Intro to Rings, Fields, and GCDs: Hardware Modeling by Modulo Arithmetic

Priyank Kalla

Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

January 14, 2022

Agenda for Today

- Wish to build a number-theoretic and algebraic model for hardware and crypto
- Modulo arithmetic model is versatile: can represent both *bit-level* and *word-level* constraints
- To build the algebraic/modulo arithmetic model:
  - Rings, Fields, Modulo arithmetic
  - Multiplicative Inverses and the GCD
  - Finite fields $\mathbb{F}_p$, $\mathbb{F}_{p^k}$ and $\mathbb{F}_{2^k}$
  - Linear Congruences
  - Basics of symmetric key ciphers: affine ciphers
- Later on, we will study
  - Polynomials, Polynomial functions, Polynomial Rings over $\mathbb{F}_{2^k}$
  - For use is modern Block-ciphers

Motivation for Algebraic Computation

- Modeling basic affine Crypto algorithms in $\mathbb{Z}_p$, works well in software
- For hardware: Modeling for bit-precise algebraic computation
  - Arithmetic RTLs: functions over *k*-bit-vectors
  - k-bit-vector $\mapsto$ integers $\pmod{2^k} = \mathbb{Z}_{2^k}$
  - k-bit-vector $\mapsto$ Galois (Finite) field $\mathbb{F}_{2^k}$
- For many of these applications Boolean models fail miserably!
- Number theory, Computer Algebra and Algebraic Geometry + SAT/SMT
  - Model: Circuits as polynomial functions $f : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_{2^k}$, $f : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$

All we need is an algebraic object where we can ADD, MULTIPLY, DIVIDE.
These objects are Rings and Fields.

Groups, $(G, 0, +)$

An **Abelian group** is a set G and a binary operation "$+$" satisfying:

- *Closure:* For every $a, b \in G, a + b \in G$.
- *Associativity:* For every $a, b, c \in G, a + (b + c) = (a + b) + c$.
- *Commutativity:* For every $a, b \in G, a + b = b + a$.
- *Identity:* There is an identity element $0 \in G$ such that for all $a \in G; a + 0 = a$.
- *Inverse:* If $a \in G$, then there is an element $a^{-1} \in G$ such that $a + a^{-1} = 0$.

Example: The set of Integers $\mathbb{Z}$ or $\mathbb{Z}_n$ with $+$ operation.

Rings $(R, 0, 1, +, \cdot)$

A **Commutative ring with unity** is a set R and two binary operations $"+"$ and $"\cdot"$, as well as two distinguished elements $0, 1 \in R$ such that, R is an Abelian group with respect to addition with additive identity element 0, and the following properties are satisfied:

- *Multiplicative Closure:* For every $a, b \in \mathrm{R}$, $a \cdot b \in \mathrm{R}$.
- *Multiplicative Associativity:* For every $a, b, c \in \mathrm{R}$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Multiplicative Commutativity:* For every $a, b \in \mathrm{R}$, $a \cdot b = b \cdot a$.
- *Multiplicative Identity:* There is an identity element $1 \in \mathrm{R}$ such that for all $a \in \mathrm{R}$, $a \cdot 1 = a$.
- *Distributivity:* For every $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ holds for all $a, b, c \in R$.

Example: The set of Integers $\mathbb{Z}$ or $\mathbb{Z}_n$ with $+, \cdot$ operations.

Rings

- Examples of rings: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}$
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ where $+, \cdot$ computed $+, \cdot \pmod{n}$
- Modulo arithmetic:
  - $(a + b) \pmod{n} = (a \pmod{n} + b \pmod{n}) \pmod{n}$
  - $(a \cdot b) \pmod{n} = (a \pmod{n} \cdot b \pmod{n}) \pmod{n}$
  - $-a \pmod{n} = (n - a) \pmod{n}$
- Arithmetic k-bit vectors $\mapsto$ arithmetic over $\mathbb{Z}_{2^k}$
- For $k = 1$, $\mathbb{Z}_2 \equiv \mathbb{B}$

