MATH 22

Lecture R: 10/30/2003

THE FUNDAMENTAL THEOREM of ARITHMETIC

You must remember this,
A kiss is still a kiss,
A sigh is just a sigh;
The fundamental things apply,
As time goes by.

—Herman Hupfeld

Administrivia

- http://denenberg.com/LectureR.pdf

- Exam 2
  - Statistics
  - Problem 1 [Grimaldi 5.8 #1d]
  - Problem 2
  - Problem 3 [Grimaldi 4.1 #23b, cf Lecture P]
  - Problem 4 [Grimaldi 4.1 #1c]
  - Problem 5 [half of Grimaldi 3.2 #6b, cf Lecture P]
  - Problem 6 [Grimaldi 3.4 #8, cf Lecture P]
    (ordered, unordered, mathematician's solutions)
  - Problem 7 [Grimaldi 5.2 #12, cf Lecture P]
  - Problem 8 [Grimaldi 5.4 #6 simplified, cf Lect. P]
  - Problem 9 [Grimaldi 5.6 #8b, cf Lecture P]
  - Problem 10 [Grimaldi 5.6 #21]

- Next exam: Monday November 24

- Reception in Clarkson Room, Thursday 11/6, 4:30–5:30, to discuss next semester's courses

Review

- Divisibility and properties of the $\mid$ relation

- Primes and the infinity of primes

- The Division Theorem:
If x and y are integers with $y > 0$, then there exist unique integers q and r such that $x = qy + r$ with $0 \leq r < y$.

- Application: Change of (positive) base

- GCD: Definition, existence, uniqueness

- Properties of the GCD and of the binary operation gcd

- Finding the GCD: The Euclidean Algorithm

- Correctness and complexity of the Euclidean Algorithm

- Applications of GCD as smallest linear combination [Grimaldi page 235] (can't really do this justice!)

- LCM: Definition and properties

F. T. of A.

The Fundamental Theorem of Arithmetic:
Every integer greater than 1 can be written as a product of primes in exactly one way.

Note that order doesn't matter when counting products: 30 = 2*3*5 = 3*5*2 = 5*2*3 etc. is just 1 product.
[Blackboard demonstration of the canonical way to write down the *prime factorization* of any number N > 1.]

We have already proved this theorem (in Project 4) except for the "in exactly one way" piece.

(By the way, do we know what the Fundamental Theorem of Algebra is? The Fundamental Theorem of Calculus?)

Just something to slip in: Grimaldi introduces $\prod$ notation in this section, but we've all seen it before. Recall that $\prod$ is just like $\sum$ except that you multiply instead of adding.

Another note: Grimaldi proves here that $\sqrt{2}$ is irrational. We did this as a first example of proof by contradiction. Review it!

Proof of Uniqueness

Lemma: Suppose x and y are positive integers and p is a prime. Then if p divides xy, it divides x or y (or both). [Proof in Grimaldi]

Lemma: Suppose $x_1, x_2, \ldots, x_n$ are positive integers and p is a prime. Then if p divides the product of the x_i it must divide one of them. [Proof by Mathematical Induction, using the first Lemma.]

Proof of the uniqueness part of the F.T.of A.:
By Mathematical Induction (strong form).

Base case: 2 has a unique prime factorization,

Inductive case: Assuming that all numbers up to N–1 have a unique prime factorization, we must prove that N does as well. So suppose otherwise, i.e. suppose that N has two prime factorizations.

Let p be any prime in the first factorization. So $p \mid N$. By the Lemma, p must divide one of the primes in the second factorization. But if p divides a prime number, that number must be p. So p appears at least once in each factorization. If we remove one factor of p from each factorization, the result is two factorizations of N/p. By the Induction Hypothesis these are the same. So an additional factor of p yields identical factorizations.

How Many Divisors?

How many (positive) divisors does N have?

Write N in its unique prime factorization $p^a q^b \ldots s^d$ where $p, q, \ldots, s$ are prime. Then any divisor of N has the form $p^x q^y \ldots r^z$ where $0 \le x \le a$, $0 \le y \le b, \ldots,$ $0 \le z \le d$.

Said another way: To make a divisor of N we form a product consisting of at most a factors of p, at most b factors of q, etc.

