Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução da 2ª Frequência

21 de Dezembro de 2005

---

1. (3 valores)

Uma vez que $16 \equiv 5 \pmod{11}$, $16^{182} \equiv 5^{182} \pmod{11}$. Por outro lado, 11 é primo e $(11,5) = 1$ logo, do Teorema de Fermat, tem-se $5^{10} \equiv 1 \pmod{11}$, concluindo-se que

$$16^{182} \equiv \left(5^{10}\right)^{18} 5^2 \pmod{11} \equiv 1^{18} 5^2 \pmod{11} \equiv 25 \pmod{11} \equiv 3 \pmod{11}.$$

De modo análogo, porque $15 \equiv 4 \pmod{11}$ e $(4,11) = 1$, obtém-se

$$15^{121} \equiv \left(4^{10}\right)^{12} 4 \pmod{11} \equiv 1^{12} 4 \pmod{11} \equiv 4 \pmod{11}.$$

Então $16^{182} - 15^{121} \equiv 3 - 4 \pmod{11} \equiv -1 \pmod{11} \equiv 10 \pmod{11}$ e o resto da divisão inteira de $16^{182} - 15^{121}$ por 11 é 10.

---

2. (3,5 valores)
Observe-se que, de $p \equiv 3 \pmod{4}$, resulta que $p-1$ é par. Pelo Teorema de Wilson tem-se que $(p-1)! \equiv -1 \pmod{p}$, isto é,

$$1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p-1}{2}+1\right) \times \cdots \times (p-2) \times (p-1) \equiv -1 \pmod{p}.$$

Considerem-se

$$a = 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \tag{1}$$

e

$$b = \left(\frac{p-1}{2}+1\right) \times \cdots \times (p-2) \times (p-1). \tag{2}$$

Cada um dos factores presentes em (2) é congruente módulo p com o simétrico de exactamente um dos factores presentes em (1). Assim,

$$\begin{aligned}
b &= \left(\frac{p-1}{2}+1\right) \times \left(\frac{p-1}{2}+2\right) \times \cdots \times (p-2) \times (p-1) \\
&= \left(\frac{p+1}{2}\right) \times \left(\frac{p+3}{2}\right) \times \cdots \times (p-2) \times (p-1) \\
&= \left(p - \frac{p-1}{2}\right) \times \left(p - \frac{p-3}{2}\right) \times \cdots \times (p-2) \times (p-1) \\
&\equiv \left(-\frac{p-1}{2}\right) \times \left(-\frac{p-3}{2}\right) \times \cdots \times (-2) \times (-1) \pmod{p} \\
&\equiv (-1)^{\frac{p-1}{2}} a \pmod{p}.
\end{aligned}$$

Então, de $-1 \equiv ab \pmod p$, resulta que $-1 \equiv (-1)^{\frac{p-1}{2}} a^2 \pmod p$, concluindo-se que $a^2 \equiv (-1)^{\frac{p-1}{2}+1} \pmod p$. Uma vez que $p \equiv 3 \pmod 4$, $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ é par e, portanto, $a^2 \equiv 1 \pmod p$.

---

3. (4,5 valores)
Uma vez que 2, 5 e 7 são primos dois a dois, o Teorema chinês dos resíduos garante que o sistema

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv -1 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases} \tag{3}$$

tem solução. sendo o conjunto das soluções uma classe de congruência módulo $2\times5\times7 = 70$. Resolvam-se as congruências auxiliares $\frac{70}{2} b_1 \equiv 1 \pmod 2$, $\frac{70}{5} b_2 \equiv 1 \pmod 5$ e $\frac{70}{7} b_3 \equiv 1 \pmod 7$.

$\frac{70}{2} b_1 \equiv 1 \pmod 2 \Leftrightarrow 35b_1 \equiv 1 \pmod 2 \Leftrightarrow b_1 \equiv 1 \pmod 2$.

$\frac{70}{5} b_2 \equiv 1 \pmod 5 \Leftrightarrow 14b_2 \equiv 1 \pmod 5 \Leftrightarrow -b_2 \equiv 1 \pmod 5 \Leftrightarrow b_2 \equiv -1 \pmod 5$.

$\frac{70}{7} b_3 \equiv 1 \pmod 7 \Leftrightarrow 10b_3 \equiv 1 \pmod 7 \Leftrightarrow 3b_3 \equiv 1 \pmod 7 \Leftrightarrow b_3 \equiv 5 \pmod 7$.

Considerem-se $b_1 = 1$, $b_2 = -1$ e $b_3 = 5$.

Então $0 \times \frac{70}{2} b_1 + (-1) \times \frac{70}{5} b_2 + 5 \times \frac{70}{7} b_3 = 0 + (-1) \times 14 \times (-1) + 5 \times 10 \times 5 = 264$ é uma solução de (3) e (Teorema chinês dos resíduos) o conjunto das soluções de (3) é $[264]_{70} = [54]_{70}$. O menor inteiro positivo que é solução de (3) é 54.

---

4. (4,5 valores)
Por definição, $\varphi(mn)$ é o número de elementos de qualquer sistema reduzido de resíduos módulo mn. Assim, a demonstração é feita provando que qualquer sistema reduzido de resíduos módulo mn tem $\varphi(m)\varphi(n)$ elementos.

