Integer Divisibility

Victor Adamchik

Fall of 2005

Lecture 3 (out of seven)

Plan

1. Methods of Proofs (review)
2. Geometry of divisors
3. The greatest common divisor
4. Euclidean Algorithm

Methods of Proofs

The most theorems you want to prove are in the form

$$P \Longrightarrow Q$$

where P and Q are some statements.

Direct Proofs

A direct proof is a flow of implications beginning with P and ending with Q.

Proofs by Contradiction

In this method of proof we negate the result we need to prove, namely statement Q.

Therefore, we assume P and Not Q (denote as $\neg Q$). In the proof flow we must arrive to some conclusion that either contradicts our assumptions or is something obviously not true.

$$P \wedge \neg Q \Longrightarrow \text{False}$$

Theorem. *If x is integer and x^2 is even, then x is even.*

$$x \in \mathbb{Z} \ \bigwedge \ x^2 \text{ is even} \Longrightarrow x \text{ is even}$$

Proof.

$$x \in \mathbb{Z} \ \bigwedge \ x^2 \text{ is even} \ \bigwedge \ x \text{ is odd} \Longrightarrow \text{False}$$

Given $x^2 = 2k$ and $x = 2n + 1$. Combine them together

$$2k = (2n+1)^2$$

$$2k = 4n^2 + 4n + 1$$

$$2(k - 2n^2 - 2n) = 1$$

Proofs by Contrapositive

In this method of proof we reverse the logical implication

$$\neg Q \Longrightarrow \neg P$$

In the method of Contrapositive the goal of your proof is clear - you must prove $\neg P$.

Theorem. *If x and y are two integers whose product is odd, then both must be odd.*

$$x, \ y \in \mathbb{Z} \ \bigwedge \ x * y \text{ is odd} \Longrightarrow x \ \bigwedge \ y \text{ are odd}$$

Proof.

$$\text{either } x \ \bigvee \ y \text{ is even} \Longrightarrow x * y \text{ is even}$$

Given $x = 2k$ and $y = 2n$. Combine them together.

Proofs by Mathematical Induction

This proof technique can be stated as

$$[P(0) \ \bigwedge \forall \ k(P(k) \Longrightarrow P(k+1))] \Longrightarrow \forall \ n \ P(n)$$

First we prove that the theorem is true in the initial case. Then we prove that if it is true for any given case it is true for the next case. This will prove that it is true for all positive integers.

Counting divisors

Theorem. *For any positive integer*

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

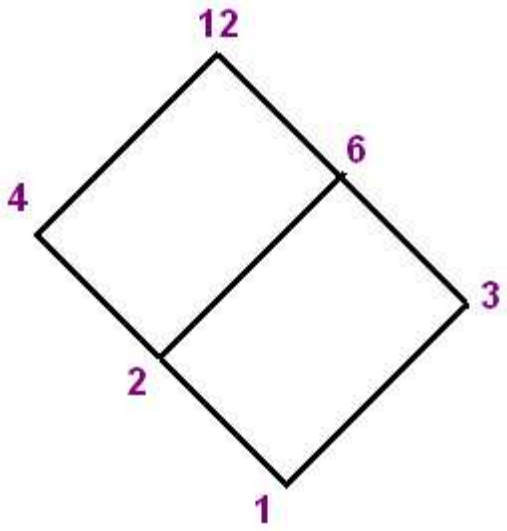
the number of divisors is given by

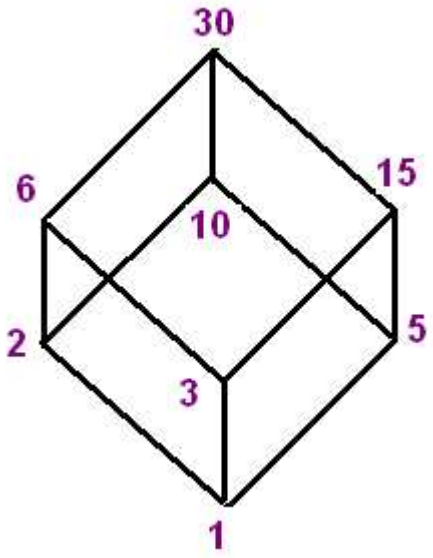
$$(e_1 + 1) * (e_2 + 1) * ... * (e_m + 1)$$

Example. 72 has 12 divisors:

$$72 = 2^3 * 3^2$$

The positive divisors of an integer are pictured in a Hasse diagram as follows: two divisors a and b are connected by a path going up if a is a divisor of b.





Exercise. Draw a Hasse diagram for p^k where p is prime.

How does the diagram help us to do algebra? It can be used to compute GCD and LCM. Observe that each element in the diagram generates a downward cone of divisors and upward code of multiples. Therefore, the intersection of downward cones gives the GCD of two numbers, and the intersectionof two upward cones gives the LCM.

Problem. A CMU football team has 100 lockers that initially closed. Student #1 opens all lockers. Student #2 closes all even lockers. Student #3 changes the status of each locker multiple of 3.And so on, student #k changes the status of each locker multiple of k. Which lockers are open after all 100 students have done their job?

Solution.
Think about what it takes to make a locker to end up open. It takes an odd number of changes. Which means an odd number of divisors.

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.
Thus $(e_1 + 1)(e_2 + 1) \ldots (e_m + 1)$ is odd or each factor is odd. Therefore, each e_k is even. So x must be a perfect square. Open lockers are those which are 1, 4, 9, 16, 25, ...

