Chapter 00

Introducing Foundations

Outline

- Relative Prime and Prime Factorization [5-6, 9-12, 13-15]
- An Extension of Euclid Algorithm [17-25]
- Modular Division and Inverse Modulo n Computation [40-45]

Elementary Number-Theoretic Notions

An application of number-theoretic algorithms is in ***cryptography***

- the discipline concerned with encrypting a message sent from one party to another, such that someone who intercepts the message will not be able to decode it.

Let the set Z = { …., -2, -1, 0, 1, 2, 3, ….} of integers.

Let the set N = {0, 1, 2, 3, ….} of natural numbers (nonnegative integers.

The notation d | a (read "d ***divides*** a") means

- that a = k*d for some integer k, (i.e., a is k multiple of d).

Prime Factorization and Relative Prime

Relatively prime integers

Two integers a and b are *relatively prime* if, and only if gcd(a, b) = 1, that is, iff their only common divisor is 1.

For example:

8 and 15 are relatively prime, because gcd(8, 15) =1.

gcd(8 15) = 1, because

the divisors of 8 are 1, 2, 4, and 8, and

the divisors of 15 are 1, 3, 5, and 15.

Pairwise relatively prime integers

Integers $a_1, a_2, a_3, \ldots, a_n$ are *pairwise relatively primes*

if, and only if gcd$(a_i, a_j) = 1$,

for all integers i and j with $1 \leq i,\ j \leq n \text{ and } i \neq j$.

- 2, 3, 5, 7, 9, 11, 13, 17, 19, 21, 23, 25; they are *not* pairwise relatively prime, for gcd(3, 9) $\neq$ 1. So as, gcd(3, 21) $\neq$ 1 and gcd(5, 25) $\neq$ 1.
- 2, 7, 9, 11, 13, 17, 19, 21, 23, 25 are pairwise relative primes. Although 21 and 25 are not primes, they are pairwise relatively primes with other integers.

Prime Factorization and Relative Prime

Every integer greater than *one* can be written as a unique product of primes.

We next develop theory that proves this assertion.

The following theorem states that if two integers are each *relatively prime* to an integer p, then their product is relatively prime to p.

Example: Let p = 15, x = 4, y = 16 such that gcd(4, 15) = 1 and gcd(16, 15) = 1. Then gcd(4*16, 15) = 1.

Theorem 0.7

For all primes p and all integers a, b, if $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both). That is, $\gcd(a, p) = 1$ or $\gcd(b, p) = 1$.

Example: Let $p = 15$, $x = 4$, $y = 16$ such that $\gcd(4, 15) = 1$ and $\gcd(16, 15) = 1$. Then $\gcd(4*16, 15) = 1$.

A consequence of Theorem 0.7 is that

- every integer $n > 1$ has a unique factorization as a product of prime numbers.

The following *unique factorization theorem* is also called *the fundamental theorem of arithmetic*. Every integer greater than *one* can be written as a unique product of primes.

Theorem 0.8 (Unique factorization)

There is exactly *one way* to write any composite integer n as a product of the form

$$n = p_1^{e_1} p_2^{e_2} \dots p_j^{e_j},$$

where the p_i are prime, $p_1 < p_2 < p_3 < \dots < p_j$, and the e_i are positive integers.

This representation of n is *unique*.

The integer e_i is called the *order* of p_i in n.

Theorem 0.9

The gcd(m, n) is a product of the primes that are common to m and n, where the power of each prime in the product is the *smaller* of its orders in m and n.

Proof: The proof is left as an exercise.

Example 0.40:

- $300 = 2^2 \times 3^1 \times 5^2$ and $1125 = 3^2 \times 5^3$.
- So $\gcd(300, 1125) = 2^0 \times 3^1 \times 5^2 = 75$.

- $\gcd(300, 1125) = 4*300 + (-1)*1125$
  $= 75\{4*4 + (-1)*15\}$, where $0 < 4*4 + (-1)*15 = 1$
  $= 75$

Computing the Greatest Common Divisor

Theorem 0.9 gives us a straightforward way to compute the greatest common divisor of two such integers. We simply

- find the unique factorizations for the two integers,
- determine which primes they have in common, and
- determine the greatest common divisor to be a product whose terms are these common primes, where the power of each prime in the product is the smaller of its orders in the two integers.

