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 $\gcd(34, 55)$.

$$\begin{aligned} 55 &= 34 \cdot 1 + 21 \\ 34 &= 21 \cdot 1 + 13 \\ 21 &= 13 \cdot 1 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

We have found remainder 0, so we are done running the algorithm, and $\gcd(34, 55) = 1$.

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

$$\begin{array}{lll} 55 = 34 \cdot 1 + 21 \rightarrow & 21 = 55 - 34 \rightarrow & 1 = 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\ 34 = 21 \cdot 1 + 13 \rightarrow & 13 = 34 - 21 \rightarrow & 1 = 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\ 21 = 13 \cdot 1 + 8 \rightarrow & 8 = 21 - 13 \rightarrow & 1 = 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ 13 = 8 \cdot 1 + 5 \rightarrow & 5 = 13 - 8 \rightarrow & 1 = 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\ 8 = 5 \cdot 1 + 3 \rightarrow & 3 = 8 - 5 \rightarrow & 1 = 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ 5 = 3 \cdot 1 + 2 \rightarrow & 2 = 5 - 3 \rightarrow & 1 = 3 - (5 - 3) = 2 \cdot 3 - 5 \\ 3 = 2 \cdot 1 + 1 \rightarrow & 1 = 3 - 2 \rightarrow & 1 = 3 - 2 \\ 2 = 1 \cdot 2 + 0 & & \end{array}$$

So our answer is $1 = 34(-21) + 55(13)$.

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.

   Since 34 and 55 are relatively prime (their gcd is 1), then 34 has an inverse mod 55 and 55 has an inverse mod 34. Take the equation $1 = 34(-21) + 55(13)$ mod 34 and mod 55 to get:

$$\begin{aligned} 1 \equiv 34(-21) + 55(13) \equiv 34(-21) \equiv 34(34) &\quad \text{mod } 55 \\ 1 \equiv 34(-21) + 55(13) \equiv 55(13) &\quad \text{mod } 34 \end{aligned}$$

   so 34 and -21 are inverses mod 55 and 55 and 13 are inverse mod 34.

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

$$\begin{aligned} 11 &= 10 \cdot 1 - 1 \\ 10 &= 1 \cdot 10 - 0 \end{aligned}$$

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

   Directly: $1 = 10(-1) + 11(1)$.

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

   Try guess and check. Find: $1 = 10(-12) + 11(11)$.

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.

$$\begin{aligned} 1 \equiv 10(-1) + 11(1) \equiv 10(-1) \equiv 10(10) &\quad \text{mod } 11 \\ 1 \equiv 10(-1) + 11(1) \equiv 11(1) &\quad \text{mod } 10 \end{aligned}$$

   so 10 and -1 are inverses mod 11 and 11 and 1 are inverses mod 10.

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.

$$\begin{aligned} 1 \equiv 10(-12) + 11(11) \equiv 10(-12) &\quad \text{mod } 11 \\ 1 \equiv 10(-12) + 11(11) \equiv 11(11) &\quad \text{mod } 10 \end{aligned}$$

   so 10 and -12 are inverses mod 11 and 11 and 11 are inverses mod 10.

   Note that $-12 \equiv -1 \mod 11$ and $11 \equiv 1 \mod 10$, so these “different” inverses we found are essentially the same.