

IT-math F2003 : Selected Solution(s)

Episode 5, March 4, 2003

FP1(c). Solve $14 \cdot x \equiv 17 \pmod{31}$.

Solution. From FP1(b) we have that $z = 20$ is a solution to $14 \cdot z \equiv 1 \pmod{31}$. Multiply both parts by 17: $14 \cdot 17 \cdot z \equiv 17 \pmod{31}$. So $x = 17 \cdot z = 17 \cdot 20 \equiv 30 \equiv -1 \pmod{31}$ is a solution to $14 \cdot x \equiv 17 \pmod{31}$.

FP3. Show that $[n - 1]_n$ is a unit of \mathbb{Z}_n for any integer $n \geq 2$.

Solution. We have $(n - 1) \cdot (n - 1) = n^2 - 2n + 1 \equiv 1 \pmod{n}$, so $[n - 1]_n \cdot [n - 1]_n = [1]_n$ in \mathbb{Z}_n , hence $[n - 1]_n$ is a unit of \mathbb{Z}_n .

SC2. Show that if $a \neq 0$ and $\gcd(a, b) = \gcd(a, c) = 1$ then $\gcd(a, b \cdot c) = 1$.

Solution. Since $\gcd(a, b) = \gcd(a, c) = 1$, we know that the prime factorization of a has neither any primes in common with the prime factorization of b , nor with the prime factorization of c . The prime factorization of $b \cdot c$ is obtained by putting the prime factorizations of b and c together. This clearly still has no primes in common with the prime factorization of a . Hence a and $b \cdot c$ are relatively prime.

SC3. Suppose that $[r]_n \in \mathbb{Z}_n$ is a unit (i.e. has an inverse) and that $[m]_n \in \mathbb{Z}_n$. Show that, if $[r]_n \cdot [m_1]_n = [r]_n \cdot [m_2]_n$, then $[m_1]_n = [m_2]_n$.

Solution. Since $[r]_n$ is a unit of \mathbb{Z}_n , there is a $[t]_n \in \mathbb{Z}_n$ such that $[r]_n \cdot [t]_n = [1]_n$. Multiply both sides of $[r]_n \cdot [m_1]_n = [r]_n \cdot [m_2]_n$ by $[t]_n$: $[t]_n \cdot [r]_n \cdot [m_1]_n = [t]_n \cdot [r]_n \cdot [m_2]_n$. One then has

$$[m_1]_n = [1]_n \cdot [m_1]_n = [t]_n \cdot [r]_n \cdot [m_1]_n = [t]_n \cdot [r]_n \cdot [m_2]_n = [1]_n \cdot [m_2]_n = [m_2]_n$$

as required.

LH2. Show that for non-zero integers a and b , the numbers $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are relatively prime: $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$.

Solution. By the Corollary to Euclid's Algorithm, there exist integers x and y such that $a \cdot x + b \cdot y = \gcd(a, b)$. Divide both parts of this equality by $\gcd(a, b)$. We get

$$\frac{a}{\gcd(a,b)} \cdot x + \frac{b}{\gcd(a,b)} \cdot y = 1.$$

Observe that $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are non-zero integers, so any prime dividing both of these will have to divide 1. Since 1 is not divisible by any prime, $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$ are relatively prime.

LH3. Show that inverses in \mathbb{Z}_n are unique: if $[r]_n \cdot [s_1]_n = [r]_n \cdot [s_2]_n = [1]_n$, then $[s_1]_n = [s_2]_n$.

Solution. This follows at one from SC3 by putting $m_i = s_i$.