APPLICATIONS OF THE ORDER FUNCTION

LECTURE NOTES: MATH 432, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

In this lecture we will explore several applications of order functions including formulas for GCDs and LCMs, a method of showing certain numbers are irrational, and counting the number of zeros at the end of $n!$.

1. Review

We begin with a review of results from the previous lecture.

Definition 1. If m is a nonzero integer and if p is a prime, then $\mathrm{Ord}_p(m)$ is the largest integer k such that p^k divides m.

Proposition 2. *Let p be a prime and m be a nonzero integer. Then $p \mid m$ if and only if $\mathrm{Ord}_p(m) > 0$.*

Proposition 3. *Let m be a nonzero integer, and p be a prime. Then $\mathrm{Ord}_p(m) = k$ if and only if $m = up^k$ for some u relatively prime to m.*

Proposition 4. *If p is a prime and u is an integer such that $p \nmid u$, then $\mathrm{Ord}_p(up^k) = k$.*

Proposition 5. *Let p be a prime. If $a, b \in \mathbb{Z}$ are non-zero then*

$$\mathrm{Ord}_p(ab) = \mathrm{Ord}_p(a) + \mathrm{Ord}_p(b).$$

More generally, if each $a_1, \ldots, a_n \in \mathbb{Z}$ is nonzero then

$$\mathrm{Ord}_p(a_1 \cdots a_n) = \mathrm{Ord}_p(a_1) + \ldots + \mathrm{Ord}_p(a_n).$$

Proposition 6. *If $a \in \mathbb{Z}$ is non-zero and if $k \geq 0$ then*

$$\mathrm{Ord}_p\left(a^k\right) = k\,\mathrm{Ord}_p(a).$$

Proposition 7. *Suppose $p_1, \ldots, p_k$ are distinct primes. Then*

$$\mathrm{Ord}_p\left(p_1^{m_1} \cdots p_k^{m_k}\right) = \begin{cases} m_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, \ldots, p_k\} \end{cases}$$

Proposition 8 (Product formula)**.** *Let n be a positive integer, and let $p_1, \ldots, p_k$ be a finite sequence of distinct primes that includes every prime divisor of n. Then*

$$n \;=\; \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)}.$$

Exercise 1. Let n be a positive integer. Show that n is a perfect square if and only if $2 \mid \mathrm{Ord}_p(n)$ for all primes p. Hint: one direction uses the product formula.

Date: Spring 2008. Version of March 5, 2009.

2. Additional Results

Here are a few useful formulas involving order.

Proposition 9. *If $n \in \mathbb{Z}$ is nonzero, and p is a prime, then*

$$\mathrm{Ord}_p(-n) = \mathrm{Ord}_p(n).$$

Proposition 10. *Suppose m and n are positive integers. If $\mathrm{Ord}_p(m) = \mathrm{Ord}_p(n)$ for all primes p, then $m = n$.*

Proof. Let $p_1, \ldots, p_k$ be a finite sequence of distinct primes that include all primes dividing m and n. By the product formula

$$n \;=\; \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(n)} \;=\; \prod_{i=1}^{k} p_i^{\mathrm{Ord}_{p_i}(m)} \;=\; m.$$

□

The connection between the order functions and divisibility is described by the following theorem.

Theorem 11. *Suppose $m, n \in \mathbb{Z}$ are both non-zero. Then*

$$m \mid n \qquad \textit{if and only if} \qquad \mathrm{Ord}_p(m) \leq \mathrm{Ord}_p(n) \textit{ for all primes } p.$$

Remark. Since $\mathrm{Ord}_p(m) = \mathrm{Ord}_p(n) = 0$ for all p not dividing m and n, we only need to check the right-hand condition for p dividing m or dividing n.

Proof. Suppose $m \mid n$. Then $n = ml$ for some $l \in \mathbb{Z}$. So $\mathrm{Ord}_p(n) = \mathrm{Ord}_p(m) + \mathrm{Ord}_p(l)$ for all primes p. This implies that $\mathrm{Ord}_p(m) \leq \mathrm{Ord}_p(n)$ for all primes p.

