Extended Euclid Algorithm & its Applications

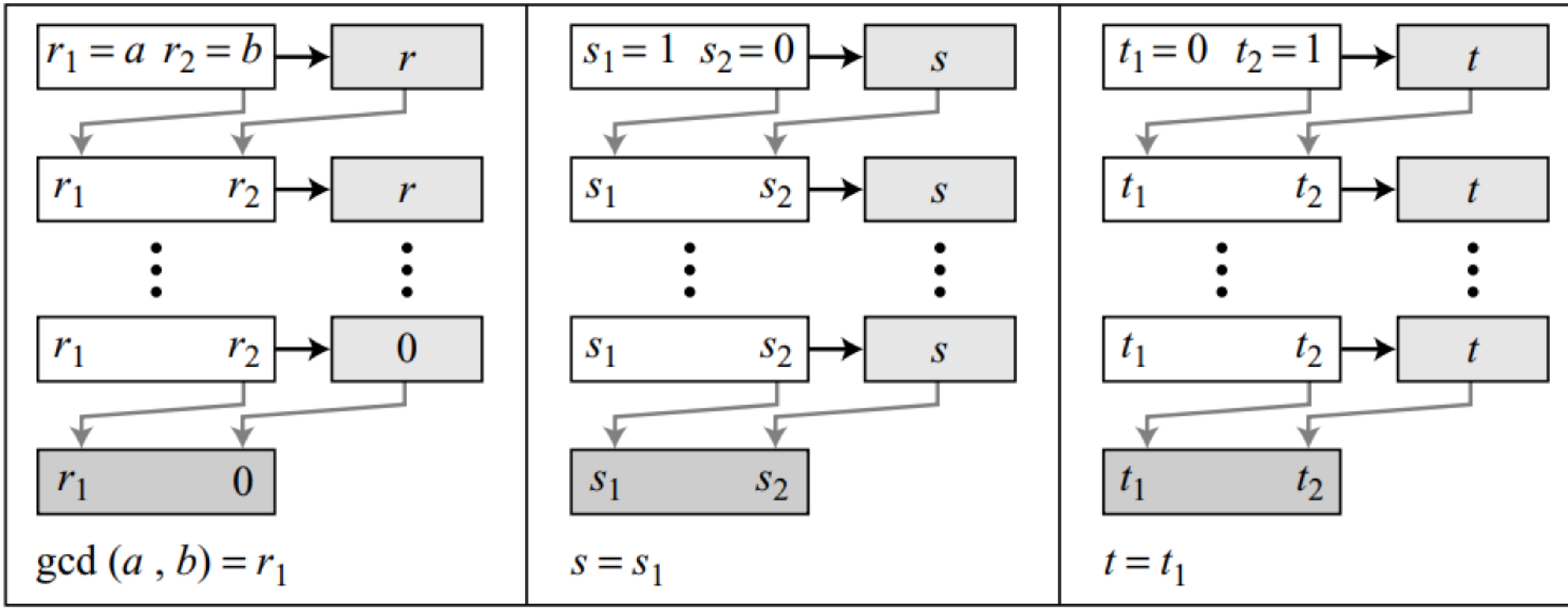
19CSE311 Computer Security

Jevitha KP
Department of CSE

Extended Euclid's Algorithm

- Given two integers a and b, we often need to find other two integers, s and t, such that $\mathbf{s \times a + t \times b = gcd\ (a, b)}$
- The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.
- the extended Euclidean algorithm uses the same number of steps as the Euclidean algorithm.
- In each step, we use three sets of calculations and exchanges instead of one.
- The algorithm uses three sets of variables, r's, s's, and t's.

