Math 214 – Foundations of Mathematics   Homework 3/18   Your name

(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 $n \in \mathbb{Z}, n \geqslant 2$ and p_i, q_k is prime. Then,
n can be factored into primes, represented as $p_1 p_2 ... p_i$ given by Prop 6.28.
Next we continue by strong induction on k:

Base Case, $i = 1$:
For the purpose of contradiction, let n have two distinct prime factorization:
$n = p_1 p_2 ... p_i$ and $n = q_1 q_2 ... q_k$.

$$\begin{aligned} p_1 &| n \\ p_1 &| q_1 q_2 ... q_k \\ \text{Without loss of generality } p_1 &| q_1 && \text{Prop 6.32.5} \\ p_1 &= q_1 && \text{Property of Prime} \end{aligned}$$

Inductive step:

WLG we can say $i \leqslant k$, We can now assume that $p_n = q_n$ for all $1 \leqslant n < i$
Now we prove the $n + 1$ case:
$n = p_1 ... p_n p_{n+1} ... p_i = q_1 ... q_n q_{n+1} ... q_k$
Because p is the same as q through n, We can substitute j in for their place, that is:

$$\begin{aligned} n = j(q_{n+1} ... q_k) &= j(p_{n+1} ... p_i) \\ \text{we can define } x \text{ such that } n &= jx \\ x = q_{n+1} ... q_k &= p_{n+1} ... p_i \\ q_{n+1} &| x \\ q_{n+1} &| p_{n+1} ... p_i \\ \text{Without loss of generality } q_{n+1} &| p_{n+1} && \text{Prop 6.32.5} \\ p_{n+1} &= q_{n+1} && \text{Property of Prime} \end{aligned}$$

Up to p_i n can be factored uniquely.
For purpose of contradiction assume $i \neq k$, WLG we can say $i < k$, that is:
$n = p_1 ... p_i = q_1 ... q_i ... q_k$.

$$\begin{aligned} \text{Shown above: } p_1...p_i &= p_1...p_i...q_k \\ 1 * p_1...p_i &= p_1...p_i...q_k \\ 1 &= p_{i+1}...q_k \end{aligned}$$

$p_{i+1}...q_k$ all equal 1, a contradiction of q_k being prime, so $i = k$.
Proving 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, $(-1)(-1)^{p-1} = (-1)1 = -1$ $\square$