Now suppose that $\mathrm{Ord}_p(m) \leq \mathrm{Ord}_p(n)$ for all primes p. First assume that m and n are positive. Let $p_1, \ldots, p_k$ be a finite sequence of distinct primes that includes all prime divisors of m and n. Let $a_i = \mathrm{Ord}_{p_i}(m)$ and $b_i = \mathrm{Ord}_{p_i}(m)$. By assumption, $a_i \leq b_i$. Define $l \in \mathbb{Z}$ by the formula

$$l \;\stackrel{\text{def}}{=}\; \prod_{i=1}^{k} p_i^{b_i - a_i}$$

By Proposition 7, $\mathrm{Ord}_{p_i}(l) = b_i - a_i$. Thus, for all p_i in the sequence $p_1, \ldots, p_k$,

$$\mathrm{Ord}_{p_i}(ml) = \mathrm{Ord}_{p_i}(m) + \mathrm{Ord}_{p_i}(l) = a_i + (b_i - a_i) = b_i = \mathrm{Ord}_{p_i}(n).$$

For p not in the sequence,

$$\mathrm{Ord}_p(ml) = \mathrm{Ord}_p(m) + \mathrm{Ord}_p(l) = 0 + 0 = 0 = \mathrm{Ord}_p(n).$$

By Proposition 10, $ml = n$. So $m \mid n$ as desired.

If m and n are not both positive, then $\mathrm{Ord}_p(|m|) \leq \mathrm{Ord}_p(|n|)$ for all primes p (Proposition 9). Thus$|m| \mid |n|$ by the above argument. But $|m| \mid |n|$ implies that $m \mid n$. □

Corollary 12. *Suppose $a, b, d \in \mathbb{Z}$ are non-zero. Then d is a common divisor of a and b if and only if $\mathrm{Ord}_p(d) \leq \min\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$ for all primes p.*

Corollary 13. *Suppose a and b are non-zero integers. Let $p_1, \ldots, p_k$ be a finite sequence of distinct primes that include all divisors of a and b. Then*

$$\mathrm{GCD}(a,b) = \prod_{i=1}^{k} p_i^{n_i}$$

where $n_i = \min\left(\mathrm{Ord}_{p_i}(a), \mathrm{Ord}_{p_i}(b)\right)$.

Proof. Let $g = \prod_{i=1}^{k} p_i^{n_i}$. Proposition 7 and definition of n_i,

$$\mathrm{Ord}_{p_i}(g) = n_i = \min\left(\mathrm{Ord}_{p_i}(a), \mathrm{Ord}_{p_i}(b)\right)$$

for all p_i in the finite sequence, and $\mathrm{Ord}_p(g) = 0$ for other p. Thus

$$\mathrm{Ord}_p(g) = \min\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$$

for all primes p. By Corollary 12, g is a common divisor.

Suppose d is any other positive divisor. By Corollary 12,

$$\mathrm{Ord}_p(d) \leq \min\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right) = \mathrm{Ord}_p(g)$$

for all primes p. Thus $d \mid g$ by Theorem 11. Thus $d \leq g$. This shows that g is the greatest common divisor. □

3. Least common multiplies (LCM)

We start with a criterion for a number to be a common multiple.

Proposition 14. *Suppose $a, b, m \in \mathbb{Z}$ are non-zero. Then m is a common multiple of a and b if and only if $\mathrm{Ord}_p(m) \geq \max\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$ for all primes p.*

Proof. If m is a common multiple of a and b, then $a \mid m$ and $b \mid m$. By Theorem 11, this means that $\mathrm{Ord}_p(a) \leq \mathrm{Ord}_p(m)$ and $\mathrm{Ord}_p(b) \leq \mathrm{Ord}_p(m)$ for all primes p. In other words, $\mathrm{Ord}_p(m) \geq \max\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$ for all primes p.

