Modular Multiplicative Inverses

This Theorem is in the current version of **Applied Discrete Structures**, but not attributed to Bézout.

Étienne Bézout, 1730–1783

Theorem 11.4.9 Bézout's lemma. *If a and b are positive integers, the smallest positive value of $ax + by$ is the greatest common divisor of a and b,* $\gcd(a, b)$.

□

Computing Modular Multiplicative Inverses. Unlike the nice neat formula for additive inverses mod n, multiplicative inverses can most easily computed by applying Bézout's lemma. If a is an element of the group $\mathbb{U}_n$, then by definition $\gcd(n, a) = 1$, and so there exist integers s and t such that $1 = ns + at$. They can be computed with the Extended Euclidean Algorithm.

$$1 = ns + at \Rightarrow at = 1 + (-s)n \Rightarrow a \times_n t = 1$$

Since t might not be in $\mathbb{U}_n$ you might need take the remainder after dividing it by n. Normally, that involves simply adding n to t.

For example, in $\mathbb{U}_{2048}$, if we want the muliplicative inverse of 1001, we run the Extended Euclidean Algorithm and find that

$$gcd(2048, 1001) = 1 = 457 \cdot 2028 + (-935) \cdot 1001$$

Thus, the multiplicative inverse of 1001 is 2048-935 $= 1113$. See the SageMath Note below to see how to run the Extended Euclidean Algorithm .

Extended Euclidean Algorithm with Mathematica

```
ExtendedGCD[2048, 1001]
```

{1, {457, –935}}

... and with SageMath:

```
xgcd(2048,1001)
```

Evaluate

```
(1, 457, -935)
```

These exercises are being added in the next version of **Applied Discrete Structures**.

13. Given that $1 = 2021 \cdot (-169) + 450 \cdot 759$, explain why 450 is an element of the group $\mathbb{U}_{2021}$ and determine its inverse in that group.

14. Let $n = 2021$. Solve $450 \times_n x = 321$ for x in the group $\mathbb{U}_n$

15. Let p be an odd prime. Find all solutions to the equation $x^2 = x \times_n x = 1$ in the group $\mathbb{U}_p$.