Sejam $R = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$, $S = \{s_1, s_2, \ldots, s_{\varphi(n)}\}$ e $T = \{t_1, t_2, \ldots, t_{\varphi(mn)}\}$ sistemas reduzidos de resíduos módulos m, n e mn, respectivamente.

Considere-se $R \times S = \{(r_i, s_j) : i = 1, 2, \ldots, \varphi(m)\,,\ j = 1, 2, \ldots, \varphi(n)\}$. Vamos definir uma função bijectiva $f : T \to R \times S$.

Seja $t_k \in T$, qualquer. De $(t_k, mn) = 1$ resulta que $(t_k, m) = 1$ e, porque R é um sistema reduzido de resíduos módulo m, existe um e um só $i \in \{1, 2, \ldots, \varphi(m)\}$ tal que $t_k \equiv r_i \pmod m$. De modo análogo, porque $(t_k, n) = 1$, existe um e um só $j \in \{1, 2, \ldots, \varphi(n)\}$ tal que $t_k \equiv s_j \pmod n$. Defina-se $f(t_k) = (r_i, s_j)$.

Verifique-se que f é injectiva. Sejam $t_k, t_h \in T$ e suponha-se que $f(t_k) = f(t_h)$. Sejam $i \in \{1, 2, \ldots, \varphi(m)\}$ e $j \in \{1, 2, \ldots, \varphi(n)\}$ tais que $f(t_k) = (r_i, s_j) = f(t_h)$. Atendendo à forma como f foi definida,

$$\begin{cases} t_k \equiv r_i \pmod m \\ t_h \equiv r_i \pmod m \\ t_k \equiv s_j \pmod n \\ t_h \equiv s_j \pmod n \end{cases} \Rightarrow \begin{cases} t_k \equiv t_h \pmod m \\ t_k \equiv t_h \pmod n \end{cases} \Rightarrow t_k \equiv t_h \pmod{[m, n]}\,.$$

Uma vez que $(m, n) = 1$ tem-se $[m, n] = mn$ e $t_k \equiv t_h \pmod{mn}$, daqui resultando (porque T é um sistema reduzido de resíduos módulo mn) que $t_k = t_h$.

Prove-se agora que f é sobrejectiva. Sejam $i \in \{1, 2, \ldots, \varphi(m)\}$ e $j \in \{1, 2, \ldots, \varphi(n)\}$, quaisquer. Como $(m, n) = 1$, o teorema chinês dos resíduos garante a existência de $x \in \mathbb{Z}$ tal que $x \equiv r_i \pmod{m}$ e $x \equiv s_j \pmod{n}$. De $x \equiv r_i \pmod{m}$ e $(r_i, m) = 1$ conclui-se que $(x, m) = 1$. Analogamente $(x, n) = 1$ e, portanto, $(x, mn) = 1$. Então (porque T é um sistema reduzido de resíduos módulo mn) existe um e um só $t_k \in T$ tal que $x \equiv t_k \pmod{mn}$. Assim $t_k \equiv r_i \pmod{m}$ e $t_k \equiv s_j \pmod{n}$, concluindo-se que $f(t_k) = (r_i, s_j)$.

Uma vez que f é bijectiva,

$$\varphi(mn) = \sharp T = \sharp(R \times S) = \varphi(m)\varphi(n)\,.$$

---

5. (4,5 valores)

Comece-se por determinar $(9, 21)$. De $21 = 2 \times 9 + 3$ e $9 = 3 \times 3$, por aplicação do algoritmo de Euclides, conclui-se que $(9, 21) = 3$.

Uma vez que $84 = 3 \times 28$, $(9, 21) \mid 84$ e a equação $9x + 21y = 84$ tem soluções inteiras.

De $3 = -2 \times 9 + 21$ resulta que $84 = -56 \times 9 + 28 \times 21$ e portanto $x_0 = -56$ e $y_0 = 28$ são inteiros que verificam a equação $9x + 21y = 84$. Sejam x e y inteiros tais que $9x + 21y = 84$. Então

$$9x + 21y = 9x_0 + 21y_0 \Leftrightarrow 9(x - x_0) = 21(y_0 - y) \Leftrightarrow 3(x - x_0) = 7(y_0 - y)\,,$$

concluindo-se, porque $(3, 7) = 1$, que $7 \mid x - x_0$ e $3 \mid y_0 - y$. Isto é, existem $q, t \in \mathbb{Z}$ tais que $x = x_0 + 7q$ e $y = y_0 - 3t$. Uma vez que

$$\begin{aligned} 9x + 21y = 84 &\Leftrightarrow 9x_0 + 9 \times 7 \times q + 21y_0 - 21 \times 3 \times t = 84 \\ &\Leftrightarrow 84 + 63(q - t) = 84 \\ &\Leftrightarrow q = t\,, \end{aligned}$$

as soluções inteiras de $9x + 21y = 84$ são dadas por

$$\begin{cases} x = -56 + 7q \\ y = 28 - 3q \end{cases}, \quad q \in \mathbb{Z}\,.$$
