3.2). Como as funções $f(n) = 1$ e $f(n) = n$ são multiplicativas, então as funções $\tau(n)$ e $\sigma(n)$ também são.

3.3 - A FUNÇÃO DE MÖBIUS


August Ferdinand Möbius

August Ferdinand Möbius (17 de novembro de 1790 - 26 de setembro de 1868) foi um matemático e astrônomo alemão. A ele se devem a fita de Möbius, seu trabalho mais conhecido, a função de Möbius, as transformações de Möbius e a fórmula de inversão de Möbius. Nesta seção estamos interessados na função de Möbius, uma função aritmética que veio a ter aplicações na Engenharia Eletrônica, na área de processamento digital de sinais, no final do século XX [Tufts 88], [Reed 90, 92], [Knock 94], [Cintra 2001].

Definição 3.4: Chama-se função de Möbius à função aritmética

$$\mu(n) = \begin{cases} 1, & se\ n = 1, \\ 0, se\ \exists p:\ p^2|n,\ \ p \text{ primo}, \\ (-1)^{\mathrm{r}}, \text{se } n = p_1 p_2 \ldots p_{\mathrm{r}}, \end{cases}$$

em que os p_i são primos distintos. ■

Essencialmente a definição da função de Möbius significa que $\mu(n) = 0$ se n tem um fator quadrático e $\mu(n) = (-1)^r$ se n é o produto de r primos distintos.

Exemplo 3.2: Se p é um número primo, então $\mu(p) = -1$ e $\mu(p^k) = 0$ para $k \geq 2$. A Tabela 3.1 mostra os valores de $\mu(n)$ para os dez primeiros inteiros positivos:

Tabela 3.1 – Alguns valores da função de Möbius.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

■

3.3.1 – Propriedades da função de Möbius

A função $\mu(n)$ apresenta algumas propriedades interessantes e que desempenham um papel importante em aplicações da mesma.

M1) A função de Möbius é multiplicativa.

Prova: O que queremos mostrar é que, se $\text{MDC}(m,n) = 1$ então $\mu(mn) = \mu(m)\mu(n)$. Sem perda de generalidade, vamos considerar que m e n não têm fatores quadráticos (em caso contrário, a expressão é trivialmente satisfeita resultando em $0 = 0$). Dessa forma, se $m = q_1 q_2 \dots q_s$ e $n = p_1 p_2 \dots p_r$, em que os q_i e p_j são todos primos distintos, podemos escrever

$$\mu(mn) = \mu(q_1 q_2 \dots q_s p_1 p_2 \dots p_r) = (-1)^{s+r}$$

e

$$\mu(mn) = (-1)^s(-1)^r = \mu(m)\mu(n).$$ ■

M2) Se n é um inteiro positivo, então

$$\sum_{d|n} \mu(d) = \begin{cases} 1, se\ n = 1, \\ 0, se\ n > 1. \end{cases}$$

Prova: Definindo a função

$$F(n) = \sum_{d|n} \mu(d),$$

tem-se, para $n = 1$,

$$F(1) = \textstyle\sum_{d|1} \mu(d) = \mu(1) = 1.$$

Do Teorema 3.2 podemos afirmar, uma vez que a função de Möbius é multiplicativa, que a função $F(n)$ é multiplicativa. Assim, considerando a fatoração canônica de n, $F(n)$ pode ser calculada por meio de $F(p^k)$ (veja o comentário após a Definição 3.3). Como

$$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k),$$

então

$$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) = 1 + (-1) = 0$$

e portanto

$$F(n) = \prod_{i=1}^{r} F(p_i^{k_i}) = 0.$$ ■

Exemplo 3.3: Para $n = 30$, temos

$$\sum_{d|30} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(5) + \mu(6) + \mu(10) + \mu(15) + \mu(30) =$$
$$= 1 - 1 - 1 - 1 + 1 + 1 + 1 - 1 = 0.$$

M3) Se $f(n)$ e $g(n)$ são funções aritméticas tais que

$$g(n) = \sum_{d|n} f(d),$$

então

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Esta é a bem conhecida fórmula de inversão de Möbius. A prova é deixada como um exercício para o leitor [Santos 98].

3.4 - A FUNÇÃO DE EULER

A função de Euler é provavelmente a função aritmética mais importante no contexto das aplicações em Engenharia Eletrônica.

Definição 3.5: A função de Euler, $\phi(n)$, representa o número de inteiros positivos $i, 1 \leq i < n$, que são relativamente primos com n, isto é, $\text{MDC}(i, n) = 1$. ■

Exemplo 3.4: Se p é um número primo, então $\phi(p) = p - 1$. De fato, $\phi(n) = n - 1$ se e só se n é primo. A Tabela 3.2 mostra os valores de $\phi(n)$ para os dez primeiros inteiros positivos:

Tabela 3.2 - Alguns valores da função de Euler.

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

■

3.4.1 – Propriedades da função de Euler

E1) Se p é um número primo e k é um inteiro positivo, então $\phi(p^k) = p^{k-1}(p-1)$.

Prova: Uma condição necessária e suficiente para que $\text{MDC}(i, p^k) = 1$ é que p não seja divisor de i. Assim, para contar quantos inteiros existem, entre 1 e p^k, que não são relativamente primos com p^k, basta contar quantos são os múltiplos de p nesse intervalo. Como existem p^{k-1} tais inteiros, o valor procurado é dado por

$$\phi(p^k) = p^k - p^{k-1}$$

e o resultado segue. ■

E2) A função de Euler é multiplicativa (a prova é deixada para o leitor) [Burt 10].

E3) Se a fatoração canônica de n é $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, então

$$\phi(n) = n \prod_{i=1}^{r} \frac{(p_i - 1)}{p_i} \qquad (3.1)$$

Prova: Das propriedades E1 e E2 podemos escrever

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1),$$

ou seja,

$$\phi(n) = \prod_{i=1}^{r} \frac{p_i^{k_i}(p_i - 1)}{p_i}$$

e, uma vez que $n = \prod_{i=1}^{r} p_i^{k_i}$, o resultado segue. ■

E4) $\phi(n)$ é par para $n > 2$.

Prova: O resultado é uma consequência imediata da propriedade E1. ■

Exemplo 3.5: Dado o valor de A na equação $\phi(n) = A$, determine o valor de n.

Solução: Há um procedimento sistemático, baseado na propriedade E3, para resolver esse tipo de equação. Reescrevendo a expressão (3.1) na forma

$$\frac{n}{\prod p_i} = \frac{\phi(n)}{\prod (p_i - 1)}, \qquad (3.2)$$

observa-se que os fatores primos p_i são tais que $(p_i - 1) | A$. Portanto, n pode ser determinado por meio dos passos:

i) Listam-se todos os divisores de A, que são os possíveis valores para $(p_i - 1)$.
ii) Da lista obtida no passo anterior, chega-se aos possíveis valores para p_i.
iii) Usando-se a expressão (3.2), testam-se os p_i candidatos, levando-se em conta que os mesmos fatores devem estar em ambos os lados da expressão.

Exemplo 3.6: Para ilustrar o procedimento, considere que $\phi(n) = 10$. Nesse caso, tem-se que $(p_i - 1)$ assume os valores 1, 2, 5 e 10, ou seja, os candidatos aos valores dos p_i são 2, 3, 6 e 11. Assim, a lista a que se refere o item (*ii*) é 2, 3 e 11. Testando esses valores, obtemos:

• $p_1 = 2; \frac{n}{2} = \frac{10}{1} = 10$ e nenhuma solução é gerada.

• $p_1 = 3; \frac{n}{3} = \frac{10}{2} = 5$ e nenhuma solução é gerada.

• $p_1 = 11; \frac{n}{11} = \frac{10}{10} = 1$ e $n = 11$ é uma solução.

• $p_1 = 2$ e $p_2 = 3$; $\frac{n}{2.3} = \frac{10}{1.2} = 5$ e nenhuma solução é gerada.

• $p_1 = 2$ e $p_2 = 11$; $\frac{n}{2.11} = \frac{10}{1.10} = 1$ e $n = 22$ é uma solução.

Os valores $p_1 = 3$ e $p_2 = 11$ produzem um valor não inteiro no lado direito da expressão (3.2) e não precisam ser testados. O mesmo acontece para $p_1 = 2$, $p_2 = 3$ e $p_3 = 11$. Assim, as soluções de $\phi(n) = 10$ são $n = 11$ e $n = 22$. ■

3.4.2 - O teorema de Euler

A primeira prova do pequeno teorema de Fermat foi estabelecida por Euler, em 1736. Cerca de 24 anos depois, Euler conseguiría generalizar este teorema, chegando ao resultado conhecido como teorema de Euler.

Teorema 3.3 (o teorema de Euler): Se os inteiros a e n são relativamente primos, então

$$a^{\phi(n)} \equiv 1(mod\ n). \qquad (3.3)$$

Prova: Os passos para se chegar à expressão (3.3) são essencialmente os mesmos usados na demonstração do pequeno teorema de Fermat. A diferença está que agora os $\phi(n)$ múltiplos inteiros de a, a saber, $a_1a, a_2a, a_3a \ldots a_{\phi(n)}a$ são considerados, em que MDC $(a_i, n) = 1$. O leitor é convidado a acrescentar os passos que faltam para a conclusão da prova. ■

Note que quando n é um número primo, a expressão (3.3) reduz-se ao pequeno torema de Fermat.

Exemplo 3.7: Para determinar o dígito das unidades de 3^{302} podemos partir do teorema de Euler com $n = 10$, uma vez que esse dígito (o das unidades) é igual a $n(mod\ 10)$. Assim, considerando que $3^{\phi(10)} \equiv 1(mod\ 10)$, ou $3^4 \equiv 1(mod\ 10)$, vem

$$3^{302} = (3^4)^{75}3^2 \equiv 9(mod\ 10)$$

e o dígito procurado é 9. ■

3.5 - O CRIPTOSSISTEMA RSA

Um dos principais criptossistemas de chave pública em uso comercial hoje em dia é o criptossistema RSA [Rivest 78]. A função unidirecional em que se baseia o RSA, proposta por D. Knuth em 1976, é a da fatoração de inteiros; dados os primos distintos p e q, ambos

com cerca de r dígitos, a complexidade multiplicativa para se computar o produto $n = pq$ é $O(r^2)$, enquanto que o problema da fatoração, isto é, a determinação dos primos p e q, a partir de n, requer uma complexidade multiplicativa exponencial! [Pieprzyk 10]. Baseado nessa função unidirecional, Ronald Rivest, Adir Shamir e Leonard Adleman, na época (1978) pesquisadores do Instituto de Tecnología de Massachussets (MIT), usando o teorema de Euler, introduziram um *trapdoor* nesse cenário e construiram o que é, até hoje, um dos mais bem sucedidos criptossistemas de chave pública.

No criptossistema RSA (ou algoritmo RSA, como também é chamado), mensagens e criptogramas são números inteiros positivos pertencentes a Z_n, o conjunto dos inteiros módulo n, em que n é o produto de dois números primos distintos *grandes*, p e q. O valor de n faz parte da chave pública do algoritmo e os valores de p e q definem a sua chave privada. Os procedimentos de cifragem e decifragem no RSA são explicados a seguir.

i) **Cifragem**

Para cifrar a mensagem M e obter o criptograma C, faz-se

$$C = M^e (mod\ n), \tag{3.4}$$

em que o inteiro e, chamado o expoente de cifragem, faz parte da chave pública que é, portanto, formada pelo par de inteiros (n, e).

i) **Decifragem**

Para expressar M em função de C, a partir da expressão (3.4), eleva-se ambos os membros dessa expressão a um expoente d, que é calculado a partir da congruência

$$ed \equiv 1\big(mod\ \phi(n)\big), \tag{3.5}$$

em que a condição necessária e suficiente para encontrarnos o valor de d é que MDC $(e, \phi(n)) = 1$. Chega-se então a

$$C^d = M^{ed} = M^{k\phi(n)+1} (mod\ n).$$

Agora entra em cena o teorema de Euler que nos permite escrever, se MDC$(M, n) = 1$,

$$M^{\phi(n)} \equiv 1 (mod\ n),$$

de modo que

$$C^d \equiv M (mod\ n),$$

o que leva à expressão de decifragem

$$M = C^d (mod\ n). \tag{3.6}$$

Embora a condição MDC$(M, n) = 1$ tenha sido usada para se chegar à decifragem, mesmo que isso não ocorra, é possível mostrar que o texto claro M ainda pode ser obtido pela expressão (3.6) (veja o problema 3.20). O expoente d é denominado expoente de

decifragem. Claro, o valor de d deve permanecer privado. Assim, podemos nos referir à chave privada do sistema como sendo o par de números primos distintos (p, q) ou o inteiro d.

Exemplo 3.8: Com $p = 5$ e $q = 11$, tem-se $n = 55$ e $\phi(n) = 40$. Escolhendo-se $e = 7$, a chave privada d é a solução da congruência

$$7d \equiv 1(mod\ 40),$$

ou seja, $d = 23$. A mensagem $M = 2$ é cifrada em $C = 2^7(mod\ 55) = 18$. Para decifrar C é suficiente computar $C^d(mod\ n) = 18^{23}(mod\ 55) = 2$. ■

3.5.1 – Assinaturas digitais

O conceito de assinatura digital é uma das mais importantes contribuições da criptografia de chave pública, introduzida em 1976 por Diffie e Hellman [Diffie, 76]. Como mensagem e criptograma são números inteiros $\in Z_n$, os algoritmos de cifragem e de decifragem representam automorfismos de Z_n em Z_n. Especificamente, se $E(.)$ e $D(.)$ representam esses algoritmos, definidos pelas expressões (3.4) e (3.6), respectivamente, então é verdade que $E\big(D(M)\big) = D\big(E(M)\big) = M$. Dessa forma, um número pode ser transformado em outro por qualquer das duas expressões e o que chamamos cifragem ou decifragem é arbitrário, ou seja, podemos obter C a partir de M usando qualquer um dos dois expoentes, e ou d. O que chamamos assinatura digital é o resultado de usarmos a expressão (3.4) com o expoente d. Nesse caso a expressão (3.6) é usada com o expoente e para verificar a assinatura. Portanto, as expressões para assinar uma mensagem e verificar a assinatura são, respectivamente

$$C = M^d(mod\ n) \tag{3.7}$$

e

$$M = C^e(mod\ n), \tag{3.8}$$

respectivamente. Como a chave privada d é do conhecimento apenas do usuário proprietário do sistema, seu uso para gerar a assinatura (a mensagem assinada) C o identifica. O usuário receptor da mensagem assinada, ao usar a expressão (3.8) para recuperar M, verifica (confirma) a identidade do emissor da mensagem, uma vez que as chaves (e, d) estão ligadas pela expressão (3.5) (numa aritmética $mod\ \phi(n)$ só há um par (e, d) satisfazendo a expressão).

3.5.2 – Pontos fixos do RSA

Definição 3.6: Uma mensagem M é dita ser um ponto fixo do RSA se satisfaz

$$C = M^e \equiv M(mod\ n).$$

Como $n = pq$, isso é o mesmo que

$$\begin{cases} M^e \equiv M (mod\ p), \\ M^e \equiv M (mod\ q); \end{cases} \tag{3.9}$$

pela propriedade **E4** da função de Euler e sabendo que MDC $(e, \phi(n)) = 1$, podemos afirmar que, para $n > 2$, o expoente e de cifragem é ímpar. Assim, três valores de M que satisfazem o sistema (3.9) são 1, 0 e -1. Isso significa que M pode ser determinado pelos sistemas

$$\begin{cases} M \equiv 0, 1, -1 (mod\ p), \\ M \equiv 0, 1, -1 (mod\ q), \end{cases}$$

o que leva a um total de 9 valores para M.

Exemplo 3.9: Para o RSA em que $p = 3$ e $q = 5$, as seguintes mensagens são pontos fixos:

1: $\begin{cases} M \equiv 0\ (mod\ 3), \\ M \equiv 0\ (mod\ 5), \end{cases} M = 0.$ **2:** $\begin{cases} M \equiv 0\ (mod\ 3), \\ M \equiv 1\ (mod\ 5). \end{cases} M = 6.$ **3:** $\begin{cases} M \equiv 0\ (mod\ 3), \\ M \equiv -1\ (mod\ 5). \end{cases} M = 9.$

4: $\begin{cases} M \equiv 1\ (mod\ 3), \\ M \equiv 0\ (mod\ 5). \end{cases} M = 10.$ **5:** $\begin{cases} M \equiv 1\ (mod\ 3), \\ M \equiv 1\ (mod\ 5). \end{cases} M = 1.$ **6:** $\begin{cases} M \equiv 1\ (mod\ 3), \\ M \equiv -1\ (mod\ 5). \end{cases} M = 4.$

7: $\begin{cases} M \equiv -1\ (mod\ 3), \\ M \equiv 0\ (mod\ 5). \end{cases} M = 5.$ **8:** $\begin{cases} M \equiv -1\ (mod\ 3), \\ M \equiv 1\ (mod\ 5). \end{cases} M = 11.$ **9:** $\begin{cases} M \equiv -1\ (mod\ 3), \\ M \equiv -1\ (mod\ 5). \end{cases} M = 14.$

■

É possível calcular o número exato de pontos fixos presentes em um criptossistema RSA, que é dado por [Pieprzyk, 10],

$$\#\text{PF} = [1 + \text{MDC}(e - 1, p - 1)][1 + \text{MDC}(e - 1, q - 1)]. \tag{3.10}$$

Nessa expressão, considerando que e, p e q são ímpares, podemos afirmar que cada MDC vale, no mínimo, 2; isso implica que todo RSA tem, pelo menos 9 pontos fixos, como havíamos demonstrado anteriormente.

