Theorem: For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b.

What does this tell us??

Theorem: For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b.

Outline of Proof:

1. Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

2. The Well-Ordering Principle tells us S has a smallest element.
   Let $d =$ the smallest element of S. Since $d \in S$, there exist integers M and N such that $d = aM + bN$.

   > (All we're doing here is naming the smallest possible linear combination of a and b)

   Show $d|a$, $d|b$, so d is a common divisor of a and b.

3. Show $d = gcd(a, b)$, that is, d is the largest of all the common divisors.

1. For $n = 8, 27$, find all positive integers less than n and relatively prime to n.

2. If $a = 2^4 \cdot 3^2 \cdot 5 \cdot 7^2$ and $b = 2 \cdot 3^3 \cdot 7 \cdot 11$, determine $gcd(a, b)$ and $lcm(a, b)$.

3. Determine 51 mod 13.

4. $gcd(12, 35) = 1$, of course. Find integers s and t so that $1 = 12s + 35t$. Are s and t unique?

   Remember to use the Euclidean Algorithm: use division repeatedly (you may need to look in your books)

5. Let $S = \mathbb{R}$ and define $a \sim b \Longleftrightarrow a^2 = b^2$.

   (a) Show $\sim$ is an equivalence relation.

   (b) What are the equivalence classes?

September 3, 2004