Theorems

1. Division algorithm: Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there are unique integers $q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < d$. We call r the *remainder*.

2. Bézout's identity: Let $a, b \in \mathbb{Z}^+$. Then there are (not necessarily unique!) integers $s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$.

3. Euclidean algorithm: Let $a, b \in \mathbb{Z}^+$. The Euclidean algorithm computes the gcd of a and b by repeatedly applying the division algorithm and the following theorem:

4. Let $a, b, q, r \in \mathbb{Z}^+$ and suppose $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

5. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then a and b are inverses mod m iff $ab \equiv 1 \mod m$. (Compare this to the usual situation with numbers, where we say two numbers x, y are inverses if $xy = 1$.) The Euclidean algorithm gives a concrete way to compute the inverse (if it exists) of a given number mod m.

Exercises

1. Use the Euclidean algorithm to compute $\gcd(34, 55)$.

2. Use your work in the previous problem to find a, b such that $34a + 55b = \gcd(a, b)$.

3. Does 34 have an inverse mod 55? Does 55 have an inverse mod 34? If so, compute them using your work from the previous problem.

4. Use the Euclidean algorithm to find that $\gcd(10, 11) = 1$.

5. Use your work in the previous problem to find a, b such that $10a + 11b = 1$.

6. Find another pair a', b' such that $10a' + 11b' = 1$.

7. Since $\gcd(10, 11) = 1$, then 10 has an inverse mod 11 and 11 has an inverse mod 10. Use part 5 to find inverses for 10 and 11.

8. Now use part 6 to find another set of inverses for 10 and 11. Check that the inverses you found for 10 are equivalent mod 11, and that the inverses you found for 11 are equivalent mod 10.