Extended Euclid's Algorithm



a. Process

Extended Euclid's Algorithm

```
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

Extended Euclid's Algorithm

- In each step, r1, r2, and r have the same values in the Euclidean algorithm.
- The variables r1 and r2 are initialized to the values of a and b, respectively.
- The variables s1 and s2 are initialized to 1 and 0, respectively.
- The variables t1 and t2 are initialized to 0 and 1, respectively.
- The calculations of r, s, and t are similar, with one warning. Although r is the remainder of dividing r1 by r2, there is no such relationship between the other two sets.
- There is only one quotient, q, which is calculated as r1/r2 and used for the other two calculations.

Example

- Given a = 161 and b = 28, find gcd (a, b) and the values of s and t
- $q = r1 / r2$
- $r = r1 - q \times r2$
- $s = s1 - q \times s2$
- $t = t1 - q \times t2$

Example

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
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	

- **s × a + t × b = gcd (a, b)**
- **-1 * 161 + 6 * 28 = 7**

Example

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	

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

Example 2

» Given a = 17 and b = 0, find gcd (a, b) and the values of s and t.

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
	17	0		1	0		0	1	

- **s × a + t × b = gcd (a, b)**
- **1 * 17 + 0 * 0 = 17**

Example 3

» Given a = 0 and b = 45, find gcd (a, b) and the values of s and t.

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		1	0	

- **s × a + t × b = gcd (a, b)**
- **0 * 0 + 1*45 = 45**

Example 4

- » $a = 1759$ and $b = 550$. Calculate $\gcd(a, b)$ and s and t.

- » $q = r1 / r2$
- » $r = r1 - q \times r2$
- » $s = s1 - q \times s2$
- » $t = t1 - q \times t2$

Example 4

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
3	1759	550	109	1	0	1	0	1	-3
5	550	109	5	0	1	-5	1	-3	16
21	109	5	4	1	-5	106	-3	16	-339
1	5	4	1	-5	106	-111	16	-339	355
4	4	1	0	106	-111	550	-339	355	-1759
	1	0		**-111**	550		**355**	-1759	

Example 4

» s*a + t*b = gcd (a,b)

» **-111***1759 + **355***550 = **1**

Applications of Extended Euclid Algorithm

» Finding Multiplicative Inverse

» Solution for Linear Diophantine Equations

Finding Inverses

» Recap..
  » Aim : To find the inverse of a number relative to an operation.
  » Additive inverse (relative to an addition operation)
  » Multiplicative inverse (relative to a multiplication operation)

Finding Inverses

- Additive Inverse
  - In Z_n, two numbers a and b are additive inverses of each other if **$a + b \equiv 0 \pmod{n}$**
  - In Z_n, the additive inverse of a can be calculated as **$b = n - a$**.
  - Example, the additive inverse of 4 in Z_{10} is $10 - 4 = 6 \bmod 10$