Rings

- Examples of rings: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}$
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ where $+, \cdot$ computed $+, \cdot \pmod{n}$
- Modulo arithmetic:
  - $(a + b) \pmod{n} = (a \pmod{n} + b \pmod{n}) \pmod{n}$
  - $(a \cdot b) \pmod{n} = (a \pmod{n} \cdot b \pmod{n}) \pmod{n}$
  - $-a \pmod{n} = (n - a) \pmod{n}$
- Arithmetic k-bit vectors $\mapsto$ arithmetic over $\mathbb{Z}_{2^k}$
- For $k = 1$, $\mathbb{Z}_2 \equiv \mathbb{B}$

But, what about division?

- Over $\mathbb{Q}$, can you divide $\frac{2}{3}$ by $\frac{4}{5}$?
- Over $\mathbb{C}$, can you divide $\frac{a+ib}{c+id}$?
- Over $\mathbb{Z}$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 8$, can you divide $\frac{3}{4}$?
- Over $\mathbb{Z} \pmod 7$, can you divide $\frac{3}{4}$?

Division is multiplication by a (multiplicative) inverse!

Division

For an element a in a ring R, $\frac{a}{b} = a \times b^{-1}$. Here, $b^{-1} \in R$ s.t. $b \cdot b^{-1} = 1$.

Multiplicative Inverses

- Over $\mathbb{Q}$: if $b = \frac{2}{3}$, $b^{-1} = \frac{3}{2}$?
- Over $\mathbb{Z}$: if $b = 4$, $b^{-1} =$?
- Over rings: inverses may not exist
- Over $\mathbb{Z}_8$: if $b = 3, b^{-1} =$?
- Over $\mathbb{Z}_8$: if $b = 6, b^{-1} =$?
- Over $\mathbb{Z}_7$: if $b = 6, b^{-1} =$?

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

Fields

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

$\mathbb{Z}_n, n \neq p$ is a ring but not a field. So, $\mathbb{Z}_{2^k}$ is not a field, as even numbers in $\mathbb{Z}_{2^k}$ have no inverses.

Field $(\mathbb{F}, 0, 1, +, \cdot)$

A **field** $\mathbb{F}$ is a commutative ring with unity, where every element in $\mathbb{F}$, except 0, has a multiplicative inverse:
$\forall a \in (\mathbb{F} - \{0\}), \quad \exists \hat{a} \in \mathbb{F}$ such that $a \cdot \hat{a} = 1$.

A field is called a **finite field** or **Galois field** when $\mathbb{F}$ has a finite number of elements.

The set $\mathbb{Z}_p = \mathbb{Z} \pmod{p} = \{0, 1, \ldots, p-1\}$ is a finite field, when p is a prime integer.

$\mathbb{Z}_n, n \neq p$ is a ring but not a field. So, $\mathbb{Z}_{2^k}$ is not a field, as even numbers in $\mathbb{Z}_{2^k}$ have no inverses.
$\mathbb{Z}_2 \equiv \mathbb{F}_2 \equiv \mathbb{B} \equiv \{0, 1\}$

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B} \to \mathbb{F}_2$:

$$\begin{aligned} \neg a &\to a + 1 \pmod 2 \\ a \vee b &\to a + b + a \cdot b \pmod 2 \\ a \wedge b &\to a \cdot b \pmod 2 \\ a \oplus b &\to a + b \pmod 2 \end{aligned} \tag{1}$$

where $a, b \in \mathbb{F}_2 = \{0, 1\}$.

- Boolean AND-OR-NOT can be mapped to $+, \cdot \pmod 2$

$\mathbb{B} \to \mathbb{F}_2$:

$$\begin{aligned} \neg a &\to a + 1 \pmod 2 \\ a \vee b &\to a + b + a \cdot b \pmod 2 \\ a \wedge b &\to a \cdot b \pmod 2 \\ a \oplus b &\to a + b \pmod 2 \end{aligned} \tag{1}$$

where $a, b \in \mathbb{F}_2 = \{0, 1\}$.

