

## Section 34 - Dividing

Recall that we have not yet shown that every integer is either even or odd, but not both. Today, we finally get to prove this.

Consider the following division problem: What is  $23 \div 5$ ? One way to answer this is 4.6. However, there is another way to answer this that you have certainly seen before. We could say that the *quotient* is 4 and the *remainder* is 3. That is, if you have 23 objects, then you have 4 full sets of 5 with 3 left over. Now, note that we don't say that for  $23 \div 5$  the quotient is 2 and the remainder is 13 even though 2 sets of 5 and 13 left over do make 23. So how do we choose the correct quotient and remainder? The following theorem gives the requirements.

**Theorem 31.1 (Division Theorem - also sometimes called the Division Algorithm):** Let  $a, b \in \mathbb{Z}$ , with  $b > 0$ . There exists a unique pair of integers  $q$  (quotient),  $r$  (remainder) so that

$$a = qb + r \text{ and } 0 \leq r < b$$

So, for  $a = 23$  and  $b = 5$ , we get  $q = 4$  and  $r = 3$ .

Note that while  $b$  must be greater than 0,  $a$  need not be.

**Ex:** Let  $a = -23, b = 5$ . Then it might be tempting to think that we should have  $q = -4$ , but if we do this then  $r = a - qb = -23 - (-4)(5) = -3$  so  $r$  does not satisfy the requirement that  $0 \leq r < b$ . We must let  $q = -5$  and  $r = 2$  to satisfy the requirements of the Division Theorem.

Some Notation.

For  $q, r$  as in the theorem, we write  $a \operatorname{div} b = q$  and  $a \operatorname{mod} b = r$ . Thus  $23 \operatorname{div} 5 = 4$  and  $23 \operatorname{mod} 5 = 3$ .

It probably seems strange that we are seeing mod again in an entirely different context than the equivalence relation  $x \equiv y \pmod{n}$ . If you think about it, however, you can convince yourself that if  $r = a \operatorname{mod} b$  then  $r \equiv a \pmod{b}$ . Also:

**Proposition 31.6:** Let  $a, b, n \in \mathbb{Z}$  with  $n > 0$ . Then  $a \equiv b \pmod{n}$  iff  $a \operatorname{mod} n = b \operatorname{mod} n$ .

Now, let's prove that every integer is either even or odd, but not both.

**Proof:** Let  $x \in \mathbb{Z}$ .

Then, by the Division Theorem (with  $a = x, b = 2$ ) there exists a unique pair of integers  $q, r$  so that  $x = 2q + r$  and  $0 \leq r < 2$ . Since  $r$  must be either 0 or 1, we have  $x = 2q$  or  $x = 2q + 1$  and  $q \in \mathbb{Z}$ . Thus  $x$  is either even or odd. Since the remainder is unique,  $x$  cannot be both even and odd.

**Conclusion:**  $x$  is either even or odd, but not both.

Homework: Section 34, P. 297 #1,2,5