Finding Inverses

- Properties of Additive Inverse
  - In modular arithmetic, **each integer has an additive inverse.**
  - The sum of an integer and its additive inverse is congruent to **0 modulo n**
  - **Each number has an additive inverse**
  - The inverse is **unique**
  - Each number has **one and only one additive inverse.**
  - **Inverse** of the number may be the **number itself**

Finding Inverses

- Multiplicative Inverse
  - In Z_n, two numbers a and b are multiplicative inverse of each other if **$a \times b \equiv 1 \pmod{n}$**
  - Example in Z_{10}, the multiplicative inverse of 3 is 7 => $(3 \times 7) \bmod 10 = 1$

Finding Inverses

- Properties of Multiplicative Inverse
  - In modular arithmetic, an integer **may or may not** have a multiplicative inverse.
  - When it does, the **product** of the integer and its multiplicative inverse is congruent to **1 modulo n.**
  - An integer a has a multiplicative inverse in Z_n **if and only if**
    - **gcd (n, a) = 1 or gcd (n, a) ≡1 (mod n), ie** n and a are relatively prime

Finding Multiplicative Inverse using Extended Euclid Algorithm

- The extended Euclidean algorithm can find the multiplicative inverse of **b in Zn**
  - when n and b are given
  - and the inverse exists
- **Extended Euclid's algorithm :**

  Given two integers a and b, we often need to find other two integers, s and t, such that $\mathbf{s \times a + t \times b = gcd\ (a, b)}$

Finding Multiplicative Inverse using Extended Euclid Algorithm

- **$s \times a + t \times b = \gcd(a, b)$** [replace the first integer a with n (the modulus).]
- **$s \times n + t \times b = \gcd(n, b)$**.
- **$s \times n + t \times b = \gcd(n, b) = 1$** [If the multiplicative inverse of b exists, gcd (n, b) must be 1]
- **$s \times n + t \times b = 1$**

Finding Multiplicative Inverse using Extended Euclid Algorithm

» **$s \times n + t \times b = 1$** [Apply the modulo operator to both sides / map each side to Zn.]

» **$(s \times n + t \times b) \bmod n = 1 \bmod n$**

» **$[(s \times n) \bmod n] + [(b \times t) \bmod n] = 1 \bmod n$**

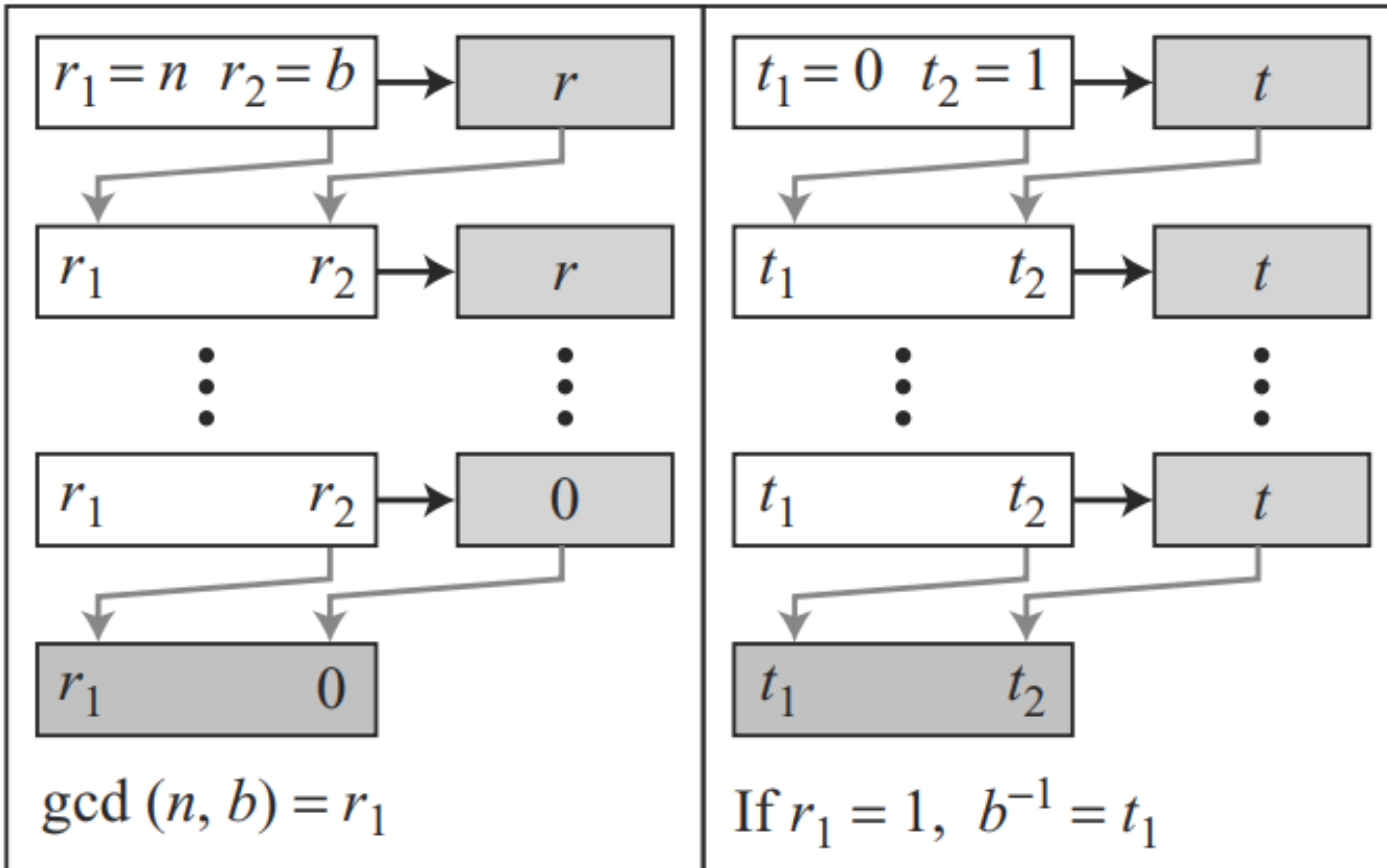
» **$0 + [(b \times t) \bmod n] = 1$** [$[(s \times n) \bmod n] = 0$ because if we divide $(s \times n)$ by n, the quotient is s but the remainder is 0]

» **$(b \times t) \bmod n = 1$ ==> t is the multiplicative inverse of b in Z_n**

Finding Multiplicative Inverse using Extended Euclid Algorithm

- The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd (n, b) =1.
- The multiplicative inverse of b is the value of t after being mapped to Z_n.

Finding Multiplicative Inverse using Extended Euclid Algorithm



a. Process

Finding Multiplicative Inverse using Extended Euclid Algorithm

