Page 18 #25: Prove that there are infinitely many pairs of integers $x, y$ satisfying $x + y = 100$ and $\gcd(x, y) = 5$.

Write $y = 100 - x$ and $x = 5a$. If neither 2 nor 5 divide $a$, then the only prime divisor of $100 - x = 100 - 5a = 2^25^2 - 5a$ and $x = 5a$ is 5, and $25 \nmid 100 - x$. This makes $\gcd(x, 100 - x) = 5$. Certainly there are infinitely many possibilities for $a$; for instance, $a$ could be any prime not equal to 2 or 5.

#44: Prove that any positive integer can be written uniquely as a sum of the form $2^{j_0} + 2^{j_1} + \cdots + 2^{j_m}$, where $0 \leq j_0 < j_1 < \cdots < j_m$.

The crucial observation is the following fact (look in your calculus text if you lack faith): for any non-negative integer $z$,

$$1 + 2 + 2^2 + \cdots + 2^z = 2^{z+1} - 1 < 2^{z+1}.$$

Using this, one can proceed by induction on $n$. The case $n = 1$ is certainly true (let $m = 0 = j_0$). Now suppose $n > 1$ and let $z$ be the largest integer such that $2^{z+1} \leq n$. Note that $z \geq 0$ since $n \geq 2$. If $n = 2^{z+1}$ we’re done. Otherwise, $n - 2^{z+1} > 0$, and by the induction hypothesis

$$n - 2^{z+1} = 2^{j_0} + \cdots + 2^{j_m}$$

with $0 \leq j_0 < \cdots < j_m$. By construction, $j_m \leq z$, so that

$$n = 2^{j_0} + \cdots + 2^{j_m} + 2^{z+1}.$$

So what about UNIQUENESS? Well, this can by proven by induction on $n$ as well. Suppose first that $n = 1 = 2^0$. If $2^0 = 2^{j_0} + \cdots + 2^{j_m} \geq 2^{j_m}$, then certainly $j_m = 0 = m$. Now suppose $n > 1$ and

$$n = 2^{j_0} + \cdots + 2^{j_m} = 2^{k_0} + \cdots + 2^{k_l}$$

with $0 \leq j_0 < \cdots < j_m$ and $0 \leq k_0 < \cdots < k_l$. Without loss of generality, $j_m \leq k_l$. If $j_m < k_l$, then by what was shown above (the crucial observation),

$$n = 2^{j_0} + \cdots + 2^{j_m} \leq 1 + 2 + \cdots + 2^{j_m} < 2^{k_l} \leq n.$$
Thus $j_m = k_l$. So now look at $n - 2^{j_m} = n - 2^{k_l} < n$. By the induction hypothesis, $m - 1 = l - 1$ and $j_i = k_i$ for $i = 0, \ldots, m - 1$. This proves the uniqueness of the expansion.

Page 29, #31: Prove that no polynomial $f(x)$ of positive degree with integral coefficients can represent a prime for every positive integer $x$.

The hint in the back of the book was pretty good, but you were supposed to prove the assertions in that hint. Suppose $f(x)$ is a polynomial of positive degree with integral coefficients. If $f(1)$ is not a prime, we’re done. Otherwise, $f(1) = p$ for some prime $p$. By the binomial theorem, for a given integer $k$ and any non-negative integer $i$, $(1 + kp)^i = 1 + k'p$ for some integer $k'$ (depending on $k$ and $i$). Thus, for a given integer $k$, $f(1 + kp) = f(1) + k''p = (1 + k'')p$ for some integer $k''$. Now this will be a prime if and only if $k'' = 0$, so that $f(1 + kp) = p$. But the equation $f(x) = p$ can have at most $\deg(f)$ solutions since $f(x)$ is not a constant. Therefore, $k'' = 0$ for only finitely many $k$, so that $f(1 + kp)$ is a prime for only finitely many $k$. 

2