Integer Divisibility

Victor Adamchik

Fall of 2005

Lecture 2 (out of seven)

■ Plan

1. Division Algorithm
2. The fundamental theorem of arithmetic
3. Counting the number of divisors

■ The Division Algorithm

The division algorithm is actually not an algorithm in the computer science sense of the word, but rather an assertion that one can make sense out of integer division.

Theorem (The Division Algorithm)
Let $b > 0$, and a arbitrary integers. Then there exist and unique integers q (the *quotient*) *and r* (the *remainder*) *such that*

$$a = q * b + r, \text{ where } 0 \le r < b.$$

Dividend = Quotient * Divisor + Remainder

Proof.

First we prove <u>existence</u>. Two cases:

a) b does divide a

b) b does not divide a

Case a) is trivial.

Case b).

Given that b does not divide a. Consider the following set

$$S = \{ a - q * b \mid q \in \mathbb{Z} \wedge a - q * b > 0 \} \subseteq \mathbb{N}.$$

Example, $b = 3$ and $a = 10$

$$\{10 - q * 3\} = \{1, 4, 7, 10, 13, \ldots\}$$

$$q = 3, 2, 1, 0, -1, \ldots$$

S is not empty. We must prove this statement. Again, two cases to consider.

If $a > 0$, choose $q = 0$, so $a \in S$.

If $a < 0$, choose $q = a$, then $a - a * b = -a * (b - 1) > 0$ is in the set. Observe, that $a * (b - 1) \neq 0$ since b cannot be equal 1. Why? Because of our assumption "b does not divide a."

Axiom (Well-Ordering Principle)

Every nonempty set of natural numbers contains a smallest element.

Since S is the set of non-negative integers it must contain a least element, say, r_0.

$$r_0 = \min(S)$$

$$0 < r_0 = a - q_0 * b$$

We prove that $r_0 < b$ (by contradiction)

Case 1. Let $r_0 = b$

Substitute this into the above formula for r_0

$$0 < b = a - q_0 b$$

Collect terms in b

$$a = b + q_0 b = (q_0 + 1) b$$

This implies that

$$b \mid a$$

which contradicts to Case b) assumption that $b \nmid a$.

Case 2. Let $r_0 > b > 0$.

Consider $r_0 - b$. It's positive $r_0 - b > 0$ and also $r_0 - b < r_0$.

Next we show that $r_0 - b \in S$

$$r_0 - b = (a - q_0 * b) - b = a - (q_0 + 1) * b \in S$$

Therefore, $r_0 - b$ is in S and it is smaller than r_0. Contradiction to the minimality of r_0.

It remains to prove that q and r are <u>unique</u>.

Suppose that

$$\begin{aligned} a &= q_0 * b + r_0 \\ a &= q_1 * b + r_1 \end{aligned}$$

where $0 \leq r_i < b$ and $r_0 \leq r_1$.

Substract one equation frpm another, we obtain

$$0 = q_0 * b - q_1 * b + r_0 - r_1$$

$$0 = b * (q_0 - q_1) + r_0 - r_1$$

$$b * (q_0 - q_1) = r_1 - r_0$$

According to our assumption $0 \leq r_1 - r_0 < b$. Therefore,

$$0 \leq b * (q_0 - q_1) < b$$

$$0 \leq q_0 - q_1 < 1$$

$$q_0 = q_1$$

QED

The cancellation law. We have used an important property of the integers:

$x * y = 0$ implies $x = 0$ or $y = 0$.

It says that there are no nonzero zero-divisors in the integers.

Exercise. Where will the proof fail if you allow negative remainders?

Exercise. Reformulate the above theorem when $b \neq 0$ is not necessarily positive.

Here is a simple application of the Division Algorithm.

Lemma: *Let p be prime. Then* $p \mid (a * b)$ *implies that* $p \mid a$ *or* $p \mid b$.