In $\mathbb{Z}_2 \equiv \mathbb{F}_2, -1 = +1 \pmod 2$

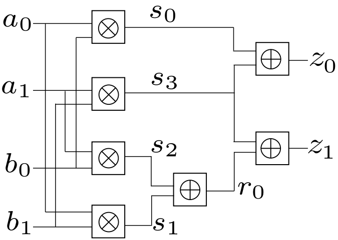


Figure: $\otimes$ = AND, $\oplus$ = XOR.

$$f_1 : s_0 + a_0 \cdot b_0; \quad f_2 : s_1 + a_0 \cdot b_1,$$
$$f_3 : s_2 + a_1 \cdot b_0; \quad f_4 : s_3 + a_1 \cdot b_1,$$
$$f_5 : r_0 + s_1 + s_2; \quad f_6 : z_0 + s_0 + s_3,$$

$$f_7 : z_1 + r_0 + s_3$$

- $\mathbb{Z}_p$: field of p elements, p $= 2, 3, 5, 7, \ldots, 163, \ldots$
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)
- Fields are unique factorization domains (UFDs)

Finite Fields

- $\mathbb{Z}_p$: field of p elements, p = 2, 3, 5, 7, ..., 163, ...
- Is there a field of 4 elements $\mathbb{F}_4$?
- Yes, we can have fields of p^k elements $\mathbb{F}_{p^k}$
- These are called extension fields, we will study them later
- In fact, we are interested in $\mathbb{F}_{2^k}$ (k-bit vector arithmetic)
- Fields are unique factorization domains (UFDs)

Fermat's Little Theorem

$$\forall x \in \mathbb{F}_p, \; x^p - x = 0 \pmod{p}$$

Zero Divisors

Zero Divisors (ZD)

For $a, b \in R, a, b \neq 0, a \cdot b = 0$. Then a, b are zero divisors of each other. $\mathbb{Z}_n, n \neq p$ has zero divisors. What about $\mathbb{Z}_p$?

Integral Domains

Any set (ring) with no zero divisors: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p, \mathbb{F}_{2^k}$. What about $\mathbb{Z}_{2^k}$?

Relationships

Commutative Rings $\supset$ Integral Domains (no ZD) $\supset$ Unique Factorization Domains $\supset$ Fields

For Hardware: Our interests – non-UFD Rings ($\mathbb{Z}_{2^k}$) and Fields $\mathbb{F}_{2^k}$.
For Software: $\mathbb{F}_p \equiv Z_p$ also works.

Ambiguities in non-UFDs UFDs

- In 3-bit arithmetic $\mathbb{Z}_8$: $(x^2 + 6x) \pmod 8$
- Factorize according to its roots: $x(x + 6)$
- What about $(x + 2)(x + 4)$?
- Degree 2 polynomial has more roots than the degree? Roots $x = 0, 2, 4, 6$?
- $\mathbb{Z}_8 =$ non-UFD
- Cannot use factorization to prove equivalence over non-UFDs.

Consolidating the results so far...

- Over fields $\mathbb{Z}_p, \mathbb{F}_{2^k}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$
  - We can ADD, MULTIPLY, DIVIDE
  - No zero-divisors, can uniquely factorize a polynomial according to its roots
- Rings $\mathbb{Z}$: integral domains, unique factorization, but no inverses
- Over Rings $\mathbb{Z}_n, n \neq p$; e.g. $n = 2^k$
  - Presence of zero divisors
  - non-UFDs, polynomial can have more zeros than its degree
  - Cannot perform division

Let's focus on $\mathbb{Z}_n, \mathbb{Z}_p$: $p =$ prime integer, $n =$ any integer

Computation of Multiplicative Inverses in $\mathbb{Z}_n$

The integer $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $GCD(a, n) = 1$.

We compute GCDs using the Euclid's algorithm.

