Math 104A, Number Theory, Fall 2002.
Summary of Lecture 8.

Lemma 2.3.1. *If integers* $p_1^{a_1} \dots p_k^{a_k} | p_1^{b_1} \dots p_k^{b_k}$ *then* $a_j \le b_j$ *for each* j.

Example 2.3.6 If $a^2|b^2$ then $a|b$.

For a positive integer n, the number of positive divisors (including 1 and n) is denoted by $\nu(n)$.

Proposition 2.3.2 If n has prime decomposition $p_1^{a_1} \cdots p_k^{a_k}$, then $\nu(n) = (a_1 + 1) \cdots (a_k + 1)$.

Example. Determine the numbers with $\nu(n) = 18$. We solve this be determining a_1, a_2, a_3 with $(a_1+1)(a_2+1)(a_3+1) = 18$.

18	p_1^{17}
$2 \cdot 9$	$p_1 p_2^8$
$3 \cdot 6$	$p_1^2 p_2^5$
$2 \cdot 3 \cdot 3$	$p_1 p_2^2 p_3^2$

Example. Show that if a and b are integers, not both zero, the common divisors of a and b are the divisors of (a, b).

We go back to consider (a, b) again.

Example. $(a/(a,b), b/(a,b)) = 1$. (You can prove this in two ways now.)

Example. If $x|yz$ and $(x, y) = 1$, then $x|z$.

Recall we had the result:

Theorem. *If* a, b *are not both zero there exist* x, y *with*

$$(a, b) = xa + yb.$$

Now we will see what all the solutions are.

Theorem 2.6.1. *(Brahmagupta) The equation* $ax + by = m$ *has a solution if and only if* $(a, b)|m$. *In this case, if* (x_0, y_0) *is a solution, then*

$$m = \left(x_0 + \frac{b}{(a,b)}k\right) a + \left(y_0 - \frac{a}{(a,b)}k\right) b, \qquad k \in \mathbb{Z},$$

and this gives all solutions.

Example. Compute all the solutions of $8x + 3y = 1$.

$(3, 8) = 1$ and $8 \cdot (-1) + 3 \cdot 3 = 1$. We have

$$8(-1 + 3k) + 3(3 - 8k) = 1,$$

and as k ranges over the integers, this gives all the solutions.