```
r₁ ← n; r₂ ← b;
t₁ ← 0; t₂ ← 1;

while (r₂ > 0)
 {
  q ← r₁ / r₂;

   r  ← r₁ − q × r₂;
   r₁ ← r₂;  r₂ ← r;

   t  ← t₁ − q × t₂;
   t₁ ← t₂;  t₂ ← t;

 }
  if (r₁ = 1) then b⁻¹ ← t₁
```

b. Algorithm

Example 1

» Find the multiplicative inverse of 11 in Z26.

q	r1	r2	r= r1 − q × r2	t1	t2	t = t1 − q × t2
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		**-7**	26	

Example 1

» Find the multiplicative inverse of 11 in Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	–2
2	11	4	3	1	–2	5
1	4	3	1	–2	5	–7
3	3	1	0	5	–7	26
	1	0		–7	26	

- GCD = 1 ; T1 = -7
- t1 = −7 ==> (−7) mod 26 = 19.
- 11 and 19 are multiplicative inverse in Z26.
- (11 × 19) mod 26 = 209 mod 26 = 1.

Example 2

» Find the multiplicative inverse of 23 in Z_{100}.

q	r1	r2	r= r1 − q × r2	t1	t2	t = t1 − q × t2
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		**-13**	100	

Example 2

» Find the multiplicative inverse of 23 in Z_{100}.

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

- GCD = 1; T1 = -13
- t1 = −13 ==> (−13) mod 100 = 87.
- 23 and 87 are multiplicative inverse in Z100.
- (23 × 87) mod 100 = 2001 mod 100 = 1.

Example 3

» Find the multiplicative inverse of 12 in Z_{26}.

Example 3

» Find the multiplicative inverse of 12 in Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	−2
6	12	2	0	1	−2	13
	2	0		−2	13	

The gcd (26, 12) = 2 ≠ 1, which means there is no multiplicative inverse for 12 in Z26

Inverses Z10

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Addition Table in $\mathbf{Z}_{10}$

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Multiplication Table in $\mathbf{Z}_{10}$

Application of Inverses

- In cryptography we often work with inverses.
- If the sender uses an **integer** (as the **encryption key**), the receiver uses the **inverse of that integer (as the decryption key**).
- If the operation (encryption/decryption algorithm) is **addition**, Zn can be used as the **set of possible keys** because **each integer** in this set has an **additive inverse**.
- On the other hand, if the operation (encryption/decryption algorithm) is **multiplication**, **Zn cannot be the set of possible keys** because only **some members** of this set have a **multiplicative inverse.**

Set Zn*

» The Zn* set, is a subset of Zn which includes **only integers in Zn that have a unique multiplicative inverse**.

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

$$Z_6^* = \{1, 5\}$$

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$Z_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$Z_{10}^* = \{1, 3, 7, 9\}$$

Zn

- The result of the modulo operation with modulus n is always an integer between 0 and $n - 1$.
- The result of **a mod n** is always a nonnegative integer less than n.
- Modulo operation creates a set, which in modular arithmetic is referred to as the **set of least residues modulo n, or Zn**.
- Although we have only one set of integers (Z), we have infinite instances of the set of residues (Zn), one for each value of n.

Zn

$$\mathbf{Z}_n = \{\, 0, 1, 2, 3, \; . \; . \; . \; . \;, (n - 1) \,\}$$

$$\mathbf{Z}_2 = \{\, 0, 1 \,\} \qquad \mathbf{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\} \qquad \mathbf{Z}_{11} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \,\}$$

Zp and Zp*

- Cryptography often uses two more sets: **Zp and Zp*.**
- The modulus in these two sets is a **prime number.**
- A prime number has only two divisors: **integer 1 and itself.**

Zp

» The set Zp is the same as Zn except that **n is a prime**.

» Zp contains all integers from **0 to p – 1**.