A segurança do criptossistema RSA é baseada na dificuldade de fatorar o módulo $n = pq$. Implementações consideradas computacionalmente seguras usam valores de n cujo comprimento varia entre 1024 a 2048 bits, ou 309 a 617 dígitos decimais. Entretanto, não há uma prova de que para se criptoanalisar (*quebrar*) o RSA é necessário um esforço computacional igual ao da fatoração de n.

PROBLEMAS

3.1) Prove a fórmula de inversão de Möbius.

3.2) Prove que a função de Möbius é multiplicativa.

3.3) É verdade que, se k é um inteiro positivo, $\mu(k)\mu(k+1)\mu(k+2)\mu(k+3)=0$? Por quê?

3.4) Prove que, para qualquer inteiro $r > 0$, existe uma sequência de r inteiros consecutivos $a, a+1, \ldots, a+r-1$, satisfazendo $\mu(a) = \mu(a+1) = \cdots = \mu(a+r-1) = 0$.

3.5) Encontre o dígito das unidades e o dígito das dezenas de 3^{400}.

3.6) Considerando a fatoração $n = p_1^{k_1} p_2^{k_2} \ldots . p_r^{k_r}$, qual o valor das somas:
i) $\sum_{d|n} \mu(d)$. *ii)* $\sum_{d|n} |\mu(d)|$?

3.7) Considerando a fatoração prima $n = p_1^{k_1} p_2^{k_2} \ldots . p_r^{k_r}$, expresse, em termos de $f(p_i)$, o valor da soma $\sum_{d|n} \mu(d) f(d)$.

3.8) Qual o valor da soma $\sum_{d|n} \mu(d)/\phi(d)$? Por quê?

3.9) Mostre que $n = \sum_{d|n} \phi(d)$.

3.10) Se MDC(m, n) = 1, prove que $m^{\phi(n)} + n^{\phi(m)} \equiv 1 (\mathrm{mod}\, mn)$.

3.11) Para que valores de n tem-se $\phi(n^2) = n\,\phi(n)$? Justifique.

3.12) Para que valores de n tem-se $\phi(2n) = 2\phi(n)$? Justifique.

3.13) Apresente um procedimento sistemático para encontrar o valor de n na equação $\phi(n) = A$. Ilustre seu método para: *i*) $A = 16$. *ii*) $A = 20$.

3.14) Para que valores de p a equação $\phi(n) = 2p$, onde p é primo, tem solução? Por quê?

3.15) Use o teorema chinês dos restos para determinar um valor para n, inteiro positivo, satisfazendo $3\phi(n) = 2 (mod\ 2)$, $2\phi(n) = 1 (mod\ 3)$ e $4\phi(n) = 4 (mod\ 10)$.

3.16) Quantos inteiros n existem tais que $\phi(n) = n/4$?

3.17) Existe um número infinito de inteiros n tais que $\phi(n)$ é um quadrado perfeito? Por quê?

3.18) Encontre n tal que $\phi(n) = 14$.

3.19) Considere o problema de desenhar uma estrela regular de n pontas, sem tirar o lápis do papel. A estrela é construída partindo-se de um vértice arbitrário, saltando k-1 pontos e conectando os dois vértices e assim por diante. A figura abaixo ilustra o caso $n = 5$, $k = 2$.
i) Para um dado n, quantas estrelas diferentes podem será construídas?
ii) Para que valor(es) de n existem 6 estrelas diferentes?

3.20) Como você explica o fato de que, apesar do teorema de Euler, o criptossistema RSA é capaz de lidar com mensagens M tais que MDC (M, $\phi(n)$) > 1?

3.21) Se a chave pública de um usuário é o par $(e, n) = (31, 3599)$, qual sua chave privada?

3.22) Qual o valor da soma $\sum_{d|30030}[\mu(d)\phi(d)/d]$?

3.23) Em um criptossistema RSA com $n = 91$, a chave privada é solução do sistema de congruências lineares: $3x = 3(mod\ 4)$, $3x \equiv 6(mod\ 9)$ e $4x \equiv 6(mod\ 7)$. Determine a chave pública do sistema e assine a mensagem $M = 3$.

3.24) Se p é um primo ímpar, para que valores de n a equação $\mu(n) + \phi(n) = 2p$ tem solução? Por quê?

3.25) Se p é primo, prove que (p-1)! $\equiv p$-1 (mod 1+2+3+.....+ (p-1)).

3.26) Expresse, em termos dos fatores primos de n, o valor da soma $F(n) = \sum_{d|n}[\mu(d)\phi(d)\frac{1}{d}]$.
Para o caso em que n satisfaz $\mu(n) = 0$, expresse $F(n)$ em termos de n.

3.27) Quantas frações positivas irredutíveis menores que 1 e com denominador menor ou igual a n existem? Por quê?

3.28) Para que valores de n, $\phi(3^n - 1)$ é múltiplo de n? Justifique.

3.29) Encontre os valores de n satisfazendo $\mu(n) + \phi(n) = 18$.

3.30) Use o teorema chinês do resto para resolver a congruência $19x \equiv 1$ (mod 140).

3.31) Considerando n = 55, mostre como o criptossistema RSA pode ser usado para gerar assinaturas digitais. Assine a mensagem M = 4 e verifique a assinatura C = 2. Considere que a chave privada do sistema é a menor possível.

3.32) Quantas soluções incongruentes módulo n, tem a congruência $x^2 \equiv -1(\mathrm{mod}\, n)$, quando: *i*) $n = 1105$. *ii*) n é um inteiro ímpar tal que $\mu(n) = (-1)^r$ (note que não é necessário resolver a congruência para responder à questão).

3.33) Quantos inteiros positivos $i \leq 480$ existem, tais que MDC(i , 160) =1?

3.34) Quantos inteiros positivos $i \leq km$ existem, tais que MDC(i , m) =1?

3.35) Use o teorema chinês do resto para encontrar valores de *n* satisfazendo a congruência $59\phi(n) \equiv 1 (\mathrm{mod} 165)$.

3.36) Calcule o valor das somas: a) $\sum_{d|n} \mu(d)\phi(d)$, n par. b) $\sum_{d|n} (\mu(d)n/d)$.

3.37) Quantos inteiros n existem tais que $10|\phi(n)$?

3.38) Apresente os parâmetros de um criptossistema RSA (valores de *n*, *p*, *q*, *e*>1, *d*, $\phi(n)$) em que, para qualquer mensagem M, tem-se M = C. Justifique.

3.39) Resolva o sistema: $\phi^2(n) \equiv 4 (\mathrm{mod} 5)$, $\phi^2(n) \equiv 1 (\mathrm{mod}\, 6)$.

3.40) Qual a forma dos divisores primos ímpares do inteiro $n^2 + 1$?

3.41) Use o teorema chinês do resto para encontrar três inteiros pares consecutivos, *a*, *b* e *c*, tais que $\mu(a) + \mu(b) + \mu(c) = 0.$

3.42) Quantas triplas (*a*, *b*, c) de inteiros consecutivos existem tais que $\mu(\mathrm{a}) = \mu(\mathrm{b}) = \mu(\mathrm{c}) = 0$? Por quê?

3.43) Resolva a congruência quadrática $x^2 \equiv 8x (\mathrm{mod}\, 35)$.

3.44) Encontre três inteiros pares $x_i > 14$, tais que a equação $\phi(n) = x_i$, i=1, 2, 3, não tenha solução. Justifique.

3.46) Encontre o valor da soma S = $a_1 + a_2 ... + a_{\phi(n)}$, onde $1 \leq a_i \leq n$ e MDC $(a_i, n) = 1$.

3.47) Encontre, sem usar busca exaustiva, os valores de *n*, incongruentes módulo 17, que satisfazem a congruência $\phi^2(n) + \mu(n)\phi(n) - 4 \equiv 0 (\mathrm{mod}\, 17).$

3.48) Em Processamento Digital de Sinais algumas transformadas discretas tem comprimento N que são divisores do inteiro ($n^2 + 1$). Nesse caso é possível encontrar uma transformada com N =19? Por quê?

3.49) Encontre um valor para o inteiro *a*, composto, tal que $(\frac{1}{2})\mu(2a) + (\frac{1}{3})\mu(3a) + (\frac{1}{6})\mu(5a) = 1.$ Quantos valores de *a* existem satisfazendo essa equação? Justifique.

3.50) Considerando *k* > 0, encontre o valor de *n* na equação $\sum_{i=0}^{k} \phi(2^i n) = 28,$ para *n* ímpar.

3.51) Dado o inteiro a e considerando o número de multiplicações a ser realizadas, qual o melhor algoritmo para se computar o valor de a^{16}? E o valor de a^{11}?

3.52) O inteiro 65537 é uma escolha muito comum para o expoente de cifragem e. Você vê alguma razão para isso?

REFERÊNCIAS

[Burt 10] M. Burton, *Elementary Number Theory*, McGraw-Hill, 5a. edição, 2010.

[Cintra 01] *Transformada Rápida de Hartley: Novas Fatorações e um Algoritmo Aritmético*, Dissertação de Mestrado, Programa de Pós-Graduação em Engenharia Elétrica, UFPE.

[Diffie, 76] W. Diffie and M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol IT-2, pp. 644-654, November 1976.

[Knock 94] L. Knockaert, A generalized Möbius transform and arithmetic Fourier transforms, IEEE Transactions on Signal Processing, vol. 42, No. 11, pp. 2967-2971, Nov. 1994.

[Pieprzyk, 10] J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of Computer Security*, Springer, 2010.

[Reed 90] I. S. Reed, D. W. Tufts, Xiaoli Yu, T. K. Truong, M. T. Shih, and X. Yin, Fourier analysis and signal processing by use of the Möbius inversion formula, *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 38, No. 3, Mar. 1990.

[Reed 92] I. S. Reed, Ming-Tang Shih, T. K. Truong, E. Hendon, and D. W. Tufts, A VLSI architecture for simplified arithmetic Fourier transform algorithm, *IEEE Transactions on Signal Processing*, vol. 40, No. 5, pp. 1122-1133, May 1992.

[Rivest 78] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, February 1978.

[Santos 98] J. P. de Oliveira Santos, *Introdução à Teoria dos Números*, Coleção Matemática Universitária, IMPA, 1998.

[Stallings 07] W. Stallings, *Criptografia e Segurança de Redes*, Pearson Prentice-Hall, 2007.

[Tufts 88] D. W. Tufts and G. Sadasiv, The arithmetic Fourier transform*, IEEE Acoustics, Speech and Signal Processing* (*ASSP*) *Magazine*, pp. 13-17, Jan. 1988.

4

RAÍZES PRIMITIVAS

4.1 - INTRODUÇÃO

Nesse capítulo continuamos a lidar com congruências exponenciais. Dois conceitos muito importantes em teoria dos números são apresentados, a saber, as noções de ordem e raiz primitiva. Aplicações dos mesmos no contexto da matemática envolvem, por exemplo, a construção do polígono regular de 17 lados, por Gauss [Schroeder 97], e a análise da expansão de frações do tipo $1/p$, em que p denota um número primo.

No cenário da Engenharia essas idéias levam, por exemplo ao chamado problema do logaritmo discreto, que envolve uma função unidirecional que está no coração de alguns modernos sistemas de criptografia de chave pública.

Ainda nesse cenário, podemos citar as sequências numéricas construídas a partir de raízes primitivas, cuja transformada de Fourier apresenta propriedades de espalhamento espectral que as tornam atraentes no projeto de salas de concerto e de aeronaves cuja detecção por sonar ou radar é mais difícil.

Iniciamos introduzindo o conceito de ordem multiplicativa módulo n, após o que passamos a explorar procedimentos que permitam computar a ordem de um dado inteiro de modo eficiente, isto é, procedimentos que apresentem uma complexidade computacional menor que aquele que encontra o valor da ordem por uma busca exaustiva. Ao final do capítulo é descrito um protocolo para distribuição pública de chaves, que vem a ser um procedimento seguro para que dois usuários combinem uma chave a ser usada em um criptossistema de chave secreta.

4.2 - ORDEM MULTIPLICATIVA MÓDULO *n*

Definição 4.1: Dado um inteiro a e um módulo n, satisfazendo $MDC(a,n) = 1$, define-se a ordem multiplicativa de a (módulo n), como sendo o menor inteiro positivo l tal que $a^l \equiv 1\ (mod\ n)$. ■

Exemplo 4.1: Considerando $n = 7$ e o inteiro $a = 2$, temos $2^1 \equiv 2(mod\ 7)$, $2^2 \equiv 4(mod\ 7)$ e $2^3 = 8 \equiv 1(mod\ 7)$. Portanto $a = 2$ tem ordem $l = 3(mod\ 7)$. A Tabela 4.1 indica as ordens de todos os inteiros módulo 7:

Tabela 4.1 – A ordem multiplicativa dos inteiros módulo 7.

a	1	2	3	4	5	6
l	1	3	6	3	6	2

Observe que o inteiro $a = 6$ tem ordem $l = 2(mod\ 7)$. Em geral, o inteiro $a = n - 1$ tem ordem $l = 2(mod\ n)$, pois $(n-1)^2 = 1(mod\ n)$. ■

Teorema 4.1: Se o inteiro a tem ordem $l(mod\ n)$, então $a^h \equiv 1(mod\ n)$ se e só se $l|h$. Em particular, $l|\emptyset(n)$.

Prova: a) $l|h \rightarrow a^h \equiv 1(mod\ n)$.
Se $l|h$ então existe um inteiro j tal que $h = jl$, de modo que $a^h = a^{jl} = (a^l)^j \equiv 1(mod\ n)$, pois a tem ordem l.
b) $a^h \equiv 1(mod\ n) \rightarrow l|h$.
Escrevendo $h = ql + r$, $0 \leq r \leq l - 1$, tem-se $a^h = a^{ql+r} \equiv a^r \equiv 1(mod\ n)$, um absurdo pois a tem ordem l e $r < l$. Portanto, a única alternativa é $r = 0$ e $l|h$.
Por fim, considerando o teorema de Euler e fazendo $h = \emptyset(n)$, tem-se que $l|\emptyset(n)$. ■

Exemplo 4.2: As possíveis ordens dos inteiros módulo 11 são os divisores de $\emptyset(11) = 10$, isto é, $l = 1, 2, 5, 10$. Em particular, para o elemento $a = 2$, $2^2 \equiv 4(mod\ 11)$, $2^5 \equiv 10 \equiv -1(mod\ 11)$ e $a = 2$ tem ordem $l = 10(mod\ 11)$. ■

4.3 - RAÍZES PRIMITIVAS

Definição 4.2: Se o inteiro a tem ordem $l = \emptyset(n)(mod\ n)$, então é dito ser uma raiz primitiva de n (escreve-se aRPn). ■

Exemplo 4.3: *i*) Do exemplo 4.2, vê-se que 2RP11.
ii) Considerando as ordens dos inteiros módulo 9, verifica-se que $a = 2$ tem ordem $\emptyset(9) = 6$ e portanto 2RP9. Nesse caso, como o módulo não é um número primo, as potências de 2 geram os 6 elementos relativamente primos com 9, a saber, 1 2, 4, 5, 7 e 8. ■

O teorema a seguir mostra que é possível determinar as ordens dos elementos de Z_n, a partir do conhecimento de uma raiz primitiva de n.

Teorema 4.2: Se o inteiro a tem ordem $l(mod\ n)$, então a^h tem ordem, módulo n, dada por

$$ord(a^h) = \frac{l}{MDC(l,h)}. \qquad (4.1)$$

Prova: Se d denota o MDC(l, h), então existem inteiros r e s, tais que $l = dr$ e $h = ds$, com MDC$(r, s) = 1$. Portanto,

$$(a^h)^r = (a^{ds})^{l/d} = (a^l)^s \equiv 1(mod\ n).$$

Denotando por m a ordem de a^h, pode-se escrever, em função do teorema 4.1, que $m|r$. Pelo mesmo motivo, considerando que

$$a^{hm} = (a^h)^m \equiv 1(mod\ n),$$

pode-se afirmar que $l|hm$, ou seja, $dr|dsm$ e assim $r|sm$. Porém, como MDC$(r, s) = 1$, tem-se que, pelo lema de Euclides [Burton 10], que $r|m$. Considerando o resultado obtido anteriormente $(m|r)$, conclui-se que

$$m = r = \frac{l}{d} = \frac{l}{MDC(l,h)}.$$ ■

Exemplo 4.4: No exemplo 4.2 vimos que 2RP11**.** Usando esse resultado e o Teorema 4.2 é possível determinar as ordens dos inteiros módulo 11. Os resultados são mostrados na Tabela 4.2

TABELA 4.2 – Ordens dos elementos de Z_{11}.

h	2^h	Ordem$(2^h)(mod\ 11)$
0	1	1
1	2	10
2	4	5
3	8	10
4	5	5
5	10	2
6	9	5
7	7	10
8	3	5
9	6	10

■

No exemplo 4.4 observa-se que o inteiro $n = 11$ tem 4 raízes primitivas, a saber, 2, 6, 7, 8. Uma informação parcial importante sobre o número de raízes primitivas de n é dada pelo corolário 4.2.

Corolário 4.2: Se o inteiro n tem uma raiz primitiva, então o mesmo tem exatamente $\emptyset(\emptyset(n))$ raízes primitivas.

