Math 214 – Foundations of Mathematics Homework 3/18 Sam Harrington

(Due Tuesday, April 1)

Theorem 6.33: Every integer n, $n \geqslant 2$, can be factored uniquely into primes. (By "unique," we mean unique up to the order in which the primes are listed.)

Proof. Let $n, x \in \mathbb{Z}, n \geqslant 2, x \leqslant i$ and p_i, q_k is prime. Then,
n can be factored into primes, represented as $p_1p_2...p_i$ given by Prop 6.28.
For the purpose of contradiction, we are assuming that n can be factored into primes two different ways: $p_1...p_i$ and $q_1...q_k$

Goal prove the $p_i = q_k$ for all $x \leqslant i$,

We being with Strong Induction on i when $i = 1$:
B.C.

$$\begin{aligned} n &= p_1 \\ p_1 &| n \\ p_1 &| q_1...q_k \\ \text{WLG } p_1 &| q_1 && \text{Prop 6.32.5} \\ p_1 &= q_1 && \text{Property of Prime} \\ 1 &= q_2...q_k \end{aligned}$$

This implies that $q_2...q_k$ are all either 1 or -1 a contradiction that q is prime.

Inductive Assumption: We can now say that for all x if n can be factored into $i-1$ or fewer primes it is unique.
We now show the $x+1$ case:
$n = p_1...p_xp_{x+1} = q_1...q_k$

$$\begin{aligned} p_{x+1} &| q_1...q_k \\ \text{WLG } p_{x+1} &| q_k && \text{Prop 6.32.5} \\ p_{x+1} &= q_k && \text{Property of Prime} \\ p_1...p_x &= q_1...q_{k-1} \end{aligned}$$

By our ind. hyp. $p_1...p_x$ is unique, that $q_1...q_{k-1}$ must be $p_1...p_x$. And because $p_{x+1} = p_k$.
Also that $k = x+1$. p is unique if it can be factored into $x+1$ primes.
This shows that every integer n, $n \geqslant 2$, can be factored uniquely into primes. □

COMPLETED Theorem 6.36: (Fermat's Little Theorem) If $m \in \mathbb{Z}$ and p is a prime, then

$$m^p \equiv m \pmod{p}.$$

Proof. Let $m \in \mathbb{Z}$ and p be prime.
Special case, $p = 2$ $m^2 - m = m(m-1) = m(m+1-2)$ by Prop 6.16 either $2|m$ or $2|m+1$
So it can be shown that in either case $2|m^2 - m$
When $p = 2 : m^p \equiv m \pmod{p}$.

Now, either $p|m$ or $p \nmid m$:

If $p|m$:
$m = pj$
$m^p - m = m(m^{p-1} - 1) = pj(m^{p-1} - 1)$
$p|m^p - m$, when $p|m, m^p \equiv m \pmod{p}$

If $p \nmid m$ we continue by induction on m:

Base Case $m = 1$: $1^p - 1 = 0$ $p|0$
When $m = 1 : m^p \equiv m \pmod{p}$

Inductive Step, We can now assume $m^p \equiv m \pmod{p}$ for all $1 \leqslant k < m$:

$$\begin{aligned}
(k+1)^p - (k+1) &= \sum_{j=0}^{p}(\binom{p}{j}k^j 1^{p-m}) - (k+1) && \text{Binomial THM} \\
&= \binom{p}{0}k^0 + px + \binom{p}{p}k^p - k - 1 && \text{Prop 6.35} \\
&= 1 + px + k^p - k - 1 \\
&= px + pz \\
&= p(x+z)
\end{aligned}$$

Now we continue in the other direction, keeping the same base case we now assume k for $m < k \leqslant 1$:

$$\begin{aligned}
(k-1)^p - (k-1) &= \sum_{j=0}^{p}(\binom{p}{j}k^j (-1)^{p-m}) - (k-1) && \text{Binomial THM} \\
&= -\binom{p}{0}k^0 + px + \binom{p}{p}k^p - k + 1 && \text{Prop 6.35} \\
&= -1 + px + k^p - k + 1 \\
&= px + pz \\
&= p(x+z)
\end{aligned}$$

Any prime greater than 2 is odd because if not that number would be divisible by more just itself

$x - 1$ is even when x is odd, as show in the proof above

$$(-1)^p = (-1)(-1)^{p-1}$$

$$p - 1 = 2j = j + j$$

$$(-1)(-1)^{p-1} = (-1)((-1)^j)^2$$

Because $((-1)^j)^2 \in \mathbb{N}$ and -1^z can only be 1, 0, or -1, $(-1)(-1)^{p-1} = (-1)1 = -1$ $\square$