HOMEWORK 8

LEANDRO RIBEIRO
(WORKED WITH KYLE FRANKE AND JOYCE GOMEZ)

Proposition 6.26. *Fix an integer $n \geq 2$. Addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}_n$ are commutative, associative, and distributive. The set $\mathbb{Z}_n$ has an additive identity, a multiplicative identity, and additive inverses.*

Proof. Take $[a] \oplus [b]$ and $[a] \odot [b]$. By definition, these are equal to $[a+b]$ and $[a \cdot b]$ respectively. We may commute to have $[b+a]$ and $[b \cdot a]$. By definition again, these can be rewritten to $[b] \oplus [a]$ and $[b] \odot [a]$. Thus, $\odot$ and $\oplus$ are commutative.

Take $([a] \oplus [b]) \oplus [c]$ and $([a] \odot [b]) \odot [c]$. By definition, these are equal to $([a+b]) \oplus [c]$ and $([a \cdot b]) \odot [c]$ respectively. We may rewrite this to be $[(a+b)+c]$ and $[(a \cdot b) \cdot c]$. We can apply associativity to get $[a+(b+c)]$ and $[a \cdot (b \cdot c)]$. By definition again we can write $[a] \oplus ([b+c])$ and $[a] \odot ([b \cdot c])$. Finally, this could be rewritten to $[a] \oplus ([b] \oplus [c])$ and $[a] \odot ([b] \odot [c])$. Thus, $\oplus$ and $\odot$ are associative.

Take $[c] \odot ([a] \oplus [b])$. By definition, this can be rewritten as $[c] \odot ([a+b]) = [c(a+b)]$. If we distribute, we have $[ca+cb]$. By definition, this is equal to $[ca] + [cb] = [c] \odot [a] \oplus [c] \odot [d]$. Thus, $\odot$ and $\oplus$ are distributive. □

Project 6.28. *Every integer ≥ 2 can be factored into primes.*

Proof. Let P(k) for $k \geq 2$ be the claim "There are primes $q_1 \dots q_t$ such that $k = q_1 \dots q_t$."
Base. k = 2. The number 2 is a prime, so $2 = 2$ is a prime factorization.
Successor. Suppose P(k) holds for $k \leq n$. Consider n + 1. We have two cases:
Case 1. n + 1 is a prime. In this case $n+1 = n+1$ is the desired prime factorization.
Case 2. n + 1 is composite. There are some integers $m \neq \pm 1$ and $m \neq \pm(n+1)$ such that $m | n+1$. Thus there exists a $j \in \mathbb{Z}$ such that $m \cdot j = n+1$. We may assume $m > 0$. Thus, $m, j \in \mathbb{N}$ and $m \cdot j = n+1$. Additionally $m \neq 1$, $m \neq n+1$, so $j \neq 1$ and $j \neq n+1$. That is to say $2 \leq m$, $j < n+1$. By our induction hypothesis, $k = q_1 \dots q_t$ and

Date: March 21, 2017.

$j = p_1 \dots p_r$ where $q_1 \dots q_t$ and $p_1 \dots p_r$ are primes. Clearly, $q_1 \dots q_t$ and $p_1 \dots p_r = n+1$ and is a prime factorization.
That is to say, P(n + 1) holds. $\square$

Proposition 6.30. *for all k,m,n* $\in \mathbb{Z}$,

$$gcd(km, kn) = |k| gcd(m, n).$$

Proof. $gcd(m,n) = mx + ny$. Thus, $|k|gcd(m,n) = |k|(mx + ny) = (|k|m)x + (|k|n)y$. By definition of gcd, we have$(|k|m)x + (|k|n)y = gcd(km, kn)$.
(I'm not sure I understood this proposition very well). $\square$

Proposition 6.31. *Let p be prime and m,n* $\in \mathbb{N}$. *If* $p|mn$ *then* $p|m$ *or* $p|n$.

Proof. Assume $p \nmid m$. We must prove $p \mid n$. By the definition of greatest common divisor, we have $qp + rm = gcd(p, m)$. Because p is prime and $p \nmid m$, we know gcd(p,m) = 1. Thus we have $qp+rm = 1$. If we multiply by n on both sides, we have $(qp+rm)n = qpn+rmn = n$. Because $p|mn$ and $p|qpn$, $p|(qpn + rmn)$. Thus, $p|n$ $\square$

Sources.

http://www.math.umassd.edu/∼ahausknecht/aohWebSiteSpring2017/courses/mth182Spring2017/sharedDownloads/HWSolutions/CZSection7_6Solutions.pdf

http://www.tkiryl.com/teaching/aa/les091503.pdf