If $\mathrm{Ord}_p(m) \geq \max\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$ for all primes p, then $\mathrm{Ord}_p(a) \leq \mathrm{Ord}_p(m)$ and $\mathrm{Ord}_p(a) \leq \mathrm{Ord}_p(m)$. By Theorem 11, m is a common multiple of a and b. □

Theorem 15. *Suppose a and b are non-zero integers. Then there is a unique least common positive multiple (LCM) M of a and b. Furthermore, an integer c is a common multiples of a and b if and only if c is a multiple of M. The least common (positive) multiple M is given by the formula*

$$\mathrm{LCM}(a,b) = \prod_{i=1}^{k} p_i^{n_i}$$

where $p_1, \ldots, p_k$ is a finite sequence of distinct primes that include all divisors of a and b. and $n_i = \min\left(\mathrm{Ord}_{p_i}(a), \mathrm{Ord}_{p_i}(b)\right)$.

Proof. Let $M = \prod_{i=1}^{k} p_i^{n_i}$ where n_i and p_i are as above. We will show that M has all the desired properties. Obviously M is positive (closure under multiplication). By Proposition 7 and definition of n_i,

$$\mathrm{Ord}_{p_i}(M) = n_i = \max\left(\mathrm{Ord}_{p_i}(a), \mathrm{Ord}_{p_i}(b)\right)$$

for all p_i in the finite sequence, and $\mathrm{Ord}_p(g) = 0$ for other p. Thus

$$\mathrm{Ord}_p(M) = \max\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right)$$

for all primes p. By the previous proposition, M is a common multiple.

Suppose c is any other common multiple. By Corollary 12,

$$\mathrm{Ord}_p(c) \geq \max\left(\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\right) = \mathrm{Ord}_p(M)$$

for all primes p. Thus $M \mid c$ by Theorem 11. A similar argument shows that if $M \mid c$ then c is a common multiple. So c is a common multiple of a and b if and only if c is a multiple of M.

In particular, if c is a positive common multiple, then $M \mid c$, so $M \leq c$. Thus M is smaller than any other common multiple. So M is a least common multiple. Uniqueness is obvious ($M \leq M'$ and $M' \leq M$ implies $M = M'$). □

Here is an interesting formula relating $\mathrm{LCM}(a, b)$ and $\mathrm{GCD}(a, b)$:

Theorem 16. *Let a and b be positive integers. Then*

$$\mathrm{LCM}(a, b)\,\mathrm{GCD}(a, b) = ab$$

Proof. For any prime p, let $m_p = \mathrm{Ord}_p(a)$ and $n_p = \mathrm{Ord}_p(b)$. Then, by Corollary 13, Theorem 15, and Proposition 7,

$$\mathrm{Ord}_p\big(\mathrm{GCD}(a, b)\big) + \mathrm{Ord}_p\big(\mathrm{LCM}(a, b)\big) = \min(m_p, n_p) + \max(m_p, n_p).$$

By the following lemma,

$$\min(m_p, n_p) + \max(m_p, n_p) = m_p + n_p = \mathrm{Ord}_p(a) + \mathrm{Ord}_p(b)$$

Thus $\mathrm{LCM}(a, b)\,\mathrm{GCD}(a, b)$ and ab have the same order (for all p). By Proposition 10, they are equal. □

Lemma 17. *Let $m, n \in \mathbb{Z}$. Then* $\min(m, n) + \max(m, n) = m + n$.

Exercise 2. Prove the above lemma.

Remark. This lemma does not use any special properties of $\mathbb{Z}$. In fact, it is true of $m, n \in U$ where U is any linearly ordered set, and $+$ is any commutative binary operation on U.

This above theorem generalizes:

Proposition 18. *Let a and b be non-zero integers. Then*

$$\mathrm{LCM}(a, b)\,\mathrm{GCD}(a, b) = |ab|.$$

Proof. Apply Theorem 16 to $|a|$ and $|b|$. Then use the following lemma. □

Lemma 19. *Let a and b be non-zero integers. Then*

$$\mathrm{LCM}(a, b) = \mathrm{LCM}\big(|a|, |b|\big), \qquad \mathrm{GCD}(a, b) = \mathrm{GCD}\big(|a|, |b|\big).$$

Exercise 3. Prove the above by showing that a and b have the same common divisors (and multiples) as $|a|$ and $|b|$.

