DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO – UFRJ
NÚMEROS INTEIROS E CRIPTOGRAFIA RSA

S. C. COUTINHO

1. Respostas dos exercícios do capítulo 1

(1) (a) $\text{mdc}(14, 35) = 7$; $\alpha = -2$ e $\beta = 1$;
(b) $\text{mdc}(252, 180) = 36$, $\alpha = -2$ e $\beta = 3$;
(c) $\text{mdc}(6643, 2873) = 13$, $\alpha = -16$ e $\beta = 37$.

(2) Para verificar (1) e (2) simplesmente use o algoritmo euclidiano. Para fazer (3) observe antes que:

$$(n+1)(n!+1) - ((n+1)!+1) = n.$$

Chamando de d o $\text{mdc}(n!+1, (n+1)!+1)$, concluímos que d divide n. Então este d divide $n!+1$ e n, logo d divide 1; isto é $d = 1$.

(3) Digamos que dividindo n por m temos quociente q e resto r; isto é, $n = mq + r$. Queremos mostrar que $2^r - 1$ é o resto da divisão de $2^n - 1$ por $2^m - 1$; isto é, queremos mostrar que existe um inteiro Q tal que

$$2^n - 1 = (2^m - 1)Q + 2^r - 1 \quad \text{e} \quad 0 \leq 2^r - 1 < 2^m - 1.$$

Observe que se estas equações são satisfeitas então o resto é $2^r - 1$ por causa da unicidade do resto da divisão. Note que, como $0 \leq r < m$, então

$$2^0 \leq 2^r < 2^m \quad \text{donde} \quad 0 \leq 2^r - 1 < 2^n - 1.$$

Precisamos agora mostrar que existe um inteiro Q tal que $2^n - 1 = (2^m - 1)Q + 2^r - 1$. Mas desta equação concluímos que

$$Q = \frac{(2^n - 1) - (2^r - 1)}{2^m - 1} = \frac{2^n - 2^r}{2^m - 1}.$$

Como $2^n - 2^r = 2^r(2^{n-r} - 1) = 2^r(2^{mq} - 1)$, então

$$\frac{2^n - 2^r}{2^m - 1} = \frac{2^r(2^m - 1)(2^{mq-1} + \cdots + 1)}{2^m - 1} = 2^r(2^{mq-1} + \cdots + 1),$$

é um número inteiro, e isto completa a solução.

(4) (1) Pelo exercício anterior temos que $2^{2^n} - 1$ é divisível por $2^{2^{m+1}} - 1$, já que 2^{m+1} divide 2^n. Assim existe Q tal que

$$\begin{aligned} 2^{2^n} - 1 &= (2^{2^{m+1}} - 1)Q \\ &= (2^{2^m} + 1)(2^{2^m} - 1)Q, \end{aligned}$$

o que mostra que $2^{2^m} + 1$ divide $2^{2^n} - 1$ quando $n > m$. O quociente é $(2^{2^m} - 1)Q$, onde Q é calculado como no exercício anterior.

(2) De (1) temos que

$$\begin{aligned} 2^{2^n}+1 &= (2^{2^n}-1)+2 \\ &= (2^{2^m}+1)(2^{2^m}-1)Q+2. \end{aligned}$$

Portanto o resto da divisão de $2^{2^n}+1$ por $2^{2^m}+1$ é 2.
(3) Basta aplicar o algoritmo euclidiano. Dividindo $2^{2^n}+1$ por $2^{2^m}+1$ temos resto 2. Dividindo $2^{2^m}+1$ por 2 temos resto 1. Logo o mdc desejado é 1.

(5) (1) Copie a idéia da demonstração do *Algoritmo Euclidiano*. Mostre que dividindo f_n por f_{n-1} o quociente é 1 e o resto é f_{n-2}. Conclua que o *mdc* de dois números de Fibonacci consecutivos é sempre o mesmo. Com isto o problema se reduz a calcular $\text{mdc}(f_2, f_3) = \text{mdc}(1, 2) = 1$.
(2) Temos que fazer $n-1$ divisões para calcular $\text{mdc}(f_n, f_{n-1})$ se $n \geq 4$; supondo que a última divisão é a que dá resto zero.

(6) Seja m o menor múltiplo comum de a e b e seja $r = a'b'd$. Como

$$r = a'b'd = ab' = a'b,$$

então r é um múltiplo comum de a e b. Portanto $m \leq r$.

Por outro lado, como m é um múltiplo de a e também de b, então existem inteiros x e y tais que $m = ax = by$. Seja $d = \text{mdc}(a, b)$. Logo existem inteiros a' e b' tais que $a = da'$ e $b = db'$; observe que $\text{mdc}(a', b') = 1$. Cancelando d de ambos os membros de $ax = by$, concluímos que $a'x = b'y$. Pelo algoritmo euclidiano estendido existem inteiros α e β tais que $a'\alpha + b'\beta = 1$. Multiplicando esta equação por x ficamos com $xa'\alpha + xb'\beta = x$. Mas $xa' = yb'$, donde

$$x = yb'\alpha + xb'\beta = b'(y\alpha + x\beta).$$

Portanto b' divide x. Temos então que $a'b'd$ divide $ax = a'dx$. Logo $r \leq m$. Como já havíamos provado que $m \leq r$, concluímos que $m = a'b'd = ab/d$.

(7) Usando a notação do exercício temos que $a = da'$ e $b = db'$. Portanto se a equação $ax + by = c$ tem solução x_0, y_0, obtemos

$$c = ax_0 + by_0 = da'x_0 + db'y_0 = d(a'x_0 + b'y_0).$$

Donde concluímos que a equação só pode ter solução se d dividir c. Se isto acontecer, então escrevendo $c = dc'$, substituindo isto na equação acima e cancelando d, temos

$$c' = a'x_0 + b'y_0.$$

Chamando $a'x + b'y = c'$ de *equação reduzida*, concluímos que qualquer solução da equação original também é solução da reduzida. Mas a recíproca também é verdadeira, porque para passar da reduzida para a equação original basta multiplicá-la por d.

Finalmente é fácil obter soluções da equação reduzida usando o algoritmo euclidiano estendido. Observe que como $d = \text{mdc}(a, b)$ e $a = da'$ e $b = db'$, então $\text{mdc}(a', b') = 1$. Aplicando o algoritmo euclidiano estendido encontramos inteiros α e β tais que $a\alpha + b\beta = 1$. Multiplicando por c',

temos que $c' = a(c'\alpha) + b(c'\beta)$. Logo $x = c'\alpha$ e $y = c'\beta$ é uma solução da equação reduzida; e, portanto, da equação original, conforme já vimos acima.

2. Respostas dos exercícios do capítulo 2

(1) Fatorando 26 e 39, a equação dada toma a forma

$$2^{x+y} \cdot 3^4 \cdot 13^y = 3^z \cdot 13^z.$$

Como a fatoração em primos é única, podemos comparar os expoentes dos dois lados, obtendo

$$x + y = 0, \quad z = 4, \quad z = y.$$

Como x, y, e z são inteiros não negativos, concluímos da primeira equação que $x = y = 0$. Portanto o sistema é impossível; isto é, não existem inteiros não-negativos que satisfaçam à equação dada.

(2) Observe que se $1 < i \leq k$, então $k! + i$ é divisível por i. Como $k! + i > i > 1$, temos que $k! + i$ é composto. Dado um inteiro qualquer m, a seqüência

$$(m+1)! + 2, \ldots, (m+1)! + (m+1)$$

tem m inteiros consecutivos que, como vimos, são todos compostos.

(3) Um fator de 175557 é 421, um fator de 455621 é 677 e um fator de 731021 é 857.

(4) (a) Escreva $\sqrt{6}$ como uma fração reduzida e obtenha uma contradição. Mas cuidado: 6 não é primo!
(b) É, porque a soma de duas frações é sempre uma fração.
(c) Não. Sabemos que $\sqrt{2}$ é irracional e que $2 - \sqrt{2}$ é irracional por (2). Mas a soma dos dois é 2, que é racional.
(d) Não. Elevando ao quadrado

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}.$$

Se $\sqrt{2} + \sqrt{3}$ fosse uma fração, então o seu quadrado também seria. Mas isto implicaria que $\sqrt{6}$ é racional, o que sabemos ser falso por (1).

(5) Temos que $R(n) = (10^n - 1)/3$ e $R(k) = (10^k - 1)/3$. Portanto para mostrar que $R(k)$ divide $R(n)$, basta mostrar que $10^k - 1$ divide $10^n - 1$. Suponhamos que $n = kt$; então

$$10^n - 1 = 10^{kt} - 1 = (10^k - 1)(10^{k(t-1)} + 10^{k(t-2)} + \cdots + 10^k + 1),$$

que mostra o que queremos.

(6) Como p é o menor fator primo de n, temos que $p \leq \sqrt{n}$. Mas, por hipótese, $p \geq \sqrt{n}$. Logo $p = \sqrt{n}$; ou seja $n = p^2$. Aplicando o algoritmo euclidiano a $6n + 7$ e $3n + 2$, verificamos que têm mdc igual a 1. Como $p - 4$ divide este mdc, devemos ter que $p - 4$ é 1 ou -1. No primeiro caso $p = 5$, no segundo $p = 3$. Portanto os valores possíveis para n são 9 e 25.

(7) A multiplicidade de p_i na fatoração do $\mathrm{mdc}(a,b)$ é $\min\{e_i, r_i\}$. A multiplicidade de p_i na fatoração de $\mathrm{mmc}(a,b)$ é $\max\{e_i, r_i\}$.

(8) Como estamos supondo que $2^{s+1}-1$ é primo, os divisores de $2^s(2^{s+1}-1)$ são

$$1, \qquad 2, \qquad 2^2, \qquad \ldots, \qquad 2^s;$$

$$2^{s+1}-1, \quad 2(2^{s+1}-1), \quad 2^2(2^{s+1}-1), \quad \ldots, \quad 2^s(2^{s+1}-1).$$

Os divisores na primeira linha formam uma progressão geométrica de razão 2 e primeiro termo 1; os da segunda linha formam uma progressão geométrica de razão 2 e primeiro termo $2^{s+1}-1$. Isto verifica o que é pedido em (1); passemos a (2). Assim a soma dos divisores da primeira linha é $2^{s+1}-1$ e a soma dos divisores da segunda linha é $(2^{s+1}-1)(2^{s+1}-1)$. Somando os dois obtemos

$$2^{s+1}-1+(2^{s+1}-1)(2^{s+1}-1) = (2^{s+1}-1)(1+2^{s+1}-1) = 2^{s+1}(2^{s+1}-1)$$

que é o dobro de $2^s(2^{s+1}-1)$. Portanto este número é perfeito.