Exercise. How many positive integers less than 100 have exactly 6 divisors?

■ GCD

Definition. Suppose a and b are integers. A greatest common divisor (GCD) is defined as

$$\gcd(a, b) = \max(\, d \in P \mid d \mid a \wedge d \mid b \,).$$

Definition. Integers a and b are relatively prime (or coprime) iff $\gcd(a, b) = 1$

It is clear from the definition that

$$\gcd(-a, -b) = \gcd(a, b)$$
$$1 \le \gcd(a, b) \le \min(a, b).$$

Exercise. Prove that

$$\gcd(a, b) = \gcd(b, a - b)$$

Given a pair of numbers. Does a GCD always exist? Does it unique?

Let us prove it for positive integers!

Theorem. $\forall\, a, b \in \mathbb{Z}^+, \exists!\, d \in \mathbb{Z}^+$, *that is the GCD of a and b.*

Proof.
Let

$$S = \{n * a + m * b \mid n, m \in \mathbb{Z},\ n * a + m * b > 0\}$$

Set S has a least element. Let us call it d. We need to prove that d is a gcd.

First we prove that d exists, in other words that $d \mid a$ and $d \mid b$.

By contradiction (on minimality of d).
Assume that $d \nmid a$. Using the division algorithm, $a = q\,d + r$ where $0 < r < d$

$$r = a - q\,d = a - q\,(n\,a + m\,b) = (1 - q\,n)\,a + (-q\,m)\,b$$

We see that $r \in S$ and $r < d$. Contradiction, on minimality of d.

Next we prove that d is a greatest. Assume that there is c such that $c \mid a$ and $c \mid b$. Therefore, c divides their linear combination $c \mid (n * a + m * b) \Longrightarrow c \mid d$.

Finally we prove that d is unique. Let d_1 and d_2 be gcds of a and b. Suppose d_1 is a greatest, and d_2 is a common divisor. Then from the previous paragraph, we see that $d_2 \mid d_1$. Reversing rules, then $d_2 \mid d_1$. Therefore, $d_1 = d_2$.
QED

Corollary. $\gcd(a, b) = n * a + m * b$, where $n, m \in \mathbb{Z}$.

```
gcd (56, 24) = 8 = 56 * 1 + 24 * (-2)
```

■ Euclidean Algorithm

Given a pair of numbers a and b.
Find $gcd(a, b)$
Find such n, m *that* $gcd(a, b) = n * a + m * b$

A useful lemma that is used in an algorithm for finding gcd.

Lemma. *Let* $a = b\,q + r$, *then* $gcd(a, b) = gcd(b, r)$

Proof. Denote

$$d_1 = \gcd(a, b)$$
$$d_2 = \gcd(b, r)$$

Since $d_1 = \gcd(a, b) \Rightarrow d_1 \mid r \Rightarrow d_1$ divides both r and b therefore $d_1 \mid d_2$.
Conversely, since $d_2 = \gcd(b, r) \Rightarrow d_2 \mid a \Rightarrow d_2$ divides both a and b therefore $d_2 \mid d_1$.Hence, $d_1 = d_2$. QED

Theorem (Euclidean Algorithm)
The algorithm computes a GCD of two positive integers a, b. We apply the division algorithm

$$\begin{aligned}
a &= b * q_1 + r_1, && 0 \le r_1 < b \\
b &= r_1 * q_2 + r_2, && 0 \le r_2 < r_1 \\
r_1 &= r_2 * q_3 + r_3, && 0 \le r_3 < r_2 \\
&\ldots \\
r_{k-2} &= r_{k-1} * q_k + r_k, && 0 \le r_k < r_{k-1} \\
r_{k-1} &= r_k * q_{k+1} + 0
\end{aligned}$$

The last non-zero remainder is GCD: $\gcd(a, b) = r_k$

Proof. Let

$$S = \{r_1, r_2, \ldots, r_k\}$$

Set S contains a least element. This means that the above division will definitely terminate. Next.

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$$

QED

Example. Let us trace the algorithm to find GCD(203, 91)

$$\begin{aligned} 203 &= 2*91 + 21 \\ 91 &= 4*21 + 7 \\ 21 &= 3*7 + 0 \end{aligned}$$

Question. When does the worst performance of the Euclidean Algorithm occur?

Let us run the algorithm for GCD(21, 13)

$$\begin{aligned} 21 &= 1*13 + 8 \\ 13 &= 1*8 + 5 \\ 8 &= 1*5 + 3 \\ 5 &= 1*3 + 2 \\ 3 &= 1*2 + 1 \\ 2 &= 2*1 + 0 \end{aligned}$$

These are Fibonacci numbers (they usually denote as F_k)

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Therefore, if we set all quotients q_i to 1 in the Euclidean algorithm, we immediately obtain the following equation for the remainders

$$r_{k-2} = r_{k-1} + r_k$$

which defines Fibonacci numbers backwards. We will talk about these numbers in more details later in the course.

Theorem. *The Euclidean algorithm computes GCD(F_{k+1}, F_k) in $k - 1$ steps.*

Theorem (1845, G.Lame, french mathematician) *For two positive m and $n \le m$ the Euclidean algorithm computes GCD(m, n) in no more that $\log_{\phi}(n) + 1$ steps.*

Here ϕ (phi) is the golden ratio defined by

$$\phi = \frac{\sqrt{5}+1}{2}$$

as a solution of

$$x^2 - x - 1 = 0$$