Prova: Considerando a expressão (4.2), com aRPn e $l = \emptyset(n)$, então a^h será uma outra raiz primitiva de n se, e só se, MDC $(\emptyset(n), h) = 1$. Portanto, o número de raízes primitivas de n corresponde ao número de inteiros h relativamente primos com $\emptyset(n)$, ou seja, $\emptyset(\emptyset(n))$. ■

Exemplo 4.5: Embora o corolário 4.2 indique que o inteiro $n = 15$ tem $\emptyset(\emptyset(15)) = 4$ raízes primitivas, o fato é que 15 não tem raiz primitiva. A explicação é que a prova do corolário requer a existência de uma raiz primitiva, o que não acontece nesse caso. Isso pode ser prontamente verificado computando-se as ordens dos $\emptyset(15) = 8$ inteiros relativamente primos com 15, a saber, 1, 2, 4, 7, 8, 11, 13, 14. As ordens encontradas são $l = 1, 2, 4$, não havendo nenhum elemento de ordem 8. ■

Mostra-se que os inteiros que tem raiz primitiva são $a = 2, 4$ ou são da forma p^k, ou $2p^k$, em que p é um primo ímpar e k é um inteiro positivo (note que $n = 15$ não é dessa forma). A prova desse resultado está fora do escopo destas notas de aula, mas o leitor interessado em conhecê-la pode consultar [Burton, 2010, p. 162]. Assim, claramente, vê-se que todo número primo tem raiz primitiva.

4.4 - O SISTEMA DE TROCA DE CHAVES DIFFIE-HELMANN

No artigo que introduziu a criptografia de chave pública, em 1976 [Diffie, 76], não foi proposto nenhum criptossistema desse tipo. Entretanto, baseando-se no conceito de função unidirecional, Diffie e Hellman, nesse mesmo artigo, construiram um procedimento por meio do qual dois usuários, A e B, podem combinar (trocar) uma chave usando um canal público (inseguro). Dados um primo p e uma raiz primitiva de p, α, a troca da chave se dá por meio dos passos descritos a seguir.

a) Para o usuário A:

i) A escolhe, aleatoriamente, um inteiro, privado, X_A, tal que $1 < X_A < p - 1$. Esse valor X_A é um parâmetro privado, conhecido apenas pelo usuário A.

ii) A calcula $Y_A = \alpha^{X_A}(mod\ p)$ e envia esse valor para B.

iii) A calcula $Y_B{}^{X_A}(mod\ p) = \alpha^{X_A X_B}(mod\ p) = K_{AB}$.

b) Para o usuário B:

i) B escolhe, aleatoriamente, um inteiro X_B, tal que $1 < X_B < p - 1$. Esse valor X_B é um parâmetro privado, conhecido apenas pelo usuário B.

ii) B calcula $Y_B = \alpha^{X_B}(mod\ p)$ e envia esse valor para A.

iii) B calcula $Y_A{}^{X_B}(mod\ p) = \alpha^{X_A X_B}(mod\ p) = K_{AB}$.

O número K_{AB} é a chave combinada. Vejamos um exemplo.

Exemplo 4.6: $\alpha = 3$ é uma raiz primitiva de $p = 17$. Então

- A escolhe $X_A = 3$ e B escolhe $X_B = 7$.
- A calcula $Y_A = \alpha^{X_A}(mod\ p) = 3^3(mod\ 17) = 10$ e envia para B.
- B calcula $Y_B = \alpha^{X_B}(mod\ p) = 3^7(mod\ 17) = 11$ e envia para A.
- A calcula $Y_B{}^{X_A}(mod\ p) = 11^3(mod\ 17) = 5$.
- B calcula $Y_A{}^{X_B}(mod\ p) = 10^7(mod\ 17) = 5$.

O valor $K_{AB} = 5$ é a chave combinada. ■

4.4.1 - A segurança do sistema Diffie-Hellman

Se um usuário não autorizado consegue descobrir o valor de X_A, então êle terá acesso à chave secreta combinada por A e B. Para tal, êle precisa encontrar X_A na equação

$$Y_A = \alpha^{X_A} (mod\ p),$$

em que α, p e Y_A são conhecidos (α e p são públicos e Y_A é transmitido por um canal público). Isso equivale a computar

$$X_A = \log_\alpha Y_A\ (mod\ p),$$

o logaritmo discreto ou logaritmo numérico (do inglês number- theoretic logarithm) de Y_A [Pieprzyk, 10], [Simmons, 92]. Para o parãmetro X_B a situação é a mesma. Quando p é da mesma ordem de grandeza do módulo n usado no RSA, a complexidade para se encontrar o logaritmo discreto é comparável à da fatoração de n. Êsse é o chamado "problema do logaritmo discreto" (PLD), uma função unidirecional cuja complexidade é uma função exponencial do módulo, p.

O PLD deu origem ao criptossistema do logaritmo discreto, proposto em 1985 por El Gamal [Gamal 85], o qual faz parte do padrão oficial de assinatura digital do governo americano (o DSS, do *inglês digital signature standard*).

Posteriormente, as mesmas idéias foram empregadas num contexto matemático diferente, o de curvas elípticas. Com a definição do logaritmo discreto sobre uma curva elíptica, foi criada a área de criptografia de curvas elípticas (ECC, do inglês *Eliptic Curve Cryptography*) [Hankerson 04].

PROBLEMAS

1) Prove que $\phi(2^n - 1)$ é múltiplo de n para qualquer $n>1$.

2) No conjunto Z_n^*, quantos elementos tem ordem $\phi(n)$? Quantos tem ordem d? Por que?

3) O número de dígitos (k) da parte periódica da expansão decimal de $1/p$, p um número primo ímpar diferente de 5, pode ser encontrado fazendo-se $\frac{1}{p} = \frac{r}{10^k}(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \frac{1}{10^{3k}} + ...)$. Usando seus conhecimentos sobre ordem multiplicativa módulo p, determine:
a) O valor máximo de k.
b) Os valores de k e r para $p = 13$.

4) Qual a condição para que a congruência exponencial $a^x \equiv b \pmod p$ tenha solução? Quantas soluções incongruentes módulo p existem? Por que?

5) Resolva, sem usar busca exaustiva, a congruência $10^x \equiv 28 \pmod{31}$.

6) Considere a construção de sequências de números inteiros usando aritmética módulo p, onde o i-ésimo termo da sequência é dado por $a_i = \alpha^i \pmod p,\ i \geq 0$ e $\alpha \in Z_p^*$.
a) Essas sequências são periódicas? Por que? Em caso positivo, qual seu período?
b) Com $p = 31$, é possível construir uma tal sequência com período 11? Por que?
c) Qual o menor valor de p capaz de produzir uma sequência com período 8? Quantas sequências desse tipo existem? Construa uma delas.

7) Sabendo que 3 tem ordem 16 (mod 17), encontre as raízes primitivas de 17.

8) Para quantos valores de b, incongruentes módulo p, a congruência $a^x \equiv b \pmod p$ tem solução (considere o valor de a fixo) ? Encontre esses valores quando $a = 9$ e $p = 13$. Em geral, considerando todos os valores de b, quantas soluções tem a congruência $a^x \equiv b \pmod p$? Justifique

9) Sabendo que 3 é uma raiz primitiva de 17, indique quantas soluções incongruentes cada uma das seguintes congruências tem: a) $x^{12} \equiv 16 \pmod{17}$. b) $x^{48} \equiv 9 \pmod{17}$. c) $x^{20} \equiv 13 \pmod{17}$. d) $x^{11} \equiv 9 \pmod{17}$. (Sugestão: $3^8 \equiv 16 \pmod{17}$; não é necessário resolver nenhuma das congruências). Justifique.

10) Raízes primitivas podem ser usadas no projeto de salas de concerto, para produzir uma distribuição de energia sonora mais uniforme. Para isso, o teto da sala deve ter um perfil

com degraus de altura $d_n = \frac{\lambda s_n}{p}$, onde λ é o comprimento de onda e s_n, n = 0, 1, ..., é uma sequência gerada por uma raiz primitiva α de p. Com p =17, qual a raiz primitiva (α) e a sequência (s_n) usadas, para um perfil de teto (em cm) d_n = 2, 6, 1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1,...? Considere a frequência de projeto f = 1 kHz e v_{som} = 340 m/s.

11) Bruno e Adriana usam o sistema Diffie-Hellman com $\alpha = 7$, escolhendo $X_A = 5$ e $X_B = 12$. Encontre valores possíveis para Y_A e Y_B. Qual a chave secreta combinada?

12) Seja a um inteiro tendo ordem 3 módulo p. Determine: i) O valor da soma $a^2 + a + 1 (\text{mod } p)$. ii) A ordem de ($a$+1).

13) Para quantos valores de b, incongruentes módulo 17, a congruência $10^x \equiv b (\text{mod} 17)$ tem solução ? Quais são esses valores? Justifique.

14) Dado que 3 é raiz primitiva de 50, encontre todos os inteiros positivos, menores que 50, tendo ordem 10 módulo 50.

15) O polinômio ciclotômico $C_l(x)$, com coeficientes em Z_p, é o polinômio mônico cujas raízes são os elementos de ordem l em Z_p. a) Qual a grau de $C_l(x)$? Em Z_7, encontre $C_6(x)$.

REFERÊNCIAS

[Burt 10] M. Burton, *Elementary Number Theory*, McGraw-Hill, 5a. edição, 2010.

[Diffie 76] W. Diffie and M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol IT-2, pp. 644-654, November 1976.

[Gamal 85] T. El Gamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol. IT-31, No. 4, pp. 469-472, July 1985.

[Hankerson 04] D. Hankerson, A. J. Menezes and S. vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.

[Pieprzyk 10] J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of Computer Security*, Springer, 2010.

[Rivest 78] R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, February 1978.

[Santos 98] J. P. de Oliveira Santos, *Introdução à Teoria dos Números*, Coleção Matemática Universitária, IMPA, 1998.

[Schroeder 97] M. R. Schroeder, *Number Theory in Science and Communication*, 3a. edição, Springer, 1997.

[Simmons 92] G. J. Simmons (editor), *Contemporary Cryptology The Science of Information Integrity*, IEEE press, 1992.

[Stallings 07] W. Stallings, *Criptografia e Segurança de Redes*, Pearson Prentice-Hall, 2007.

5

GRUPOS FINITOS

O duelo foi a pistola de 25 passos...

5.1 - INTRODUÇÃO


Évariste Galois

A teoria dos grupos é um dos ramos mais antigos e mais ricos da álgebra moderna, tendo dado seus primeiros passos na segunda metade do século 18 (~1770) quando o matemático italiano Joseph-Louis Lagrange (25 de janeiro de 1736 – 10 de abril de 1813) investigou o problema de se ter soluções por radicais para equações polinomiais. Nessa época, as equações de grau ≤ 4 já haviam sido resolvidas, porém nada se sabia sobre equações de grau maior. Lagrange conseguiu encontrar um procedimento geral que justificava as soluções já determinadas, o qual dependia da existência de certas funções das raízes da equação. O método, porém, falhava quando aplicado à equação do grau 5, chamada quíntica. Lagrange interrompeu a investigação da questão neste ponto, não mais retornando à mesma, e foi o matemático norueguês Niels Henrik Abel (5 de agosto de 1802 - 6 de abril de 1829) que provou definitivamente, em 1829, a inexistência de uma solução por radicais para a quíntica, usando rudimentos de teoria dos grupos.

Foi o jovem matemático francês Évariste Galois [25 de outubro de 1811 – 31 de maio de 1832] que resolveu definitivamente o problema provando que, em geral, não existem soluções por radicais para equações algébricas de grau maior do que quatro. Galois, que foi o primeiro a usar o termo *grupo* para designar a estrutura algébrica que estamos estudando nesse capítulo, ao resolver esse antigo problema criou ramos inteiramente novos da álgebra abstrata: a teoria dos grupos e a teoria de Galois. Tendo vivido em uma época de grande agitação política e social, Galois foi um gênio da matemática que morreu prematuramente em um duelo quando tinha apenas 20 anos e sete meses de idade [Stewart 80] [Galois 11], [Turnbull 11].

5.2 - CONCEITOS BÁSICOS

Definição 5.1: A estrutura algébrica $< G,* >$, em que G é um conjunto e $*$ é uma operação binária definida em G, é um grupo se, $\forall g, h, k \in G$ (axiomas G1 a G4):

G1 – Fechamento: $g * h \in G$.

G2 – Associatividade: $g * h * k = g * (h * k) = (g * h) * k$.
G3 – Elemento identidade (do alemão *enheit*): $\exists e \in G$ tal que $e * g = g * e = g$.
G4 – Elemento Inverso: $\exists g^{-1} \in G$ tal que $g * g^{-1} = g^{-1} * g = e$. ■

Se, além dos axiomas acima, tivermos $g * h = h * g$, $\forall g, h \in G$, então a estrutura $< G, * >$ é dita ser um grupo abeliano ou comutativo. Um grupo é dito ser infinito caso o conjunto G tenha cardinalidade infinita. Caso contrário, o grupo é dito ser finito.

A partir desse ponto passamos a nos referir ao grupo $< G, * >$ simplesmente como o grupo G.

Exemplo 5.1: As seguintes estruturas algébricas são grupos infinitos:

$< Z, + >,\ < Q, + >,\ < R, + >,\ < C, + >,\ < \mathbb{Q}^*, \cdot >,\ < \mathbb{R}^*, \cdot >,\ < \mathbb{C}^*, \cdot >,$

em que $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ denotam, respectivamente, os conjuntos dos números inteiros, racionais, reais e complexos. A notação $\mathbb{R}^*$ denota o conjunto dos números reais sem o elemento zero. O mesmo vale para os símbolos $\mathbb{Q}^*$ e $\mathbb{C}^*$. ■

Exemplo 5.2: O número de elementos de um grupo é chamado a ordem do grupo. As seguintes estruturas algébricas são grupos finitos de ordem n e $(p-1)$, respectivamente:

i) $< \mathbb{Z}_n, +_n >$, em que $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ denota o conjunto dos inteiros módulo n e $+_n$ denota adição módulo n. A tabela a seguir, denominada tabela de Cayley (ou tabela de composição), em homenagem ao matemático inglês Arthur Cayley (16 de agosto de 1821 - 26 de janeiro de 1895), que primeiro usou uma tabela desse tipo, em 1854, mostra a "taboada" desse grupo para o caso em que $n = 4$,

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

ii) $< Z_p^*, \bullet_p >$, em que p denota um número primo e $\bullet_p$ denota multiplicação módulo p. Nessa estrutura, o módulo da aritmética tem que ser um número primo para que os axiomas do fechamento e do elemento inverso sejam satisfeitos. ■

Algumas propriedades de um grupo G são listadas a seguir [Stone 73]:

PG1) O elemento identidade em um grupo G é único.

PG2) Em um grupo G, o elemento inverso de um elemento g é único.

PG3) O inverso do elemento $k = g * h$ em um grupo G é $k^{-1} = h^{-1} * g^{-1}$.

PG4) Em um grupo G todo elemento é cancelável, isto é, se $h_1 * g = h_2 * g$ e $g * h_1 = g * h_2$, então $h_1 = h_2$. Dessa propriedade decorre que, na tabela de composição de um grupo, não há

elementos repetidos nas linhas ou nas colunas. Assim, cada linha ou coluna da tabela representa uma permutação dos elementos do grupo, ou seja, elas contêm os mesmos elementos do grupo, escritos em alguma ordem.

PG5) Para quaisquer elementos a e b em um grupo G, a equação $a * x = b$ tem uma única solução.

Exemplo 5.3: A seguir estão mostradas as tabelas de composição de grupos de ordem 1, 2 e 3,

i)

$*$	e
e	e

ii)

$*$	e	g
e	e	g
g	g	e

iii)

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Observe que, considerando a propriedade (PG4), não há outra maneira de preencher estas tabelas. Isto significa que, não considerando isomorfismos, existe apenas um grupo de ordem 1, de ordem 2 e de ordem 3 e todos são grupos abelianos. ■

Nesse ponto o leitor é convidado a refletir sobre as possíveis maneiras de se construir a tabela de composição de um grupo de ordem 4 e a responder à pergunta: sem considerar isomorfismos, quantos grupos de ordem 4 existem? Esses grupos são abelianos?

5.2.1 - Subgrupos e classes laterais

Um dos conceitos chave em teoria de grupos é o de subgrupo de um grupo G.

Definição 5.2: Se um subconjunto H dos elementos de um grupo G é um grupo em relação à operação de G, dizemos que H é um *subgrupo* de G. ■

Quando H é um subgrupo de G escrevemos $H \leq G$ (lê-se H é subgrupo de G). É possível mostrar que o elemento identidade em H é o mesmo em G e que os elementros inversos coincidem (são os mesmos) em H e G.

Exemplo 5.4: Considere o grupo G dos inteiros módulo 12 munidos da operação de adição módulo 12. Os conjuntos H_i listados a seguir denotam os subgrupos de ordem i do grupo G:

$H_1 = \{0\}$;

$H_2 = \{0, 6\}$;

$H_3 = \{0, 4, 8\}$;

$H_4 = \{0, 3, 6, 9\}$;

$H_6 = \{0, 2, 4, 6, 8, 10\}$ e

$H_{12} = G$. ■

No exemplo 5.4 pode ser observado que as ordens dos subgrupos H_i são divisores da ordem de G. Esse fato sempre ocorre e é conhecido como teorema de Lagrange; sua prova requer a definição do que chamamos classe lateral. Inicialmente, a notação: se K é um subconjunto dos elementos de um grupo G e g é um elemento de G, então gK denota o conjunto $\{g * k \,|k \,\epsilon\, K\}$.