(9) (1) Qualquer inteiro positivo r tem pelo menos dois fatores: 1 e r. Portanto $S(r) \geq 1+r$, qualquer que seja r. Se $S(r) = 1+r$, então r não pode ter nenhum outro fator além de 1 e r; logo r tem que ser primo.
(2) Isto á apenas a definição de número perfeito.
(3) Sejam d, b_1, b_2 e d_1 e d_2 como no problema. Como d_1 divide d, podemos escrever $d = d_1c$, para algum inteiro positivo c. Como $\mathrm{mdc}(d_1, d_2) = 1$ e d_2 divide $d = d_1c$, então pelo lema da seção 6 temos que d_2 divide c; em particular $d_2 \leq c$. Por outro lado, $\mathrm{mdc}(c, b_1) = 1$, e c divide $d = b_1b_2$. Portanto, novamente pelo lema da seção 6 temos que c divide b_2. Assim c é um divisor comum entre b_2 e d, donde $c \leq d_2$. Concluímos daí que $d_2 = c$, e a demonstração do resultado está completa.
(4) Vamos listar os divisores de b_1 e de b_2:

$$\begin{array}{lccccc} \text{divisores de } b_1\text{:} & a_0 = 1, & a_1, & a_2, & \ldots, & a_m \\ \text{divisores de } b_2\text{:} & c_0 = 1, & c_1, & c_2, & \ldots, & c_n \end{array}$$

Mas

$$S(b_1)S(b_2) = (1+a_1+a_2+\cdots+a_m)(1+c_1+c_2+\cdots+c_n).$$

Efetuando o produto, concluímos que $S(b_1)S(b_2)$ é a soma dos números da forma a_ic_j com $0 \leq i \leq m$ e $0 \leq j \leq n$ que, como vimos acima, são exatamente os divisores de b_1b_2. Portanto $S(b_1)S(b_2) = S(b_1b_2)$.

(10) (1) Suponhamos que n é um inteiro positivo par. Então podemos fatorar a maior potência possível de 2 que divide n e escrever $n = 2^st$, onde t é um inteiro positivo ímpar. Como $\mathrm{mdc}(2^s, t) = 1$ podemos usar (4) do exercício anterior para concluir que $S(2^st) = S(2^s)S(t)$. Mas os fatores de 2^s são $1, 2, \ldots, 2^s$; que formam uma progressão geométrica cuja soma é $2^{s+1}-1$. Portanto

$$S(n) = (2^{s+1}-1)S(t).$$

Suponhamos, agora, que n é perfeito; isto é, que $S(n) = 2n$. Então

$$(\star) \qquad 2^{s+1}t = (2^{s+1}-1)S(t).$$

Como $\text{mdc}(2^{s+1}, 2^{s+1}-1) = 1$, concluímos que 2^{s+1} divide $S(t)$.
(2) De (1) sabemos que podemos escrever $S(t) = 2^{s+1}q$, para algum inteiro positivo q. Substituindo na fórmula $(\star)$ acima

$$2^{s+1}t = (2^{s+1}-1)2^{s+1}q,$$

donde $t = (2^{s+1}-1)q$.
(3) Queremos mostrar que $q = 1$. Digamos, por contradição, que $q > 1$. Então t tem pelo menos três fatores: 1, q e t; donde $S(t) \geq 1 + q + t$. Mas, por outro lado,

$$S(t) = 2^{s+1}q = (2^{s+1}-1)q + q = t + q,$$

uma contradição. Logo $q = 1$.
(4) Como $q = 1$ por (3), temos que

$$t = 2^{s+1} - 1 \quad \text{e} \quad S(t) = 2^{s+1}.$$

Juntamente com (1) do exercício anterior isto implica que t é primo.

Reunindo o que provamos temos:

- $n = 2^s t$;
- $t = 2^{s+1} - 1$;
- t é primo.

Isto mostra que n é euclidiano.

3. Respostas dos exercícios do capítulo 3

(1) Procedendo como no caso do polinômio de grau 2, concluímos que h tem que satisfazer à desigualdade

$$ap^2h^2 + (3amp + bp)h + (3am^2 + 2mb + c) > 0.$$

Sejam $\alpha \leq \beta$ as raízes da equação do segundo grau à esquerda da desigualdade. Como $ap^2 > 0$, a desigualdade será satisfeita quando $h < \alpha$ ou $h > \beta$. Mas só estamos interessados em valores positivos de h, por isso basta tomar $h > \beta$.

(2) Temos que $13^\sharp + 1 = 59 \cdot 509$ e $17^\sharp + 1 = 19 \cdot 97 \cdot 277$.

(3) $(4n+1)(4k+1) = 4(4nk + n + k) + 1$. Note que é preciso escolher letras diferentes k e n, porque os números $4n+1$ e $4k+1$ *podem ser diferentes*.

(4) Qualquer número dividido por 4 tem resto 0, 1, 2 ou 3. Como um primo diferente de 2 é ímpar, os únicos restos possíveis neste caso são 1 e 3.

(5) Não. Por exemplo $3 \times 7 = 21 = 4 \times 5 + 1$.

(6) Pelo Teorema de Fatoração Única, o número $4(p_1 \dots p_k) + 3$ pode ser escrito como um produto de primos. Estes primos *não* podem pertencer ao conjunto $\{p_1, \dots, p_k\}$. Só resta mostrar que os primos na fatoração de $4(p_1 \dots p_k) + 3$ não podem ser todos da forma $4n + 1$. Mas se fosse este o caso, o produto destes primos seria da forma $4n + 1$ pelo exercício 4, o que não é verdade: $4(p_1 \dots p_k) + 3$ deixa resto 3 na divisão por 4.

(7) Suponha, por absurdo, que $\{3, p_1, \ldots, p_k\}$ é o conjunto de todos os primos da forma $4n + 3$ e aplique o exercício anterior.

(8) Seja p_n um primo que divide o número de Fermat $F(n)$. Se houvesse um quantidade finita de primos, então, como há infinitos números de Fermat, teríamos que ter $p_n = p_m$ para dois inteiros m e n *diferentes*. Mas isto significaria que $p_m = p_n$ dividiria $F(m)$ e $F(n)$; assim

$$\text{mdc}(F(n), F(m)) \geq p_n > 1,$$

o que contradiz o fato de que $\text{mdc}(F(n), F(m)) = 1$ se $m \neq n$, que foi provado no exercício 4 do capítulo 1.

(9) Suponhamos que p, $p+2$ e $p+4$ sejam primos. Observamos que p tem que ser ímpar, já que se $p = 2$ então $p + 2 = 4$ é composto. Logo p tem que ser da forma $3k$, $3k+1$ ou $3k+2$. Mas $3k$ é composto se $k \geq 2$, logo $p = 3k+1$ ou $p = 3k + 2$. No primeiro caso $p + 2 = 3k + 3$ é composto, no segundo $p + 4 = 3k + 6$ é composto. Logo a única possibilidade é $p = 3k$ e $k = 1$, que dá $p = 3$, $p + 2 = 5$ e $p + 4 = 7$; todos primos.

4. Respostas dos exercícios do capítulo 3

(1) (1) não é transitiva nem reflexiva, mas (2) é de equivalência.

(2) (1) 1; (2) 6; (3) 7.

(3) (1) 4; (2) 7; (3) 132; (4) 14.

(4) $1000! \equiv 0 \pmod{3^{300}}$.

(5) $U(4) = \{\overline{1}, \overline{3}\}$ e $\overline{3}$ é inverso dele mesmo.

$U(11) = \mathbb{Z}_{11} \setminus \{\overline{0}\}$; onde $\overline{10}$ é inverso dele próprio e os outros pares de inversos são: $\overline{2}$ e $\overline{6}$, $\overline{3}$ e $\overline{4}$, $\overline{7}$ e $\overline{8}$, $\overline{5}$ e $\overline{9}$.

$U(15) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$. Os elementos $\overline{4}$, $\overline{11}$ e $\overline{14}$ são seus próprios inversos; os outros pares de inversos são: $\overline{2}$ e $\overline{8}$, $\overline{7}$ e $\overline{13}$,

(6) (1) não tem solução; (2) $x \equiv 2 \pmod{4}$; (3) $x \equiv 4 \pmod{15}$.

(7) $\overline{a} = \overline{3}$ satisfaz à propriedade.

(8) Se $x^2 - 7y^2 = 3$ tivesse solução inteira, então a equação $x^2 \equiv 3 \pmod{7}$ teria solução. Mas o resto da divisão do quadrado de qualquer inteiro por 7 só pode ser 0, 1, 2 ou 4. Logo a congruência não tem solução, portanto a equação original também não tem.

(9) Efetuando os cálculos módulo $p = 274177$, temos:

$$7^8 \equiv 7084, \quad 9^8 \equiv 932 \quad \text{e} \quad 17^8 \equiv 146207.$$

Portanto

$$1071^8 \equiv (7 \cdot 9 \cdot 17)^8 \equiv 7084 \cdot 932 \cdot 146207 \equiv 274176 \equiv -1 \pmod{p}.$$

Logo

$$(1071 \cdot 2^8)^8 \equiv 1071^8 \cdot 2^{64} \equiv -2^{64} \pmod{p}.$$

Como $(1071 \cdot 2^8)^8 \equiv 1 \pmod{p}$, obtemos $-2^{64} \equiv 1 \pmod{p}$; isto é $2^{64}+1 \equiv 0 \pmod{p}$. Logo p divide $F(6)$.