» Each member in Zp has an additive inverse

» Each member except 0 has a multiplicative inverse.

Zp*

» The set Zp* is the same as Zn* except that n is a prime.

» Zp* contains all integers from **1 to p − 1**.

» Each member in Zp* has an additive and a multiplicative inverse.

» Zp* is used when we need a set that supports both **additive and multiplicative inverse.**

Zp and Zp*

» Example

$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Z_{13}{*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Linear Diophantine Equations (LDE)

» A Diophantine equation is a **polynomial equation** with 2 or more **integer unknowns**.

» The integer unknowns are each to **at most degree of 1.**

» Linear Diophantine equation in two variables takes the form of **$ax + by = c$,** where $x, y \in Z$ are unknowns and a, b, c are integer constants

Linear Diophantine Equations (LDE)

» Another application of Extended Euclid's algorithm is to find the solutions to the Linear Diophantine equations of two variables, $ax + by = c$.

» We need to find integer values for x and y that satisfy the equation.

» This type of equation has either **no solution or an infinite number of solutions**.

Linear Diophantine Equations (LDE)

- Let $d = \gcd(a, b)$.
- If d does not divide c, then the equation has **no solution.**
- If $d \mid c$, then we have an **infinite number of solutions.**
- One of them is called the **particular solution**; the rest, **general solution**

Linear Diophantine Equations (LDE)

- Particular Solution
  - If d| c, a particular solution to the above equation can be found using the following steps:
    - Reduce the equation to $\mathbf{a_1x + b_1y = c_1}$ by dividing both sides of the equation by d.
    - This is possible because d divides a, b, and c by the assumption
    - Solve for s and t in the relation $a_1s + b_1t = 1$ using the extended Euclidean algorithm
    - The particular solution can be found:
    - **$x_0 = (c/d)s$ and $y_0 = (c/d)t$**

Linear Diophantine Equations (LDE)

- **General Solutions**
  - **$x = x0 + k (b/d)$**
  - **$y = y0 - k (a/d)$,**
  - where k is an integer

Example 1

- Find the particular and general solutions to the equation $21x + 14y = 35$
  - **Check if solution is present**

Example 1

- $21x + 14y = 35$
  - **Check if solution is present**
  - $GCD(21,14) = 7$
  - Since $7|35$, the equation has an infinite number of solutions
  - Dividing LHS, RHS by 7 => $\mathbf{3x+2y = 5}$

Example 1

- Using the extended Euclidean algorithm, we find s and t such as 3s + 2t = 1
-

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
	1	0		**1**	-2		**-1**	3	

Example 1

- » s = 1 and t = −1
- » 3x+2y = 5 ==> a = 3, b =2, c =5
- » d = gcd(3,2) = 1
- » **Particular Solution :**
- » x_0 = (c/d)s and y_0 =(c/d)t
- » **x0 = (5/1) × 1 = 5 ;**
- » **y0 = (5/1) × (−1) = −5**

Example 1

- **General Solution : $x = x_0 + k\ (b/d)$ and $y = y_0 - k\ (a/d)$, k is n integer**
- $x = 5 + k \times (2/1)$ and $y = -5 - k \times (3/1)$
- k=0 ==> (5,-5)
- k=1 ==> (7,-8)
- k=2 ==> (9, -11)

Example 2

- An interesting application in real life is when we want to find different combinations of objects having different values.
- For example, imagine we want to cash a \$100 check and get some \$20 and some \$5 bills.
- We have many choices, which we can find by solving the corresponding Diophantine equation $\mathbf{20x + 5y = 100}$.

Example 2

- **$20x + 5y = 100$**
  - **Check if solution is present**

Example 2

- **$20x + 5y = 100$**
  - **Check if solution is present**
  - GCD(20,5) = 5