So there are $(a+1)$ ways to choose the number of factors of p (namely $0, 1, 2, \ldots a$), there are $(b+1)$ ways to choose the number of factors of q, etc. The total number of divisors of N is therefore $(a+1)(b+1)\ldots(d+1)$.

Note that these divisors of N include 1 (choose 0 factors of each prime!) and N itself (choose all a factors of p, all b factors of q, etc.).

Example [from G]: $29338848000 = 2^8 3^5 5^3 7^3 11^1$, so it must have $(8+1)(5+1)(3+1)(3+1)(1+1) = 1728$ positive divisors, including itself and 1.

Square Divisors

How many divisors of N are perfect squares?

A number is a perfect square if and only if *each of the exponents in its prime factorization is even.* (Obvious?)

So to build a divisor of N that's a perfect square, we can take 0, 2, 4, . . ., or $2\lfloor a/2 \rfloor$ factors of p. The number of choices is no longer $a+1$ but rather $\lfloor a/2 \rfloor + 1$. And the same applies to the other primes in the factorization of N. So N has

$$(\lfloor a/2 \rfloor + 1)(\lfloor b/2 \rfloor + 1) \ldots (\lfloor d/2 \rfloor + 1)$$

divisors that are perfect squares.

Example: The number of perfect square divisors of 29338848000 is $(4+1)(2+1)(1+1)(1+1)(0+1) = 60$.

We can do lots of other things by counting choices for number of prime factors. Grimaldi, for example, counts divisors that are multiples of 360. Note also that *a number is a perfect cube if and only if each of the exponents in its prime factorization is divisible by three*. Lots of good potential for problems here.

A Small Result

The product of three consecutive positive integers is never a perfect square.

Proof: Suppose to the contrary that

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

for positive integers m and n.

Let p be any prime divisor of $m+1$. Then p can't be a divisor of m since m and $m+1$ are relatively prime. (Any two consecutive integers are relatively prime.) Similarly, p can't be a divisor of $m+2$.

Now p clearly divides n^2, and must appear in n^2 an even number of times. Therefore it must appear in $m+1$ an even number of times, since it doesn't appear in m or in $m+2$. This means that $m+1$ must be a square, and therefore the product $m(m+2)$ must be a square since it's the quotient of two squares.

But $m^2 < m(m+2) < m^2 + 2m + 1 = (m+1)^2$.
So the square root of $m(m+2)$ must be strictly between m and $m+1$, which means $m(m+2)$ can't be a perfect square, and we have a contradiction.

GCD and LCM

When one number is a multiple of another, the smaller is their GCD and the larger is their LCM. If both numbers are powers of a single prime, e.g. $8 = 2^3$ and $32 = 2^5$, we can just take the min or max of the exponent: we get $\gcd(2^3,2^5) = 2^{\min(3,5)} = 2^3 = 8$, and doing the same thing with max gives $\operatorname{lcm}(2^3,2^5) = 32$. In general,

$$\gcd(2^x,2^y) = 2^{\min(x,y)} \quad \text{and} \quad \operatorname{lcm}(2^x,2^y) = 2^{\max(x,y)}$$

and of course this is true for any prime, not just 2.

Even more generally, we can do this with arbitrary numbers by taking the primes separately:

$$\gcd(2^a3^b5^c\ldots, 2^x3^y5^z\ldots) = 2^{\min(a,x)}3^{\min(b,y)}5^{\min(c,z)}\ldots$$

$$\operatorname{lcm}(2^a3^b5^c\ldots, 2^x3^y5^z\ldots) = 2^{\max(a,x)}3^{\max(b,y)}5^{\max(c,z)}\ldots$$

[Blackboard examples]

Proving these is a good exercise in thinking about prime factors and what you can do with them.

If we multiple the left and right sides of this identity and use the fact that $a+b = \max(a,b)+\min(a,b)$, we get

$$\gcd(2^a3^b\ldots, 2^x3^y\ldots)\operatorname{lcm}(2^a3^b\ldots, 2^x3^y\ldots) = 2^{a+x}3^{b+y}\ldots$$

and we have proved that $\gcd(x,y)\operatorname{lcm}(x,y) = xy$.