(10) (1) Se o número é par então é da forma $2k$, mas

$$(2k)^2 \equiv 4k^2 \equiv 0 \pmod{4}.$$

Se o número é ímpar, então pode ser escrito na forma $2k+1$, donde

$$(2k+1)^2 \equiv 4(k^2+k)+1 \equiv 1 \pmod{4}$$

(2) Sejam x e y inteiros, então x^2 e y^2 só podem ser congruentes a 0 ou 1 módulo 4 por (1). Temos a seguinte tabela:

x	y	x^2+y^2
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$

Logo x^2+y^2 só pode ser congruente a 0, 1 ou 2 módulo 4.
(3) Se existissem inteiros x e y tais que $x^2+y^2 = 4n+3$ então teríamos $x^2+y^2 \equiv 3 \pmod{4}$ o que não é verdade por (2).

5. Respostas dos exercícios do capítulo 5

(1) (1) Se $n = 1$ então $n^3+2n = 1+3$ é divisível por 3. Suponha que o resultado vale para n e vamos prová-lo para $n+1$. Expandindo o produto notável e agrupando termos:

$$(n+1)^3+2(n+1) = (n^3+2n)+3(n^2+3n+1)$$

A expressão no primeiro parêntesis é divisível por 3 pela hipótese de indução. Como a segunda parcela é múltipla de 3, obtemos o que queremos.

(2) Um inteiro positivo ímpar é da forma $n = 2k+1$. Logo desejamos mostrar que

$$n^3-n = (2k+1)^3-(2k+1) = 4(2k^3+3k^2+k)$$

é divisível por 24. Para isto basta mostrar que a expressão entre parêntesis é divisível por 6. Vamos fazer isto por indução. Se $k = 1$ então $2k^3+3k^2+k = 6$. Suponha que $2k^3+3k^2+k$ é divisível por 6, vamos mostrar que o mesmo vale para $k+1$. Temos que:

$$2(k+1)^3+3(k+1)^2+(k+1) = (2k^3+3k^2+k)+6(k^2+2k+1).$$

A primeira parcela é divisível por 6 pela hipótese de indução e a segunda parcela já é um múltiplo de 6, provando o que queríamos.

Outra maneira: Se $n = 1$, então $n^3-n = 0$ é divisível por 24. Suponhamos que n é um número ímpar e que n^3-n é divisível por 24. O *número ímpar seguinte a* n é $n+2$, para completar a indução basta mostrar que $(n+2)^3-(n+2)$ é divisível por 24. Mas:

$$(n+2)^3-(n+2) = (n^3-n)+6(n^2+2n+1) = (n^3-n)+6(n+1)^2.$$

Sabemos que n^3-n é divisível por 24 pela hipótese de indução; falta verificar que $6(n+1)^2$ é divisível por 24. Na verdade, basta provar que $(n+1)^2$

é divisível por 4. Mas n é ímpar, logo $n+1$ é par. Portanto $(n+1)^2$ é múltiplo de 4, o que completa a demonstração.

(3) Calculando pela fórmula vemos que o número de diagonais de um triângulo é *zero*, o que corresponde à verdade e nos permite iniciar a indução. Suponhamos que a fórmula esteja correta para um polígono de n lados e vamos mostrar que vale para um de $n+1$ lados. Sejam A, B e C três vértices consecutivos do polígono de $n+1$ lados. Removendo o vértice B, obtemos um polígono de n lados. Quantas diagonais foram perdidas? Do vértice B partiam $n-2$ diagonais: uma para cada vértice do polígono, excluindo o próprio B e os adjacentes a B, isto é A e C. Além disso, a diagonal AC passou a ser um lado. Portanto o polígono de $n+1$ lados tem $(n-2)+1$ diagonais a mais do que o polígono de n lados obtido removendo-se C. Usando a hipótese de indução temos que o polígono de n lados tem:

$$\frac{n(n-3)}{2} + (n-1) = \frac{(n+1)(n-2)}{2}$$

diagonais, conforme predito pela fórmula.

(4) Somando um único termo temos $1 \cdot 2 = 2$; e fazendo $n = 1$ na fórmula temos $1 \cdot 2 \cdot 3/3 = 2$. Suponhamos agora que a fórmula vale para n e vamos prová-la para $n+1$. Temos que:

$$\sum_{k=1}^{n+1} k(k+1) = \sum_{k=1}^{n} k(k+1) + (n+1)(n+2).$$

Substituindo o valor da soma até n dado pela hipótese de indução:

$$\sum_{k=1}^{n+1} k(k+1) = n(n+1)(n+2)/3 + (n+1)(n+2);$$

Donde,

$$\sum_{k=1}^{n+1} k(k+1) = (n+1)(n+2)(n+3)/3.$$

conforme predito pela fórmula.

(2) Vamos denotar por S_n a soma dos n primeiros números hexagonais. Isto é

$$S_n = h_1 + h_2 + h_3 + \cdots + h_n.$$

Tabelando a soma destes números, como indicado, verificamos que S_n deve ser igual a n^3. Vamos provar isto por indunção em n. Se $n = 1$ o resultado é imediato porque $h_1 = 1 = S_1$. Digamos que $S_k = k^3$ (*hipótese de indução*) e vamos determinar quem é S_{k+1}. Mas, por definição, $S_{k+1} = S_k + h_{k+1}$. Usando a hipótese de indução, temos

$$S_{k+1} = S_k + h_{k+1} = k^3 + (1 + 3(k+1)k) = k^3 + 3k^2 + 3k + 1 = (k+1)^3.$$

Portanto $S_{k+1} = (k+1)^3$ e a fórmula $S_n = n^3$ está demonstrada por indução.

(3) Experimente passar de um conjunto de uma bola para um conjunto de duas bolas. Por que é que a indução não funciona neste caso?

(4) Se $n = 1$, temos apenas três moedas. Escolha duas delas e ponha uma em cada prato da balança. Se uma for mais leve, você achou a moeda adulterada. Se os pratos se equilibrarem, a adulterada é a que ficou de fora. Portanto 1 pesagem é sufuciente quando temos apenas 3 moedas.

Suponha agora que k pesagens bastam quando há 3^k moedas; esta é a *hipótese de indução*. Digamos que temos 3^{k+1} moedas e vamos tentar provar que $k+1$ pesagens bastam neste caso. Divida as moedas em 3 grupos de 3^k moedas. Ponha dois destes na balança. Se um deles é mais leve, é lá que está a moeda adulterada. Se os pratos se equilibram, a moeda adulterada está no grupo de moedas que não foi para a balança. Até agora fizemos apenas uma pesagem, e com isto descobrimos em qual dos 3 grupos de 3^k moedas está a adulterada. Mas sabemos que entre 3^k moedas a mais leve pode ser achada com k pesagens (isto é a hipótese de indução). Portanto k pesagens, além da que já fizemos bastam para encontrar a moeda adulterada; isto dá um total de $k+1$ pesagens, quando há 3^{k+1} moedas, e conclui a demonstração.

(5) Lembre-se que mostramos no Cap. 3 que o menor fator primo q de $p_1 \dots p_n + 1$ é maior que p_n. Logo $p_{n+1} \leq q$. Mas q é fator de $p_1 \dots p_n + 1$, logo $q \leq p_1 \dots p_n + 1$. Combinando as duas desigualdades, obtemos $p_{n+1} \leq p_1 \dots p_n + 1$. Isto mostra (1).

Vamos mostrar (2) por indução em n. Como $p_1 = 2$, temos claramente que $p_1 \leq 2^{2^1} = 4$. Vamos usar a versão do princípio de indução enunciada na seção 4. Suponhamos que $p_n \leq 2^{2^n}$ sempre que $n \leq k-1$ e vamos tentar mostrar que $p_k \leq 2^{2^k}$. Mas já vimos em (1) que $p_k \leq p_1 \dots p_{k-1} + 1$; logo, usando a hipótese de indução

$$\begin{aligned} p_k \leq p_1 \dots p_{k-1} + 1 &\leq 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 \\ &\leq 2^{2+2^2+\cdots+2^{k-1}} + 1 \\ &\leq 2^{2+2^k} + 1 \\ &\leq 2^{2^{k+1}} \end{aligned}$$

provando assim a afirmação.

(6) Temos que $70 = 12 \cdot 5 + 10$. Logo usando o Teorema de Fermat:

$$2^{70} + 3^{70} \equiv (2^{12})^5 \cdot 2^{10} + (3^{12})^5 \cdot 3^{10} \equiv 2^{10} + 3^{10}$$

módulo 13. Mas $3^2 \equiv 9 \equiv -4 \equiv -2^2$ módulo 13. Portanto:

$$2^{70} + 3^{70} \equiv 2^{10} + (3^2)^5 \equiv 2^{10} - (2^2)^5 \equiv 0$$

módulo 13.

(7) Observe que se a_0 é o algarismo das unidades de a então $a \equiv a_0 \ (mod 10)$. Logo basta mostrar que a_0^5 e a_0 têm o mesmo algarismo das unidades. Mais uma vez, isto significa que $a_0^5 \equiv a_0 \ (mod 10)$. Como a_0 é um *algarismo*, isto é, um número entre 0 e 9, você pode verificar isto por tentativa. Uma maneira mais sofisticada de proceder é a seguinte. Dizer que $a_0^5 \equiv a_0$ módulo 10 é dizer que $a_0^5 - a_0$ é divisível por 10. Para um número ser divisível por 10 basta que seja divisível por 2 e por 5 (isto é verdade por causa do Exercício 1 desta lista). Mas é claro que $a_0^5 - a_0$ é divisível por 5:

isto é o Teorema de Fermat. Fica para você verificar que $a_0^5 - a_0$ é sempre par.

(8) Queremos mostrar que a expressão dada é congruente a zero módulo 9. Expandindo pelo binômio e esquecendo os termos que são claramente múltiplos de 9 ficamos com: $n^3 + (n+1)^3 + (n+2)^3 \equiv 3(n^3 + 2n)$ módulo 9. Esta última expressão será múltipla de 9 se $n^3 + 2n$ for divisível por 3, mas usando Fermat:

$$n^3 + 2n \equiv n + 2n \equiv 3n \equiv 0 (\text{mod } 3)$$

como queríamos.

(9) O número 111 é divisível por 3. logo podemos supor que $p > 5$. Pelo Teorema de Fermat $10^{p-1} - 1 = 9(1 \ldots 1)$ é divisível por p. Como p é primo ele tem que dividir um dos fatores: 9 ou $11 \ldots 11$. Mas $p > 3$ não divide 9; logo p divide $11 \ldots 11$ que é o que desejávamos mostrar.