4. Irrationality Theorem

In this section we will see that $n^{1/k}$ is irrational unless n is a kth power. For example, $\sqrt{5}$ is irrational since 5 is not a square, $4^{1/3}$ is irrational since 4 is not a cube, $10^{1/5}$ is irrational since 10 is not a 5th power. We will also see an example of how to show certain logarithms are irrational.

One problem with these results is that they are not phrased in terms of *integers*. They appeal to certain real numbers and assert that these number are not in $\mathbb{Q}$. Fortunately we can convert these results into number theory problems.

Begin by supposing that $n^{1/k}$ is rational, and can be written as a/b. Then $n^{1/k}b = a$. Thus $nb^k = a^k$. In other words, the equation $ny^k = x^k$ has a solution with positive x, y. Conversely, any solution to to $ny^k = x^k$ with x, y positive integers gives a fraction x/y for the root $n^{1/k}$. So we can rephrase the problem of showing $n^{1/k}$ is irrational to the problem of showing that $ny^k = x^k$ has no solution with x, y positive integers.

We begin with a couple illustrations. Then we consider the general theorem.

Theorem 20. *The equation $x^2 = 5y^2$ has no positive integer solutions. In other words, $\sqrt{5}$ is irrational.*

Proof. Suppose otherwise, that $5y^2 = x^2$ has solution x_0, y_0. So $x_0^2 = 5y_0^2$. Thus

$$\mathrm{Ord}_5(x_0^2) = \mathrm{Ord}_5(5y_0^2).$$

This implies that

$$2\mathrm{Ord}_5(x_0) = \mathrm{Ord}_5(5) + 2\,\mathrm{Ord}_5(y_0) = 1 + 2\mathrm{Ord}_5(y_0)$$

The left hand side is an even integer, the right hand side is an odd integer. Contradiction. □

Theorem 21. *The equation $x^3 = 2y^3$ has no positive integer solutions. In other words, $2^{1/3}$ is irrational.*

Proof. Suppose otherwise, that $x^3 = 2y^3$ has solution x_0, y_0. So $x_0^3 = 2y_0^3$. Thus

$$\mathrm{Ord}_2(x_0^3) = \mathrm{Ord}_2(2y_0^3).$$

This implies that

$$3\,\mathrm{Ord}_2(x_0) = \mathrm{Ord}_2(2) + 3\ \mathrm{Ord}_2(y_0) = 1 + 3\,\mathrm{Ord}_2(y_0)$$

The left hand side is divisible by three, but the right hand side is not. Contradiction. □

Theorem 22. *Suppose n is a positive integer and that n is not of the form m^k with $m \in \mathbb{Z}$. Then $ny^k = x^k$ has no positive integer solutions. In other words, $n^{1/k}$ is irrational unless n is a kth power.*

Proof. Suppose otherwise, that $ny^k = x^k$ has solution x_0, y_0. Let p be a prime. Then

$$\mathrm{Ord}_p(ny_0^k) = \mathrm{Ord}_p(x_0^k).$$

Thus

$$\mathrm{Ord}_p(n) + k\,\mathrm{Ord}_p(y_0) = k\,\mathrm{Ord}_p(x_0).$$

This implies that

$$\mathrm{Ord}_p(n) \equiv 0 \mod k$$

By the following lemma, this implies that n is a kth power, contradicting the hypothesis. □

Lemma 23. *Let n be a positive integer. Then n is a kth power if and only if $k \mid \mathrm{Ord}_p(n)$ for all primes p.*

Proof. If $n = m^k$ then $\mathrm{Ord}_p(n) = k\,\mathrm{Ord}_k(m)$ (Proposition 6). Thus $k \mid \mathrm{Ord}_p(n)$ for all p.