Definição 5.3: Seja $H \leq G$. As classes laterais à esquerda (respectivamente à direita) de G com relação a H são os conjuntos gH (respectivamente Hg), em que $g \in G$. ■

Exemplo 5.5: As classes laterais à esquerda do subgrupo $H_4 = \{0, 3, 6, 9\}$ do exemplo 5.4, com relação ao grupo $< Z_{12}, +_{12} >$ (denotado por G no exemplo) são:

C1: com $g = e$, tem-se $g +_{12} H_4 = e +_{12} H_4 = 0 +_{12} \{0, 3, 6, 9\} = \{0, 3, 6, 9\} = H_4$;

C2: com $g = 1$, tem-se $g +_{12} H_4 = 1 +_{12} H_4 = 1 +_{12} \{0, 3, 6, 9\} = \{1, 4, 7, 10\}$;

C3: com $g = 2$, tem-se $g +_{12} H_4 = 2 +_{12} H_4 = 2 +_{12} \{0, 3, 6, 9\} = \{2, 5, 8, 11\}$.

Em forma de tabela:

$g \downarrow$	0	3	6	9	←elementos do subgrupo H_4
0	0	3	6	9	← C1
1	1	4	7	10	← C2
2	2	5	8	11	← C3

Observa-se que as classes laterais são disjuntas e sua união é igual a Z_{12}, ou seja, as classes laterais formam uma partição de Z_{12}.

Teorema 5.1: As classes laterais à esquerda (ou à direita) de G em relação a um subgrupo H formam uma partição de G. Além disso, as classes tem o mesmo número de elementos.

Sem perda de generalidade vamos considerar as classes laterais à esquerda. Precisamos mostrar que (*i*) classes distintas são disjuntas e (*ii*) que todo elemento de G está em alguma classe.
i) Se g_1H e g_2H não são disjuntas, então $\exists g \in G$ tal que $g \in g_1H$ e $g \in g_2H$, ou seja, $\exists\, h_1$ e $h_2 \in H$, tais que $g_1 * h_1 = g = g_2 * h_2$. Desse modo,

$$g_1H = g_1(h_1H) = (g_1 * h_1)H = (g_2 * h_2)H = g_2(h_2H) = g_2H$$

e as classes são iguais.

ii) Como $e \in H$, gH contém o elemento $g * e = g$. Assim, o elemento g está na classe lateral $gH, \forall g \in G$. Por fim, como as classes não tem elementos repetidos, pois os elementos de um grupo são canceláveis, todas tem o mesmo número de elementos, a saber, $|H|$. ■

Das considerações anteriores decorre o seguinte importante resultado:

Teorema 5.2 (Lagrange 1771): Se $H \leq G$, então $|H|$ é um divisor da $|G|$.

Prova: Denotando o número de classes laterais à esquerda (ou à direita, não faz diferença) de G em relação a H por $[G:H]$, temos

$$|G| = |H|[G:H],$$

e o resultado segue. Denominamos $[G:H]$ de índice de H sobre G. ■

As partições de G em classes laterais gH e Hg são trivialmente iguais para subgrupos abelianos. De uma maneira geral, H é dito ser um *subgrupo normal* de G se $gH = Hg$, $\forall g \in G$ e a partição de G induzida pelo subgrupo normal H é denotada por G/H (lê-se G módulo H). Claramente, todo subgrupo de um grupo abeliano é normal. A motivação para essa definição decorre da existência de grupos não abelianos que contêm subgrupos normais.

Os elementos de G/H são as classes laterais (de mesmo tipo) e a classe lateral contendo o elemento g é denotada por $[g]$. A estrutura $< G/H, \bullet >$, denominada uma estrutura quociente, em que $\bullet$ é uma operação entre classes laterais definida por $[g]\bullet[h] = [g * h]$, é um grupo chamado o grupo quociente de G relativo ao subgrupo normal H. Nesse ponto o leitor deve se convencer de que a operação $\bullet$ é bem definida na estrutura quociente, ou seja, de que $\forall g_1 \in [g]$ e $\forall h_1 \in [h]$, o *produto* $(g_1 * h_1)$ está sempre em $[g * h]$. Mostra-se que a estrutura quociente é uma imagem homomórfica do grupo G, ou seja, o mapeamento entre G e G/H que associa, a cada elemento g em G, sua classe lateral em G/H, é um homomorfismo (de fato, um epimorfismo) de G em G/H [Stone 73].

5.3 - FAMÍLIAS ESPECIAIS DE GRUPOS

Nesta seção vamos estudar três famílias de grupos que tem aplicações em diversas áreas da ciência. Inúmeras outras famílias de grupos existem e o leitor interessado terá acesso às mesmas consultando, por exemplo, [Gallian 02] ou [Durbin 96].

5.3.1 - Grupos cíclicos

A família mais simples de grupos é a dos grupos cíclicos. Embora os mesmos constituam uma clase muito *estreita* de grupos finitos (só existe um grupo cíclico de uma dada ordem!), eles desempenham o papel de blocos construtores básicos para todos os grupos finitos abelianos, de forma semelhante ao papel que os números primos representam para os

números inteiros e que os elementos químicos representam para os compostos químicos [Gallian 02, cap. 11].

Definição 5.4: A ordem de um elemento g em um grupo é o menor inteiro positivo r tal que

$$g^r \triangleq (\underbrace{g * g * \ldots * g}_{r\ vezes} = e. \qquad \blacksquare$$

A definição 5.4 é uma generalização da definição de ordem multiplicativa módulo n, que vimos no capítulo 4 quando estudamos raízes primitivas, conforme ilustra o exemplo a seguir.

Exemplo 5.6: Considere o grupo de ordem 6 $< Z_7^*, \bullet_7 >$, com elemento identidade $e = 1$. A partir da definição 5.4 calculamos as ordens dos elementos da estrutura, conforme mostra a Tabela 5.1.

Tabela 5.1: Ordem dos elementos de $< Z_7^*, \bullet_7 >$

Elemento (g)	1	2	3	4	5	6
Ordem (r)	1	3	6	3	6	2

Note que existem $\phi(6) = 2$ elementos de ordem 6, a saber $g = 3$ e $g = 5$, que foram denominados, no capítulo 4, de raízes primitivas. No contexto de teoria dos grupos esses elementos são chamados de elementos geradores do grupo. ■

Um grupo G é dito ser um grupo cíclico gerado pelo elemento g se todo elemento de G puder ser expresso como uma potência de g. Existe apenas um grupo cíclico de ordem n, o qual é denotado por C_n [Stone 73], isto é,

$$C_n = \{g^i | i = 1, 2, \ldots, n\}.$$

Claramente a relação $g^n = e$ pode ser usada para definir esse grupo. Assim, um grupo de ordem n é cíclico se possui um elemento de ordem n. Um grupo cíclico pode ter vários elementos geradores e, se g é um deles, escreve-se $G =< g >$.

Exemplo 5.7: São cíclicos os grupos

i) $< Z_n, +_n >$; existem $\phi(n)$ geradores, dentre os quais $g = 1$ e $g = n - 1$.

ii) $< Z_p^*, \bullet_p >$; nesse caso toda raiz primitiva de p é um elemento gerador do grupo. Existem portanto, $\phi(\phi(p)) = \phi(p - 1)$ elementos geradores. ■

Teorema 5.3: A ordem de um elemento é um divisor da ordem do grupo.

Prova: Se $g \in G$ é um elemento de ordem l, então o conjunto

$$H = \{e, g, g^2, \ldots, g^{l-1}\}$$

é um subgrupo cíclico de G. Como H tem ordem l então, do teorema de Lagrange, tem-se que $l|G$. ■

A estrutura dos subgrupos de qualquer grupo cíclico é bem estabelecida. De fato, é possível mostrar que se G é um grupo cíclico de ordem $|G|$, então, para todo divisor d dessa ordem, G tem um único subgrupo cíclico H cuja ordem é d [Gallian 02].

5.3.2 - Grupos de permutações

Permutações desempenham um papel importante em aplicações da teoria de grupos à Engenharia Eletrônica moderna. Elas surgem no estudo de máquinas sequenciais, códigos corretores de erros e criptografia, apenas para citar alguns exemplos.

Definição 5.5: Uma permutação p de um conjunto X é uma bijeção de X em X. O grau de uma permutação é a cardinalidade de X.

Para representarmos uma permutação p usaremos a notação de ciclos (Cauchy 1815)

$$(i, p(i), p^2(i), \ldots\ p^{k-1}\ (i)), \qquad (5.1)$$

em que $p^k(i) = i$. A k-upla (5.1) é dita ser um ciclo de comprimento k. Aqui vamos considerar que a composição de permutações é feita da direita para a esquerda, isto é, $(ab) \cdot (ac) = (acb)$.

Definição 5.6: Um grupo de permutações é um conjunto de permutações que forma um grupo erm relação à composição de permutações.

Exemplo 5.7: As 3! = 6 permutações sobre um conjunto de 3 elementos, X = {1, 2, 3},

$p_1 = (1)(2)(3)$, $p_2 = (12)(3)$, $p_3 = (13)(2)$,

$p_4 = (1)(23)$, $p_5 = (123)$ e $p_6 = (132)$,

formam um grupo de permutações de ordem 6 chamado o grupo simétrico de grau 3, cuja tabela de composição é mostrada na Tabela 5.2. Em geral, se |X| = n, o grupo formado por todas as $n!$ permutações de grau n é denominado o grupo simétrico de grau n e denotado por S_n.

Tabela 5.2 - Tabela de composição dos elementos de S_3.

Composição	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_6	p_5	p_4	p_3
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_5	p_1	p_3	p_2
p_5	p_5	p_3	p_4	p_2	p_6	p_1
p_6	p_6	p_4	p_2	p_3	p_1	p_5

Observe que S_3 não é um grupo abeliano. É possível provar que S_n não é abeliano para $n \geq 3$ (Problema 24). ■

A importância dos grupos de permutações vem do fato de que todo grupo é isomorfo a um grupo de permutações, conforme demonstrado por A. Cayley, em 1854.

Teorema 5.4 (o teorema de Cayley): Todo grupo é isomorfo a um grupo de permutações. ■

Esse é um teorema fundamental em teoria dos grupos e sua prova pode ser encontrada na maioria dos livros sobre o assunto [Herstein 75], [Birk 77]. Mais informações sobre Cayley podem ser encontradas em [Cayley 11].

A notação de ciclos que estamos empregando é muito útil para o estudo de grupos de permutações e permite, de forma simples, que se estabeleçam as seguintes propriedades sobre permutações (as provas são deixadas para o leitor [Gallian 02]):

P1 - Toda permutação de um conjunto com um número finito de elementos pode ser expressa como um produto de ciclos disjuntos ou como um único ciclo.

P2 - Ciclos disjuntos comutam.

P3 - A ordem de uma permutação de um conjunto finito, que está expressa na forma de ciclos disjuntos, é o mínimo múltiplo comum dos comprimentos de seus ciclos.

P4 - Toda permutação em S_n, $n > 1$, é o produto de ciclos de comprimento 2.

Um subconjunto de interesse de S_n é aquele formado pelas permutações que trocam apenas dois elementos. Essas permutações tem a forma $(ab)(c)(d)(e)\ldots$ e são denominadas *transposições*, sendo denotadas simplesmente por (ab). As transposições de S_n estão relacionadas com um importante subgrupo de S_n.

Definição 5.7: Uma permutação é dita ser *par* (respectivamente, *ímpar*), se ela é a composição (aqui podemos usar também o termo *produto*) de um número par (respectivamente, *ímpar*) de transposições. ■

Esta definição só tem utilidade se nenhuma permutação puder ser expressa como um produto de um número par de transposições e, ao mesmo tempo, como um produto de um número ímpar de transposições. Isso de fato acontece e, especificamente, mostra-se que ciclos de comprimento par são ímpares e ciclos de comprimento ímpar são pares. Por exemplo, $(abc) = (ac) \cdot (ab)$, $(abcd) = (ad) \cdot (ac) \cdot (ab)$, etc.

Teorema 5.5: As permutações pares de S_n formam um subgrupo de S_n de ordem $n!/2$. Este subgrupo é normal e é denominado o grupo alternante de grau n, sendo denotado por A_n. ■

Prova: Um subconjunto finito de um grupo G que é fechado em relação à operação definida em G, é um subgrupo de G [Stone 73]. Portanto, como o produto de permutações pares

resulta em uma permutação par, A_n é fechado em relação à composição de permutações e assim é um subgrupo de S_n. Resta então mostrar que, em S_n, o número de permutações pares (N_p) é igual ao número de permutações ímpares (N_i). Isso ocorre porque se f é uma permutação par, então $(12) \cdot f$ é uma permutação ímpar; assim $N_i \geq N_p$. Por outro lado, se f é uma permutação ímpar, então $(12) \cdot f$ é uma permutação par. Portanto, $N_p \geq N_i$ e o resultado segue. ■

Exemplo 5.8: O grupo formado pelas permutações pares do grupo simétrico de grau 3 é o grupo alternante de grau 3, $A_3 = \{e, (123), (132)\}$. A_3 é um subgrupo normal de S_3, isto é, as classes laterais à esquerda e à direita de S_3 são iguais (o leitor deve verificar esse resultado construindo essas classes laterais). ■

Para concluir essa breve introdução sobre os grupos de permutações, vamos mencionar um importante resultado relacionado ao grupo alternante. Primeiramente, precisamos do conceito de grupo simples.

Definição 5.8: Um grupo é dito ser simples se não possuir nenhum subgrupo normal próprio.

O seguinte resultado era conhecido por Galois [Stewart 76]:

Teorema 5.6: Se $n \geq 5$ então o grupo alternante A_n é simples.

Galois usou esse resultado para provar que nenhuma equação polinomial de grau ≥ 5 é solúvel por radicais. Uma equação polinomial é dita ser solúvel por radicais quando suas raízes podem ser determinadas por expressões (fórmulas) que envolvem as quatro operações e a extração de raízes [Galois 97].

O conceito de grupo simples foi introduzido por Galois há cerca de 180 anos atrás. Tais grupos são importantes porque todos os grupos podem ser construídos a partir deles [Gallian 76]. Um dos resultados mais importantes do século 20 foi a descoberta e a classificação de todos os grupos simples finitos, uma verdadeira *guerra* que levou cerca de 25 anos e terminou em janeiro de 1981. No processo, foi construido o maior dos grupos simples esporádicos, o "Monstro", assim chamado por possuir uma quantidade de elementos muito maior do que a quantidade de átomos no planeta terra! A ordem do Monstro é 808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000, o que significa $\approx 8 \times 10^{53}$ elementos! Cada um desses elementos pode ser expresso como uma matriz de dimensões 196.883 × 196.883. A prova de que a lista dos grupos simples está completa envolve mais de 10.000 páginas de periódicos científicos! [Gardner 80], [Gorenstein 85].

5.3.2 - Grupos de simetria

Do mesmo modo que os números reais podem ser usados para medir comprimentos, os grupos podem ser usados para medir simetria. O termo simetria deriva da palavra grega *symmetros* (συμμετρος) que significa *de mesma medida*. Formalmente, se F representa uma figura no plano ou no espaço, uma *simetria* da figura F é uma bijeção $f: F \to F$ que preserva

distâncias, isto é, para quaisquer pontos a e $b \in F$, a distância euclideana entre a e b é igual à distância entre $f(a)$ e $f(b)$.

O conjunto de todas as simetrias de uma figura F, munido da operação de composição de simetrias, é um grupo, pois

i) A composição de funções que preservam distâncias, também preserva distâncias, ou seja, a composição de simetrias é uma simetria;
ii) Composição de funções é uma operação associativa;
iii) A função identidade é uma simetria, e
iv) A inversa de uma simetria também é uma simetria.

Esse grupo é denominado o grupo de simetrias de F. É a ordem do grupo de simetrias de uma figura que dá uma medida do grau de simetria da mesma.

Exemplo 5.9: O grupo de simetrias de um retângulo com lados diferentes. O grupo é formado pelas rotações $\{e, x, y, z\}$. As rotações $\boldsymbol{x}$ e $\boldsymbol{y}$ não podem ser executadas sem que se

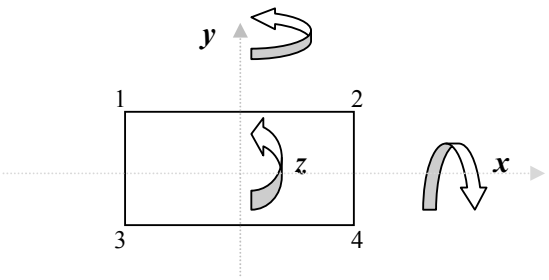


Figura 5.1 - Simetrias de um retângulo com lados desiguais.

deixe o plano do retângulo e são denominadas impróprias (são reflexões em torno dos eixos x e y, respectivamente), enquanto que a rotação z (em torno do eixo que passa pela origem e é perpendicular ao plano do retângulo) pode ser realizada no plano do retângulo e é dita ser uma rotação própria (Figura 5.1). Esse grupo é também denominado o grupo de Klein [Klein 11], em homenagem ao matemático alemão Felix Klein (25 de april de 1849 - 22 de junho de 1925). A tabela de Cayley do grupo de Klein, que algumas vezes é denotado por $\boldsymbol{K_4}$, é mostrada na Tabela 5.3. Se considerado como um subgrupo de $\boldsymbol{S_4}$, os elementos de $\boldsymbol{K_4}$

Tabela 5.3 - Tabela de composição do grupo K_4.

·	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

podem ser expressos como e, $x = (13)(24)$, $y = (12)(34)$ e $z = (14)(23)$. ■

O grupo cíclico C_n, introduzido na Seção 5.3.1, pode ser expresso como um grupo de simetrias. Considere o conjunto de todas as n rotações próprias, de $l(2\pi/n)$ radianos, $l = 0,1, \ldots n-1$, de um polígono regular de n lados (Figura 5.2). Se r denota uma rotação de

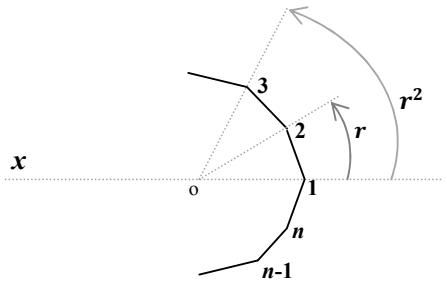


Figura 5.2 – Construção do grupo das simetrias próprias de um polígono regular.