(10) Digamos que a equação tenha soluções inteiras x_0 e y_0. Então $x_0^{13} + 12x_0 + 13y_0^6 = 1$. Esta é uma igualdade entre números inteiros, temos portanto que

$$x_0^{13} + 12x_0 + 13y_0^6 \equiv 1 \pmod{13}.$$

Mas $13 \equiv 0 \pmod{13}$ e pelo teorema de Fermat $x_0^{13} \equiv x_0 \pmod{13}$. Fazendo estas substituições na equação acima, obtemos

$$x_0 + 12x_0 \equiv 1 \pmod{13}.$$

Daí chegamos a $0 \equiv 1 \pmod{13}$, uma contradição. Logo a equação não pode ter solução inteira.

(11) Vamos usar congruência e o teorema de Fermat. Observe que 2251 é primo. Para verificar isto experimente dividir 2251 pelos primos menores que $\sqrt{2251} = 47,44$. Por outro lado $2251 - 1 = 2250 = 2 \cdot 3^2 \cdot 5^3$. Portanto 2250 divide 50!; digamos que $50! = 2250 \cdot k$. Assim, pelo teorema de Fermat

$$39^{50!} \equiv (39^{2250})^k \equiv 1^k \equiv 1 \pmod{2251}.$$

Logo o resto neste caso é 1.

No segundo exercício, temos novamente que 191 é primo. Dividindo $39^4 = 2313441$ por 190, obtemos quociente 12176 e resto 1. Portanto, usando o teorema de Fermat, temos que

$$19^{39^4} \equiv (19^{190})^{12176} \cdot 19^1 \equiv 1 \cdot 19 \equiv 19 \pmod{191}.$$

Logo o resto é 19 neste caso.

(12) Seja $p = 4n + 1$ um número primo e sejam x e y dois inteiros primos com p. Lembre-se que, como $p - 1 = 4n$ e p é primo, temos pelo teorema de Fermat que

$$x^{4n} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Da mesma forma $y^{4n} \equiv 1 \pmod{p}$. Portanto, se $a = x^n$ e $b = y^n$, concluímos que

$$(a^2 - b^2)(a^2 + b^2) \equiv x^{4n} - y^{4n} \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Logo $(a^2-b^2)(a^2+b^2)$ é divisível por p, o que verifica (1). Pela propriedade fundamental dos primos concluímos que ou p divide a^2-b^2 ou p divide a^2+b^2. No segundo caso provamos o que queríamos. Vejamos o que acontece se este segundo caso nunca é verificado para nenhuma escolha de x e y. Isto é, suponhamos por absurdo que, dados quaisquer x e y primos com p, temos que $x^{2n}-y^{2n}$ é divisível por p. Em particular isto deve valer quando $y=1$. Mas isto significa que p divide $x^{2n}-1$, isto é que $x^{2n}\equiv 1 \pmod{p}$. Pela hipótese que fizemos esta congruência deve valer *para qualquer x primo com p*. Logo a equação $x^{2n}\equiv 1 \pmod{p}$ deve ter $p-1=4n$ soluções distintas módulo p. Como isto dá um número de soluções maior que o grau, obtivemos uma contradição com o teorema da §4, o que verifica (3).

Resumindo: entre os números inteiros primos com p têm que existir dois, digamos x e y, tais que $x^{2n}+y^{2n}$ é divisível por p. Logo p divide a^2+b^2, onde $a=x^n$ e $b=y^n$; que é o que queríamos mostrar.

(13) Vamos mostrar que os elementos de S são todos distintos. Consideremos dois elementos de S, digamos $\overline{k}\overline{a}$ e $\overline{r}\overline{a}$. Se forem iguais

$$\overline{k}\overline{a}=\overline{r}\overline{a}.$$

Mas $\overline{a}\neq\overline{0}$ em $\mathbb{Z}_p$, logo $\overline{a}$ tem inverso em $\mathbb{Z}_p$. Digamos que o inverso é $\overline{\alpha}$. Multiplicando a equação acima por $\overline{\alpha}$, verificamos que $\overline{k}=\overline{r}$. Portanto $\overline{k}\overline{a}$ e $\overline{r}\overline{a}$ só podem ser iguais se $\overline{k}$ e $\overline{r}$ forem iguais.

Assim os elementos de S são todos distintos, o que significa que S tem $p-1$ elementos. Porém $S\subseteq U(p)$, e este último conjunto também tem $p-1$ elementos. Logo $S=U(p)$. Em particular, o produto dos elementos de S tem que ser igual ao produto dos elementos de $U(p)$, já que são os mesmos elementos, apenas listados em ordem diferente. Isto dá

$$\overline{a}\cdot\overline{2a}\cdots\overline{(p-1)a}=\overline{1}\cdot\overline{2}\cdots\overline{p-1}=\overline{(p-1)!}.$$

Agrupando os $\overline{a}$ no termo da esquerda, vemos que é igual a $\overline{a}^{p-1}\cdot\overline{(p-1)!}$. Igualando com o termo da direita

$$\overline{a}^{p-1}\cdot\overline{(p-1)!}=\overline{(p-1)!}.$$

Como p é primo $\overline{(p-1)!}\neq\overline{0}$. Portanto podemos cancelar $\overline{(p-1)!}$ na última equação acima, obtendo assim que $\overline{a}^{p-1}=\overline{1}$ que é o teorema de Fermat.

(14) Multiplicando temos

$$\overline{a}^{p-2}\cdot\overline{a}=\overline{a}^{p-1}=\overline{1},$$

onde a última igualdade segue do teorema de Fermat, já que a não é divisível por p.

(15) Por exemplo, se $p=7$ e $a=3$ ou 5, então a equação não tem solução.

Digamos que a equação *tem* solução; vamos chamar de b a solução. Então $b^2\equiv a \pmod{p}$. Queremos verificar que $b\equiv\pm a^{k+1} \pmod{p}$. Como p é primo, a equação só pode ter duas soluções, por isso basta verificar que a^{k+1} é solução da equação. Mas

$$(a^{k+1})^2\equiv a^{2k+2}\equiv b^{4k+4} \pmod{p},$$

já que, por hipótese $b^2 \equiv a \pmod{p}$. Mas

$$b^{4k+4} \equiv b^{4k+3} \cdot b \pmod{p}.$$

Como, pelo teorema de Fermat, $b^{4k+3} \equiv b \pmod{p}$, concluímos que

$$(a^{k+1})^2 \equiv b^2 \equiv a \pmod{p},$$

onde a última congruência vale pela hipótese feita sobre b. Portanto a^{k+1} é solução de $x^2 \equiv a \pmod{p}$, *desde que esta equação tenha solução.*

6. Respostas dos exercícios do capítulo 6

(1) 645 é pseudoprimo para a base 2, 567 é composto e não é pseudoprimo para a base 2 e 701 é primo. Nenhum dos números é pseudoprimo para a base 3

(2) Se n é pseudoprimo para a base ab, então

$$a^n b^n \equiv (ab)^n \equiv ab \ (mod\ n).$$

Mas n também é pseudoprimo para a base a, logo $a^n \equiv a \ (mod\ n)$. Portanto,

$$ab^n \equiv ab \ (mod\ n).$$

Como $mdc(a, n) = 1$, podemos cancelar a na equação acima e concluir que n é pseudoprimo para a base b.

(3) Efetuando a multiplicação, temos que,

$$n - 1 = p_1 p_2 p_3 - 1 = 36n(36n^2 + 11n + 1)$$

que é claramente divisível por $p_1 - 1 = 6n$, por $p_2 - 1 = 12n$ e por $p_3 - 1 = 18n$. Logo n é um número de Carmichael.

Quando $n = 1$, temos $p_1 = 7$, $p_2 = 13$ e $p_3 = 19$ e o número de Carmichael correspondente é 1729. Quando $n = 6$ temos $p_1 = 37$, $p_2 = 73$ e $p_3 = 421$ e o número de Carmichael correspondente é 294409. Finalmente, quando $n = 35$, temos que $p_1 = 211$, $p_2 = 421$ e $p_3 = 631$, e o número de Carmichael correspondente é 56052361.

(4) Fatorando $29341 = 13 \times 37 \times 61$. Como

$$29340 = 12 \times 2445 = 36 \times 815 = 60 \times 489$$

então 29341 é um número de Carmichael.

(5) Seja $n = p_1 p_2$, então

$$n - 1 = p_1 p_2 - 1 = (p_2 - 1)p_1 + (p_1 - 1).$$

Portanto, $n - 1 \equiv p_1 - 1 \ (mod\ p_2 - 1)$. Como $p_1 - 1 < p_1 < p_2$, temos que $p_1 - 1 \not\equiv 0 \ (mod\ p_2 - 1)$. Isto é $p_2 - 1$ não divide $n - 1$, o que contradiz as hipóteses do exercício. Para concluir daí que um número de Carmichael não pode ter apenas dois fatores primos você precisa usar o teorema de Korselt.

(6) 645 não é pseudoprimo forte para a base 2, $2047 = 23 \times 89$ é pseudoprimo forte para a base 2 e 2309 é primo. Nenhum dos números é psudoprimo forte para a base 3.

(7) Como n é ímpar, escrevemos $n-1 = 2^k q$, onde $k \geq 1$ e q é um número ímpar. Se n é um pseudoprimo forte para a base b então ou $b^q \equiv 1 \pmod{n}$ ou $b^{2^j q} \equiv -1 \pmod{n}$, onde $0 \leq j \leq k-1$. No primeiro caso temos que

$$b^{n-1} \equiv (b^q)^{2^k} \equiv 1^{2^k} \equiv 1 \pmod{n}.$$

No segundo caso

$$b^{n-1} \equiv (b^{2^j q})^{2^{k-j}} \equiv (-1)^{2^{k-j}} \equiv 1 \pmod{n}.$$

Observe que $k > j$, logo $k - j \geq 1$ e, portanto, $(-1)^{2^{k-j}} = 1$. Em qualquer dos dois casos obtivemos que $b^{n-1} \equiv 1 \pmod{n}$. Logo n é um pseudoprimo para a base b.

