Chapter 7 Number Theory

<u>Section 35 Dividing</u>

Six children find a bag containing 25 marbles. How should they share them?

Theorem 35.1 (Division). Let *a* and *b* be integers with *b > 0*. There exists integers *q* and *r* such that $a = qb + r$ and $0 \leq r < b$. Moreover, there is only one such pair *(q, r)* that satisfies these conditions. The integer *q* is called the quotient and *r* is called the remainder.

*In the previous example, $25 = 6(4) + 1 \rightarrow a = qb + r$

Example: Find the integers *q* and *r* given *a* and *b*.

(1) $a = 23; b = 10$

(2) $a = -37; b = 5$

Recall Proposition 20.3: No integer is both even and odd.

Corollary 35.4. Every integer is either even or odd, but not both.

Proof:

Recall Definition 15.3: Let *n* be a positive integer. We say that integers *x* and *y* are ***congruent modulo n*** and we write $x \equiv y(mod\ n)$ provided that $n|(x - y)$. In other words, $x \equiv y(mod\ n)$ if and only if *x* and *y* differ by a multiple of *n*.

Examples: (a) $2 \equiv 0(mod\ 2)$

(b) $3 \equiv 13(mod\ 5)$

Corollary 35.5. Two integers are congruent modulo 2 if and only if they are both even or both odd.

Proof:

Div and Mod

$div = quotient \;\; ; mod = remainder$

Definition. Let *a* and *b* be integers with $b > 0$. By the Division Theorem, there exists a unique pair of integers *q* and *r* with $a = qb + r$ and $0 \le r < b$. We define the operations ***div*** and ***mod*** by $a \; div \; b = q$ and $a \; mod \; b = r$.

Examples: (a) 12 div 3 = and 12 mod 3 =
(b) 23 div 10 = and 23 mod 10 =
(c) -37 div 5 = and -37 mod 5 =

*** Remember that *r* is never negative!***

There are now two definitions of ***mod***.
(1) $a \equiv b(mod \; n)$means that $a - b$ is a multiple of *n.* (This is an equivalence relation.)
(2) $a \; mod \; b$ means "divide and take the remainder."

Is there a connection between the two definitions? Yes!

Proposition 35.8. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then $a \equiv b(mod \; n)$ if and only if $a \; mod \; n = b \; mod \; n$.

Example: $53 \equiv 23 \; (mod \; 10)$ and $53 \; mod \; 10 = 23 \; mod \; 10 = 3$.