Proof:

By the division algorithm, we can write

$$a = q_1 * p + r_1 \quad \text{and} \quad b = q_2 * p + r_2.$$

where $0 \leq r_1, \ r_2 < p$. Hence,

$$a * b = q_1 \, q_2 \, p^2 + q_1 \, r_2 * p + q_2 \, r_1 \, p + r_1 * r_2$$

$$a * b = p\,(q_1 \, q_2 \, p + q_1 \, r_2 + q_2 \, r_1) + r_1 * r_2$$

Given that p divides $a * b$, therefore, $p \mid (r_1 * r_2)$. It follows then that the remainder $r_1 \, r_2$ must be 0. But then r_1 or r_2 must be 0, so that p divides a or b. QED

Exercise. Argue that $p \nmid (r_1 * r_2)$ if $r_1 * r_2 \neq 0$. Note p is prime.

Application.We prove that $\sqrt{2}$ is irrational.

Proof. (by contradiction)

Let $\sqrt{2} = \frac{p}{q}$, in lowest terms - no common divisors. Then

$$2 = \frac{p^2}{q^2} \Rightarrow 2\,q^2 = p^2 \Rightarrow 2 \mid p^2 \Rightarrow 2 \mid (p * p) \Rightarrow 2 \mid p$$

Assume $p = 2 * c$, $c \in \mathbb{Z}^+$

Then

$$2\,q^2 = p^2 \Rightarrow 2\,q^2 = 4\,c^2 \Rightarrow q^2 = 2\,c^2 \Rightarrow 2 \mid q^2 \Rightarrow 2 \mid q$$

Contradiction, p and q have a common divisor 2. QED.

Exercise. Where will the proof fail if you try to prove that $\sqrt{4}$ is irrational?

■ The Fundamental Theorem of Arithmetic

One of the beautiful properties of the prime numbers is that every positive integer can be written as a product of primes.

Theorem (The Fundamental Theorem of Arithmetic)

Let $n \geq 2$ *be an integer. Then there exist primes* $p_1, p_2, \ldots, p_k$ *such that*

$$n = p_1 * p_2 * \ldots * p_k.$$

If we require in addition that the sequence $p_1, p_2, \ldots, p_k$ *is ordered, then it is uniquely determined by* n*.*

Example of prime factorization

$$300 = 2 * 2 * 3 * 5 * 5$$

Proof.

First existence. We use in induction on n.

The base case $n = 2$ is obvious

Inductive Hypothesis: numbers up to $n - 1$ can be writen as a product of primes.

Inductive step:

If n is prime, there is nothing to show.

Otherwise, $n = a * b$ where $1 < a, b < n$.

By IH, both a and b can be written as products of primes, and our claim follows.

Uniqueness of the factorization. Suppose

$$n = p_1 * p_2 * \ldots * p_k = q_1 * q_2 * \ldots * q_s$$

where both sequences of primes are ordered.

Since p_1 divides the second product, we must have $p_1 \mid q_i$ for some i. But then $p_1 = q_i$.

By a similar argument, $q_1 = p_j$ for some j.

It follows from the order assumption that $p_1 = q_1$, so that

$$p_2 * \ldots * p_k = q_2 * \ldots * q_s.$$

By continuing in this way, we see that each p_k must be paired with q_j. Apart from the order of the factors. QED.

Corollary. *Every positive integer > 1 can be written uniquely (except for order) in the form*

$$x = p_1^{e_1} * p_2^{e_2} * \ldots * p_n^{e_m}, \qquad p_i \neq p_j \text{ for } i \neq j$$

Counting divisors

Observation. Count the number of positive divisors

2 has two divisors 1 and 2, $2 = 2^1$

4 has three divisors 1,2 and 4, $4 = 2^2$

12 has six divisors 1,2,3,4,6 and12, $12 = 2^2 * 3$

300 has 18 divisors, $300 = 2^2 * 3 * 5^2$

Each divisor of $300 = 2^2 * 3 * 5^2$ must be in the form

$$2^i * 3^j * 5^k$$

where $0 \le i \le 2$, $0 \le j \le 1$, $0 \le k \le 2$, otherwise it won't divide 300. These will give us $3 * 2 * 3 = 18$ choices. We use here the rule of product.

The rule of product:
Friday night out:
assuming that you can go to movies (5 choices) and then go to a party (3 choices), in how many ways can you spend the evening?

Theorem. *Integer*

$$x = p_1^{e_1} * p_2^{e_2} * \ldots * p_n^{e_m}$$

has $(e_1 + 1) * (e_2 + 1) * \ldots * (e_m + 1)$ *divisors.*