7. Respostas dos exercícios do capítulo 7

1. $x \equiv 17 \pmod{60}$.

2. A quantidade (mínima) total de arroz é $3 \cdot 105288$.

3. 137

4. 2913

5. Suponhamos que o sistema dado tem soluções α e β. De

$$\alpha \equiv a \pmod{m} \quad \text{e} \quad \beta \equiv a \pmod{m}$$

concluímos que $\alpha - \beta$ é múltiplo de m. Analogamente $\alpha - \beta$ tem que ser múltiplo de n. Seja μ o mínimo múltiplo comum entre m e n. Então $\mu < \alpha - \beta$ e dividindo $\alpha - \beta$ por μ obtemos

$$\alpha - \beta = \mu \cdot q + r \quad \text{onde} \quad 0 \leq r < \mu.$$

Observe que, como $\alpha - \beta$ e μ são múltiplos de m e de n, então isto também tem que ser verdade sobre r. Logo r é um múltiplo comum de m e de n que é menor que μ. Como μ é o mínimo múltiplo comum deduzimos que $r = 0$. Portanto $\alpha \equiv \beta \pmod{\mu}$.

6. $2^{45632} \equiv 10201$ e $3^{54632} \equiv 9876$ ambos módulo $12155 = 5 \cdot 11 \cdot 13 \cdot 17$.

7. $x \equiv 84 \pmod{105}$.

8. Digamos que a seqüência de primos *consecutivos* seja $p_1, \ldots, p_k$. O primeiro elemento é 11, logo $p_1 = 11$. Além disso a seqüência deve ter limiar 3; o que significa que

$$p_1 p_2 p_3 > p_{k-1} p_{k-2}.$$

Mas $p_1 = 11$, $p_2 = 13$ e $p_3 = 17$; logo $p_1 p_2 p_3 = 2431$. Assim

$$2431 = p_1 p_2 p_3 > p_{k-1} p_{k-2} > p_{k-1}^2.$$

Concluímos que $p_{k-1} < [\sqrt{2431}] = 49$. O maior primo menor que 49 é 47, e o primo seguinte a 47 é 53. Entretanto $47 \cdot 53 = 2491 > 2431$, e não temos o limiar correto. O primo anterior a 47 é 43 e $43 \cdot 47 = 2021 < 2431$. Portanto escolhendo $p_k = 47$ e $p_{k-1} = 43$ temos a seqüência desejada, que é:

$$11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Como a seqüência tem 11 elementos, temos $k = 11$. Procedendo da mesma maneira para limiar 4, obtemos $p_1p_2p_3p_4 = 46189$. Queremos que

$$46189 = p_1p_2p_3p_4 > p_{k-2}p_{k-1}p_k > p_{k-2}^3.$$

Assim $p_{k-2} < 35$. Portanto o maior valor possível de p_{k-2} é 31. Neste caso teríamos $p_{k-1} = 37$ e $p_k = 41$, donde $p_{k-2}p_{k-1}p_k = 47027$, que é maior que 46189. Escolhendo para p_{k-2} o primo anterior a 31, teremos $p_{k-2} = 29$. Neste caso

$$p_{k-2}p_{k-1}p_k = 29 \cdot 31 \cdot 37 = 33263,$$

que satisfaz às hipóteses. Assim a seqüência de primos desejada é

$$11, 13, 17, 19, 23, 29, 31, 37,$$

que tem 8 elementos.

9. Seja α_1 uma solução de $x^2 \equiv a \pmod{p}$ e α_2 uma solução de $x^2 \equiv a \pmod{q}$. Resolvendo o sistema

$$\begin{aligned} x &\equiv \alpha_1 \pmod{p} \\ x &\equiv \alpha_2 \pmod{q} \end{aligned}$$

digamos que obtivemos β como solução. Vamos mostrar que a forma reduzida de β^2 módulo n é a. Observe que, módulo p temos

$$\beta^2 \equiv \alpha_1^2 \equiv a \pmod{p}.$$

De modo que $\beta^2 - a$ é divisível por p. Analogamente $\beta^2 - a$ é divisível por q. Como p e q são primos entre si, seque que $\beta^2 - a$ é divisível por $pq = n$.

8. Respostas dos exercícios do capítulo 7

1. Seja ρ a rotação de 90^o. Então ρ, ρ^2, ρ^3 são simetrias do quadrado. As outras simetrias são reflexões. Temos dois tipos de reflexões: duas reflexões em torno das diagonais e duas reflexões em torno da reta que liga os meios dos lados. Juntamente com a transformação identidade, isto nos dá os oito elementos de D_4. Observe que cada reflexão é seu próprio inverso. Por outro lado o inverso de ρ é ρ^3 e o inverso de ρ^2 é ele próprio.

Vamos denotar por α_1 e α_2 as reflexões que deixam fixos os vértices $1, 3$ e $2, 4$, respectivamente; e vamos denotar por β_1 a reflexão que troca os vértices 1 por 4 e 2 por 3, e por β_2 a reflexão que troca os vértices 1 por 2 e 3 por 4. Com esta notação, a tabela do grupo é a seguinte:

	e	ρ	ρ^2	ρ^3	α_1	α_2	β_1	β_2
e	e	ρ	ρ^2	ρ^3	α_1	α_2	β_1	β_2
ρ	ρ	ρ^2	ρ^3	e	β_1	β_2	α_2	α_1
ρ^2	ρ^2	ρ^3	e	ρ	α_2	α_1	β_2	β_1
ρ^3	ρ^3	e	ρ	ρ^2	β_2	β_1	α_1	α_2
α_1	α_1	β_2	α_2	β_1	e	ρ^2	ρ^3	ρ
α_2	α_2	β_1	α_1	β_2	ρ^2	e	ρ	ρ^3
β_1	β_1	α_1	β_2	α_2	ρ	ρ^3	e	ρ^2
β_2	β_2	α_2	β_1	α_1	ρ^3	ρ	ρ^2	e

2. Temos um grupo G com uma operação $\star$, tal que $x^2 = e$ para todo $x \in G$. Sejam $x, y \in G$. Queremos mostrar que $x \star y = y \star x$. Mas sabemos que $(x \star y)^2 = e$, isto é:

$$x \star y \star x \star y = e.$$

Multiplicando esta equação à esquerda por x e à direita por y, obtemos:

$$x^2 \star y \star x \star y^2 = x \star y.$$

Como $x^2 = y^2 = e$, por hipótese, então $x \star y = y \star x$, como queríamos mostrar.

3. $\phi(125) = 100$, $\phi(16200) = 4320$ e $\phi(10!) = 2^{11}.3^4.5$.

4. Note que se p é um primo que divide n então podemos escrever $n = p^r \cdot m$, onde p não divide m. Assim $\text{mdc}(m, p) = 1$ e portanto

$$\phi(p^r \cdot m) = \phi(p^r)\phi(m) = p^{r-1}(p-1)\phi(m).$$

Logo $p - 1$ divide $\phi(n)$, o que prova (1). Para que p divida n mas *não* divida $\phi(n)$ basta que $r = 1$.

Finamente, se $n = p_1^{e_1} \dots p_s^{e_s}$ onde $p_1 < \dots < p_s$ são primos, então

$$\phi(n) = \phi(p_1^{e_1}) \dots \phi(p_s^{e_s}).$$

Logo, basta mostrar que se p é primo então $\phi(p^e) < p^e$. Mas

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

já que $p - 1 < p$.

5. Temos que $\phi(19) = 18$ e $\phi(11) = 10$. Por outro lado, se $\phi(n) = 14$, e p é um primo que divide n então $p - 1$ é igual a $1, 2, 7$ ou 14. Logo p é 2 ou 3. Então $n = 2^r 3^s$. Mas neste caso $\phi(n) = 2^r 3^{s-1}$ não pode ser igual a 14. Portanto não existe n tal que $\phi(n) = 14$.

6. Como $\phi(n)$ é sempre par, então $\phi(n)$ só pode ser primo se $\phi(n) = 2$. Mas se p é fator primo de n então $p - 1$ divide 2. Logo $p - 1 = 1$ ou $p - 1 = 2$, donde $p = 2$ ou $p = 3$. Assim $n = 2^e 3^r$. Observe que se $r > 1$ então 3 dividiria $\phi(n) = 2$, o que não é verdade. Portanto $r = 0$ ou 1. Se $r = 0$ então $n = 2^e$ e é fácil ver que $e = 2$. Se $r = 1$, então $n = 2^e 3$ e é fácil ver que $e = 0$ ou $e = 1$. Logo os possíveis valores de n são 3, 4 e 6.

7. Seja q o maior primo que divide n. Podemos escrever $n = q^e c$ onde c é um inteiro cujos fatores primos são todos menores que q. Então

$$n\phi(n) = q^e c\phi(q^e c) = q^e c \cdot \phi(q^e)\phi(c) = q^{e-1}(q-1)\phi(c)$$

Como $\text{mdc}(q, c) = 1$, temos que

$$n\phi(n) = q^e c\phi(q^e)\phi(c) = q^e c \cdot q^{e-1}(q-1)\phi(c),$$

donde

$$(\star) \qquad n\phi(n) = q^{2e-1}(q-1)c\phi(c).$$

Observe que os primos que dividem $(q-1)c\phi(c)$ têm que ser todos menores que q. Assim, se p é o maior primo que divide k e se $k = n\phi(n)$ precisamos ter $p = q$ e a multiplicidade de p na fatoração de k tem que ser ímpar, já que $2r - 1$ é sempre ímpar. Observe que esta conclusão só vale para o maior primo que divide

n; um primo que divide c poderia dividir também $q-1$ e assim ter expoente par na fatoração de $n\phi(n)$. Por exemplo, se $n = 14$ então

$$n\phi(n) = 14 \cdot 6 = 2^2 \cdot 3 \cdot 7$$

e 2 tem expoente par na fatoração de $n\phi(n)$, mas 7, que é o maior primo, tem expoente ímpar, como já sabíamos. Com isto provamos (1) e (2).

