CSC3631 Cryptography
- Number Theory & Algebra
Computing a Multiplicative Inverse

Thomas Gross

Ingredients to Compute the Multiplicative Inverse

1. Definition of congruence under a modulus.
2. Multiplicative modular inverse as congruence.
3. Relation to Bézout's Identity
4. Computing the parameters of Bézout's Identity with the Extended Euclidian Algorithm (EEA)

Mod Arithmetic in $\mathbf{Z}_N$ as Expected

- **We say: *a* is congruent to *b* modulo *N***
  $a = b \pmod N \quad \Leftrightarrow \quad N \mid (a-b) \quad \Leftrightarrow \quad a = b + kN$
- **Closed**:
  under modular addition & multiplication (+, ·).
- **$\mathbf{Z}_N$ is well-behaved:**
  Commutative, **associative**, **distributive**, e.g.,
  $(a + b)\cdot c \pmod N = a\cdot c + b\cdot c \pmod N$
- **Neutral elements:**
  - Addition: **0** | $a + 0 \pmod N = a \pmod N$
  - Multiplication: **1** | $a \cdot 1 \pmod N = a \pmod N$
- **Convention:** elements of $\mathbf{Z}_N$ always **positive**.

[See Shoup, Chapter 1-2, for advanced details on congruences in $\mathbf{Z}_N$]

Multiplicative Modular Inverse

Modular Inverse: y is called multiplicative inverse of x modulo N if

$$x \cdot y = 1 \pmod{N}$$

Consider what this congruence means:

- $x \cdot y = 1 \pmod{N}$ ⇔
- $x \cdot y = 1 + kN$ (over the integers) ⇔
- $1 = x \cdot y + (-k)N$ (over the integers)

Bézout's Identity

Bézout's identity: For all non-zero a, b in **Z**, there exist s, t in **Z**, such that

$$\mathbf{gcd}(a, b) = s \cdot a + t \cdot b$$

Note: the same structure as the congruence for the multiplicative inverse (reordered):

$$1 = y \cdot x + (-k)N$$

Existence of Modular Inverses

Bézout's Identity thereby gives rise to the rule, when the multiplicative inverse of x modulo N exists:

x has a multiplicative inverse modulo *N*

if and only if

$$\mathbf{gcd}(x, N) = 1 = y \cdot x + (-k)N$$

(if x and N are coprime)

How to Compute the Multiplicative Inverse

- **Key Equation: gcd**$(x, N) = 1 = y \cdot x + (-k)N$
- $x \cdot y = 1 \pmod{N} \Leftrightarrow 1 = x \cdot y + (-k)N$
- To find the multiplicative inverse y of x modulo N, we establish Bézout's Identity.
- **Remember:** to find the parameters of Bézout's Identity y and $(-k)$, we can compute the **Extended Euclidian Algorithm (EEA).**
- **To compute the inverse, compute: EEA**(x, N)

Find the Inverse of 19 Modulo 1013

- First, we notice that the inverse must exist because x=19 and N=1013 are coprime
- **gcd**(x, N) = **gcd**(19, 1013) = 1
- **Bézout's Identity**: 1 = y·19 + t·1013
- Compute **EEA**(19, 1013) to gain inverse y, t.
  - y = 160
  - t = -3
- y=160 is the inverse of x=19, under N=1013.

How to compute **EEA**(19, 1013)?

GCD Recursion	Division w/ Remainder	EEA Equation
gcd(1013, 19)	1013/19 = 53 remainder 6	6 = 1013 + (-53)·19
gcd(19, 6)	19/6 = 3 remainder 1	1 = 19 + (-3)·6
gcd(6, 1)	6/1 = 6 remainder 0	

- 1 = 19 + (-3)·6
- 1 = 19 + (-3)·(1013 + (-53)·19) | Substitute 6 = 1013 + (-53)·19
- 1 = 19 + (-3)·1013 + 159·19 | Distributivity
- 1 = 160·19 + (-3)·1013 | Collect terms