Math 445 Homework 1 Solutions

1. Show that if $n > 4$ is *not* prime, then $n|(n-1)!$.

   If n4isn'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 $ab|(n-1)!$, 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 $2a^2|(n-1)!$, so $n = a^2|(n-1)!$.

2. Show that for $n > 1$, $n^4 + 4$ is *never* prime.

   $f(x) = x^4 + 4$ can be factored, over $\mathbb{R}$, into linear and irreducible quadratic factors. $f(x)$ has no real roots, so it must be the product of quadratics. If we were to make a guess, the best ones would be $(x^2 + ax + 1)(x^2 + bx + 4)$ or $(x^2 + ax + 2)(x^2 + bx + 2)$ or $(x^2 + ax - 1)(x^2 + bx - 4)$ or $(x^2 + ax - 2)(x^2 + bx - 2)$, to get the x^4 and 4 to work out. (Alternatively, we could note that the complex roots are the square roots of $\pm 2i$, which are $1 \pm i$ and $-1 \pm i$, and pair up the linear factors from the conjugates to find the answer.) Either way, we find that

   $$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

   Since (from calculus) both of these quadratics are increasing for $x \geq 1$, and take values 6 and 2 at $x = 2$, for $n > 1$ each factor of $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$ is an integer greater than 2, so $n^4 + 4$ is composite.

   [Or, even better? We find that $x^2 + 2x + 2, x^2 - 2x + 2$ are equal to ± 1 only when $x = \pm 1$ (by solving the equations!), so for any other integer, they give a non-trivial factorization.]

3. Show, by induction, that $f(n) = \frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for every $n \geq 1$. (Note, however, that it is *not* a multiple of n !)

   Base case, $n = 1$: $f(1) = \frac{1}{5} + \frac{1}{3} + \frac{7}{15} = \frac{3}{15} + \frac{5}{15} + \frac{7}{15} = \frac{15}{15} = 1$ is an integer.

   Now suppose $f(n) = \frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = N$ is an integer. Then

   $$\begin{aligned}
   f(n+1) &= \frac{1}{5}(n+1)^5 + \frac{1}{3}(n+1)^3 + \frac{7}{15}(n+1) \\
   &= \frac{1}{5}(n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) + \frac{1}{3}(n^3 + 3n^2 + 3n + 1) + \frac{7}{15}(n+1) \\
   &= \frac{1}{5}n^5 + n^4 + 2n^3 + 2n^2 + n + \frac{1}{5} + \frac{1}{3}n^3 + n^2 + n + \frac{1}{3} + \frac{7}{15}n + 1\frac{7}{15} \\
   &= (\frac{1}{5}n^5 + \frac{1}{3}n^3\frac{7}{15}n) + n^4 + 2n^3 + 2n^2 + n + n^2 + n + \frac{1}{5} + \frac{1}{3} + +1\frac{7}{15}
   \end{aligned}$$

$=f(n) + n^4 + 2n^3 + 3n^2 + 2n + f(1)$

which is (by hypothesis) a sum of six integers, so is an integer. So the inductive step is verified (if $f(n)$ is an integer then $f(n+1)$ is an integer), so by induction, $f(n)$ is an integer for every $n \geq 1$.

However, $f(2) = f(1)+1+2+3+2+f(1) = 10$, and so $f(3) = f(2)+16+16+12+4+f(1) = 59$, which is not a multiple of 3.

4. Show, by induction on n that

$$[\text{for every integer } x \geq 1,\ n! \text{ divides } x(x+1)\cdots(x+n-1).]$$

Base case, $n = 1$: $1! = 1$ divides anything, including the integer x.

Now suppose that for every $x \geq 1$, $n!$ divides $x(x+1)\cdots(x+n-1)$. We wish to show that for every $x \geq 1$, $(n+1)!$ divides $x(x+1)\cdots(x+n)$. We proceed by induction!

Base case $x = 1$ $1(1+1)\cdots(n+1) = (n+1)!$ is indeed divisible by $(n+1)!$.

Now suppose $(n+1)!$ divides $f(x) = x(x+1)\cdots(x+n)$. Then
$f(x+1) = (x+1)(x+2)\cdots(x+n)(x+n+1) = (x+1)(x+2)\cdots(x+n-1)x + (x+1)(x+2)\cdots(x+n-1)(n+1) = f(x) + (n+1)[(x+1)(x+2)\cdots(x+n-1)]$

By hypothesis, $(n+1)!|f(x)$, and by the *other* hypothesis, $n!|(x+1)(x+2)\cdots(x+n-1)$, so $(x+1)(x+2)\cdots(x+n-1) = An!$ so $(n+1)(x+1)(x+2)\cdots(x+n-1) = An!(n+1) = A(n+1)!$, so $(n+1)!|(n+1)[(x+1)(x+2)\cdots(x+n-1)]$. Therefore , $(n+1)!$ divides their sum, $f(x+1)$.

So by induction, for every $x \geq 1$, $(n+1)!$ divides $x(x+1)\cdots(x+n)$. Therefore, by induction, for every $n \geq 1$ and every $x \geq 1$, $n!$ divides $x(x+1)\cdots(x+n-1)$.

[Note: there is a much faster way (if you know a certain formula):

$$\binom{x+n-1}{n} = \frac{(x+n-1)!}{n!(x-1)!} = \frac{x(x+1)\cdots(x+n-1)}{n!}$$

is an integer, so of course the bottom divides the top!]

5. For $a \geq 2$, show that if $a^n - 1$ is prime, then n is prime.

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

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

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

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