Se $k = n\phi(n)$, então já sabemos que $k = p^{2e-1}k'$, para algum inteiro positivo $k' < k$. Igualando isto a expressão para $n\phi(n)$ obtida em $(\star)$, obtemos

$$\frac{k'}{p-1} = c\phi(c).$$

Se $p-1$ dividir k podemos continuar o processo e tentar calcular c. Observe que $k' < k$, portanto continuando desta maneira obtemos uma seqüência estritamente decrescente de inteiros positivos. Portanto o algoritmo tem que parar.

8. Se $\phi(n) = n-1$, então todos os inteiros positivos menores que n têm que estar em $U(n)$. Isto é o máximo divisor comum entre qualquer inteiro positivo menor que n e o próprio n é 1. Mas isto só acontece se nenhum inteiro positivo menor que n, exceto 1, não dividir n. Portanto n não tem divisores menores que n execeto 1; logo n é primo.

9. Dado um número n qualquer podemos escrevê-lo na forma $n = 2^k r$, onde r é um número ímpar. Observe que $mdc(2^k, r) = 1$. Como ϕ é uma função multiplicativa:

$$\phi(n) = \phi(2^k r) = \phi(2^k)\phi(r) = 2^{k-1}\phi(r).$$

Se $\phi(n) = n/2$ então podemos concluir que $n/2 = 2^{k-1}\phi(r)$. Isto é $n = 2^k\phi(r)$. Como $n = 2^k r$ temos que $\phi(r) = r$, o que só é possível quando $r = 1$. Mas neste caso $n = 2^k$ é uma potência de 2.

10. Se m divide n então as fatorações de m e n serão

$$m = p_1^{r_1} \dots p_k^{r_k} \text{ e } n = p_1^{s_1} \dots p_k^{s_k}$$

onde $p_1 < \dots < p_k$ são primos e $r_1 \leq s_1, \dots, r_k \leq s_k$. Logo:

$$mn = p_1^{r_1+s_1} \dots p_k^{r_k+s_k}.$$

Aplicando a fórmula para calcular $\phi(mn)$, obtemos:

$$\begin{aligned}\phi(mn) &= p_1^{r_1+s_1-1} \dots p_k^{r_k+s_k-1}(p_1-1)\dots(p_k-1) \\ &= p_1^{r_1} \dots p_k^{r_k}\left(p_1^{s_1-1} \dots p_k^{s_k-1}(p_1-1)\dots(p_k-1)\right) \\ &= m\phi(n).\end{aligned}$$

11.
Subgrupos de ordem 1: $\{e\}$. Subgrupos de ordem 2: $\{e, \alpha_1\}$, $\{e, \alpha_2\}$, $\{e, \beta_1\}$, $\{e, \beta_2\}$ e $\{e, \rho^2\}$.
Subgrupos de ordem 4: $\{e, \rho, \rho^2, \rho^3\}$, $\{e, \rho^2, \alpha_1, \alpha_2\}$ e $\{e, \rho^2, \beta_1, \beta_2\}$.
Subgrupos de ordem 8: D_4.

12. Temos que $U(2)$ tem ordem 1 e $U(4)$ tem ordem 2 logo são cíclicos. Já $U(8)$ tem ordem 4 mas todos os seus elementos têm ordem 2.

13. Digamos que G seja cíclico com gerador a. Então

$$G = \{e, a, a^2, a^3, \ldots, a^{n-1}\}.$$

Como m divide n, temos que $n = km$ para algum inteiro positivo k. Verifique agora que o elemento a^k tem ordem m.

14. (1) A ordem de $U(20)$ é

$$\phi(20) = \phi(4)\phi(5) = 2 \cdot 4 = 8.$$

Os elementos de $U(20)$ são:

$$U(20) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}.$$

(2) Pelo teorema de Lagrange, a ordem de qualquer elemento de $U(20)$ tem que dividir 8. Os elementos de ordem 2 são $\overline{9}$, $\overline{11}$ e $\overline{19}$. Os demais elementos têm ordem 4, execeto o $\overline{1}$, que tem ordem 1.
(3) O grupo não é cíclico porque não tem elementos de ordem 8.
(4) Os subgrupos de ordem 4 são:

$$\{\overline{1}, \overline{3}, \overline{9}, \overline{7}\}$$
$$\{\overline{1}, \overline{13}, \overline{9}, \overline{17}\}$$
$$\{\overline{1}, \overline{9}, \overline{11}, \overline{19}\}$$

(5) O último dos subgrupos acima não é cíclico.

15.
(1) Em primeiro lugar, como S_1 e S_2 contêm o elemento neutro e, então $e \in S_1 \cap S_2$. Digamos que $x, y \in S_1 \cap S_2$. Como $x, y \in S_1$ e S_1 é um subgrupo de G por hipótese, então $x \star y \in S_1$. Analogamente $x \star y \in S_2$. Assim $x \star y \in S_1 \cap S_2$. Finalmente, se $x \in S_1 \cap S_2$ então $x \in S_1$. Como S_1 é um subgrupo por hipótese, temos que o inverso x' de x em G pertence a S_1. Analogamente $x' \in S_2$. Portanto $x' \in S_1 \cap S_2$. Concluímos assim que $S_1 \cap S_2$ é um subgrupo de G.
(2) Como $S_1 \cap S_2$ é um subgrupo e está contido em S_1 e em S_2, então $S_1 \cap S_2$ é um subgrupo de S_1 e também é um subgrupo de S_2. Portanto a ordem de $S_1 \cap S_2$ tem que dividir a ordem de S_1 e a ordem de S_2. Se as ordens de S_1 e S_2 forem primas entre si, isto só pode acontecer se $S_1 \cap S_2$ tiver ordem 1. Mas neste caso $S_1 \cap S_2 = \{e\}$.
(3) Basta dar um exemplo em que a união de subgrupos não é um subgrupo. Por exemplo, se $G = D_3$ e $S_1 = \{e, \rho, \rho^2\}$ e $S_2 = \{e, \sigma_2\}$ então $S_1 \cup S_2 = \{e, \rho, \rho^2, \sigma_2\}$ tem 4 elementos, logo não pode ser subgrupo de D_3, já que 4 não divide 6.

16. A afirmação (1) é verdadeira. Vamos mostrar primeiro que se $\overline{b_1}, \overline{b_2} \in H(n)$, então $\overline{b_1 b_2} \in H(n)$. Isto é fácil:

$$(b_1 b_2)^{n-1} \equiv b_1^{n-1} b_2^{n-1} \equiv 1 \pmod{n}.$$

A operação é associativa e é claro que $\overline{1} \in H(n)$. Falta mostrar que se $\overline{b} \in H(n)$ então seu inverso $\overline{\beta}$ também está em $H(n)$. Mas $\overline{b} \cdot \overline{\beta} = \overline{1}$, logo

$$1 \equiv (b\beta)^{n-1} \equiv b^{n-1}\beta^{n-1} \equiv \beta^{n-1} \pmod{n},$$

que prova o desejado.

A afirmação (2) é falsa. Se n é Carmichael, então $H(n) = U(n)$. A afirmação (3) é verdadeira. Se $U(n)$ tem um elemento de ordem $n-1$, então $U(n)$ tem ordem pelo menos $n-1$. Mas $\phi(n) \leq n-1$ e mais, $\phi(n) = n-1$ se, e somente se, n é primo.

17. Usando o teorema de Euler é fácil verificar que $7^{9876} \equiv 1 \pmod{60}$ e $3^{87654} \equiv 44 \pmod{125}$.

18. Digamos que p^r seja um pseudoprimo para a base b, onde $\text{mdc}(b,p) = 1$, então,

$$b^{p^r} \equiv b \pmod{p^r}.$$

Mas $p^r(p-1) = p\phi(p^r)$, donde

$$b^{(p-1)} \equiv (b^{p^r})^{p-1} \equiv (b^{\phi(p^r)})^p \equiv 1 \pmod{p^r}.$$

pelo teorema de Euler. Reciprocamente, se $b^{p-1} \equiv 1 \pmod{p^r}$, então como $(p-1)(p^{r-2} + \cdots + p + 1) = p^r - 1$, temos

$$b^{p^r-1} \equiv (b^{p-1})^{(p^{r-2}+\cdots+p+1)} \equiv 1 \pmod{p^r}.$$

19. Pelo exercício anterior, basta mostrar que $2^{1092} \equiv 1 \pmod{1093^2}$. Use que $1092 = 4{\cdot}3{\cdot}91$. Mesmo assim os cálculos são muito trabalhosos em uma calculadora!

9. Respostas dos exercícios do capítulo 9

1. Se a equação $x^p \equiv 1 \ (mod\ q)$ tem uma solução $x \not\equiv 1 \ (mod\ q)$ então $\overline{1} \neq \overline{x} \in U(q)$. Como p é primo, então x tem ordem p. Pelo Teorema de Lagrange, a ordem de x divide a ordem de $U(q)$. Em outras palavras, p divide $\phi(q)$. Mas q é primo, logo $\phi(q) = q-1$. Assim, p divide $q-1$, isto é: $q \equiv 1 \ (mod\ p)$.

2. 43 é primo e $\phi(43) = 2 \times 3 \times 7$. Logo 17 não divide $\phi(43)$. Portanto, pelo exercício anterior a única solução da equação é $x \equiv 1 \ (mod\ 43)$.

3. Os geradores de $U(17)$ são: $\overline{3}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{10}$, $\overline{11}$, $\overline{12}$ e $\overline{14}$. Observe que, como $\phi(17) = 16 = 2^4$, a ordem de cada elemento de $U(17)$ tem que ser uma potência de 2 com expoente menor que 4. Assim, para verificar que $\overline{a} \in U(17)$ não é gerador, basta testar se $a^8 \equiv 1 \pmod{17}$.

Temos que $7 \equiv 3^{11} \pmod{17}$ e $6 \equiv 3^{15} \pmod{17}$. A partir de $7^x \equiv 6 \pmod{17}$ obtemos $3^{11x} \equiv 3^{15} \pmod{17}$. Isto é $3^{11x-15} \equiv 1 \pmod{17}$. Assim a ordem de 3 módulo 17 divide $11x - 15$. Mas $\overline{3}$ gera $\mathbb{Z}_{17}$. Logo 3 tem ordem 16 módulo 17. Então $11x \equiv 15 \pmod{16}$. Resolvendo a equação temos $x \equiv 13 \pmod{16}$.