$2\pi/n$ radianos no sentido anti-horário, então r tem ordem n e o conjunto $\{e, g, g^2, \dots, g^{n-1}\}$, munido da operação de composição de simetrias, é um grupo cíclico de ordem n. Como existe apenas um grupo cíclico de ordem n, esse grupo é denotado por C_n [Gilb 03].

Agora vamos considerar o grupo de todas as simetrias de um polígono regular de n lados. Esse grupo pode ser obtido a partir da Figura 5.2 se permitirmos rotações impróprias (aqui denotadas por h) em torno do eixo x, que une o centro do polígono e o vértice 1. Essas reflexões tem ordem 2, isto é, $h^2 = e$. O grupo obtido com a inclusão da reflexão h tem ordem $2n$ e é denominado grupo dihedral, sendo denotado por D_n. Observe que D_n não é um grupo cíclico e que seus elementos são

$$\{e, g, g^2, \dots, g^{n-1}, h, hg, hg^2, \dots, hg^{n-1}\},$$

de onde se percebe que C_n é um subgrupo normal em D_n. Para $n > 2$, o grupo dihedral não é abeliano [Gilb 03].

Exemplo 5.10: O grupo dihedral D_4. Considere o conjunto de todas as simetrias, próprias e impróprias, do quadrado. A Figura 5.3 mostra o efeito da *ação* dessas simetrias sobre um quadrado de vértices 1, 2, 3 e 4.

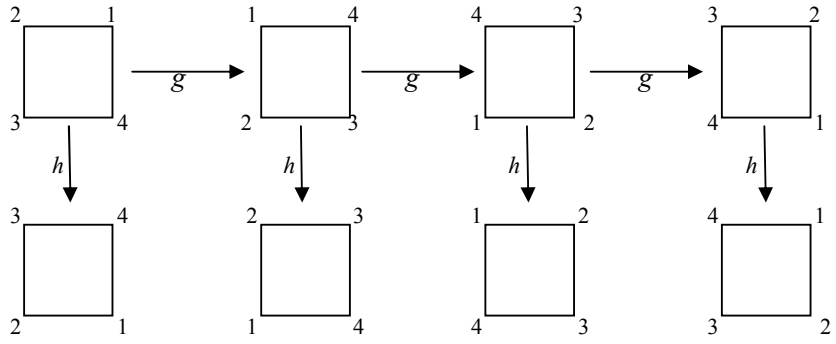
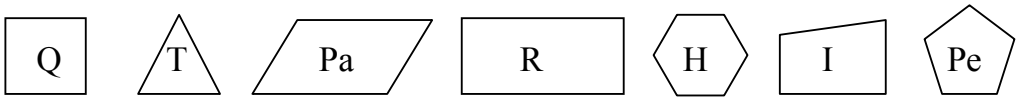


Figura 5.3 - Construção do grupo dihedral D_4.

Note que $h \cdot g^i = g^{4-i} \cdot h$, para $i = 0, 1, 2, 3$. Em geral, o grupo D_n satisfaz $h \cdot g^i = g^{n-i} \cdot h$, para $i = 0, 1, \dots, n-1$. ■

Exemplo 5.11: O grupo de simetrias de algumas figuras geométricas. Identifique o grupo de simetrias das figuras indicadas e liste as mesmas em ordem crescente de simetria. Os polígonos mostrados (triângulo, quadrado, pentágono, hexágono) são regulares. A figura que



apresenta maior simetria é aquela cujo grupo de simetrias, G, tem a maior ordem. A lista é:
I ($G = C_1$), Pa ($G = C_2$), R ($G = C_2 \otimes C_2$), T ($G = D_3$), Q ($G = D_4$), Pe ($G = D_5$), H ($G = D_6$).
■

PROBLEMAS

1) Encontre um subgrupo H de ordem 4 de $< Z_{60}, +_{60} >$ e construa a classe lateral a esquerda em relação a H que contém o elemento 40. H é isomórfico a $< Z_4, +_4 >$? Por quê?

2) Encontre um subgrupo H de ordem 4 de $G = \langle Z_{13}^*, \bullet_{13} \rangle$ e construa as classes laterais de G em relação a H.

3) Encontre um subgrupo de ordem 10 do grupo simétrico de grau 7.

4) Encontre todos os subgrupos cíclicos de $\langle Z_7^*, \bullet_7 \rangle$.

5) É verdade que a união de dois subgrupos de um grupo G é também um grupo? Por quê?

6) É verdade que a interseção de dois subgrupos de um grupo G é também um grupo? Por quê?

7) Prove que se $g^2 = e$, para qualquer elemento g em um grupo G, então G é abeliano.

8) Prove que, em um grupo G, os elementos g e g^{-1} tem a mesma ordem.

9) Prove que todo grupo cíclico é abeliano.

10) Para cada $g \in G$, o conjunto $N_g = \{h : hgh^{-1} = g, g,h \in G\}$ é chamado o normalizador de g. Prove que N_g é um subgrupo de G, $\forall g$.

11) Prove que o subconjunto C(G) dos elementos de G que comutam com qualquer elemento de G, é um subgrupo de G. C(G) é chamado o centro de G.

12) Prove que, se H é um subgrupo de G, então $g^{-1}Hg$ é também um subgrupo de G, $\forall g \in G$.
13) Prove que se G é um grupo com um número primo de elementos, então G é cíclico.
14) Construa a tabela de composição de um grupo não abeliano de ordem 6. Encontre subgrupos de ordem 2 e 3 deste grupo.

15) Prove que se G é um grupo abeliano, então $(gh)^n = g^n h^n$, $\forall g,h \in G$ e para qualquer inteiro positivo n.

16) Determine a maior ordem que encontramos dentre os elementos de S_n, quando n vale : a) 8. b)12. c) 15.

17) Prove o teorema de Lagrange.

18) Prove que se G é um grupo finito, então a ordem de qualquer elemento de G divide $|G|$.

19) Seja X = {a, b, c} e P(X) o conjunto das partes de X. Identifique qual das estruturas a seguir é um grupo: a) $\langle P(X), \cup \rangle$. b) $\langle P(X), \cap \rangle$

20) O conjunto das simetrias de um retângulo é um grupo em relação à operação de composição de funções? Por quê?

21) Um grupo G tem um subgrupo H de ordem 6, tal que [G:H] >4 e |G|<50. Quais os possíveis valores de |G|?

22) Qual dos grupos abaixo é cíclico? Por quê? ($\otimes$ denota produto direto e a operação em Z_n é soma módulo n): i) $Z_8 \otimes Z_2$. ii) $Z_7 \otimes Z_{10}$

23) Considerando o produto direto de $<Z_m, +_m>$ por $<Z_n, +_n>$, indique os grupos cíclicos: i) $Z_3 \otimes Z_3$. ii) $Z_4 \otimes Z_2$. iii) $Z_3 \otimes Z_4$ (Justifique).

24) Para que valores de n o grupo simétrico S_n é abeliano? Justifique.

25) Para que valores de n o grupo simétrico S_n é cíclico? Justifique.

26) Seja H o único subgrupo de ordem | H | do grupo finito G. Mostre que H é um subgrupo normal de G.

27) Construa um grupo de ordem 4 onde nenhum elemento tem ordem 4.

28) Encontre um subgrupo cíclico de S_5 que tenha ordem 6.

29) Encontre um subgrupo não cíclico de S_5 que tenha ordem 6.

30) Construa um subgrupo comutativo de ordem 6 de S_5.
31) Construa um subgrupo de ordem 12 de S_5.

32) Construa um subgrupo cíclico H de D_n, de ordem n/2. Para n = 6 e 8, esboce uma figura plana que tenha H como grupo de simetrias.
33) Quais das posições (A ou B) pode ser obtida partindo-se da posição inicial? Por quê?

Posição Inicial

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(A)

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	

(B)

8	14	11	3
12	2	15	9
6	4	13	1
	7	10	5

34) Seja P um conjunto de permutações com |P| = 9. A estrutura < P, • >, onde • denota composição de permutações, pode ser um grupo? P pode ser um subgrupo de S_n? Em caso positivo, para que valores de n? Se $f \in P$, f pode gerar um grupo cíclico? Por quê?

35) Distribua os dígitos decimais de 0 a 9 em conjuntos cujos elementos tem o mesmo grupo de simetria. Para cada conjunto identifique o grupo de simetria correspondente.

36) Qual o grupo de simetria de uma estrela regular de 5 pontas? Por quê?

37) O conjunto dos inteiros {4, 8, 12, 16} é um grupo em relação à operação de multiplicação módulo 20? Por quê? Caso sua resposta seja afirmativa, encontre o elemento identidade do grupo e diga se o mesmo é, ou não, cíclico.

38) A tabela abaixo pode ser a tabela de composição de um grupo de ordem 5? Por quê?

•	a	b	c	d	f
a	a	b	c	d	f
b	b	a	d	f	c
c	c	f	a	b	d
d	d	c	f	a	b
f	f	d	b	c	a

39) A estrutura <Z, •>, onde Z denota o conjunto dos números inteiros e • é a operação binária definida por a•b = a+b-4, é um grupo? Por quê?

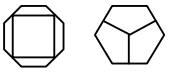
40) A estrutura <R, •>, onde R denota o conjunto dos números reais e • é a operação binária definida por a•b = a+b-ab, é um grupo? Por quê?

41) Apresente dois exemplos de subgrupos abelianos não triviais de D_n.

42) Quantos subgrupos tem o produto direto $<Z_p, +_p>$ por $<Z_p, +_p>$? Por quê?

43) Se g é um elemento gerador de um grupo G de ordem n e g^k , onde k|n, é um elemento gerador de H, qual o valor de [G:H]?

44) Qual o grupo de simetria das figuras ao lado? Expresse G em termos de C_n ou D_n Justifique.



45) Identifique o grupo das rotações próprias e o grupo de todas as rotações da figura. Expresse suas respostas usando os grupos C_n ou D_n. Justifique.

46) Os grupos C_{60} e $(C_{10} \otimes C_6)$ são isomórficos? Por quê?

47) Encontre um subgrupo normal de S_3. Justifique.

48) O conjunto dos inteiros {3, 6, 9, 12} é um grupo em relação à operação de multiplicação módulo 15? Por quê? Caso sua resposta seja afirmativa, encontre o elemento identidade do grupo e diga se o mesmo é, ou não, cíclico.

49) Em um cassino em Las Vegas, uma máquina faz o seguinte embaralhamento em um baralho com 2n cartas: $\begin{pmatrix} i: & 1 & 2 & 3 & 4 & \ldots\ldots & n & n+1 & n+2 & \ldots\ldots & 2n \\ f(i): & 2 & 4 & 6 & 8 & \ldots\ldots & 2n & 1 & 3 & \ldots\ldots & 2n-1 \end{pmatrix}$. Qual o número mínimo de embaralhamentos desse tipo, que precisa ser feito em um baralho com 22 cartas, para que as cartas voltem à sua posição inicial? E se o baralho tivesse 14 cartas? Justifique (a solução não deve ser encontrada por busca exaustiva).

50) O grupo $C_6 \otimes C_{10}$ tem subgrupos cíclicos? Em caso positivo, de que ordens? Justifique.

51) O conjunto de todas as cartas de copas de um baralho foi submetido a dois embaralhamentos do mesmo tipo por meio de uma máquina. Considerando que as cartas entraram na máquina na ordem crescente e que saíram na ordem 7, 2, 6, J, 5, A, 4, 3, K, 8, Q, 9, 10, qual a ordem das cartas após o primeiro embaralhamento? Depois de quantos embaralhamentos o baralho volta à posição inicial?

52) O conjunto {7, 35, 49, 77}, juntamente com a operação de multiplicação módulo 84, é um grupo? Em caso positivo, o grupo é cíclico? Justifique.

53) Quais as ordens dos subgrupos cíclicos de S_7?

54) Um grupo onde todo elemento, excetuando o elemento identidade, tem ordem 2, é abeliano? Por quê?

55) Encontre um subgrupo abeliano de S_9 que tenha ordem 10.

56) Distribua as 23 letras do alfabeto em conjuntos, de modo que as letras de um dado conjunto tenham o mesmo grupo de simetrias. Expresse, em termos de C_n ou D_n, o grupo de simetria associado a cada conjunto.

57) Construa um subgrupo de ordem 12 de S_5.

58) Apresente uma figura cujo grupo de simetrias seja cíclico, tenha ordem maior que três e só possua subgrupos triviais.

59) Apresente uma figura cujo grupo de simetria é C_3. Justifique.

60) O grupo simétrico S_{16} tem algum subgrupo cíclico de ordem 16? Por quê?

61) Um conjunto de doze cartas de um baralho foi submetido a três embaralhamentos do mesmo tipo (π) por meio de uma máquina. Considerando que as cartas entraram na máquina na ordem crescente e que saíram na ordem (6 5 1 2 9 11 10 12 4 8 3 7), determine π. Depois de quantos embaralhamentos as cartas voltam à posição inicial?

62) O conjunto G = {1, 5, 7, 11}, juntamente com a operação de multiplicação módulo *n*, é um grupo não cíclico. Encontre *n*.

63) Encontre um subgrupo abeliano de ordem 12 de S_8.

64) Encontre dois subgrupos comutativos não triviais de D_5. Descreva esses grupos por meio das rotações do pentágono.

65) Encontre dois subgrupos não cíclicos de D_4.

66) Existe um grupo não cíclico cujos subgrupos próprios são, todos, cíclicos? Em caso positivo, apresente um exemplo de um tal grupo.

67) Encontre três elementos σ_1, σ_2 e σ_3 em S_{10}, tais que $\sigma_1^3 = \sigma_2^3 = \sigma_3^3 = (157)(283)(469)$.

68) Seja G um grupo contendo elementos de ordens 1, 2, 3, ..., 10. Qual a menor ordem possível para G? Por quê?

69) Pode um grupo ter mais subgrupos do que elementos? Justifique.

70) Encontre um subgrupo H de $Z_{12} \otimes Z_{20}$ isomórfico a $Z_4 \otimes Z_5$ (Se H for cíclico, é suficiente indicar um elemento gerador).

71) Se G é um grupo finito, mostre que existe um número ímpar de elementos $x \in G$ satisfazendo $x^3 = e$.

72) O conjunto de todas as matrizes 2x2 do tipo $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$, onde a ($\neq 0$) $\in Z_p$, equipado com a operação de multiplicação de matrizes módulo *p*, é um grupo? Por quê? Sua resposta seria diferente se *a* fosse um número real?

73) Qual o centro do grupo dihedral D_4? Justifique.

74) O conjunto de todos os elementos de um grupo G que satisfaz a equação $x^n = e$ é um subgrupo de G? Por quê?

75) Existe algum elemento de ordem 4 em A_5? Justifique.

76) Determine todos os grupos cíclicos finitos que tem exatamente dois geradores.

77) Prove que o subconjunto C(g), g∈G, dos elementos de G que comutam com g, é um subgrupo de G. C(g) é chamado o centralizador de g em G. Qual o centralizador de h em D_4?

78) Seja G um grupo de ordem 24 contendo um elemento g que satisfaz $g^8 \neq e$ e $g^{12} \neq e$. Pode-se afirmar que G é um grupo cíclico? Por quê?

79) Seja $P = (13579)(246)(8\ 10)$ um elemento de S_{10}. Se P^m é um ciclo de comprimento 5, o que se pode afirmar sobre o valor de *m*? Justifique.

80) Esboce uma figura cujo grupo de simetrias seja um subgrupo não trivial de C_n, para algum valor de $n > 4$ (escolha o valor de *n* e mostre a figura).

81) Encontre um grupo que contém elementos a e b tais que ordem(a) = 2, ordem(b) = 11 e ordem(a∗b) = 2.

82) Seja G um grupo que tem exatamente dois subgrupos não triviais. G é cíclico? O que se pode afirmar sobre a ordem de G? Por quê?

82) Apresente uma figura cujo grupo de simetrias é $C_2 \otimes C_3$. Justifique.

83) Escolha um valor para *n* e encontre elementos *a* e *b* em S_n, tais que ordem(*a*) = ordem(*b*) =3 e ordem(ab) = 5.

84) Complete a frase: Em um grupo finito a ordem do elemento *g* é igual à ordem do elemento g^2 se, e somente se, a ordem de *g* é ..... . Justifique.

85) Liste todos os elementos de ordem 8 em $<Z_{80,} +_{80}>$.

86) Apresente uma figura cujo grupo de simetrias é $C_4 \otimes C_3$. Justifique.

87) Encontre um subgrupo H de $Z_{16} \otimes Z_{20}$ isomórfico a $Z_2 \otimes Z_5$. Se H for cíclico, é suficiente indicar um elemento gerador (em Z_n a operação é soma módulo *n*).

88) Em S_4, encontre um subgrupo não cíclico de ordem 8.

89) Apresente quatro exemplos de grupos não isomórficos de ordem 8.

REFERÊNCIAS

[Birk 77] G. Birkhoff and S. Mac Lane, *A Survey of modern Algebra*, Macmillan, 1977.

[Cayley 11] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Cayley.html, acesso em 23/10/2011.

[Durbin 96] A. M. Durbin, *Modern Algebra,* Prentice-Hall, 1996.

[Gallian 76] J. A. Gallian, The Search for Finite Simple Groups, *Mathematics Magazine* 49. pp. 163-179, 1976.

[Gallian 02] J. A. Gallian, *Contemporary Abstract Algebra*, Houghton Mifflin, 2002.

