

IT-math F2003 : Selected Solution(s)

Episode 4, February 25, 2003

General Comment. For integers n, m with $n \neq 0$, the expression $n \mid m$ means that n divides m (or, equivalently, that m is divisible by n). This notation is (reasonably) widely accepted, even though our textbook does not use it. $n \mid m$ expresses a *statement*, and not a number. In particular, this notation cannot be used to express the number $\frac{m}{n}$, nor $\frac{n}{m}$.

The expressions $\frac{m}{n}$ and $\frac{n}{m}$ refer to *numbers*, which means that neither expression can be used to express the fact that m is divisible by n .

SC1. Let $a, b, k \in \mathbb{Z}_+$. Show that $\gcd(k \cdot a, k \cdot b) = k \cdot \gcd(a, b)$.

Solution. To prove that $\gcd(k \cdot a, k \cdot b) = k \cdot \gcd(a, b)$ we are going to show that (i) $\gcd(k \cdot a, k \cdot b) \leq k \cdot \gcd(a, b)$, and (ii) $k \cdot \gcd(a, b) \leq \gcd(k \cdot a, k \cdot b)$.

(i). Since $\gcd(a, b) = a \cdot x + b \cdot y$ for some integers x and y , we have $k \cdot \gcd(a, b) = k \cdot a \cdot x + k \cdot b \cdot y$. Since $\gcd(k \cdot a, k \cdot b) \mid k \cdot a$ and $\gcd(k \cdot a, k \cdot b) \mid k \cdot b$ by the definition of \gcd , we also have $\gcd(k \cdot a, k \cdot b) \mid k \cdot a \cdot x + k \cdot b \cdot y = k \cdot \gcd(a, b)$. Therefore $\gcd(k \cdot a, k \cdot b) \leq k \cdot \gcd(a, b)$.

(ii). Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ by the definition of \gcd , we also have $k \cdot \gcd(a, b) \mid k \cdot a$ and $k \cdot \gcd(a, b) \mid k \cdot b$. Thus $k \cdot \gcd(a, b)$ is a divisor of both $k \cdot a$ and $k \cdot b$, and as such cannot be larger than the greatest common divisor of $k \cdot a$ and $k \cdot b$. So, $k \cdot \gcd(a, b) \leq \gcd(k \cdot a, k \cdot b)$.

SC2. Recall the Fibonacci numbers defined by the recursions $f_0 = 0$, $f_1 = 1$ and $f_{n+2} = f_n + f_{n+1}$ for $n \geq 0$. Show that $\gcd(f_n, f_{n+1}) = 1$ for all $n \in \mathbb{N}$.

Solution. We use induction on $n \geq 0$.

For $n = 0$ we have $\gcd(f_0, f_1) = \gcd(0, 1) = 1$ as required.

For $n > 0$, assume $\gcd(f_n, f_{n+1}) = 1$. Let us show that $\gcd(f_{n+1}, f_{n+2}) = 1$. We have:

$$\gcd(f_{n+1}, f_{n+2}) = \gcd(f_{n+1}, f_n + f_{n+1}) \stackrel{(*)}{=} \gcd(f_{n+1}, f_n) = \gcd(f_n, f_{n+1}) \stackrel{\text{(I.H.)}}{=} 1,$$

where the equality marked by (*) follows by a lemma we proved in the lecture ($\gcd(a, b) = \gcd(a, a + b)$), and the equality marked by (I.H.) follows by the induction hypothesis. Thus the induction step and hence the solution are completed.

SC3. Show that if $a, b > 1$, $\gcd(a, b) = 1$, $a \mid n$, and $b \mid n$, then $a \cdot b \mid n$.

Solution. Since $\gcd(a, b) = 1$, we have

$$1 = a \cdot x + b \cdot y \tag{*}$$

for some $x, y \in \mathbb{Z}$. Since $a \mid n$ and $b \mid n$, we have $n = a \cdot z = b \cdot w$ for some $z, w \in \mathbb{Z}$. Multiplying both sides of (*) by n , we get

$$n = n \cdot a \cdot x + n \cdot b \cdot y = b \cdot w \cdot a \cdot x + a \cdot z \cdot b \cdot y = a \cdot b \cdot (w \cdot x + z \cdot y).$$

Since $w \cdot x + z \cdot y \in \mathbb{Z}$, we conclude $n \mid a \cdot b$.

LH2. Show that if $2^n - 1$ is prime then so is n .

Solution. We use the method of contraposition. Namely, we assume that n fails to be prime, and show that in that case $2^n - 1$ cannot be prime either.

So suppose n is not prime. Then $n = p \cdot q$ for some positive integers $p, q < n$. Observe that $p, q > 1$ for if one of them were equal to 1, the other would have to be equal to n , whereas p and q are smaller than n . But then

$$2^n - 1 = (2^p)^q - 1 = (2^p - 1) \cdot (2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1)$$

(this uses the general formula $x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$ which can be checked directly). Since $p > 1$, we have $2^p - 1 > 1$. We also have $2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1 > 1$ because $q > 1$. Therefore $2^n - 1$, being a product of two positive integers larger than 1, cannot be prime.