HOMEWORK 9

LEANDRO RIBEIRO
(WORKED WITH KYLE FRANKE)

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, $p|n$. $\square$

Theorem 6.35. *If $m \in \mathbb{Z}$ and p is prime, then*

$$m^p \equiv m \text{ (mod p)}.$$

Proof. **Case 1.** m = 0. $0^p \equiv 0$. Clearly, $0^p \equiv 0$ (mod p).

Case 2. $m \geq 1$ We argue by induction on $m \geq 1$ for P(m) "$m^p \equiv m$ (mod p)."

Base. m = 1. So $1^p = 1$. Clearly, $1^p \equiv 1$ (mod p).

Successor. Suppose P(m) holds. Consider $(m+1)^p$. By the binomial theorem, $(m + 1)^p = \sum_{n=0}^{p} \binom{p}{n} m^n \cdot 1^{p-n} = \sum_{n=0}^{p} \binom{p}{n} m^n = \binom{p}{0} m^0 + \sum_{n=1}^{p-1} \binom{p}{n} m^n + \binom{p}{p} m^p$. By proposition 6.34, $p|\binom{p}{n}$ and $p|\binom{p}{n}m^n$ for $1 \leq n \leq p-1$. Thus, $p|\sum_{n=1}^{p-1}\binom{p}{n}m^n$. We may write $\sum_{n=1}^{p-1}\binom{p}{n}m^n$ as $p \cdot j$ for some j. Hence, $(m+1)^p = \binom{p}{0} + p \cdot j + \binom{p}{p} m^p = 1 + p \cdot j + m^p$. We now see that $(m + 1)^p$ mod p = $1 + pj + m^p$ mod p = 1 mod p + pj mod p + m^p mod p = 1 mod p + 0 mod p + m^p mod p. = $(1 + 0)$ mod p + m^p mod p = 1 mod p + m^p mod p. By induction, we may rewrite this as 1 mod p + m mod p = (1 + m) mod p. We conclude that $(m+1)^p \equiv (m+1)$ mod p. This completes the induction.

Case 3. $m \leq -1$.

Base. m = -1. So $-1^p = \pm 1$. Clearly, $-1^p \equiv -1$ (mod p).

Successor. Suppose P(m) holds. Consider $-(m+1)^p$. Because we've already proven P(m + 1) holds and $\equiv$ is an equivalence relation, we may negate both sides of the equality to see that $-(m+1)^p \equiv -(m+1)$ mod p $\square$

Date: March 27, 2017.

Proposition 6.33. *Let m, $n \in \mathbb{N}$. If m divides n and p is a prime factor of n that is not a prime factor of m, then m divides $\frac{n}{p}$.*

Proof. Since $m|n$, we can find $j \in \mathbb{Z}$ such that $m \cdot j = n$. From Euclid's lemma, since $p|n$, it must be the case that $p|m$ or $p|j$. Since $p|j$, we can write $j = i \cdot p$, so $n = m \cdot i \cdot p$. We can conclude that $m|\frac{n}{p}$. $\square$

Lemma. *Let p be a prime. If $p|(a_1 \dots a_n)$, then $p|a_i$ for some $1 \leq i \leq n$.*

Proof. let P(k) be the statement "$p|a_i$" for some $1 \leq i \leq k$. Let's first observe P(1).
Base. n = 1. $p|a_1$ because it is the only number given to us.
Base. n = 2. $p|a_1 \cdot a_2$. By Euclid's lemma, p must divide a_1 or a_2.
Successor. Assume P(n) holds. That is, $p|a_i$ for some $1 \leq i \leq n$. Consider the event that $p|(a_1 \dots a_{n+1})$. By Euclid's lemma, either $p|(a_1 \dots a_n)$ or $p|a_{n+1}$. If $p|a_{n+1}$, we are done. Otherwise, our induction hypothesis states that $p|a_i$ for some $1 \leq i \leq n$. Therefore the proposition holds by induction. $\square$