Notes 6

Daniele's 1pm and 2pm recitations have been moved to 24-115, and Alex's 1pm recitation has been moved to 36-156.

11 Natural Numbers and Integers

We review some basic concepts: divisibility, primes, composite numbers, modular arithmetic, etc., and give basic theorems about these notions, and some simple algorithms based on these theorems.

Today we will talk about

- Fundamental theorem of arithmetic – every number has unique factorization into primes.
- Algorithm for finding GCD, the greatest common divisor of two numbers.

This subject matter is usually called *number theory*, and used to be just for fun, but recently has become very important in practice, mainly because of applications to security. Next time, we'll see one—the RSA public key encryption scheme.

11.1 Divisibility and Primes

Definition 11.1 If a and b are integers, $a \neq 0$, then a *divides* b (written $a \mid b$) if $(\exists c)$, where c is an integer, such that $b = ac$.

We say a *goes into* b (in elementary school), or b is *divisible* by a.

This makes sense even for negative integers, but we'll mainly think of positive integers.

Definition 11.2 If a is a natural number ≥ 2, then a is *prime* if the only natural numbers dividing a are 1 and a.

Definition 11.3 If a is a natural number ≥ 2, then a is *composite* if $a = bc$ for natural numbers $b, c \neq 1, a$.

Basic divisibility properties:

Theorem 11.4 1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.

2. If $a \mid b$ then $a \mid bc$ for any c.
3. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. (Of part 1) By the definition of divisibility, $(\exists t) b = at$ and $(\exists s) c = as$.
Therefore, $b + c = at + as = a(t + s)$.
Therefore, by definition, $a \mid b + c$.

Parts 2 and 3 are similar (use 2 to prove 3). ∎

In lecture 3 and last Friday's recitation, we already saw some results of these theorems – e.g., the division algorithm, and half of the Fundamental Theorem of Arithmetic:

Theorem 11.5 The Fundamental Theorem of Arithmetic
Every natural number ≥ 1 has a factorization into primes. Moreover, the factorization is unique (except for reordering the factors).

We proved existence using strong induction, and later today, we will also prove uniqueness.

Another useful definition is:

Definition 11.6 If x and y are integers, where $y > 0$, then $x \bmod y$ is the remainder on division of x by y.

$x \bmod y$ is well-defined by the division algorithm, and we find that $0 \leq x \bmod y < y$.

11.2 GCDs and LCMs

Remember Die Hard? Why did buckets of size 5 and 3 work but not 6 and 3? What if the buckets had sizes of 21 and 133, and goal was 13 gallons?

Definition 11.7 Let a, b be integers, not both 0. The *greatest common divisor* of a and b, written $\mathrm{GCD}(a, b)$, is the largest natural number g such that $g \mid a$ and $g \mid b$.

We can prove that GCD is well-defined, using well-ordering to prove that any nonempty upper-bounded set has a *largest* element.

The set of common divisors includes 1, and is finite because it is bounded above by either number. Note that GCD is always positive.

It turns out that in Die Hard, buckets of size a, b always produce numbers divisible by $\mathrm{GCD}(a, b)$. Can all such numbers in range $0, \ldots, \max(a, b)$ be produced?

The following is an interesting theorem that shows that a GCD is always expressible as a sum. We will this theorem for many purposes, especially in proving the uniqueness part of the Fundamental Theorem of Arithmetic.

Theorem 11.8 Let x and y be integers, not both 0. Then $\mathrm{GCD}(x, y)$ can be expressed in the form $ax + by$ for some integers a and b.

For example, if $x = 22$, $y = 16$, then the $\mathrm{GCD}(x,y)$ is 2, express as $2 = 3(22) + (-4)(16)$. Note that we can use negative integers.

If $x = -22$, $y = 16$, the GCD is again 2, and can be expressed as $2 = (-3)(-22) + (-4)(16)$. (The GCD is always nonnegative.)

Proof. This is a nontrivial proof. Until now, we've been looking at mechanics of proving things. This proof also requires some creativity.

Assume without loss of generality that $x, y \geq 0$. (Otherwise, use negative coefficients as above.) If either is 0, then the GCD is defined to be the other. So we're left with the case where x and y are both positive.

Let S be the set of positive integers expressible in the form $ax + by$, where a and b are integers. Fix l to be the smallest element in S, which exists by well-ordering, since S is nonempty because $x \in S$. Fix a and b such that $l = ax + by$.

As an example, let $x = 22$, and $y = 16$. S includes all numbers $ax + by$, for all integers x and y. It includes:

$$\begin{aligned}
0x + 1y &= 16 \\
1x + (-1)y &= 8 \\
(-1)x + 2y &= 10 \\
2x + (-2)y &= 12 \\
3x + (-4)y &= 2
\end{aligned}$$

and many others. $l = 2$ turns out to be the smallest element in S. We claim l is what we want, *i.e.*, $\mathrm{GCD}(x, y)$. We need to show:

1. l is a common divisor of x and y.

