

Solution 1: (a) The truth table reads

p	q	$p \rightarrow q$	$\neg p \vee q$
T	T	T	$F \vee T = T$
T	F	F	$F \vee F = F$
F	T	T	$T \vee T = T$
F	F	T	$T \vee F = T$

(b)

$p \wedge (p \rightarrow q) \rightarrow q$	
$\Leftrightarrow \neg(p \wedge (\neg p \vee q)) \vee q$	Part (a) twice
$\Leftrightarrow (\neg p \vee \neg(\neg p \vee q)) \vee q$	deMorgan
$\Leftrightarrow (\neg p \vee (p \wedge \neg q)) \vee q$	deMorgan and double negation
$\Leftrightarrow ((\neg p \vee p) \wedge (\neg p \vee \neg q)) \vee q$	Distributive law
$\Leftrightarrow (T \wedge (\neg p \vee \neg q)) \vee q$	Excluded middle
$\Leftrightarrow (\neg p \vee \neg q) \vee q$	Domination
$\Leftrightarrow \neg p \vee \neg q \vee q$	Associativity
$\Leftrightarrow \neg p \vee T$	Excluded middle
$\Leftrightarrow T$	Domination

Solution 2: (a) Running the Euclidean algorithm forward gives

$$\begin{aligned} 32 &= 4 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \quad \rightarrow \quad \boxed{\gcd(32, 7) = 1.} \end{aligned}$$

(b) Working backward, we find $\gcd(32, 7)$ as a linear combination of 32 and 7:

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) \\ &= -1 \cdot 7 + 2 \cdot 4 = -1 \cdot 7 + 2 \cdot (32 - 4 \cdot 7) \\ &= 2 \cdot 32 - 9 \cdot 7. \end{aligned}$$

Taking this mod 32 gives

$$1 \equiv -9 \cdot 7 \equiv 23 \cdot 7 \pmod{32} \quad \rightarrow \quad \boxed{d = 23.}$$

Check: $7 \cdot 23 = 161 = 5 \cdot 32 + 1 \equiv 1 \pmod{32}$.

(c) As in the Chinese Remainder Theorem, we seek a solution x of the form

$$x = x_1 \cdot 17 + x_2 \cdot 3,$$

which yields independent decoupled congruences

$$\begin{aligned} 17x_1 &\equiv 2x_1 \equiv 2 \pmod{3} \\ 3x_2 &\equiv 9 \pmod{17} \end{aligned}$$

for x_1 and x_2 . Since $\gcd(2, 3) = \gcd(3, 17) = 1$, both are easy to solve: $x_1 = 1$ and $x_2 = 3$. Putting it all back together, $\boxed{x = 26}$. Check: $x \bmod 3 = 2$ and $x \bmod 17 = 9$.

(d) The original message is

$$M = C^d \bmod N.$$

Here d is the inverse of $e \pmod{(p-1)(q-1)}$ with $N = pq$, which is the inverse of $7 \pmod{32}$. From part (b), we know $d = 23$, so

$$M = 2^{23} \pmod{51}.$$

Fermat's little Theorem says that $a^{p-1} \equiv 1 \pmod{p}$ if p is prime and $\gcd(a, p) = 1$. In the present case, FLT implies

$$\begin{aligned} 2^2 &\equiv 1 \pmod{3} \\ 2^{16} &\equiv 1 \pmod{17}, \end{aligned}$$

so

$$\begin{aligned} 2^{23} &\equiv 2 \pmod{3} \\ 2^{23} &\equiv 2^7 \equiv (-1) \cdot 2^3 \equiv -8 \equiv 9 \pmod{17}, \end{aligned}$$

(e) By parts (c) and (d), we have $M = 26$. Check: $26^7 = 52^3 13^3 26 \equiv 13^4 2 \equiv 16^2 2 \equiv 2 \pmod{51}$.

Solution 3: (a) Since $f(5/3) = f(3/5) = 8$, f is not one-to-one.

(b) Since $0/1$ and $1/0$ do not belong to \mathbf{Q}^+ , there is no element of \mathbf{Q}^+ which f maps to 1. Hence f is not onto.

(c) Since \mathbf{Z}^+ is \mathbf{N} with 0 removed, it is infinite and countable. We know that the rationals are countable, and a subset of a countable set is countable, so \mathbf{Q}^+ is countable. Clearly it is infinite, so \mathbf{Z}^+ and \mathbf{Q}^+ have the same cardinality.

Solution 4: (a) Straightforward arithmetic gives

$$1 = f_2, 2 = f_3, 3 = f_4, 4 = f_4 + f_2, 5 = f_4 + f_3 = f_5, 6 = f_5 + f_2,$$

$$7 = f_5 + f_3, 8 = f_5 + f_4 = f_6, 9 = f_6 + f_2, 10 = f_6 + f_3, 11 = f_6 + f_4, 12 = f_6 + f_4 + f_2.$$

(b) The sequence is the "digits" of n in the Fibonacci number system:

$$n = b_2 f_2 + b_3 f_3 + \cdots + b_m f_m$$

where each b_i is 0 or 1. Thus (b_2, \dots, b_m) tells us which distinct Fibonacci numbers sum to n .

(c) The procedure takes exactly m steps, each at worst costing one subtraction. We know that

$$f_m = \text{nearest integer to } \frac{1}{\sqrt{5}} \varphi^m = O(\varphi^m)$$

where $\varphi = (1 + \sqrt{5})/2$, so

$$f_m \leq n < f_{m+1} \rightarrow \varphi^m = O(n) \rightarrow m = O(\log_\varphi n) = O(\log n)$$

and the procedure has worst-case complexity $O(\log n)$.

(d) **Base:** From (a), the statement is true for $n = 1$.

Induction: Suppose it is true for $1, 2, \dots, n-1$. Let's prove it is true for n . Choose m so that $f_m \leq n < f_{m+1}$, and let $k = n - f_m$. Note that $k < f_{m+1} - f_m = f_{m-1}$. Since $k < n$, the inductive hypothesis implies that k is a sum of distinct Fibonacci numbers, and since $k < f_{m-1}$ the Fibonacci numbers which sum to k must be taken from the set $\{f_2, f_3, \dots, f_{m-2}\}$. Hence $n = k + f_m$ has a representation as a sum of *distinct* Fibonacci numbers.