Definition

A Euclidean domain $\mathbb{D}$ is an integral domain where:

1. associated with each non-zero element $a \in \mathbb{D}$ is a non-negative integer $f(a)$ s.t. $f(a) \leq f(ab)$ if $b \neq 0$; and
2. $\forall a, b \ (b \neq 0), \exists (q, r)$ s.t. $a = qb + r$, where either $r = 0$ or $f(r) < f(b)$.

- Can apply the Euclid's algorithm to compute $g = GCD(g_1, \ldots, g_t)$
- $GCD(a, b, c) = GCD(GCD(a, b), c)$
- Then $g = \sum_i u_i g_i$, i.e. GCD can be represented as a linear combination of the elements

Euclid's Algorithm

Algorithm 1 Euclid's Algorithm

Inputs: Elements $a, b \in \mathbb{D}$, a Euclidean domain
Outputs: $g = GCD(a, b)$

```
Assume a > b, otherwise swap a, b  {/* GCD(a, 0) = a */}
while  b ≠ 0  do
    t := b
    b := a (mod b)
    a := t
end while
return  g := a
```

GCD(84, 54) = 6

$$\begin{aligned} 84 &= 1 \cdot 54 + 30 \\ 54 &= 1 \cdot 30 + 24 \\ 30 &= 1 \cdot 24 + \underline{6} \\ 24 &= 4 \cdot \underline{6} + 0 \end{aligned}$$

$$\begin{aligned} 6 &= 30 - 1 \cdot 24 \\ &= 30 - 1(54 - 30) \\ &= 2 \cdot 30 - 1 \cdot 54 \\ &= 2 \cdot 84 - 3 \cdot 54 \end{aligned}$$