The following example illustrated this.

Example 0.43:

$$3{,}185{,}325 = 3^4 \times 5^2 \times 11^2 \times 13^1$$

$$7{,}276{,}500 = 2^2 \times 3^3 \times 5^3 \times 7^2 \times 11^1$$

$\gcd(3{,}185{,}325,\ 7{,}276{,}500) = 3^3 \times 5^2 \times 11^1 = 7{,}425.$

The problem with this technique is:

- Not easy to find the unique factorization of an integer.
    - Some difficulty factoring these integers in this example.
    - imagine the difficulty if the integer has 25 digits instead of 7.
- *no one* has ever found a polynomial-time algorithm for determining the factorization of an integer.

Example 0.43: find gcd(7,276,500, 3,185,325)

gcd(7,276,500, 3,185,325)
= gcd(3,185,325, 905,850)   7,276,500 = 2*3,185,325 + 905,850 →
= gcd(905,850, 467,775)   3,185,325 = 3* 905,850 + 467,775
= gcd(467,775, 438,075)   905,850 = 1* 467,775 + 438,075
= gcd(438,075, 29,700)   467,775 = 1* 438,075 + 29,700
= gcd(29,770, 22,275)   438,075 = 14* 29,700 + 22,275
= gcd(22,275, 7,425)   29,770 = 1* 22,275 + 7425
= gcd(7,425, 0)   22,275 = 3 * 7,425 + 0
= 7,425   7,425 = 0 * 0 + 7,425

7,425 = 1* 7,425 = 1*(1* 29,770 - 1* 22,275)
= 1* (1*467,775 - 1* 438,075) – (1 * 438,075 -14* 29,700))
= 1*467,775 - 2* 438,075 + 14* 29,700)
= 1*467,775 -2*(1* 905,850 -1* 467,775) + 14*(1* 467,775 - 1* 438,075)
= 17*467,775 -2* 905,850 - 14* 438,075
= 17*(3,185,325 - 3* 905,850)- 2*(7,276,500 -2*3,185,325) -14*(905,850 - 1* 467,775)
= 17*3,185,325 - 51* 905,850 - 2*7,276,500 +4*3,185,325 -14*905,850 +14* 467,775
= - 2*7,276,500 + 21*3,185,325 - 65* 905,850 + 14* 467,775
= - 2*7,276,500 + 21*3,185,325 - 65* 7,276,500 + 130*3,185,325) + 14* *3,185,325 - 42* 905,850
= - 67*7,276,500 + 166*3,185,325 - 42* 7,276,500 + 84*3,185,325)
= - 109*7,276,500 + 250*3,185,325
= -109 * 980 * 7425 + 250 * 429 * 7425
= (-109 * 980 + 250 *429)*7425

Euclid's Algorithm

The recursive Euclid's algorithm is based on Theorem 0.4.

For any nonnegative integer a and any positive integer b,

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Algorithm Euclid (m, n)

//Compute gcd(m, n) by Euclid's algorithm

Input: two non-negative m and n, not both zero integers

Output: the greatest common divisor of m and n

```
if (n == 0)
    then return m;
    else Euclid(n, m mod n);
```

the total running time is $2n * O(n^2) = O(n^3)$

Analysis of `Algorithm Euclid(m, n)`

Let's analyze the Algorithm Euclid (m, n) using binary encoding.

The input size is the number of bits it takes to encode the numbers m and n, which are $\lfloor \log_2 m \rfloor + 1$ and $\lfloor \log n \rfloor + 1$, respectively.

Worst-Case Time Complexity (Euclid Algorithm)

- Basic operation: One-bit manipulation in the computation of a remainder.
- Input size: The number of bits s it takes to encode m and the number of bits t it takes to encode n. That is,

  $$s = \lfloor \log_2 m \rfloor + 1 \qquad\qquad t = \lfloor \log n \rfloor + 1.$$

- For the case $1 \leq m < n$, the worst-case number of recursive calls for input size s, t is

  $$W(s, t) \in \theta(t).$$

An extension of Euclid Algorithm

An extension of Euclid Algorithm

- How can we check that d is claimed to be the GCD(a, b)?

- When we *check* that d | a and d | b, this only shows d to be a common factor, *not necessarily* the greatest (largest) one

- *Here is a test* that can be used if d = ai + bj, for some integers i and j.