[Galois 97] R. Bourgne et J-P Azra, *Évariste Galois Écrits et Mémoires Mathématiques*, Gauthier-Villars, 1997.

[Galois 11] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Galois.html, acesso em 23/10/2011.

[Gardner 80] M. Gardner, The Capture of the Monster: A Mathematical Group with a Ridiculous Number of Elements, *Scientific American* 242 (6), pp. 20-32, 1980.

[Gilb 03] W. J. Gilbert and W. K. Nicholson, *Modern Algebra with Applications*, John Wiley, 2003.

[Gorenstein 85] D. Gorenstein, The Enormous Theorem, *Scientific American* 253 (6), pp. 104-115, 1985.

[Herstein 75] I. N. Herstein, *Topics in Algebra*, John Wiley, 1975.

[Klein 11] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Klein.html, acesso em 24/10/2011.

[Stallings 07] W. Stallings, *Criptografia e Segurança de Redes*, Pearson Prentice-Hall, 2007.

[Stewart 76] I. Stewart, *Galois Theory*, Chapman and Hall, 1976.

[Stone 73] H.S Stone, *Discrete Mathematical Structures and Their Applications*, SRA, 1973.

[Turnbull 11] http://turnbull.mcs.st-and.ac.uk/, acesso em 23/10/2011.

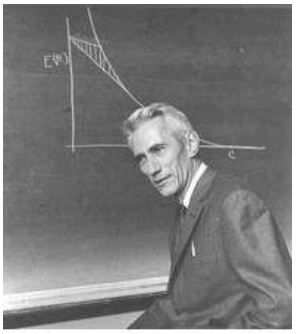
6

CÓDIGOS DE GRUPO

Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?

Richard Hamming

6.1 - INTRODUÇÃO



Claude Shannon

A disciplina Teoria da Informação foi criada por Claude Elwood Shannon (30 de abril de 1916 – 24 de fevereiro de 2001) em 1948 [Shannon 48]. Ela é um corpo de conhecimento que estabelece limites em relação ao desempenho que pode ser obtido por meio de um sistema de comunicações que usa sinais elétricos. Shannon é considerado uma das personalidades mais criativas do século XX, tendo dado muitas contribuições importantes para as ciências da Engenharia Elétrica. Sua formação acadêmica compreende uma graduação dupla em Engenharia Elétrica e Matemática pela universidade de Michigan, um mestrado em Engenharia Elétrica e um doutorado em Matemática, ambos pelo Instituto de Technologia de Massachussets (MIT). Dentre as áreas que muito se beneficiaram de seu trabalho, podemos citar Engenharia de Telecomunicações, Processamento Digital de Sinais, Criptografia, Eletrônica Digital, Inteligência Artificial, entre outras [Sloane, 93]. A maioria das contribuições de Shannon tiveram grande impacto nas áreas em que atuou. Como um exemplo, êle é considerado o fundador da teoría de projeto de circuitos e computadores digitais, devido à sua dissertação de mestrado, apresentada em 1937, em que ele propôs a utilização de álgebra de Boole como uma ferramenta de análise e projeto do que hoje chamamos circuitos digitais [Shannon 37]. Esta dissertação é considerada, nas engenharias, a dissertação mais importante de todos os tempos.

A Figura 6.1 mostra o chamado *cavalo de batalhas* da Teoría da Informação. A fonte de informação produz a mensagem m que será enviada ao destino (terminal receptor). Para medir a quantidade de informação associada à mensagem, Shannon usou a função *entropia* da Mecânica Estatística. Para uma fonte discreta cujos n símbolos estão associados ao conjunto de probabilidades p_i, $1 \leq i \leq n$, a entropia é definida por

$$H = -\sum_i p_i \log(p_i).$$

Esta função satisfaz propriedades que a tornam atrativa como uma medida de informação [Kinchin 57]. No codificador, as mensagens geradas pela fonte são processadas de modo a torná-las *adequadas* para transmissão pelo canal. Chamamos *codificação de canal* à operação do codificador de adicionar informação redundante às mensagens de modo a protegê-las contra os possíveis erros introduzidos pelo canal. Um exemplo simples de canal,

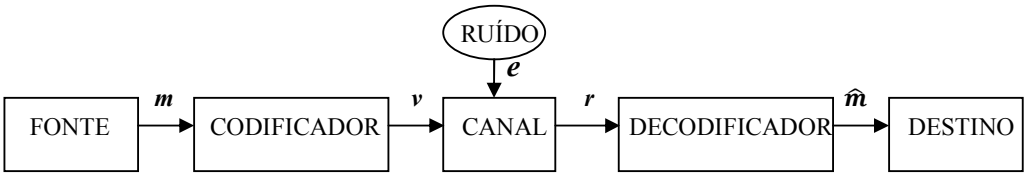


Figura 6.1 – O *cavalo de batalha* da Teoria da Informação: um sistema de transmissão de informação; *m* é a mensagem produzida pela fonte de informação, *v* a palavra-código, *e* é o vetor erro, *r* a palavra recebida e $\hat{m}$ a mensagem estimada.

denominado *canal binário simétrico* (BSC), é mostrado na figura 6.2. Neste canal os erros

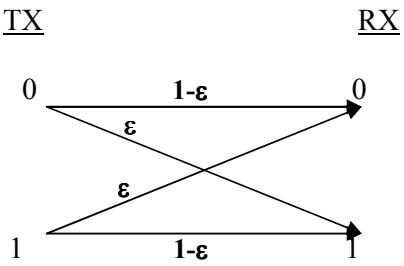


Figura 6.2 – Canal Binário Simétrico, com probabilidade de transição ε.

ocorrem com probabilidade ε. O BSC é um exemplo de um canal discreto sem memória, ou seja, os erros ocorrem de modo independente, e os esquemas de codificação de canal apresentados nesse capítulo destinam-se a combater erros neste tipo de canal. Na recepção o decodificador tenta, a partir de uma sequência (palavra) recebida, possivelmente errada, recuperar a mensagem produzida pela fonte, *m*, e entregá-la ao usuário final (destino). A mensagem recuperada é denotada por $\hat{m}$. Um dos mais importantes resultados da teoria da informação diz respeito à probabilidade P_{de} de que $\hat{m} \neq m$. Esse é o tema do segundo teorema de Shannon, o chamado teorema da codificação com ruído. Ele envolve a noção de capacidade de canal, a qual para o BSC da Figura 6.2 é dada por

$$C(\varepsilon) = 1 + \varepsilon\, log_2\varepsilon + (1-\varepsilon) log_2(1-\varepsilon).$$

Shannon provou o notável resultado de que, desde que a taxa de transmissão de informação seja menor do que a capacidade canal, então P_{de} pode ser feita arbitrariamente pequena. Formalmente, tem-se [Shannon 48]

Teorema 6.1 - (o segundo teorema de Shannon) Para qualquer $\theta > 0$, desde que a taxa de transmissão de informação não é maior que C, existe um esquema de codificação de canal para o qual $P_{de} < \theta$. ■

A prova desse teorema não é uma prova construtiva, ou seja, o teorema garante a existência de um tal esquema de codificação mas não mostra como desenvolvê-lo. Esta situação, entretanto, não durou muito e logo a disciplina *teoria da codificação* foi criada com a publicação no jornal do sistema Bell, em 1950, de um artigo de autoria de Richard Hamming, sobre códigos para detecção e correção de erros [Hamm 50]. Embora os importantes resultados obtidos por Marcel Golay [Golay 49] tenham aparecido um ano antes, foi o trabalho de Hamming que de fato contribuiu para estabelecer as fundações da teoria da codificação como nós a conhecemos hoje.

Vários desenvolvimentos importantes ocorreram durante os anos 50, os quais viram o surgimento da classes de códigos cíclicos e convolucionais e também a descoberta de cotas sobre os parâmetros de um código, como as cotas de Elias e de Gilbert-Varshamov [MacWilliams 89]. Uma das maiores descobertas nesse assunto foi feita cerca de dez anos após a criação dos códigos de Hamming, quando códigos que poderiam ser projetados, sistematicamente, para corrigir *t* erros por bloco foram construídos. A década seguinte (60) viu um progresso significativo e a teoria da codificação expandiu-se enormemente, particularmente na área de decodificação, com o desenvolvimente de novas e eficientes técnicas de decodificação para vários tipos de códigos de canal. Nas décadas de 80 e 90 a área teve um crescimento verdadeiramente explosivo com o desenvolvimente de importantes resultados de natureza teórica, que causaram grandes impactos em diversos cenários de aplicações práticas, tais como o projeto de modems de alta velocidade, sistemas de telefonia móvel digital, comunicações via satélite e espacial, e sistemas de armazenamento multimídia. Desde essa época até os dias atuais, o assunto continua sendo alvo de pesquisas de natureza teórica e prática, e os códigos corretores de erros estão presentes na maioria dos sistemas de telecomunicações e de armazenamento de dados [Lin 04].

Os principais objetivos da teoria da codificação são:

i) Determinar quão bons os códigos podem ser, ou seja, estabelecer cotas (limitantes) sobre seu desempenho e seus parâmetros.
ii) Projetar *bons* códigos.
iii) Encontrar métodos eficientes para decodificar tais códigos.

Nesse capítulo estudaremos a classe dos códigos de grupo binários, também conhecidos por códigos de bloco lineares binários. A formulação matricial desse tipo de códigos e sua decodificação por tabela de síndrome é apresentada. A família dos códigos de Hamming é descrita e algumas cotas superiores para alguns parâmetros de um código de grupo são mostradas.

6.2 - DOIS CÓDIGOS SIMPLES

Em seu artigo clássico "*A Class of Binary Signaling Alphabets*", publicado em 1956, David Slepian introduziu o conceito de *código de grupo binário* [Slepian 56]. Esse foi o primeiro trabalho a formular o assunto codificação de canal por meio de ferramentas de

álgebra moderna (teoria de grupos), o que deu um grande impulso para o desenvolvimento da teoria da codificação.

Definição 6.1: Um código de grupo é um subgrupo do grupo aditivo de todas as ênuplas *p*-árias.

Como exemplo, considere a estrutura algébrica aditiva formada pelo conjunto de todas as $2^3 = 8$ triplas binárias, munido da operação de soma módulo 2, componente a componente, isto é,

$$G = < \{000, 100, 010, 001, 110, 101, 011, 111\}, + >,$$

em que $110 + 101 = 011;\ 010 + 111 = 101;$ etc. Claramente, essa estrutura é um grupo abeliano de ordem 8, cujos elementos, excetuando o elemento identidade 000, têm ordem 2, ou seja, todo elemento é igual ao seu inverso ($g = g^{-1}$) (veja o problema 5.7).

No que se segue vamos considerar subgrupos de G, que podem ser usados para detectar e/ou corrigir erros. As palavras *v* a ser transmitidas por um BSC são os elementos de cada subgrupo. O número de símbolos diferentes de zero em cada palavra é dito ser o peso de Hamming da palavra. Vamos considerar ainda a presença de ruído aditivo no canal de modo que a palavra recebida r é da forma $r = v + e$, em que e denota o vetor erro (ou o padrão de erro) possivelmente introduzido durante a transmissão.

6.2.1 - O Código de repetição

Considere o subgrupo H_2 de G formado pelos elementos $\{000, 111\}$. Com o vetor erro podendo ser igual a qualquer elemento de G, vê-se que qualquer padrão de erro de peso ≤ 2 resultará numa palavra recebida que não está em H_2, permitindo assim a sua detecção (de erros). Considerando que a probabilidade de transição ε é menor que 50%, pode-se mostrar que a ocorrência de um erro durante a transmissão é um evento mais provável que a ocorrência de dois erros. Assim, se apenas um erro ocorre durante a transmissão, ou seja, se o vetor erro tem peso 1, então podemos estimar a palavra transmitida como sendo a palavra de H_2 que difere no menor número de posições da palavra recebida r. Este procedimento é denominado *decodificação por distância mínima* (do inglês *minimum distance decoding*). O número de posições em que duas ênuplas $u = (u_i)$ e $v = (v_i), i = 0, 1, \ldots, n-1$, diferem é denotado por $d(u, v)$ e denominado a distância de Hamming entre as ênuplas, isto é, $d(u, v) = |\{i : u_i \neq v_i\}|$. Assim, por exemplo, $d(000, 100) = 1;\ d(000, 111) = 3;$ etc. Pode-se mostrar que a distância de Hamming é uma métrica [Lin, p. 76], isto é,

i) $d(u, v) \geq 0$.
ii) $d(u, v) = d(v, u)$.
iii) $d(u, v) = 0$ se e só se $u = v$.
iv) $d(u, v) \leq d(u, w) + d(w, v)$ (desigualdade triangular).

A decodificação por distância mínima consiste então em estimar a palavra transmitida v como sendo a palavra $\hat{v}$, dentre as palavras de H_2, que minimiza a distância de Hamming $d(v, r)$, $\forall v \in H_2$. A Tabela 6.1 mostra esta estratégia de decodificação para o subgrupo H_2.

Desse modo pode-se afirmar que, se o canal se comporta como o modêlo apresentado na Figura 6.2, com ε < 50%, a aposta de que o esquema de controle de erros baseado no subgrupo H_2 é capaz de detectar até dois erros por bloco e corrigir um erro por bloco será vencedora, na maioria das vezes. As capacidades de detecção e de correção de erros, por palavra transmitida (por bloco), são denotadas, respectivamente, por e e t. No caso considerado $e = 2$ e $t = 1$.

Tabela 6.1 - Estratégia de decodificação com o subgrupo H_2.

Palavra transmitida (v)	Palavra recebida (r)	Palavra estimada ($\hat{v}$)	Decisão
000	000, 100, 010, 001	000	certa
000	110, 101, 011, 111	111	errada
111	111, 011, 101, 110	111	certa
111	000, 001, 010, 100	000	errada

O esquema de detecção e correção de erros considerado usa palavras binárias de comprimento $n = 3$. A generalização do mesmo para palavras de comprimento n arbitrário pode ser feita sem dificuldades. Nesse caso tem-se $e = n - 1$ e $t = \left\lfloor \frac{n-1}{2} \right\rfloor$, em que $\lfloor x \rfloor$ denota a parte inteira de x. Em qualquer caso, para qualquer valor de n, observa-se que as palavras transmitidas são formadas pela repetição de um único símbolo de mensagem (ou símbolo de informação; os demais símbolos são denominados símbolos de paridade), 0 ou 1. Por essa razão o esquema é denominado código de repetição e denotado por $C(n, 1, n)$, em que n representa o comprimento (número de símbolos) das palavras. Em geral, um código de grupo binário é denotado por $C(n, k, d)$, em que k denota o número de símbolos de informação (em um código de repetição, $k = 1$) e d a menor distância de Hamming entre todos os pares de palavras do esquema; d é denominada a distância mínima do código. Definem-se ainda o parâmetro que denota o número de palavras do código, $M \triangleq 2^k$, e o parâmetro denominado a taxa de informação do código, que é a relação $R \triangleq k/n$. O código de repetição tem apenas duas palavras e a menor taxa de informação possível, $R = 1/n$.

6.2.2 - O Código de um único símbolo de paridade

No grupo G considere agora o subgrupo H_4 formado por todos os elementos de peso par, ou seja, $H_4 = \{000, 110, 101, 011\}$. Considerando os elementos definidos anteriormente, percebe-se que este é um código de grupo binário $C(3, 2, 2)$, uma vez que existem $k = 2$ símbolos de informação, $M = 2^2 = 4$ palavras-código e a menor distância entre as palavras de C é $d = 2$. Como existe apenas um símbolo de paridade, o código recebe essa denominação ou, abreviadamente, SPC (do inglês *single parity-check code*). Dessa forma, esse código detecta apenas um erro por bloco e não corrige nenhum erro, sendo um exemplo do que se denomina um código detector de erros. Em sistemas de comunicações que empregam esse tipo de código, quando a ocorrência de erros é detectada, um protocolo é usado, por meio de um canal confiável (com baixa probabilidade de erro), solicitando ao transmissor que a palavra-código seja reenviada. Tais sistemas são denominados ARQ (do inglês, *Automatic Repeat reQuest* ou *Automatic Repeat Query*) [Peterson 03], [Tanembaum 11]. Em geral, um SPC binário é formado a partir do subgrupo $H_{2^{n-1}}$ cujos 2^{n-1} elementos são as ênuplas de peso par de G. Esse é um código de grupo $C(n, n-1, 2)$, com as mesmas

capacidades de detecção e correção mencionadas anteriormente, isto é, $e = 1$ e $t = 0$. Por outro lado, a taxa de transmissão de informação desse código é a maior possível, a saber $R = (n-1)/n = 1 - 1/n$.

Os códigos discutidos nesta seção representam os extremos em termos de capacidade de controle de erros (capacidades de detecção e de correção) e de taxa. Os códigos de repetição tem a máxima capacidade de detecção e de correção de erros, e a mínima taxa. Para os códigos de um único símbolo de paridade, ocorre exatamente o contrário. A construção de códigos de grupo com parâmetros diferentes desses, requer diferentes escolhas de subgrupos do grupo G. independente da escolha do subgrupo, os códigos de grupo representam, claramente, estruturas algébricas fechadas, isto é, a soma módulo 2, componente a componente, de quaisquer duas palavras-código, também é uma palavra código. Por essa razão diz-se que esses códigos são *lineares*.