First show $l \mid x$, by writing $x = ql + r$ by division algorithm, where $0 \le r < l$. Then we find that:

$$\begin{aligned} r &= x - ql \\ &= x - q(ax + by) \\ &= (1 - qa)x + (-qb)y \end{aligned}$$

So r is also expressible in the sum form in terms of x and y. We know that $0 \le r < l$, but if r were positive, it would be in S, and would be smaller than l, which would contradict our choice of l as the smallest element of S.
So it r must be 0, and so $x = ql$, which says that $l \mid x$.

Similarly, $l \mid y$.

2. Any common divisor of x and y also divides l (so l is the greatest – if a number c goes into a positive number l, then $c \le l$).

   Easy: $c \mid x$ and $c \mid y$ imply $c \mid ax + by = l$.

∎

The symmetric concept to GCD is LCM:

Definition 11.9 Let a, b be positive integers. The *least common multiple* of a and b, written LCM(a, b), is the smallest natural number l such that $a \mid l$ and $b \mid l$.

11.3 Fundamental Theorem of Arithmetic

With the addition characterization we just proved for the GCD, we are finally ready to prove the Fundamental Theorem.

Recall that we already proved existence using strong induction, so it remains to prove uniqueness. For this, we will use basic number theory lemmas:

Lemma 11.10 Let p be a prime, and a and b any integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$, we are done, otherwise, GCD$(p, a) = 1$, because the only positive divisors of p are p and 1, and p doesn't divide a. So by the addition form $ax + by$, we can write 1 as a sum of the form $1 = sa + tp$, where s and t are integers.
Multiplying by b we get $b = sab + tpb$.
We have $p \mid sab$, since $p \mid ab$. and also, $p \mid tpb$.
So since $p \mid sab + tpb$, $p \mid b$ (by Theorem 11.4). ∎

Corollary 11.11 Let p be a prime, and $a_1, \cdots, a_k$ any integers. If $p \mid a_1 a_2 \cdots a_k$, then $(\exists i) p \mid a_i$.

Proof. Homework ∎

Now prove uniqueness, in the Fundamental Theorem of Arithmetic:

Proof. (Uniqueness of prime decomposition of a number n) We argue by (strong) induction.
BASE CASE:
The base case $n = 1$ is trivial – the product of no factors is defined to be 1.
INDUCTIVE STEP:
Suppose the claim is true for all numbers less than n, show it's true for n:
Suppose for contradiction that there are two different factorizations, $n = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_l$.
Then $p_1 \mid q_1 \cdots q_l$.
By corollary, $(\exists i) p_1 \mid q_i$.
But since q_i is prime, $p_1 = q_i$.
Divide both sides, and get two factorizations of n/p_1.
This contradicts our inductive hypothesis, so the theorem is proved. ∎

Unique factorization gives us a method for computing GCD:
Factor both numbers, and then multiply out all their common factors (note that you may have multiple instances of the same prime factor).

Example: 100 vs. 120:
$100 = 2 \times 2 \times 5 \times 5$
$120 = 2 \times 2 \times 2 \times 3 \times 5$
Common factors (including multiplicities): 2, 2, 5.
Product $2 \times 2 \times 5 = 20$ is GCD.

Note that we're taking the minimum number of occurrences of each prime in each of the two numbers. Likewise, unique factorization gives us a method for computing LCM: Factor both numbers, and then multiply the maximum number of occurrences of each prime.

Example: 100 vs. 120:
Product $2 \times 2 \times 2 \times 3 \times 5 \times 5 = 600$ is LCM.

These observations lead to the following useful connection between GCD and LCM:

Theorem 11.12 Let a, b be positive integers. Then $ab = \mathrm{GCD}(a, b) \times \mathrm{LCM}(a, b)$

Example: 100 vs. 120:
$100 \times 120 = 20 \times 600$
$2^2 \cdot 5^2 \times 2^3 \cdot 3 \cdot 5 = 2^2 \cdot 5 \times 2^3 \cdot 3 \cdot 5^2$

Proof. For each distinct prime in the prime factorizations, ab uses the sum of the number of occurrences in a and b, while $\mathrm{GCD}(a, b) \times \mathrm{LCM}(a, b)$ uses the minimum plus the maximum number of occurrences. So for each distinct prime, the number of occurrences is the same (the sum of two numbers is the same as their min plus their max). ∎

11.4 Euclid's GCD Algorithm

Unfortunately, the "algorithms" given above to find GCD's and LCM's – factor and multiply some of the factors – don't work well in practice because factoring is expensive. No one knows how to do it very well – and the execution time grows exponentially as the numbers grow.