- Theorem 0.2 states that:

  If d | a and d | b, then for integers i and j, d | (ia + jb).

- This theorem entails that there are integers i and j such that gcd(a, b) = ia + jb.

Recall:

Theorem 0.3

Let x and y be integers, not both 0. Let

d = min{ix + jy | i, j ∈ Z and ix + jy > 0}.

i.e., d is the smallest positive linear combination of x and y.

Then d = gcd(x, y).

Note that gcd(x, y) = ix + jy > 0

$= d(i*\frac{x}{d} + j*\frac{y}{d}) > 0$, where $0 < (i*\frac{x}{d} + j*\frac{y}{d}) = 1$

= d = min{ix + jy | i, j ∈ Z and ix + jy > 0}.

Furthermore, $\frac{x}{d}$ and $\frac{y}{d}$ are relatively prime.

Theorem 0.3

Let x and y be integers, not both 0. Let

$$d = \min\{ix + jy \mid i, j \in Z \text{ and } ix + jy > 0\}.$$

i.e., d is the smallest positive linear combination of x and y.

Then $d = \gcd(x, y)$.

Lemma 0.4:

If d divides both x and y, and $d = i*x + j*y$ for some integers i and j then necessarily $d = \gcd(x, y)$.

[note that d is the smallest positive of the set $i*x + j*y$.]

gcd(60, 24) d=12= min{1*60 + (-2)*24, 3*60 + (-7)*24, …. }

Note that if gcd(x, y) = d, then $\{ix + jy\} = \{d\,(\frac{x}{d}\,i + \frac{y}{d}\,j)\}$.

Example 0.28: continue….

Let x = 60, y = 24. find gcd(60, 24).

$\underline{60} = 2 * \underline{24} + 12$ implies $12 = 1 * \underline{60} - 2 * \underline{24}$ (1)

$\underline{24} = 2 * \underline{12} + 0$ implies $0 = 1 * \underline{24} - 2 * \underline{12}$ (2)

$\underline{12} = \mathbf{0} * \underline{0} + 12$ implies $12 = 1 * \underline{12} - 0 * \underline{0}$ (3)

gcd(60, 24)
= gcd(24, 60%24)
= gcd(24, 12)
= gcd(12, 24%12)
= gcd(12, 0)
= 12

$12 = \mathbf{1} * \underline{12} - \mathbf{0} * \underline{0} = 1 * \underline{12} - 0 * (1 * \underline{24} - 2 * \underline{12})$ using (3) and (2)

$= \mathbf{0} * 24 + \mathbf{1} * \underline{12} = 1 * 12$

$= 1 * (1 * \underline{60} - 2 * 24) = \mathbf{1} * \underline{60} + (\mathbf{-2}) * \underline{24}$ using (1)

Thus, gcd(60, 24) = 1*60 + (-2) *24

= 12{1*5 + (- 2)*2 } = 12, where $1*\underline{5} + (-2)*\underline{2} = 1$

i*60+ j*24 = 12(i5 + j2).
gcd(60, 24) = min{12(i*5 + j*2)| i, j ε Z, i*5 + j*2 > 0}
gcd(24, 12) = min{12(i*2 + j*1)| i, j ε Z, i*2 + j*1 > 0}
gcd(12, 0) = min {12(i*1 + j*0)| i, j ε Z, i*1 + j*0 > 0}

Example 0.45:

We know 12 is the gcd(60, 24). Using the extended Euclid Algorithm, it yields i and j which are stated in the following table.

$d_{min} = 1*\underline{60} + (-2)*\underline{24} = 12(1*5 + (-2)*2)$ where $1*5 + (-2)*2 = 1 > 0$. (3rd step)

$d_{min} = 0*\underline{24} + 1*\underline{12} = 12(0*2 + 1*1)$ where $0*2 + 1*1 = 1 > 0$. (2nd step)

$d_{min} = 1*\underline{12} + 0*\underline{0} = 12(1*1 + 0*0)$ where $1*1 + 0*0 = 1 > 0$. (initial step)

x	y	$\lfloor x/y \rfloor$	gcd	i	j	
60	24	2	12	**1**	**-2**	3rd step
24	12	2	12	**0**	**1**	2nd step
12	0	-	12	**1**	**0**	1st step

d = i*60 + j*24 = min{12*(i*5 + j*2)| for i, j in Z, i*5 + j*2 >0}

gcd(x, y) = d = min{ d(i*$\frac{x}{d}$ + j*$\frac{y}{d}$)| i, j ε Z, i*$\frac{x}{d}$ + j*$\frac{y}{d}$ > 0 }.
That means i*$\frac{x}{d}$ + j*$\frac{y}{d}$ = 1 for getting the minimum d.
Furthermore, $\frac{x}{d}$ and $\frac{y}{d}$ are relatively prime.