4. De acordo com o método de Fermat, os fatores de $M(11)$ são da forma $22k+1$. Fazendo $k = 1$ verificamos que 23 divide $M(11)$. De modo semelhante, os fatores de $M(29)$ são da forma $58k+1$. Fazendo $k = 1$ temos 59 que é primo mas não é fator. Para $k = 2$ e $k = 3$ obtemos 117 e 175, respectivamente; mas nenhum dos dois é primo. Finalmente, para $k = 4$ obtemos 233 que é fator de $M(29)$. Para verificar que $M(7)$ é primo, precisamos mostrar que não tem fatores $\leq \sqrt{M(7)}$. Como a parte inteira da raiz é 11, basta verificar que $M(7)$ não tem fatores ≤ 11. Mas pelo método de Fermat, os fatores de $M(7)$ são da forma $14k+1$. O menor destes fatores é 15, que já é maior que 11. Logo $M(7)$ é primo.

5. Pelo método de Euler, os fatores de $F(4)$ são da forma $32k+1$. Para mostrar que $F(4)$ é primo, precisamos verificar que não tem fatores menores que 256, que é a parte inteira da raiz quadrada de $F(4)$. Isto nos dá: $32k+1 \leq 256$, donde obtemos $k \leq 7$. Logo se $32k+1$ não divide $F(4)$ para $k \leq 7$ então $F(4)$ é primo. Mas os únicos valores de k para os quais $32k+1$ é primo são $k=3$ e $k=6$. É fácil verificar diretamente que os números obtidos nestes casos não sõ fatores de $F(4)$.

6. (1) Temos que

$$\alpha^2 \equiv (2^{2^{k-2}}(2^{2^{k-1}}-1))^2 \equiv 2^{2^{k-1}}(2^{2^k}+1-2\cdot 2^{2^{k-1}}) \pmod{p}.$$

Como $F(k) = 2^{2^k}+1$ é divisível por p,

$$\alpha^2 \equiv -2^{2^{k-1}} \cdot 2 \cdot 2^{2^{k-1}} \equiv -2 \cdot 2^{2^k} \equiv 2 \pmod{p}.$$

Para resolver (2) usamos (1). Sabemos que 2 tem ordem 2^{k+1} módulo p, portanto

$$\alpha^{2^{k+2}} \equiv 2^{2^{k+1}} \equiv 1 \pmod{p}.$$

Logo a ordem de α tem que dividir 2^{k+2}. Se a ordem não for exatamente 2^{k+2} então tem que dividir 2^{k+1}. Se isto acontecesse, teríamos

$$\alpha^{2^{k+1}} \equiv 1 \pmod{p},$$

o que implicaria que $2^{2^k} \equiv 1 \pmod{p}$, que não é verdade. Assim α tem ordem 2^{k+2}.

Finalmente, a ordem de α módulo p (que é 2^{k+2}) divide a ordem de $U(p)$, que é $\phi(p) = p-1$. Assim existe um inteiro positivo r tal que $p = 2^{k+2}r+1$.

7. $k = 12$.

8. (1) Observe que

$$\log(2^n-1) = \log(2^n(1-2^{-n})) = n\log 2 + \log(1-2^{-n}).$$

Como $n > 2$ no exemplo, temos que $\log(1-2^{-n}) > \log(1-1/4) > -1$. Por outro lado $\log(1-2^{-n}) < \log 1 = 0$. Portanto

$$n\log 2 - 1 < \log(2^n-1) < n\log 2.$$

(2) Aplicando logaritmos na base 10 à equação

$$10^{20} < 2^{n-1}(2^n-1) < 10^{22}$$

obtemos

$$20 < (n-1)\log 2 + \log(2^n-1) < 22.$$

Combinando com as desigualdades de (1) temos

$$20 \leq (2n-1)\log 2 - 1 < (n-1)\log 2 + \log(2^n-1) < (2n-1)\log 2 \leq 22.$$

Assim $(2n-1) \geq [21/\log 2]$. Como $\log 2 < 0,302$, concluímos que $2n-1 \geq 70$, donde $n \geq 35$. Já da desigualdade à esquerda temos $(2n-1) \leq [22/\log 2]$. Como $\log 2 > 0,3$, obtemos $n \leq 37$. Assim $35 \leq n \leq 37$, como desejado.
(3) O único primo entre 35 e 37 é 37, logo $M(n)$ só pode ser primo para estes expoentes quando $n = 37$. Aplicando o método de Fermat a $M(37)$ temos que os fatores têm que ser da forma $74k+1$. O primeiro primo desta forma é 149, mas $2^{37}-1 \equiv 104 \pmod{149}$, logo 149 não é fator de $M(37)$. O primo seguinte é 223, que é fator de $M(37)$. Logo $M(37)$ é composto. Portanto não existem primos de

Mersenne com $35 \leq n \leq 37$, o que significa que não existem números perfeitos pares no intervalo dado.

10. Respostas dos exercícios do capítulo 10

1. Temos que $990 = 2 \times 3^2 \times 5 \times 11$. Podemos usar 2 como base para cada um destes fatores.

2. Se 4 não divide $n-1$ então $n-1 = 2 \cdot q$ onde q é ímpar. Logo $(n-1)/2 = q$ é ímpar. Portanto

$$(n-1)^{(n-1)/2} \equiv (n-1)^q \equiv -1 \not\equiv 1 \pmod{n}.$$

3. Temos que $2^7 - 2 = 2 \times 3^2 \times 7$. Podemos usar 2 como base para 7 e -1 como base para 2. Para o fator 3 podemos usar 3 como base.

4. (1) Como $2^{n-1} = 2^{2p} = 4^p$ e como $2^{n-1} \equiv 1 \pmod{n}$ então $4^p \equiv 1 \pmod{n}$. Se q é um fator primo de n então $4^p \equiv 1 \pmod{q}$. Mas isto implica que a ordem de $\overline{4}$ em $U(q)$ é 1 ou p. Se a ordem fosse 1 então $4 \equiv 1 \pmod{q}$, o que nos dá $3 \equiv 0 \pmod{q}$. Como 3 e q são primos, temos que $q = 3$. Mas 3 não é um fator de n por hipótese. Logo $\overline{4}$ tem ordem p em $U(q)$.
(2) Pelo teorema de Fermat, temos que $4^{q-1} \equiv 1 \pmod{q}$. Como $\overline{4}$ tem ordem p em $U(q)$, concluímos que p divide $q-1$. Isto é $q = kp+1$, para algm inteiro positivo k.
(3) Supondo que q é um fator primo de n diferente de n, temos que $q < n$. Isto é $kp + 1 < 2p + 1$. Logo $k = 1$.
(4) Para verificar que n é primo basta testar se $p+1$ divide $2p+1$, já que pelos ítens anteriores este é o único fator primo possível para n. Mas se $p+1$ dividir $2p+1$, então $2p + 1 \equiv 0 \pmod{p+1}$. Isto é $p \equiv 0 \pmod{p+1}$, o que não é possível, já que $p+1$ é maior que p.

5. (1) A indução começa com $k = 3$. Neste caso $2^k = 2^3 = 8$ e b pode assumir os valores $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. É imediato verificar que cada um destes elementos tem ordem 2 em $U(8)$. Assim se b é ímpar, $b^2 \equiv 1 \pmod{8}$.

Suponhamos então que $b^{2^{k-2}} \equiv 1 \pmod{2^k}$ para algum $k \geq 3$ (*hipótese de indução*). Queremos calcular $b^{2^{(k+1)-2}}$ módulo 2^{k+1} e mostrar que é 1. Mas $b^{2^{k-1}} \equiv 1 \pmod{2^k}$ nos diz que $b^{2^{k-2}} - 1 = 2^k \cdot a$ para algum $a \in \mathbb{Z}$. Temos a seguinte seqüência de congruências módulo 2^{k+1}:

$$b^{2^{(k+1)-2}} \equiv (b^{2^{k-2}})^2 \equiv (2^k \cdot a + 1)^2 \equiv 2^{k+1}(2^{k-1} \cdot a^2 + a) + 1 \equiv 1,$$

completando a demonstração por indução.
(2) Se $U(2^k)$ fosse cíclico, teria um elemento de ordem igual a $\phi(2^k) = 2^{k-1}$. Mas isto é equivalente a dizer que existe um b ímpar tal que

$$b^{2^{k-1}} \equiv 1 \pmod{2^k} \text{ mas } b^{2^{k-2}} \not\equiv 1 \pmod{2^k}.$$

Entretanto $b^{2^{k-2}} \equiv 1 \pmod{2^k}$ para qualquer b ímpar por (1). Logo $U(2^k)$ *não* pode ser cíclico.

6. (1) Digamos que G tem operação $\star$. Podemos agrupar os elementos de G em dois tipos: os elementos cujos inversos são diferentes deles próprios e os elementos

que são seus próprios inversos. Estes últimos são os elementos de ordem 2. Sejam $a_1, \ldots, a_{2n}$ os elementos de G do primeiro tipo. Vamos supor que numeramos os elementos de modo que a_1 seja o inverso de a_2, a_3 seja o inverso de a_4, e assim por diante. Sejam $b_1, \ldots, b_m$ os elementos de G do segundo tipo. Então

$$(e \star a_1 \star a_2 \star \ldots a_{2n}) \star b_1 \star \cdots \star b_m = b_1 \star \cdots \star b_m$$

já que $a_1 \star a_2 = e$, $\ldots$,$a_{2n-1} \star a_{2n} = e$. Observe que a ordem dos elementos no produto acima não é importante porque o grupo é abeliano.
(2) Se $\overline{a}$ é um elemento de $U(p)$ de ordem 2 então $\overline{a}^2 = \overline{1}$ em $U(p)$. Isto é $a^2 - 1$ é divisível por p. Mas $a^2 - 1 = (a-1)(a+1)$. Como p é primo, tem que dividir um destes fatores. Se dividir o primeiro, então $\overline{a} = \overline{1}$; se o segundo, então $\overline{a} = -\overline{1}$.
(3) De acordo com (1), multiplicando todos os elementos de $U(p)$ obtemos o produto dos seus elementos de ordem 2. Mas por (2), o grupo $U(p)$ tem apenas um elemento de ordem 2, que é $-\overline{1}$. Como o produto dos elementos de $U(p)$ é $\overline{(p-1)!}$, temos que $\overline{(p-1)!} = -\overline{1}$. Em outras palavras $(p-1)! \equiv -1 \pmod{p}$.
(4) Se n for composto, podemos escrevê-lo na forma ab onde a e b são inteiros positivos menores que n. Portanto a e b são ambos fatores de $(n-1)!$. Logo n divide $(n-1)!$, donde a congruência desejada.
(5) A validade do teste é conseqüência imediata de (3) e (4). A principal desvantagem deste teste é que é muito lento calcular $(n-1)!$, mesmo executando o fatorial módulo n.