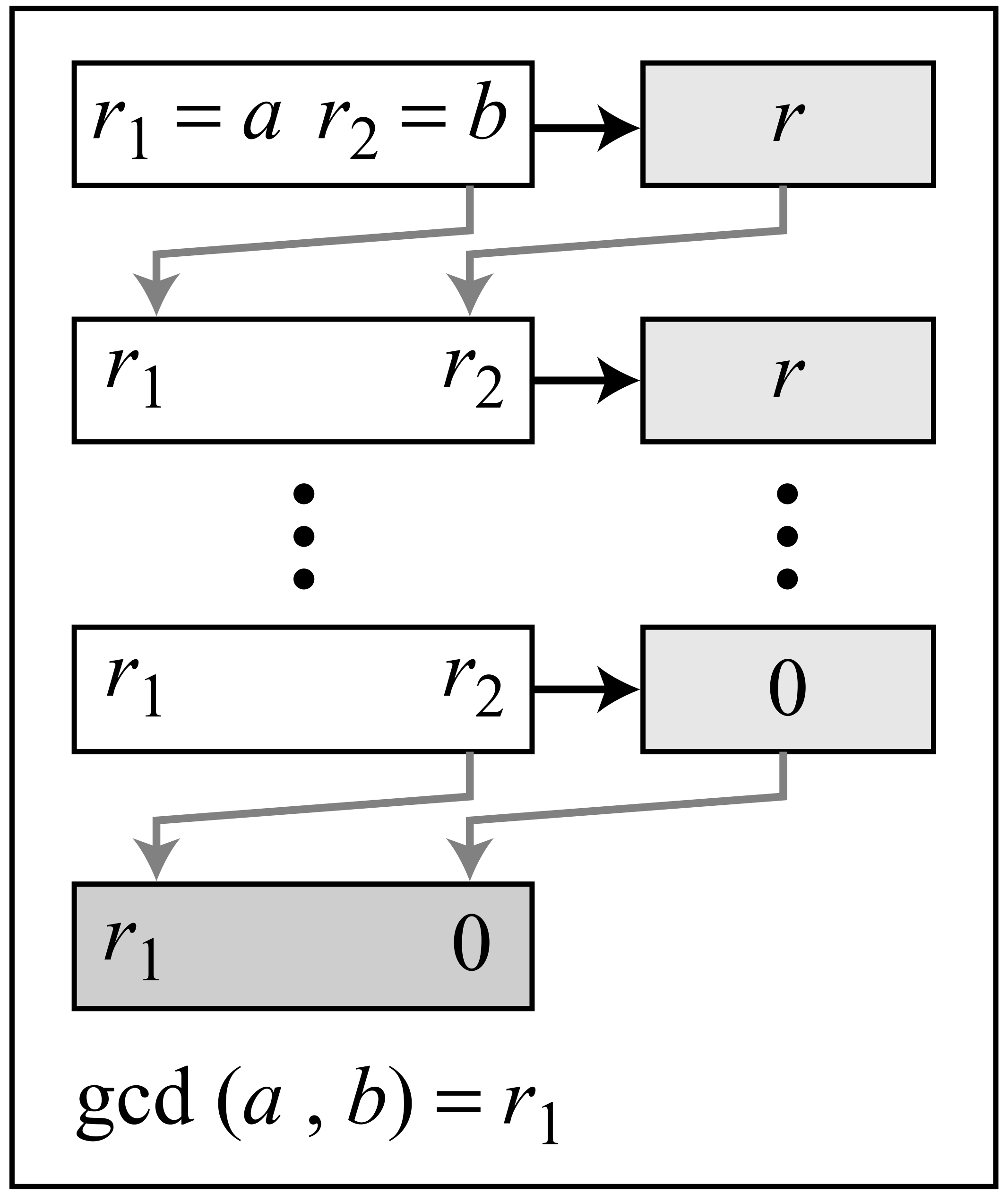
Lemma

If $g = gcd(a, b)$ *then* $\exists s, t$ *such that* $s \cdot a + t \cdot b = g$.

Unroll Euclid's algorithm to find s, t. A HW assignment!

GCD, Inverses and Euclid's Algorithm

Euclid’s Algorithm View



a. Process

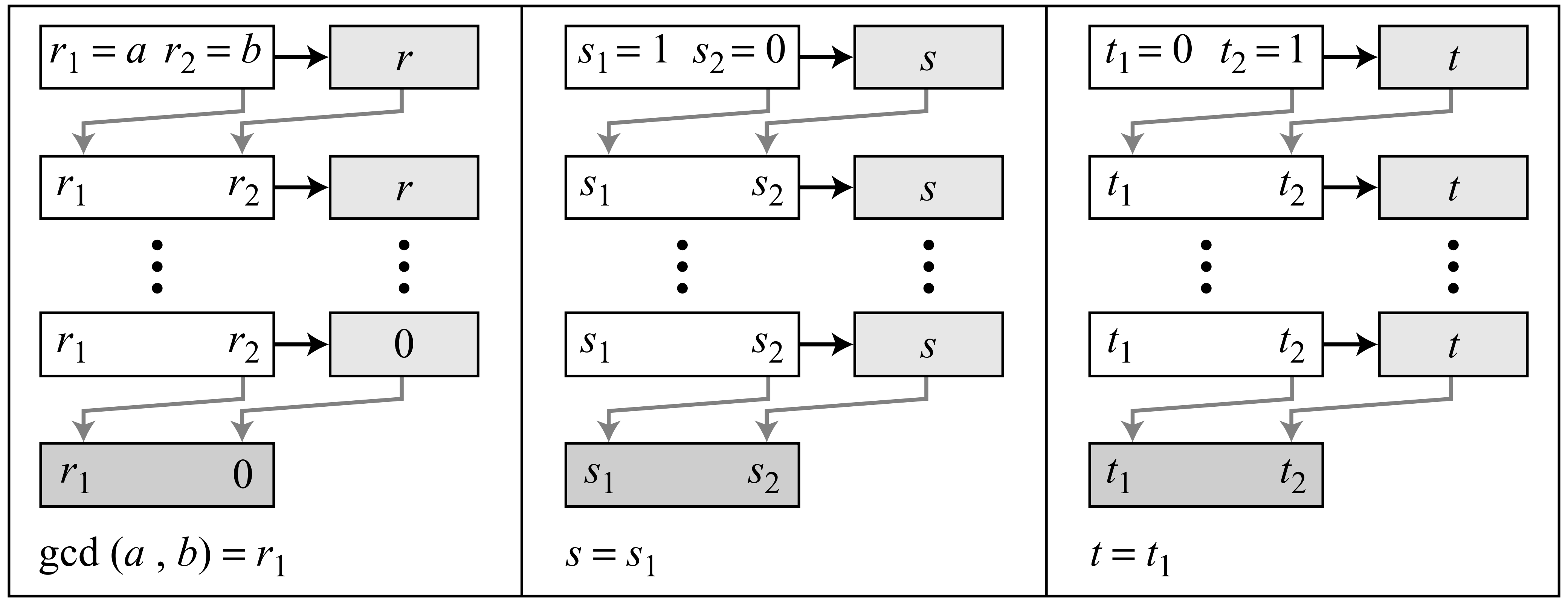
```
 r₁ ← a; r₂ ← b;    (Initialization)
while (r₂ > 0)
  {
   q ← r₁ / r₂;
   r ← r₁ − q × r₂;
   r₁ ← r₂; r₂ ← r;
  }

   gcd (a, b) ← r₁
```