But when can we find these integer numbers i and j?

- Under what circumstance can gcd(x, y) be expressed in this checkable form i*x + j*y > 0?
- It turns out that it always can.

What is even better, the coefficients i and j can be found by a small extension to Euclid's algorithm which is as follows:

Euclid(x, y)
if (y == 0)
then return x;
else Euclid(y, x mod y);

function extended-Euclid(x, y)

//For clarity, x = q * y + r, where r = x mod y.

if (y == 0) then return (1, 0, x); //return (i=1, j=0, x).

else { (i', j', d') = extended-Euclid(y, x mod y);

(i, j, d) = (j', i' - $\lfloor \frac{x}{y} \rfloor$ * j ', d');

return (i, j, d) }

```
function extended-Euclid(x, y)
```

Input: Two integers x and y with $x \geq y \geq 0$.

Output: Integers i, j, d such that d = gcd(x, y) and i*x + j*y = d.

```
if (y == 0) then return (1, 0, x); // 1*x + 0*0 = x
else {(i', j', d') = extended-Euclid(y, x mod y);
      return (j', i'-⌊x/y⌋ * j', d');}
```

$\underbrace{i' - \lfloor \frac{x}{y} \rfloor * j'}_{r \,=\, i' \bmod j'.}$

d = min{12*(i*5 + j*2)| for i, j in Z, i*5 + j*2 >0}
That is, 1*5 + (-2) *2 = 1

function extended-Euclid(x, y)
//For clarity, x = q * y + r, where r = x mod y.
if y = 0 then return (1, 0, x)
else { (i', j', d') = extended-Euclid(y, x mod y);
(i, j, d) = (j', i' - ⌊ x/y ⌋ * j', d');
return (i, j, d) }

function extended-Euclid(x, y)

e-E(x = 60, y = 24)

(i', j', d') = extended-Euclid(24, 60 mod 24 = 12);

return (j', i' - ⌊ x/y ⌋ * j', d') = (1, 0 - ⌊ 60/24 ⌋ * 1, 12)

= (1, -2, 12) which is (i', j', d)…. (3)

e-E(x = 24, y =12)

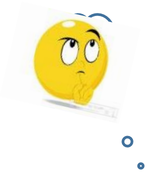
(i', j', d') = extended-Euclid(12, 24 mod 12 = 0);

return (j', i' - ⌊ x/y ⌋ * j', d') = (0, 1 - ⌊ 24/12 ⌋ * 0, 12)

= (0, 1, 12) which is (i', j', d) ….. (2)

e-E(x = 12, y = 0)

Since y = 0, return (1, 0, 12) which is (i'=1, j'=0, x=12) …..(1)



Theorem 0.11

For any positive integers a and b, the extended Euclid algorithm returns integers i, j, and d such that gcd(x, y) = d = i*x + j*y.

Consider Example 0.45:

$i^*60^* + j^*24^* = 12(i^*5 + j^*2)$.
$\gcd(60, 24) = \min\{12(i^*5 + j^*2) \mid i, j \in Z, i^*5 + j^*2 > 0\}$
$\gcd(24, 12) = \min\{12(i^*2 + j^*1) \mid i, j \in Z, i^*2 + j^*1 > 0\}$

We know 12 is the gcd(60, 24). The reason is that 60*1 + 24*(-2) = 12, or 60*(-1) + 24*3 = 12, or 60*(3) + 24*-7 = 12, (which is the least positive).

However, we know 3 | 60 and 3 | 24. But 3 is not the gcd(60, 24) for there is no integers i and j such that i*60 + j*24 = 3.