  - Since $5|100$, the equation has an infinite number of solutions
  - Dividing LHS, RHS by 5 => **$4x + y = 20$.**

Example 2

» Using the extended Euclidean algorithm, we find s and t such as 4s + t = 1

»

q	r1	r2	r= r1 − q × r2	s1	s2	s= s1 − q × s2	t1	t2	t = t1 − q × t2
4	4	1	0	1	0	1	0	1	-4
	1	0		**0**	1		**1**	-4	

Example 2

- » s = 0 and t = 1
- » **4x + y = 20** ==> a = 4, b =1, c =20
- » d = gcd(4,1) = 1
- » **Particular Solution : x_0 = (c/d)s and y_0 =(c/d)t**
- » x0 = (20/1) × 0 = 0 ;
- » y0 = (20/1) × (1) = 20

Example 2

- **General Solution : $x = x_0 + k\ (b/d)$ and $y = y_0 - k\ (a/d)$, k - integer**
- General: $x = 0 + k \times (1/1)$ and $y = 20 - k \times (4/1)$ where k is an integer
- Solutions where x and y nonnegative
- **k=0 ==> (0,20) ; k=1 ==> (1,16)**
- **k=2 ==> (2, 12) ; k =3 ==> (3, 8)**
- **k =4==> (4, 4) ; k =5 ==> (5,0)**
- k=6 ==> (6, -4) — not allowed since y is negative, we need only positive numbers

LINEAR CONGRUENCE

» Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in Zn.

» To solve equations when the power of each variable is 1 (linear equation)

Single-Variable Linear Equations

» Equations involving a single variable are of the form **$ax \equiv b \pmod{n}$.**

» An equation of this type might have **no solution or a limited number of solutions.**

» Assume that the **$\gcd(a, n) = d$.**

» If d does not divide b, there is no solution.

» If $d|b$, there are **d solutions**.

Single-Variable Linear Equations

- If $d|b$ the solutions can be found by :
  - Reduce the equation by dividing both sides of the equation (including the modulus) by d.
  - Multiply both sides of the reduced equation by the **multiplicative inverse of a** to find the particular solution x0.
  - The general solutions are
  - **$x = x0 + k\,(n/d)$ for $k = 0, 1, . . . , (d − 1)$.**

Example 1

» Solve the equation $10x \equiv 2 \pmod{15}$

Example 1

- Solve the equation $10x \equiv 2 \pmod{15}$
- gcd (10 and 15) = 5.
- Since 5 does not divide 2, we have no solution.

Example 2

» Solve the equation $14x \equiv 12 \pmod{18}$

Example 2

- Solve the equation $14x \equiv 12 \pmod{18}$
- a=14; b = 12; n =18
- gcd (14 and 18) = 2.
- Since 2 divides 12, we have exactly two solutions
- $14x \equiv 12 \pmod{18}$, divide by 2
- $7x \equiv 6 \pmod{9}$, multiply by inverse of 7
- $x \equiv 6\,(7^{-1}) \pmod{9}$
- $x_0 = (6 \times 7^{-1}) \bmod 9$

Example 2

» Find the multiplicative inverse of 7 in Z9.

q	r1	r2	r= r1 − q × r2	t1	t2	t = t1 − q × t2
1	9	7	2	0	1	-1
3	7	2	1	1	-1	4
2	2	1	0	-1	4	-9
	1	0		**4**	-9	

Example 2

- $x_0 = (6 \times 7^{-1}) \bmod 9$
- $(6 \times 4) \pmod 9 = 6$
- **$x = x0 + k\,(n/d)$ for $k = 0, 1, \ldots, (d - 1)$.**
- $k=1 \Rightarrow x1 = x0 + 1 \times (18/2) = 15$
- Both solutions, 6 and 15 satisfy the congruence relation, $14x \equiv 12 \pmod{18}$:
- $(14 \times 6) \bmod 18 = 12$ and
- $(14 \times 15) \bmod 18 = 12$.

Example 3

» Solve the equation $3x + 4 \equiv 6 \pmod{13}$

Example 3

» Solve the equation $3x + 4 \equiv 6 \pmod{13}$

» Change the equation to the form $ax \equiv b \pmod{n}$.

» Add -4 (the additive inverse of 4) to both sides,

» $3x \equiv 2 \pmod{13}$.

» Gcd (3, 13) = 1, the equation has only one solution,

» $x0 = (2 \times 3^{-1}) \bmod 13$

Example 3

» Find the multiplicative inverse of 3 in Z13.

q	r1	r2	r= r1 − q × r2	t1	t2	t = t1 − q × t2
4	13	3	1	0	1	-4
3	3	1	0	1	-4	13
	1	0		-4	13	

-4 mod 13 = 9 mod 13

Example 3

- » $x0 = (2 \times 3^{-1}) \bmod 13$
- » $x0 = (2 \times 9) \bmod 13$
- » $18 \bmod 13 = 5$.
- » Answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.