If n is <u>not</u> a prime, say $n = k \cdot l$ with $k, l < n$, then we have zero divisors : $[k][l] = [n] = [0]$ in $\mathbb{Z}_n$

This implies that $\mathbb{Z}_n$ cannot be a field for such n (because fields do not have zero divisors (see Pblm 9).

If n <u>is</u> a prime, our observation indicates that $\mathbb{Z}_n$ is a field. This req's a little proof, which we'll do in class.

(Well, I can also list it here: if n is a prime, then $(k, n) = 1$ for $k = 1, 2, \ldots n-1$. Therefore, from the Euclidean algorithm, we can write $1 = ak + bn$ with integers a, b. But this means

$ak \equiv 1 \mod n$, or, as written as an eqn in $\mathbb{Z}_n$: $[a][k] = [1]$

So $[a]$ is the mult' inverse of $[k]$. — Cute, eh?)

#22: (a) $$\frac{517 + 213i}{11 + 25i} = \frac{(517 + 213i)(11 - 25i)}{11^2 + 25^2} = \frac{(517 \cdot 11 + 213 \cdot 25) + (213 \cdot 11 - 517 \cdot 25)i}{746}$$

$$= \frac{11012 - 10582i}{746} = \underline{14 \cdot 76 - 14 \cdot 185\, i} =: \vartheta$$

So we chose q "closest" to ϑ, but $q \in \mathbb{Z}[i]$: $q = 15 - 14i$

We find r from $517 + 213i = \underbrace{(15 - 14i)(11 + 25i)}_{515 + 221i} + r$

$r = 2 - 8i$. Indeed $r_1^2 + r_2^2 = 2^2 + 8^2 = 68$ is smaller than $b_1^2 + b_2^2 = 11^2 + 25^2 = 746$

(b) $a = \vartheta b$ means $a_1 = \vartheta_1 b_1 - \vartheta_2 b_2$, $a_2 = \vartheta_1 b_2 + \vartheta_2 b_1$ (1)

$a = qb + r$ mean $a_1 = q_1 b_1 - q_2 b_2 + r_1$, $a_2 = q_1 b_2 + q_2 b_1 + r_2$ (2)

The choice of q closest to ϑ implies $|q_1 - \vartheta_1| \le \frac{1}{2}$, $|q_2 - \vartheta_2| \le \frac{1}{2}$ (3)