7. O gerador obtido é 5.

8. Note primeiro que se p é um primo ímpar, então $\phi(2p) = \phi(p) = p - 1$. Suponha que $\overline{a} \in U(p)$ é um gerador. Então $\overline{a}$ tem ordem $p-1$.
(1) Suponhamos que a é ímpar. Como $\overline{a} \in U(p)$, então p não divide a. Como a é ímpar, então $mdc(a, 2p) = 1$. Logo a classe de a em $\mathbb{Z}_{2p}$ é inversível. Qual a ordem da classe de a em $U(2p)$? Digamos que a ordem é $r > 1$. Então $a^r \equiv 1 \pmod{2p}$, donde $a^r \equiv 1 \pmod{p}$. Portanto $r \geq p - 1$. Como $U(2p)$ tem ordem $p-1$, temos de fato que $r = p - 1$ e a classe de a em $U(2p)$ gera todo este grupo.
(2) Se a for par, então a classe de a em $\mathbb{Z}_{2p}$ *não* é inversível. Vamos considerar então $a + p$. Como p é ímpar, assim também é $a + p$. Além do mais, como p não divide a, também não pode dividir $a + p$. Portanto $mdc(a + p, 2p) = 1$. Assim a classe de $a + p$ em $\mathbb{Z}_{2p}$ está de fato em $U(2p)$. Qual a ordem da classe de $a + p$ em $U(2p)$? Digamos que é $r > 1$. Então $(a + p)^r \equiv 1 \pmod{2p}$. Mas disto concluímos que $a^r \equiv 1 \pmod{p}$. Portanto $r \geq p - 1$ e, como em (1), podemos concluir que $a + p$ gera $U(2p)$.
(3) Pelo *teorema do elemento primitivo* o grupo $U(p)$ é cíclico. Vimos em (1) e (2) que, sendo o gerador de $U(p)$ par ou ímpar, podemos constuir a partir dele um gerador para $U(2p)$. Logo $U(2p)$ é cíclico.

9. Se G é um grupo cíclico de ordem n gerado por g então g também tem ordem n.
(1) Digamos que $d = \text{mdc}(k, n)$ e $d = \alpha \cdot k + \beta \cdot n$. Então

$$g^d = g^{\alpha k + \beta n} = (g^k)^\alpha \cdot (g^n)^\beta = (g^k)^\alpha,$$

já que $g^n = e$, o elemento neutro de G. Concluímos que g^d é uma potência de g^k. Se n e k são primos entre si, então $d = 1$, e $g = (g^k)^\alpha$; logo g^k é um um gerador de G, neste caso. Se $d \neq 1$, então $n = dr$ e, portanto, kr é múltiplo de n. Temos,

então, pelo lema chave, que $(g^k)^r = e$. Como $r < n$ (já que $d \neq 1$), concluímos que g^k tem ordem menor que n neste caso.
(2) Por (1), se g é um gerador de G, então os demais geradores de G serão da forma g^k, onde $k < n$ e $\text{mdc}(k, n) = 1$. Mas existem exatamente $\phi(n)$ inteiros positivos menores que n que são primos a n. Logo G tem $\phi(n)$ geradores.
(3) O grupo $U(p)$ tem ordem $\phi(p) = p - 1$, já que p é primo. Portanto, de acordo com (2), terá que ter $\phi(p - 1)$ geradores.

11. Respostas dos exercícios do capítulo 11

1. $n = 2131 \times 1667$.

2. A mensagem é 'FERMAT VIVE'.

3. Os fatores primos de n são 71 e 107, $d = 3$ e a mensagem é 'FIM'.

4. A equação $x^3 \equiv x \pmod{p}$ tem três soluções qualquer que seja o primo $p \neq 2$. De fato, se $x \not\equiv 0 \pmod{p}$ então $x^2 \equiv 1 \pmod{p}$. Esta última equação só tem raízes congruentes a 1 e -1 módulo p, como vimos no exercício 5(2) do capítulo 10.

Portanto o sistema

$$x^3 \equiv x \pmod{3}$$
$$x^3 \equiv x \pmod{p}$$

tem 9 soluções pelo teorema chinês do resto. Logo $x^3 \equiv x \pmod{3p}$ tem 9 soluções.

5. Relembrando a notação: p é primo e $\overline{g} \in U(p)$ é um gerador. O número a foi escolhido aleatoriamente no intervalo $0 < a < p - 1$. O número b é um bloco da mensagem original. Para codificá-lo escolhemos aleatoriamente um inteiro positivo k e codificamos b como sendo o par $(\overline{g}^k, \overline{b}\overline{g}^{ak})$.
(1) Decodificar significa obter b a partir do par $(\overline{g}^k, \overline{b}\overline{g}^{ak})$. Digamos que conhecemos a. Então podemos achar b calculando

$$(\overline{b}\overline{g}^{ak})(\overline{g}^k)^{(n-a)} = \overline{b} \cdot \overline{g}^{ak+(n-a)k} = \overline{b} \cdot \overline{(g^n)}^k = \overline{b}.$$

Note que isto nos dá b apenas porque escolhemos b de modo que $0 \leq b \leq p - 1$.
(2) Para decodificar *usando o método descrito em* (1), precisamos encontrar a a partir de $\overline{g}^a$ e $\overline{g}$, que são conhecidos. Isto é, queremos resolver a equação $\overline{g}^x = \overline{c}$, onde c é a forma reduzida de g^a módulo p. Se p é grande, isto é muito difícil de efetuar na prática. Observe que se g, x e c fossem números reais, então $x = \log_g c$. Por isso o valor de x que satisfaz 'a equação $\overline{g}^x = \overline{c}$ é conhecido como *logaritmo discreto* de c na base g. Na verdade, não é realmente necessário resolver $\overline{g}^x = \overline{c}$ para achar a. Bastaria que pudéssemos determinar a a partir de $\overline{g}^k$ e $\overline{g}^{ak}$, que são conhecidos. Entretanto, acredita-se (embora isto ainda não tenha sido provado), que este problema seja equivalente à determinação do logaritmo discreto.

6. Seja $u = p^{q-1} - q^{p-1}$ e vamos calcular u^2 módulo p. Usando o teorema de Fermat (e lembrando que $p \neq q$ são primos), obtemos

$$u \equiv p^{q-1} - q^{p-1} \equiv p^{q-1} \equiv 1 \pmod{q}$$
$$u \equiv p^{q-1} - q^{p-1} \equiv -q^{p-1} \equiv -1 \pmod{p}.$$

De modo que $u^2 \equiv 1 \pmod{p}$ e $u^2 \equiv 1 \pmod{q}$. Como $u^2 - 1$ é divisível por p e por q que são primos distintos, temos que $u^2 - 1$ é divisível por pq. Isto é $u^2 \equiv 1 \pmod{n}$.

Seja agora x_0 uma solução de $x^2 \equiv a \pmod{n}$. Então

$$(ux_0)^2 \equiv x_0^2 \cdot u^2 \equiv a \cdot 1 \equiv a \pmod{n}.$$

O mesmo vale para $-x_0$ e $-ux_0$.

Observe que $u \not\equiv \pm 1 \pmod{n}$. Por exemplo, se $u \equiv 1 \pmod{n}$, então u seria congruente a 1 módulo p e módulo q. Mas $u \equiv -1 \pmod{p}$.

7. É evidente que se temos uma maneira eficiente de fatorar n, então fica fácil quebrar o código. Digamos que alguém inventou uma máquina capaz de quebrar o método de Rabin com chave pública b e n. Da análise do mtodo de Rabin sabemos que o que a máquina faz é equivalente a achar uma raiz para a equação $x^2 \equiv a \pmod{n}$, para um dado inteiro a. Para falar a verdade, a máquina precisa achar as 4 raízes da equação. Vamos supor uma coisa um pouco mais fraca. Digamos que temos uma máquina que, dado um inteiro a, onde $0 \leq a < n$, calcula uma raiz de $x^2 \equiv a \pmod{n}$. Note que não precisamos saber como funciona a máquina.

Escolha agora, aleatoriamente, um inteiro positivo r, menor que n e tal que $\text{mdc}(r, n) = 1$. Calcule $a \equiv r^2 \pmod{n}$. Use então a máquina de descodificação para encontrar uma solução para $\overline{x}^2 \equiv \overline{a}$ em $\mathbb{Z}_n$. Observe que conhecemos duas soluções desta equação, que são r e $n - r$. Entretanto, como a equação tem, em geral, 4 soluções, há uma probabilidade de $1/2$ de que a solução v produzida pela máquina seja diferente de r e de $n - r$. Logo

$$(v - r)(v + r) \equiv v^2 - r^2 \equiv 0 \pmod{n}.$$

Mas $n = pq$. Assim p divide o produto $(v - r)(v + r)$, logo divide um dos fatores. Digamos que p divide $v + r$.

Sob estas hipóteses q não pode dividir $v + r$. Se dividisse, então n dividiria $v + r$; ou seja $v \equiv -r \pmod{n}$. Como $0 \leq v < n$, teríamos $v = n - r$, o que foi excluído por hipótese. Assim p divide $v + r$, mas q não divide $v + r$. Portanto $\text{mdc}(v + r, n) = p$, o que nos daria uma maneira eficiente de calcular p.

Observe que a probabilidade de obter um fator de n fazendo uma escolha aleatória de r é $1/2$. Por isso esperamos achar um fator de n fazendo, em média, duas escolhas aletórias de r, o que é bastante eficiente.

8. Não vou estragar a surpresa dizendo qual a decodificação da mensagem!