In this section, we present an algorithm for GCD (and therefore also LCM) that *is* practical. This doesn't help us in factoring the numbers , though.

The algorithm was developed by Euclid, and is based on division.

11.4.1 Euclid's Algorithm for GCD

Procedure $\mathrm{Euclid}(x, y)$, where x and y are nonnegative integers, not both 0, and $x \geq y$:

1. If $y = 0$, then return x.
2. Otherwise, return $\mathrm{Euclid}(y, x \bmod y)$.

Example execution: $\mathrm{Euclid}(22, 16)$
Call $\mathrm{Euclid}(16, 6)$.
Call $\mathrm{Euclid}(6, 4)$.
Call $\mathrm{Euclid}(4, 2)$.
Call $\mathrm{Euclid}(2, 0)$.
Return 2.

11.4.2 Correctness Proof

There are two properties we need to show:

- If it ever terminates, it gives the right answer (partial correctness).
- It eventually terminates.

Both of these are normally part of correctness proofs (for standard sequential algorithms).

Partial correctness Why does this give the correct answer, if it terminates?
We will show that each step "preserves" the GCD, which implies (by simple induction) that the whole algorithm does.

Lemma 11.13 If x, y are any integers, $y \neq 0$, then $\text{GCD}(x, y) = \text{GCD}(y, x \bmod y,)$.

Proof. We show that any nonzero integer c is a common divisor of x and y if and only if it's a common divisor of y and $(x \bmod y)$.

Write $x = qy + (x \bmod y)$, using the division algorithm.

Suppose that c is a common divisor of x and y: $c \mid x$ and $c \mid y$.
Then also $c \mid x - qy = x \bmod y$, by Theorem 11.4.
So c is a common divisor of y and $(x \bmod y)$.

On the other hand, suppose that c is a common divisor of y and $(x \bmod y)$ then $c \mid y$ and $c \mid x \bmod y$.
Then $c \mid qy + (x \bmod y) = x$ by Theorem 11.4.
So c is a common divisor of x and y. ■

Since each call reduces the problem to one with the same GCD, the algorithm, *if it terminates*, produces the correct GCD for the original arguments.

Theorem 11.14 If $\text{Euclid}(x, y)$ terminates, then its output is $\text{GCD}(x, y)$.

Proof. By induction on the number of recursive calls. Suppose true for $n-1$ calls. Consider an instance $\text{Euclid}(x, y)$ that terminates in n calls. Then The answer that is output is (by inductive hypothesis) $\text{GCD}(y, x \bmod y)$ which is (by previous lemma) $\text{GCD}(x, y)$. ■

Theorem 11.15 Euclid's algorithm terminates after at most $x + y$ recursive calls.

Proof. Strong induction on the sum of the two arguments, $x + y$.
BASE CASE:
The sum is 1, so one argument is 0, and the other 1. $\text{Euclid}(x, y)$ terminates in 1 step, with 1 as output.
INDUCTIVE STEP:
Suppose $\text{Euclid}(x, y)$ terminates whenever the sum of the arguments is $< n$, and consider $\text{Euclid}(x, y)$ where $x + y = n$. We want to show that it terminates after at most n recursive calls.
If it terminates in 1 pass, we're done, since $1 \leq n$.

If not, then it calls Euclid$(y, x \mod y)$.

The sum of the arguments in the call is $y + (x \mod y)$, which we claim is strictly less than $n = x + y$, *i.e.*, is $\leq n - 1$.
If we show this, then we can apply strong induction to show that the number of recursive calls remaining is at most $n - 1$, which adds to the present pass to yield the result.

So we just need to show that $y + (x \mod y) < x + y$, *i.e.*, $x \mod y < x$. This is true since $x \geq y$. ■

Here's an alternative proof that some might find clearer:

Proof. Strong induction on the second argument y.
INDUCTIVE STEP (complete with implicit BASE CASE): Suppose Euclid(x, y) terminates whenever $y < n$.
Consider a call to Euclid(x, n).
If $n = 0$ (base case) then we terminate in $0 \leq x + n$ calls.
If $n \neq 0$, we call Euclid$(n, x \bmod n)$. But we know $x \bmod n < n$.
Thus, by inductive hypothesis, recursive call terminates in at most $n + x \bmod n$ calls.
So our call terminate in $n + x \bmod n + 1 < n + x + 1 \leq n + x$ calls. ■

Example 1 Show that GCD$(949, 273) = 13$ as follows:

quotient	x	y
	949	273
3	273	130
2	130	13
10	13	0