The following table can be obtained by the computation as follows:

x	y	$\lfloor x/y \rfloor$	gcd	i	j	
60	24	2	12	**3**	**-7**	3rd step
24	12	2	12	**-1**	**3**	2nd step
12	0	-	12	**1**	**0**	1st step

$i^*60 + j^*24^* = \min\{12(i^*5 + j^*2) \mid \text{for } i, j \text{ in } Z, i^*5 + j^*2 > 0\}$

Consider Example 0.45 (contd.):

To compute gcd(60, 24), based on $(x = q * y + r)$, where $r = x \bmod y$.

Euclid's algorithm would proceed as follows:

gcd(60, 24) $\quad \underline{60} = 2 * \underline{24} + 12 \rightarrow 12 = 1 * \underline{60} - 2 * \underline{24}$ (3rd step)

= gcd(24, 12) $\quad \underline{24} = 2 * \underline{12} + 0 \rightarrow 0 = 1 * \underline{24} - 2 * \underline{12}$ (2nd step)

= gcd(12, 0) $\quad \underline{12} = 1 * \underline{0} + 12 \rightarrow 12 = 1 * \underline{12} - 1 * \underline{0}$ (1st step)

= 12

At each step, the gcd computation has been reduced to the underlined numbers. Thus, gcd(60, 24) = gcd(24, 12) = gcd(12, 0) = 12.

To find i and j such that $i*60 + j*24 = 12$, we start by expressing 12 in terms of the last pair (12, 0). Then we work backwards and express it in terms of (24, 12), and finally (60, 24). The process is as follows:

(x = q * y + r), where r = x mod y.   r = x – q * y.

gcd(60, 24) 60 = 2 * 24 + 12   12 = 60 – 2 * 24   ….(3)

gcd(24, 12) 24 = 2 * 12 + 0   0 = 24 – 2 * 12   ….(2)

gcd(12, 0) 12 = 1 * 0 + 12   12 = 12 – 1 * 0   …..(1)

= 12

The first step is: use the last line on the gcd computation

12 = 1 * 12 – 1 * **0**. …..(1)   (i.e., based on r = x – q * y)}

The second step is: use the second last line on the gcd computation

0 = 1 * 24 – 2 * 12 ….. (2) to replace **0** in (1)

to get 12 = 1 * 12 – (1 * 24 – 2 * 12)

= 1 * 12 – 1 * 24 + 2 * 12

= –1 * 24 + 3 * **12**. ….(2a)

The final step is: use the first line on the gcd computation

12 = 1 * 60 – 2 * 24 …..(3) to replace **12** in (2a).

to get 12 = –1 * 24 + 3 * (1* 60 - 2 * 24)

= 3 * 60 – 7 * 24 ….. (3a)

gcd(60, 24) = 3 * 60 – 7 * 24 = 12(3 * 5 – 7 *2) = 12

Example 0.43:

If we can supply two numbers x and y such that d = a*i + b*j, then we can be sure d = gcd(a, b). For instance, we know 1 is the gcd(13, 4), that is, gcd(13, 4) = 1. The reason is that 13 * 1 + 4 *(-3) = 1 (which is the least positive).

Using function extended-Euclid(13, 4), we have the following table:

x	**y**	**⌊ x/y ⌋**	**gcd**	**i**	**j**
13	4	3	1	1	-3
4	1	4	1	0	1
1	0	-	1	1	0

1 = gcd(13, 4) = 1 = 13 * 1 + 4 *(-3).
Without applying the extended algorithm, we could find i = 5, j = -16. i.e., gcd(13, 4) = 1 = 13*5 + 4*(-16) = 1 > 0.
For (i, j) ∈ {(−3, 10), (1, −3), (5, −16), …}, d = min{1*(13i + 4j) | i, j ∈ Z, (13i + 4j) > 0}. This implies that for any pair (i, j) which yields 13i + 4j =1.

d = min{1*(13i + 4j)| for i, j in Z, 13i + 4j >0}
That is, 13 * 1 + 4 * -3 = 1

function extended-Euclid(a, b)
//For clarity, x= q * y + r, where r = x mod y.
if y = 0 then return (1, 0, x)
else { (i', j', d') = extended-Euclid(y, x mod y);
(i, j, d) = (j', i' - ⌊ x/y ⌋ * j', d');
return (i, j, d) }

E(x = 13, y = 4)