b. Algorithm

Extended Euclidean algorithm

$$d = gcd(a, b) = s \times a + t \times b$$



a. Process

```
r1 ← a; r2 ← b;
s1 ← 1; s2 ← 0;        (Initialization)
t1 ← 0; t2 ← 1;
while (r2 > 0)
{
  q ← r1 / r2;
   r  ← r1 − q × r2;
   r1 ← r2;  r2 ← r;      (Updating r's)
   s  ← s1 − q × s2;
   s1 ← s2;  s2 ← s;      (Updating s's)
   t  ← t1 − q × t2;
   t1 ← t2;  t2 ← t;      (Updating t's)
}
 gcd (a , b) ← r1;   s ← s1;   t ← t1
```

b. Algorithm

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$. The answers can be tested because we have

$$(-1) \times 161 + 6 \times 28 = 7$$

Linear Diophantine Equations

$ax + by = c$, where $a, b, c \in \mathbb{Z}$. Find x, y that satisfy the equation

- $d = gcd(a, b)$. If d does not divide c, then there are no solutions
- If $d \mid c$, then the equation has infinite solutions
  - Reduce equation to $a_1x + b_1y = c_1$, by dividing both sides by d
  - Solve for $s, t : a_1s + b_1t = 1$
  - Particular solution: $x_0 = (c/d)s, y_0 = (c/d)t$
  - General solutions: $x = x_0 + k(b/d); \quad y = y_0 - k(a/d), \quad \forall k \in \mathbb{Z}$

Solving Linear Congruences

Solve equations of the form $ax \equiv b \pmod{n}$

- $d = gcd(a, n)$
- If $d \nmid b$: No solution
- If $d \mid b$: there are d solutions
- Reduce the equation by dividing both sides, including the modulus, by d
- Multiply both sides of the reduced equation by the multiplicative inverse of a to find particular solution x_0
- General Solutions: $x = x_0 + k(n/d), k = 0, \dots, d-1$

Please Review Matrices

- Please review addition, multiplication and determinants $det(\boldsymbol{A})$ of matrices on your own
- Multiplicative Inverse of a matrix: defined only for square matrix
- Inverses: $\boldsymbol{A} \times \boldsymbol{B} = \boldsymbol{B} \times \boldsymbol{A} = \boldsymbol{I}$
- Multiplicative inverse of $\boldsymbol{A}$ exists, only if $det(\boldsymbol{A})$ has an inverse in the ring.
- Integers (infinite set $\mathbb{Z}$) have no inverses, no integer matrices have no inverses
- In Crypto: we use matrices over $\mathbb{Z}_n$ – called residue matrices