Conversely, suppose $k \mid \mathrm{Ord}_p(n)$ for all primes p. Let $p_1, \ldots, p_q$ be a finite sequence of distinct primes that include all primes dividing n. Then $\mathrm{Ord}_{p_i}(n) = ka_i$ for some non-negative integer a_i (since $k \mid \mathrm{Ord}_{p_i}(n)$). By the product formula,

$$n = \prod_{i=1}^{q} p_i^{ka_i} = \prod_{i=1}^{q} \left(p_i^{a_i}\right)^k = \left(\prod_{i=1}^{q} p_i^{a_i}\right)^k.$$

Thus n is a kth power. □

Now we will see why $\log_{10}(2)$ is irrational. Of course, this generalizes to other logarithms as well. To do so, we convert the problem into a diophantine equation.

If $\log_{10}(2) = x_0/y_0$ for integers x_0, y_0 with $y_0 \neq 0$, then by definition of logarithms

$$10^{x_0/y_0} = 2.$$

In other words, $10^{x_0} = 2^{y_0}$. This implies that $10^x = 2^y$ has a solution with $y \neq 0$. Conversely, if such a solution exists, then $\log_{10}(2)$ is rational. We show this cannot happen.

Theorem 24. *The equation $10^x = 2^y$ has no solution with $x, y \in \mathbb{Z}$ and $y \neq 0$. In other words, $\log_{10}(2)$ is irrational.*

Proof. Suppose that $10^{x_0} = 2^{y_0}$ where $y_0 \neq 0$. Apply Ord_5 to both sides:

$$x_0\,\mathrm{Ord}_5(10) = y_0\,\mathrm{Ord}_5(2)$$

But $\mathrm{Ord}_5(10) = 1$ and $\mathrm{Ord}_5(2) = 0$. Thus $x_0 = 0$. This implies that $10^0 = 2^y$. So $2^y = 1$. Apply Ord_2 to both sides. This implies that $y\mathrm{Ord}_2(2) = \mathrm{Ord}_2(1)$. But $\mathrm{Ord}_2(2) = 1$ and $\mathrm{Ord}_2(1) = 0$. Thus $y_0 = 0$, a contradiction. □

5. Zeros of $n!$

How many zeros are at the end of $n!$? For example,

$$15! = 1307674368000$$

has three zeros at the end of its decimal expansion, and

$$50! = 30414093201713378043612608166064768844377641568960512000000000000$$

has 12 zeros.

The number of zeros at the end of a number's decimal expansion is just the largest power of ten dividing that number.

Lemma 25. *The largest power of 10 dividing n is $\min\big(\mathrm{Ord}_2(n), \mathrm{Ord}_5(n)\big)$.*

Exercise 4. Prove the above.

To use the above formula it helps to have a formula for $\mathrm{Ord}_p(n!)$.

Lemma 26. *If p is a prime, and n is a positive integer, then*

$$\mathrm{Ord}_p(n!) = \sum_{k=1}^{n} \mathrm{Ord}_p(k).$$

Proof. Use the formula $n! = \prod_{k=1}^{n} k$, and apply Proposition 5. □

Exercise 5. How many zeros does 56! have? How many zeros does 231! have? Hint: $\mathrm{Ord}_2(n!) \geq \mathrm{Ord}_5(n!)$ so it is enough to compute Ord_5.

6. Exercises

Here are some exercises that can be solved with the order functions Ord_p. (They can also be solved with the unique factorization theorem, but the solutions using the order functions should be a bit easier).

Exercise 6. Show that if $a^k \mid b^k$ then $a \mid b$.

Exercise 7. Show that if $3a^3b \mid c^2$ then $a \mid c$.

Exercise 8. Show that if $a^5c \mid b^4$ then $a \mid b$.

Exercise 9. Show that if ab is a square, and if a and b are relatively prime, then a and b are squares. Give a counter example when a and b are not relatively prime.

Exercise 10. Show that if $p \mid a^k$ where p is a prime, then $p \mid a$.

Exercise 11. Show that $5^{2/3}$ is irrational.