Math 445 Homework 1 solutions

1. (NZM, Problem 1.3.27) Show that if n is *not* prime, then $n|(n-1)!$.

   If $n$isn't prime, then $n = ab$, with $1 < a \leq b < n$. Then a and b are both among the factors of $(n-1)!$. So if they are *different*, then $ab|1\cdots(a-1)a(a+1)\cdots(b-1)b(b+1)\cdots(n-1) = (n-1)!$, as desired. If $a = b$, then since both are at least 2, a and $2a$ are both $\leq n-1$; if $2a > n-1$, then (since $b \geq 2$) $2a \geq n = ab$, so $b \leq 2$, so $a = b = 2$ and $n = 4$, a contradiction. So $2a^2|1\cdots(a-1)a(a+1)\cdots(2a-1)2a(2a+1)\cdots(n-1) = (n-1)!$, so $n = a^2|(n-1)!$.

2. (NZM, Problem 1.3.31) Show that if $f(x)$ is a non-constant polynomial with integer coefficients, then $f(n)$ <u>cannot</u> be prime for every $n \in \mathbb{N}$.
   (Hint: If $f(n) = p$ is prime, show that for every $k \in \mathbb{N}$ we have $p|f(n+kp)$; eventually $f(n+kp)$ is too big to <u>be</u> p ...)

   Suppose $f(n)$ is prime for every n. Since f is not constant, $f(x) \to \pm\infty$ as $x \to \infty$, so eventually we can find an $n \in \mathbb{N}$ with $|f(n)| = |p| \geq 2$ and p prime.

   Then $n + kp$ for $k \geq 1$ yields infinitely many different numbers with $f(n+kp)$, by assumption, prime. But if we write $f(x) = \sum a_i x^i$, then since $n + kp \equiv n \pmod p$, we have $(n+kp)^i \equiv n^i \pmod p$, so $f(n+kp) = \sum a_i(n+kp)^i \equiv \sum a_i n^i = f(n) \pmod p$.

   So $f(n+kp) = f(n) + (f(n+kp) - f(n) = p + pM = p(M+1)$ for some integer M, so $p|f(n+kp)$ for all k. But since these numbers are assumed to be prime, we have $f(n+kp) = \pm p$ for every k. So f takes one of the vaules p or $-p$ for infinitely many values of $n+kp$. But a polynomial can't do that, <u>unless</u> it is constant; if f has degree $d \geq 1$, then so does $f(x) - (\pm p)$, which therefore can have at most d roots $f(x) - (\pm p) = 0$, i.e., $f(x) = \pm p$. So f must be constant.

   Consequently, no non-constant polynomial with integer coefficients can have $f(n)$ prime for every natural number n.

3. (NZM, Problem 1.3.33) Show that for $n > 1$, $n^4 + n^2 + 1$ is *never* prime.
   (Hint: $f(x) = x^4 + x^2 + 1$ can be expressed as a product of quadratics; find the factorization!)

   If we are going to be able to factor $f(x)$ into quadratics <u>with</u> underbarinteger <u>coefficients</u>, then the lead and constant coefficients of each fact will need to be $1, -1$. So we try

   $x^4 + x^2 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ or $x^4 + x^2 + 1 = (x^2 + ax - 1)(x^2 + bx - 1)$, and see if we can find integers that work. And it does:

   $(x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a+b)x^3 + (1 + ab + 1)x^2 + (a+b)x + 1 = x^4 + x^2 + 1$ if $ab = -1$ and $a + b = 0$, so $b = -a$ and $a(-a) = -1$, so $a^2 = 1$. So $a = 1, b = -1$ works. So $n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1)$, which factors $n^4 + n^2 + 1$, so it isn't prime, <u>unless</u> $n^2 + n + 1 = \pm 1$ or $n^2 + n + 1 = \pm 1$. But for $n \geq 1$ $n^2 + n + 1 \geq 1 + 1 + 1 = 3$, and $n^2 - n + 1 \geq n^2 - n^2 + 1 = 1$, so the only possibility is $n^2 - n + 1 = 1$, which requires $n^2 - n = n(n-1) = 0$, so $n = 0, 1$. So for $n > 1$, $n^2 + n + 1, n^2 - n + 1 > 1$, giving a proper factorization of $n^4 + n^2 + 1$. So for $n > 1$, $n^4 + n^2 + 1$ is never prime.

4. Show that if $2^n - 1$ is prime, then n must be prime.

   It is probably most straightforward to show the contrapositive: if n is not prime, then $2^n - 1$ is not prime. Suppose that $n = rs$, with $2 \le r, s$, then

   $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1$

   But since $x^s - 1 = (x-1)(x^{s-1} + x^{s-2} + \cdots + s + 1)$ we have

   $2^n - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$. and since $r, s \ge 2$, $2^r - 1 \ge 2^2 - 1 = 3$ and $2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1 \ge 2^r + 1 \ge 2^2 + 1 = 5$. So we have found a factorization of $2^n - 1$ into factors ≥ 3, so $2^n - 1$ is composite.