6.3 - FORMULAÇÃO MATRICIAL

Considere um esquema para controle de erros em que os $n-k$ símbolos de paridade são obtidos dos k símbolos de informação a partir das equações de paridade

$$\begin{aligned} c_1 &= k_1 + k_2 + k_3, \\ c_2 &= k_1 + k_2 + k_4, \\ c_3 &= k_1 + k_3 + k_4. \end{aligned} \qquad (6.1)$$

Assim uma palavra-código tem a forma $v = (v_0 v_1 v_2 v_3 v_4 v_5 v_6) = (k_1 k_2 k_3 k_4 c_1 c_2 c_3)$. O processo de codificação da mensagem $m = (k_1 k_2 k_3 k_4)$ pode ser expresso na forma $v = mG$, em que $G(kxn)$ é a *matriz geradora* do código, dada por

$$G = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,1 \end{bmatrix}.$$

Portanto, as palavras do código são obtidas pelas combinações lineares das linhas de G. As linhas de G são linearmente independentes e o conjunto de todas as palavras-código é um subespaço vetorial, de dimensão k, do espaço vetorial de todas $2^7 = 128$ palavras binárias de comprimento 7, ou seja, as palavras-código são os vetores do espaço-linha da matriz geradora. Esse é um código $C(7,4,3)$ cujas $2^4 = 16$ palavras são

$k_1\ k_2\ k_3\ k_4\ c_1\ c_2\ c_3$	$k_1\ k_2\ k_3\ k_4\ c_1\ c_2\ c_3$	$k_1\ k_2\ k_3\ k_4\ c_1\ c_2\ c_3$	$k_1\ k_2\ k_3\ k_4\ c_1\ c_2\ c_3$
0 0 0 0 0 0 0	0 0 0 1 0 1 1	0 1 1 0 0 1 1	1 1 0 1 0 1 0
1 0 0 0 1 1 1	1 1 0 0 0 0 1	0 1 0 1 1 0 1	1 0 1 1 0 0 1
0 1 0 0 1 1 0	1 0 1 0 0 1 0	0 0 1 1 1 1 0	0 1 1 1 0 0 0
0 0 1 0 1 0 1	1 0 0 1 1 0 0	1 1 1 0 1 0 0	1 1 1 1 1 1 1.

Quando o codificador gera as palavras-código de modo que as posições de informação estão identificadas na palavra, como na lista mostrada, diz-se que o codificador é sistemático.

Observando os pesos das palavras do código, podemos definir o que se denomina a distribuição de pesos do código, isto é, a enumeração da quantidade de palavras, A_i, que tem peso i. A Tabela 6.2 mostra a distribuição de pesos do código $C(7,4,3)$ em análise.

Tabela 6.2 - Distribuição de pesos do código $C(7,4,3)$.

i	0	3	4	7
A_i	1	7	7	1

A informação mostrada nesta tabela pode ser representada pelo *polinômio enumerador de pesos*, $W(x) \triangleq \sum_{i=0}^{n} A_i\, x^i$. No caso, $W(x) = 1 + 7x^3 + 7x^4 + x^7$.

As equações de paridade (6.1) podem ser reescritas na forma $vH^T = \bar{0}$, em que H^T denota a transposta da matriz

$$H = \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,1\,0 \\ 1\,0\,1\,1\,0\,0\,1 \end{bmatrix}, \qquad (6.2)$$

que é denominada a *matriz de paridade* do código, e $\bar{0}$ representa o vetor (000). Note que a matriz H define uma condição necessária e suficiente para que a palavra $v \in C(7,4,3)$: as palavras do código são ortogonais à qualquer linha ou combinação linear das linhas de sua matriz de paridade. Esse fato permite expressar a distancia mínima do código em termos da matriz H. Se a palavra-código v tem peso w, então, a expressão $vH^T = \bar{0}$ implica que existem w colunas da matriz H que somadas resultam no vetor $(000)^T$. Denotando por h_i as colunas de H observa-se que, por exemplo, $h_1 + h_2 + h_7 = (000)^T$, o que implica que o vetor $v = (1100001) \in C$. Diante disso, pode-se afirmar que a distância mínima do código, d, é o menor número de colunas da matriz H que somadas resultam em $(000)^T$, ou seja, d é a menor quantidade de colunas da matriz que são linearmente dependentes. Um código $C(n,k,d)$ detecta $e = d - 1$ e corrige $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros por bloco.

Em geral, as matrizes G e H de um código binário $C(n,k,d)$ têm a forma $G = [I_k|P]$ e $H = [P^T|I_{n-k}]$. Dessa forma, as equações de paridade, a matriz G e a matriz H são três formas equivalentes de representar o código, e o conhecimento de uma delas determina as outras duas.

Exemplo 6.1 - Determine as matrizes G e H dos códigos: i) De repetição $C(5,1,5)$. ii) De um único símbolo de paridade $C(4,3,2)$.

Para o código $C(5,1,5)$, temos $c_1 = c_2 = c_3 = c_4 = k_1$, de modo que $G = [11111]$ e $H = \begin{bmatrix} 1\,1\,0\,0\,0 \\ 1\,0\,1\,0\,0 \\ 1\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1 \end{bmatrix}$.

Para o código $C(4,3,2)$, temos $c_1 = k_1 + k_2 + k_3$, de modo que $H = [1111]$ e $G = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}$.

■

6.3.1 - Os códigos de Hamming

Considerando códigos binários, uma forma simples de se construir um código de grupo com distância mínima $d = 3$ é construir uma matriz H com m linhas e $2^m - 1$ colunas binárias distintas não nulas. Como H não contém a coluna toda zero, então $d > 1$; como as colunas são distintas, então $d > 2$; como todas as colunas nulas estão presentes na matriz, então a soma de quaisquer duas colunas distintas resulta numa terceira coluna presente na matriz, isto é, $\forall\, h_i, h_j \in H$, com $i \neq j$, a soma $h_i + h_j = h_k \in H$. Portanto a soma das três colunas resulta na coluna toda zero e $d = 3$. Essa é uma família de códigos $C(2^m\text{-}1, 2^m - 1 - m, 3)$, em que $m \geq 3$, construída por Richard Wesley Hamming (15 de fevereiro de 1915 - 7 de janeiro de 1998) em 1948 [Shannon 48]. Embora os códigos de Hamming tenham sido usados por Shannon em seu trabalho pioneiro sobre Teoria da Informação, os mesmos só foram publicados, em formato de artigo, em 1950 [Hamming 50].

Códigos de Hamming definidos sobre Z_p, com $p \neq 2$, também podem ser construídos. Nesse caso, se h denota uma coluna da matriz H, então nenhuma coluna linearmente dependente de h pode estar presente na matriz se o código tem $d = 3$. Assim, para cada $h \in H$, as $(p-1)$ colunas que são múltiplos de h não podem ser usadas, o que implica que esse código de Hamming tem comprimento $n = \frac{p^m-1}{p-1}$. Denotando por m o número de linhas da matriz H (isto é, $m = n - k$), o código de Hamming p-ário é um código de bloco linear $C\left(\frac{p^m-1}{p-1}, \frac{p^m-1}{p-1} - m, 3\right)$.

Exemplo 6.2 - A matriz $H = \begin{bmatrix} 111110 \\ 123401 \end{bmatrix}$ é uma matriz de paridade para o código de Hamming sobre Z_5, com $m = 2$, $C(\frac{5^2-1}{5-1} = 6, 4, 3)$. Esse código tem $5^4 = 625$ palavras e sua matriz geradora é $G = \begin{bmatrix} 100044 \\ 010043 \\ 001042 \\ 000141 \end{bmatrix}$. As equações de paridade, derivadas da expressão $vH^T = \bar{0}$, são $k_1 + k_2 + k_3 + k_4 + c_1 = 0$ e $k_1 + 2k_2 + 3k_3 + 4k_4 + c_2 = 0$. ■

6.4 - DECODIFICAÇÃO POR TABELA DE SÍNDROME

A decodificação da palavra recebida r envolve duas etapas, a detecção e a correção de erros. Todo o processo se baseia na síndrome de r, um vetor de comprimento $(n-k)$ definido por

$$S \triangleq rH^T.$$

Como $r = v + e$, a síndrome é igual a

$$S \triangleq (v + e)H^T = eH^T,$$

pois $S = vH^T = 0$. Assim, a síndrome estabelece uma relação entre a palavra recebida e o vetor erro. Essa relação é um sistema de $(n-k)$ equações e n incógnitas, cuja solução é única desde que o número de componentes não nulas do vetor erro seja $\leq t$, ou seja, desde que o peso do vetor erro seja $\leq t$.

6.4.1 - Detecção de erro

É feita por meio da síndrome. Especificamente,

i) Se $S \neq 0$, pode-se afirmar que a palavra recebida não é do código e, por isso, contém erros. Assim, quando a síndrome é diferente de zero, a ocorrência de erros é detectada. Nesse caso, ou o receptor emprega o protocolo ARQ ou então prossegue a decodificação visando a correção do erro.
ii) Se $S = 0$, pode-se afirmar que a palavra recebida, r, é uma palavra do código. Sendo assim, a mesma é entregue ao usuário como sendo a palavra transmitida estimada $\hat{v}$. Entretanto, se o vetor erro e tiver sido igual a uma palavra do código, a expressão $r = v + e$ implica que $r \in C$, mas $\hat{v} = r \neq v$. Nesse caso dizemos que ocorreu um erro indetectável. Como esse erro é uma palavra do código de peso não nulo, existem $2^k - 1$ erros indetectáveis. Quando um tal erro ocorre, o decodificador comete um erro de decodificação. A probabilidade de se ter um erro indetectável é [Lin 04]

$$P_{ei} = \sum_{i=d}^{n} A_i \, \varepsilon^i (1-\varepsilon)^{n-i}.$$

Para o código $C(7,4,3)$ discutido na Seção 6.3, cuja distribuição de pesos é mostrada na Tabela 6.2, tem-se

$$P_{ei} = 7\varepsilon^3(1-\varepsilon)^4 + 7\varepsilon^4(1-\varepsilon)^3 + \varepsilon^7.$$

Considerando $\varepsilon = 10^{-2}$, tem-se $P_{ei} \approx 7x10^{-6}$. Isso significa que, se um milhão de palavras-código são transmitidas por um BSC com $\varepsilon = 10^{-2}$, então, em média, sete palavras código erradas não serão detectadas pelo decodificador.

6.4.2 - Correção de erro

A decodificação por tabela de síndrome do código $C(7,4,3)$ é apresentada a seguir. Como esse código tem $d = 3$, vamos considerar a correção de um erro, ou seja, o vetor erro tem um único símbolo não nulo $(= 1)$. Dado que a ocorrência de erros foi detectada, a síndrome da palavra recebida é

$$S = eH^T = e_i h_i^T = h_i^T,$$

que indica a ocorrência de um erro na posição i.

Exemplo 6.3 - Decodificando a palavra recebida $r = (0000111)$. Considerando a matriz *H* da expressão (6.2), a síndrome de r é

$$S = (0000111)\, H = \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,1\,0 \\ 1\,0\,1\,1\,0\,0\,1 \end{bmatrix}^{\boldsymbol{T}} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = h_1.$$

Como $S \neq 0$, a ocorrência de erro(s) foi detectada. Considerando um BSC com $\varepsilon < 50\%$, o decodificador considera que o vetor erro introduzido pelo canal foi $e = (1000000)$ (um erro na 1a. posição da palavra), de modo que a palavra-código transmitida estimada é $v = r + e = (1000111)$. Caso dois erros tivessem ocorrido, nas posições i e j, a síndrome seria $S = h_i + h_j = h_k$, em que h_k é outra coluna da matriz H, o que indicaria a ocorrência de um erro na posição k, o que não é verdade. Nesse caso, ao tentar corrigir o erro, o decodificador acrescentaria um terceiro erro à palavra transmitida, cometendo um erro de decodificação. Observe portanto que, embora esse código tenha $d = 3$, e seja capaz de corrigir um err e detectar dois erros por bloco, ele não tem a capacidade de fazer isso simultaneamente. Isso ocorre porque o decodificador não consegue distinguir a ocorrência de um único erro da ocorrência de dois erros, uma vez que ambos possuem síndrome igual à uma coluna da matriz H. ■

6.5 - OS CÓDIGOS EXPURGADO E ESTENDIDO

Para superar a dificuldade delineada no Exemplo 6.3, podemos fazer uma modificação na matriz H, de modo a obter um código que tenha a capacidade de identificar quantos erros, se 1 ou 2, ocorreram durante a transmissão. Duas abordagens com essa finalidade são apresentadas a seguir.

6.5.1 - O código expurgado C_{ex}

Para construir o código expurgado, usa-se a matriz H_{ex}, obtida acrescentando-se uma linha contendo apenas 1´s (a linha toda 1) à matriz H de (6.2), ou seja,

$$H_{ex} = \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,1\,0 \\ 1\,0\,1\,1\,0\,0\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{bmatrix}.$$

Caso ocorra apenas um erro, a decodificação procede como explicado no Exemplo 6.3. Se dois erros ocorrerem a síndrome é da forma $(h0)^T$, em que h^T é uma coluna de H. Como essa coluna não se encontra na matriz H_{ex}, então a ocorrência de dois erros foi detectada (na verdade, a ocorrência de um número par de erros), e então o decodificador não tenta corrigi-los pois sabe que sua capacidade de correção é de apenas um único erro. Assim, o código expurgado tem a capacidade de corrigie um erro e detectar dois erros, *simultaneamente*. C_{ex} é um código $(7, 3, 4)$, que só tem palavras de peso par. Isso ocorre porque as palavras de peso ímpar foram *expurgadas* (removidas) do código. Sua distribuição de pesos é mostrada na Tabela 6.3, em que se pode observar que todas as palavras-código, excetuando-se a palavra toda zero, tem peso igual a 4. Por essa razão, esse código é dito ser um código de

peso constante (do inglês, *constant weight code*). É possível mostrar que $C_{ex}(7,3,4)$ é o código dual do código de Hamming $C(7,4,3)$ (veja o problema 29).

Tabela 6.3 - Distribuição de pesos do código $C_{ex}(7,3,4)$.

i	0	4
A_i	1	7

6.5.2 - O código estendido C_{es}

Para construir o código estendido, usa-se a matriz H_{es}, obtida acrescentando-se uma linha contendo apenas 1´s (a linha toda 1) e a coluna $(0001)^T$ à matriz H de (6.2), ou seja,

$$H_{es} = \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,0\,0 \\ 1\,0\,1\,1\,0\,0\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1 \end{bmatrix}.$$

Por meio da mesma argumentação usada para o código expurgado, mostra-se que o código estendido tem, também, a capacidade de corrigir um erro e detectar dois erros, *simultaneamente*. C_{es} é um código $(8,4,4)$, que só tem palavras de peso par. Isso ocorre porque todas as suas palavras foram estendidas, acrescentando-se um bit de paridade c_4 sobre toda a palavra, isto é, $c_4 = k_1 + k_2 + k_3 + k_4 + c_1 + c_2 + c_3$. Dessa forma, todas as palavras de peso ímpar do código original, passarão a ser palavras de peso par. As palavras de peso par não terão seu peso alterado. A distribuição de pesos $C_{es}(8,4,4)$ é mostrada na Tabela 6.4. observe que estender $C_{es}(8,4,4)$ não aumenta sua distância mínima,

Tabela 6.2 - Distribuição de pesos do código $C_{es}(8,4,4)$.

i	0	4	8
A_i	1	14	1

Exemplo 6.4 - Expurgando-se e estendendo-se o código de Hamming binário $C(2^m - 1, 2^m - 1 - m, 3)$ obtém-se, respectivamente, os códigos $C_{ex}(2^m - 1, 2^m - 2 - m, 4)$ e $C_{es}(2^m, 2^m - 1 - m, 4)$.'

As técnicas apresentadas nesta seção mostram como se construir códigos novos a partir de códigos já existentes. Existem seis maneiras de fazer isso, denominadas [Camp 83]

i) Estender um código: aumentar $n - k$ (aumentando n e mantendo k constante).

ii) Perfurar um código: diminuir $n - k$ (diminuindo n e mantendo k constante).

iii) Expurgar um código: diminuir k (aumentando $n - k$ e mantendo n constante).

iv) Aumentar um código: aumentar k (diminuindo $n - k$ e mantendo n constante).

v) Alongar um código: aumentar n (aumentando k e mantendo $n-k$ constante).

vi) Encurtar um código: diminuir n (diminuindo k e mantendo $n-k$ constante).

6.6 - COTAS EM CÓDIGOS

Um dos objetivos da teoria da codificação é o de construir bons códigos. Nesse sentido um código pode ser denominado ótimo, se

i) Dados os valores de n e k, o valor de d seja o maior possível; ou então
ii) Dados os valores de n e d, o valor de k seja o maior possível; ou então
iii) Dados os valores de k e d, o valor de n seja o menor possível.

Esses critérios nem sempre levam aos mesmos códigos [MacWilliams 89]. Em qualquer caso, entretanto, os parâmetros n, k, d não são independentes, isto é, dados quaisquer dois dêles, o terceiro pode assumir valores apenas dentro de uma faixa limitada. Essa faixa é definida pelo que chamamos cotas ou limitantes.

6.6.1 - A cota de Singleton

Em um código de bloco linear binário, os blocos de informação de apenas um bit (isto é, de peso 1) vão estar presentes em k palavras-código. Ao preenchermos as seções de paridade correspondentes à essas mensagens, o melhor que se pode esperar das equações de paridade do código, em relação a se obter um peso mínimo alto das palavras, é de que elas resultem em seções de paridade contendo apenas o bit 1, isto é, em seções de paridade que tenham peso $n-k$. Diante disso, o peso mínimo de um código de bloco linear $C(n,k,d)$ não pode ser maior do que $n-k+1$, isto é, $d \leq n-k+1$. Essa é a chamada cota de Singleton, uma cota superior para a distância mínima [Singleton 64]. Um código que satisfaz a cota de Singleton na igualdade, isto é, um código em que $d = n-k+1$, é denominado código MDS (do inglês *maximum distance separable*). Os únicos códigos MDS binários são os códigos de repetição $C(n,1,n)$ e os códigos SPC $C(n,n-1,2)$. Uma classe de códigos MDS não binários muito importante, é a classe dos códigos Reed-Solomon [Wicker 95, p. 175].

