HW 1 Selected Solutions

Prof. Shahed Sharif

3.13.4 We get $2x \equiv -9 \equiv 22 \pmod{31}$. We can apply the Extended Euclidean algorithm, or we can observe by inspection that $2 \cdot 16 = 32 \equiv 1 \pmod{31}$, and therefore $2^{-1} \pmod{31} = 16$. We conclude that

$$x \equiv 22 \cdot 16 \equiv 11 \pmod{31}.$$

3.13.11 The gcd is always 1. We prove this by induction on n. The base case, $n = 2$, is $\gcd(1, 1) = 1$. For the inductive step, we suppose $\gcd(F_n, F_{n-1}) = 1$. Observe that $F_{n+1} = 1 \cdot F_n + F_{n-1}$, and since the Fibonacci numbers are strictly increasing after F_2, we have $0 \leq F_{n-1} < F_n$. Thus F_{n-1} is the remainder when we divide F_{n+1} by F_n. By the proof of the Euclidean algorithm, we therefore have $\gcd(F_{n+1}, F_n) = \gcd(F_n, F_{n-1})$. By the inductive hypothesis, the latter expression equals 1. By induction, we are done.

We skip the second part, since it will follow from the third. Set

$$x_n = \sum_{i=0}^{F_n - 1} 10^i.$$

Thus the two numbers in the second part are x_8 and x_5. Also $x_1 = x_2 = 1$, so $\gcd(x_1, x_2) = 1$. Observe that $10^{F_{n-1}} \cdot x_n$ consists of F_n 1s followed by F_{n-1} 0s. Therefore $10^{F_{n+1} - F_n} \cdot x_n + x_{n-1}$ consists of F_n 1s followed by F_{n-1} 1s; in other words,

$$x_{n+1} = 10^{F_{n-1}} \cdot x_n + x_{n-1}.$$

Therefore the remainder when we divide x_{n+1} by x_n is x_{n-1}. Thus the same two facts that made the induction proof for the Fibonacci numbers work are also true here, and so a similar proof shows that $\gcd(x_{n+1}, x_n) = 1$ for all $n \geq 1$.

3.13.13 For the first one, if $ab \equiv 0 \pmod{p}$, then $p \mid ab$. By Euclid's Lemma, $p \mid a$ or $p \mid b$. By definition of congruence, this means that $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

For the second problem, we copy the proof for the prime case. Since $\gcd(a, n) = 1$, $\exists r, s \in \mathbb{Z}$ such that $ar + ns = 1$. Multiplying through by b yields

$$abr + bns = b.$$

We know know that $n \mid ab$, and clearly $n \mid n$. But $abr + bns = (ab)r + n(bs)$ is a linear combination of the two, so $n \mid (abr + bns)$. Therefore $n \mid b$.