6 Class Lecture 10/10

Homework 2.2

1. Show that if $x, y \in \mathbb{Z}; x, y$ both odd, there is **no** $z \in \mathbb{Z}$ where $x^2 + y^2 = z^2$.

Proof. By contradiction. Let $x, y, z \in \mathbb{Z}; x, y$ are odd; $x^2 + y^2 = z^2$. Since x, y are odd, $x = 2m+1$, $y = 2n+1$ for $n, m \in \mathbb{Z}$. $x^2+y^2 = z^2$ so $(2m+1)^2+(2n+1)^2 = z^2$.

- $4m^2 + 4m + 1 + 4n^2 + 4n + 1 = z^2$.
- $4\underbrace{(m^2 + m + n^2 + n)}_{p} + 2 = z^2$. $p \in \mathbb{Z}$
- $z^2 = 4p + 2 = 2(2p + 1)$.
- $z = \sqrt{2}\sqrt{2p+1}$
- $2|z^2$

$\therefore$ z is even. $z = \sqrt{2}\sqrt{2p+1}$ and z is even $\therefore$ $z = 2q$ such that $q \in \mathbb{Z}$.

- $(2q)^2 = 4p + 2$
- $4q^2 - 4p = 2$
- $4(q^2 - p) = 2$
- $\therefore$ $q^2 - p = \frac{1}{2} \notin \mathbb{Z}$

This is a contradiction, $\therefore$ there is **no** $z \in \mathbb{Z}$ where $x^2 + y^2 = z^2$ □

GCD Continued

Theorem 6.1 (Textbook 2.4.6)**.** *Let $n, m, q \in \mathbb{Z}; q|(nm)$ and $gcd(n, q) = 1$. Then $q|m$.*

Proof. Let $n, m, q \in \mathbb{Z}$. Assume $q|(nm)$ and $gcd(q, n) = 1$. (To Show: $q|m$) Since $gcd(q, n) = 1$, $1 = qx + ny$. $\therefore m = qmx + nmy$ and we know that $q|(nm)$. $\therefore nm = qp$ such that $p \in \mathbb{Z}$. Hence, $m = qmx + qpy = q\underbrace{(mx + py)}_{\text{for } x \in \mathbb{Z}}$. So $m = qs$ $\therefore q|m$. **QED**. □

Theorem 6.2 (Corollary 2.5.2)**.** *If $p, x, y \in \mathbb{Z}$ and p is prime, and $p|(xy)$, then $p|x$ or $p|y$. (Example: $4|12$, so $4|6 * 2$).*

Proof. Let $p, x, y \in \mathbb{Z}$. Assume p is prime, and $p|(xy)$. (To Show: $p|x \vee p|y$).By Contradiction $\therefore p$ does not divide x or y. p is prime and $p|(xy)$ and p does not divide x. The only divisor p are 1 and p, and p does not divide x. $\therefore gcd(p, x) = 1$. By the previous theorem $p|y$. By assumption p does not divide y. $\therefore$ there is a contradiction, and for $p|(xy)$, then $p|x$ or $p|y$. **QED**. □

Proof. Same as above.

Case: $p|x$ ✓

2. Case: p does not divide x. $\therefore gcd(p, x) = 1$ because p is prime. We assume that $p|(xy)$. $\therefore$ by the previous theorem, $p|y$. ✓

3. **QED**.

□

Theorem 6.3. *Let $n, m, k \in \mathbb{Z}; n, m, q \geq 1$. If $n|k$ and $m|k$, and $gcd(n, m) = 1$, then $(nm)|k$. (Example: $3|24$ and $4|24$ and $(3 * 4)|24$.)*

Proof. Let $n, m, k \in \mathbb{Z}$. Assume $n, m, k \geq 1$, $n|k$, $m|k$, and $gcd(n, m) = 1$.

- $k = np$ and $k = mq$, where $p, q \in \mathbb{Z}$.
- $1 = nx + my$
- $k = knx + kmy$
- $k = nm(qx + py)$
- $\therefore (nm)|k$.
- **QED**.

□