6.6.2 - A cota de Hamming

Na decodificação por tabela de síndrome, a cada padrão de erro (o vetor erro, e) corrigível, é associado uma síndrome, um sintoma do erro. Portanto, para que o código seja capaz de corrigir todos os erros de peso até t, é necessário que exista uma quantidade de síndromes que seja, pelo menos, igual ao total de padrões de erro corrigiveis. Para um código binário $C(n,k,d)$, a síndrome é um vetor binário com $(n-k)$ componentes. Portanto, pode-se escrever que, se esse código corrige qualquer padrão de erro de peso $\leq t$, então seus parâmetros têm que satisfazer a condição

$$C_n^1 + C_n^2 + \cdots + C_n^t \leq 2^{n-k} - 1.$$

Essa é a cota de Hamming, uma cota superior para a capacidade de correção, t. Um código que satisfaz a cota de Hamming na igualdade, isto é, um código em que $\sum_{i=1}^{t} C_n^i = 2^{n-k} - 1$ é denominado código *perfeito*. O termo significa que nenhuma síndrome é desperdiçada no processo de decodificação. Os códigos de Hamming e os códigos de repetição de comprimento ímpar são perfeitos. Além destes, os únicos códigos perfeitos são os códigos de Golay [Golay 49]. De fato, não existem mais códigos perfeitos [Tietäväinen 73].

Um comentário final sobre cotas, em geral. Um código só pode existir se seus parâmetros satisfazem às cotas (todas; existem várias outras cotas além das que foram apresentadas nesse texto introdutório). Assim, se os números n, k e d violam uma cota (qualquer uma), então o código $C(n, k, d)$ não existe. Entretanto, se os mesmos satisfazem a uma ou mesmo a várias cotas, isso significa apenas que o código *pode* existir, mas não garante sua existência, a qual só é comprovada com a efetiva construção do código, por meio das equações de paridade, ou das matrizes G ou H. Em outras palavras, o atendimento às cotas é uma condição necessária para a existência de um código, mas não é uma condição suficiente.

6.6.3 - A cota de Plotkin

Essa cota tem uma interpretação simples. Dadas as notas diferentes de zero obtidas por alunos que se submeteram a uma prova, pode-se afirmar que a nota mínima é menor ou, no máximo, igual a média das notas, com a igualdade ocorrendo caso todas as notas tenham sido iguais. O mesmo vale para o peso mínimo e para a média dos pesos de um código. Existem $2^k - 1$ palavras com peso não nulo em um código de bloco linear. Para se calcular a soma dos pesos de todas essas palavras, usa-se a propriedade de que, na matriz de dimensões $2^k x\ n$, cujas linhas são as palavras do código, todas as colunas tem peso igual a 2^{k-1} (a prova desse resultado pode ser feita por indução). Portanto, a condição peso mínimo $\leq$ média dos pesos, pode ser expressa por

$$d \leq \frac{n2^{k-1}}{2^k - 1},$$

um resultado conhecido como a cota de Plotkin [MacWilliams 89, p. 41]. Códigos que satisfazem a cota de Plotkin na igualdade são denominados códigos de peso constante. O código $C_{ex}(7, 3, 4)$ da Seção 6.5.2 é um exemplo de código de peso constante.

PROBLEMAS

1) a) Mostre, a partir do código de Hamming C(15, 11, 3), como construir códigos com distancia mínima d = 4. Que valores de n e k você obtem ?
b) Dê exemplos de códigos de bloco lineares binários que tem a maior distancia mínima possível.

2) a) Projete um decodificador para o código de Hamming C(7, 4, 3) cujas equações de paridade são C1 = K1 + K2 + K3, C2 = K1 + K2 + K4 e C3 = K2 + K3 + K4 e decodifique a palavra recebida r = 1000100.
b) Projete um decodificador para o código cujas equações de paridade são C1 = K1 + K2+ K3, C2 = K1 + K3 + K4, C3 = K1 + K2 + K4, C4 = K2 + K3 + K4 e decodique a palavra recebida r = 11000011.

3) O código estendido (H_E) do código de Hamming de comprimento 7 é usado para transmissão em um canal ruidoso. Considere a seguinte matriz do código original: $H = \begin{bmatrix} 1000111 \\ 0101011 \\ 0011110 \end{bmatrix}$. Encontre os parâmetros de H_E. Justifique. Decodifique os vetores r_1 = 01110011 e r_2 = 11100010 (decodificação por síndrome).

4) Mostre que um código linear é capaz de, simultaneamente, corrigir F erros e detetar E erros se sua distancia mínima é, pelo menos, E + F + 1.

5) a) Encontre as matrizes G e H de : i) Um código de repetição. ii) Um código de um único dígito de paridade.

6) Encontre os parâmetros do código C (n, k, d) cuja matriz geradora é da forma G_1 | G_2, onde G_1 e G_2 são, respectivamente as matrizes geradoras dos códigos C_1 (N1, K1, D1) e C_2 (N2, K2, D2).

7) Encontre os parâmetros do código C (n, k, d) cujas palavras são da forma u | v, onde u $\in C_1$ (N1, K1, D1) e v $\in C_2$ (N2, K2, D2).

8) Encontre a distancia mínima e a distribuição de pesos do código C cujas palavras satisfazem as equações: 1) C1+K1+K2 = 0. 2) C2+K2+K3 = 0. 3) K1+K3+C3 = 0. Decodifique o vetor recebido r = 011001. É possível aumentar o valor de d? Como?

9) Qual a maior distancia mínima que seria possível obter considerando códigos de bloco lineares binários de comprimento 15 com 8 símbolos de informação ?

10) Prove que os códigos de Hamming são perfeitos.

11) Dado o código C(n, k, d), com matrizes G e H, considere o código C_d, com matrizes $G_d = H$ e $H_d = G$. Qual a relação entre as palavras de C e de C_d ? Prove que, se $C = C_d$, então as palavras de C tem comprimento par. C_d é chamado o código dual de C.

12) Projete os circuitos codificador e decodificador para o código de Hamming C(7, 4, 3) cujas equações de paridade são C1 = K1 + K2 + K3, C2 = K1 + K2 + K4 e C3 = K2 + K3 + K4. Decodifique a palavra recebida r = 1000100.

13) Encontre os parâmetros do código C(n, k, d) cuja matriz geradora G é da forma $G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$, onde G_1 e G_2 geram, respectivamente, códigos C_1(N1, K1, D1) e C_2(N2, K2, D2).

14) É sempre possível aumentar a distancia mínima de um código acrescentando-se um bit de paridade sobre todos os bits de suas palavras ? Por que ?

15) Prove as cotas de: a) Singleton. b) Hamming. c) Plotkin.

16) Dê exemplos de códigos de bloco lineares que tem a maior distancia mínima possível.

17) Sabendo que um código C(23, 12, d) é perfeito, determine sua distância mínima.

18) Determine a distância mínima e as capacidades de deteção e correção do código binário C = {00100, 10010, 01001, 11111}.

19) Códigos de repetição binários de comprimento ímpar são perfeitos? Por que?

20) Projete um código de bloco linear binário *C* para proteger a transmissão de 7 mensagens através de um canal ruidoso. Seu projeto deve otimizar o valor de *n* (o comprimento do código), levando em conta que o código deve ser capaz de simultaneamente corrigir um erro e detetar dois erros por bloco. Determine os valores de *n*, *k* e *d* e as equações de paridade de *C*.

21) Encontre os parâmetros do código que se obtém suprimindo-se as colunas de peso ímpar da matriz de paridade do código de Hamming que tem oito dígitos de paridade.

22) Considere um código de bloco linear binário C no qual os deslocamentos cíclicos de qualquer palavra código também são palavras código de C. Sabendo que v = (1110100) $\in$ C, decodifique as palavras: i) r = (0000111). ii) r = (0001001). Qual a distância mínima de C?

23) Dispõe-se de até 4 bits de paridade para projetar um esquema para controle de erros em um sistema de comunicação digital. Considerando que o *hardware* disponível para o projeto do codificador usa um processador de 8 bits, esse valor é escolhido para comprimento das palavras do código.

a) Nessas condições, é possível construir um código de bloco linear binário, com taxa 1/2, para proteger mensagens que podem ser ou um dos dias da semana ou um dos dígitos decimais 0, 1, ..., 9? Por que?
b) É possível construir um código para proteger as mensagens acima, que seja capaz de, simultaneamente, corrigir um erro e detectar dois erros por bloco? Por que?
c) Agora considerando apenas as informações iniciais sobre os valores de n e de n-k, encontre a matriz H e as equações de paridade de um código de taxa máxima com distancia mínima 3. Qual o valor de R?

24) Projete um código de bloco linear binário C para proteger a transmissão de 15 mensagens através de um canal ruidoso. Seu projeto deve otimizar o valor de n (o comprimento do código), levando em conta que o código deve ser capaz de, simultaneamente, corrigir um erro e detectar dois erros por bloco. Determine os valores de n, k e d e as equações de paridade de C. Repita para 8 mensagens.

25) Considere um arranjo retangular (uma matriz) onde as linhas são palavras de um código de bloco linear C1 (n1, k1, d1) e as colunas são palavras de outro código linear C2 (n2, k2, d2). Cada arranjo assim formado é uma palavra de um código Cp (n, k, d). Determine os parâmetros de Cp.

26) Em uma rede de computadores, padrões de erro de peso até dois precisam ser corrigidos por um código de bloco linear binário C de taxa máxima e dimensão 2. Construa as matrizes geradora e de paridade e as equações de paridade de C. Qual a taxa de C?

27) Dispõe-se de, no máximo, 5 bits de paridade para projetar um esquema para controle de erros em um sistema de comunicação digital. Considerando que o *hardware* disponível para o projeto do codificador usa um processador de 16 bits, esse valor é escolhido para comprimento das palavras do código. Nessas condições, É possível construir um código de bloco linear binário, com taxa 3/4, para proteger mensagens que podem ser um dos inteiros do conjunto {1, ..., 31}? Por que?

28) É possível construir um código para proteger as mensagens da questão anterior, que seja capaz de, simultâneamente, corrigir um erro e detectar dois erros por bloco? Em caso positivo, construa a matriz de paridade desse código e indique sua taxa. Caso isso não seja possível, justifique.

29) Encontre a distribuição de pesos e determine os parâmetros (n, k, d) do código dual do código de Hamming (7, 4, 3).

30) Indique dois modos distintos de construir um código de bloco linear binário com capacidade de correção de t = 4 erros. Em cada caso, indique a taxa do código obtido (não é necessário apresentar as matrizes G e H do código, nem suas equações de paridade).

31) Indique dois modos de construir um código de bloco linear binário com capacidade de correção de t = 7 erros e taxa R>50% (Não é necessário apresentar as matrizes G e H do código, nem suas equações de paridade).

32) Indique como construir um código de bloco linear binário com taxa R>50% e capacidade de corrigir 3 erros e detectar 6 erros, simultaneamente (Não é necessário apresentar as matrizes G e H do código, nem suas equações de paridade).

33) Encontre os parâmetros do código que se obtém suprimindo-se as colunas de peso ímpar da matriz H do código de Hamming que tem 10 dígitos de paridade. Esse código é melhor do que o código de Hamming C(1023, 1013, 3)? Por que?

34) Qual código tem melhor taxa: O código C(n, k, d) ou seu dual C_d?

35) A matriz geradora de um código de bloco linear C (n, k, d) tem inversa? Por que?

36) Construa, na forma sistemática, uma matriz de verificação de paridade para o código de Hamming, definido sobre GF(5), que tem dois símbolos de paridade. Quais as equações de paridade do código? Quantas palavras esse código tem? Codifique uma mensagem de peso igual a 1.

37) Considere o código de Hamming C(n, k, d) sobre GF(5), cujas equações de paridade são: i) $c_1+k_1+ k_2 + k_3 + k_4 = 0$. ii) $c_2 + k_1+ 2k_2 + 3k_3 + 4k_4= 0$. Qual a matriz G do código? Esse código é perfeito? Por que? Decodifique a palavra recebida r = (104031).

38) Qual a matriz geradora de um código produto formado pelo códigos $C_1(4, 3, 2)$ e $C_2(3, 2, 2)$. Comente sobre a capacidade de controle de erros desse código.

39) Considere o código de Hamming C(n, k, d) definido sobre GF(7), cujas equações de paridade são: i) $c_1+k_1+ k_2 + k_3 + k_4 + k_5 + k_6 = 0$. ii) $c_2 + k_1+ 2k_2 + 3k_3 + 4k_4+ 5k_5 + 6k_6 = 0$. Esse código é perfeito? Por que? Qual a matriz G do código? Decodifique a palavra recebida r = (11000050).

40) A partir do código Simplex C(7, 3, 4) cujas equações de paridade são $C_1= K_1 + K_2$, $C_2 = K_1 + K_3$, $C_3 = K_2 + K_3$ e $C_4 = K_1 + K_2 + K_3$, mostre como se obter um código linear C(4, 3, 2). Qual a matriz H de C?

41) Alongar um código C(n, k, d) significa aumentar seu comprimento para n+1, mantendo constante o número de símbolos de paridade. Determine a matriz H do código C_a que se obtém alongando-se o código C_s cujas equações de paridade são C1 = K1 + K2, C2 = K1 + K3, C3 = K2 + K3, C4 = K1 + K2 + K3. A distância mínima de C_a deve ser a mesma de C_s.

42) Considere o código produto formado por dois códigos de um símbolo de paridade sobre GF(3), C1(3, 2, 2) e C2(3, 2, 2). Quantas palavras tem esse código? Qual sua matriz H? Indique uma palavra desse código produto. Decodifique, usando a matriz H, o arranjo recebido cujas linhas são [(111) (111) (110)]. (Sugestão: em um código p-ário de um símbolo de paridade, a equação de paridade é $c_1 = -\sum_{i=1}^{n-1} k_i \pmod p$.

43) Construa um código perfeito diferente do código de Hamming. Devem ser indicados os parâmetros do código (valores de n, k e d), bem como sua matriz H. Justifique porque o código construído é perfeito.

44) Qual a taxa e a capacidade de correção do código produto formado por dois códigos de Hamming ternários com 4 símbolos de paridade? Por que?

45) Considere o código de Hamming C cujas equações de paridade são: C1 = K1 + K2 + K3, C2 = K1 + K2 + K4, C3 = K2 + K3 +K4. a) Encontre a matriz de paridade do código estendido C_E. b) Uma palavra v de C_E é transmitida por um canal ruidoso e recebida como r =(10000001). Decodifique r.

46) Apresente a matriz de paridade de um código MDS não binário.

47) Apresente um código de bloco linear binário com taxa maior que 81% e capacidade de correção de até 7 erros por bloco.

48) Considere o código de Hamming C(n, k, d) definido sobre GF(3), cujas equações de paridade são: i) $c_1+k_1+ k_2 + k_4 + k_5 + k_6 + k_7+ k_8 + k_9 = 0$. ii) $c_2 + k_1+ k_3+ 2k_5 + k_6 + 2k_7+ 2k_8 + k_9 + k_{10} = 0$. iii) $c_3 + k_2+ 2k_3+ 2k_4 + 2k_6 + k_7+ 2k_8 + k_9 + k_{10} = 0$. Decodifique a palavra recebida r = (1120000000122).

REFERÊNCIAS

[Camp 83] M. M. Campello de Souza, A Graph-Theoretic Approach to Anticodes, PhD Thesis, Manchester University, UK, 1983.

[Golay 49] M. J. E. Golay, Notes on Digital Coding, *Proc. IRE,* vol. 37, p. 637, 1949.

[Hamming 50] R. W. Hamming, Error Detecting and Error Correcting Codes, *Bell Systems Technical Journal*, vol. 29(2), pp. 147-160, april 1950.

[Khinchin 57] I. Kinchin, *Mathematical Foundations of Information Theory*, Dover, 1957.

[Lin 04] S. Lin and D. J. Costello Jr., *Error Control Coding*, 2a. ed., Pearson Prentice Hall, 2004.

[MacWilliams 89] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1978.

[Peterson 03] L. L.Peterson and B. S. Davie, *Computer Networks: A Systems Approach*, 3rd ed., Morgan Kaufmann, 2003.

[Shannon 48] C. E. Shannon, A Mathematical Theory of Communication, *Bell System Technical Journal*, , vol. 27, pp. 379–423, 623-656, July, October, 1948. Republicado em: C. E. Shannon and W. Weaver, Eds., *A Mathematical Theory of Communication*, University of Illinois Press, 1963.

[Shannon 37] A Symbolic Analysis of Relay and Switching Circuits, *MSc dissertation*, Massachussets Institute of Technology, Aug. 10, 1937.

[Singleton 64] R. C. Singleton, Maximum Distance q-nary Codes, *IEEE Transactions on Information Theory*, vol. IT-10, pp. 116-118, 1964.

[Slepian 56] D. Slepian, A Class of Binary Signalling Alphabets, *Bell System Technical Journal,* vol. 35, pp. 203-234, January, 1956.

[Sloane 93] *CLAUDE ELWOOD SHANNON*: *Collected Papers*, Eds. N.J.A Sloane and Aaron D. Wyner, IEEE press, 1993.

[Tanenbaum 11] A. S. Tanenbaum e D. Wetherall, *Redes de Computadores*, 5a. ed., Pearson, 2011.

[Tietäväinen 73] A. Tietäväinen, On the Nonexistence of Perfect Codes over Finite Fields, *SIAM Journal on Applied mathematics* 24, pp. 88-96, 1973.

[Wicker 95] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, 1995.