(i', j', d') = extended-Euclid(4, 13 mod 4 = 1);

return (j', i' - ⌊ x/y ⌋ * j', d') = (1, 0 - ⌊ 13/4 ⌋ * 1, 1)

= (1, -3, 1) is (i, j, d) …..(3)

E(x = 4, y =1)

(i', j', d') = extended-Euclid(4, 4 mod 1 = 0);

return (j', i' - ⌊ x/y ⌋ * j', d') = (0, 1 - ⌊ 4/1 ⌋ * 0, 1)

= (0, 1, 1) ⟹ (i', j', d') …..(2)

E(a = 1, b = 0)

Since b = 0, return (1, 0, 1) …..(1)

Consider Example 0.43:

To compute gcd(13, 4), Euclid’s algorithm would proceed as follows:

$$\underline{13} = 3 * \underline{4} + 1 \qquad (x = q * y + r), \text{ where } r = x \bmod y$$

$$\underline{4} = 4 * \underline{1} + 0 \qquad \gcd(4, 1)$$

$$\underline{1} = 1 * \underline{0} + 1 \qquad \gcd(1, 0) = 1$$

At each step, the gcd computation has been reduced to the underlined numbers.

Thus, gcd(13, 4) = gcd(4, 1) = gcd(1, 0) = 1.

To find x and y such that 13*i + 4*j = 1, we start by expressing 1 in terms of the last pair (1, 0). Then we work backwards and express it in terms of (4, 1), and finally (13, 4).

The first step is: we use the last line $\underline{1} = 1 * \underline{0} + 1$ to get

$$1 = \underline{1} - 1 * \underline{0} \quad \text{(i.e., based on } r = x - q * y)\}$$

$$1 = \underline{1} - 1 * \underline{0} = 1 * \underline{1} - 1 * \underline{0}. \quad \ldots\ldots(1)$$

To rewrite this in terms of (4, 1), we use substitution $0 = 1 * \underline{4} - 4 * \underline{1}$ (i.e., $r = x - q * y$), which is obtained by from the second last line on the gcd calculation

$$\underline{4} = 4 * \underline{1} + 0$$

$$0 = 1 * \underline{4} - 4 * \underline{1}$$

to get $1 = 1 * \underline{1} - \mathbf{1 * (1 * \underline{4} - 4 * \underline{1})}$

$$= 1 * \underline{1} - 1 * \underline{4} + 4 * \underline{1}$$

$$= -1 * \underline{4} + 5 * \underline{1} \quad \ldots\ldots(2)$$

$\underline{13} = 3 * \underline{4} + 1$	($x = q * y + r$), where $r = x \bmod y$
$\underline{4} = 4 * \underline{1} + 0$	gcd(4, 1)
$\underline{1} = 1 * \underline{0} + 1$	gcd(1, 0) = 1

The final step is to use substitution $1 = 1*13 - 3 * 4$, which is obtained by from the first one on the gcd calculation

$$\underline{13} = 3 * \underline{4} + 1$$

$$1 = 1 * \underline{13} - 3 * \underline{4}$$

to get $1 = -1 * \underline{4} + 5 * (1 * \underline{13} - 3 * \underline{4})$

$$= 5 * \underline{13} - 16 * \underline{4} \quad \ldots\ldots(3)$$

The first step is: we use the last line $\underline{1} = 1 * \underline{0} + 1$ to get

$$1 = \underline{1} - 1 * \underline{0} \quad \text{(i.e., based on } r = a - q * b\text{)\}}$$

$$1 = \underline{1} - 1 * \underline{0} = \mathbf{1} * \underline{1} \mathbf{-} \mathbf{1} * \underline{0}.$$

To rewrite this in terms of (4, 1), we use substitution $0 = 1 * \underline{4} - 4 * \underline{1}$ (i.e., $r = a - q * b$), which is obtained by from the second last line on the gcd calculation

$$\underline{4} = 4 * \underline{1} + 0$$

$$0 = 1 * \underline{4} - 4 * \underline{1}$$

to get $1 = 1 * \underline{1} - (1*\underline{4} - 4 *\underline{1})$

$$= 1 * \underline{1} - 1 * \underline{4} + 4 * \underline{1}$$

$$= \mathbf{-1} * \underline{4} + \mathbf{5} * \underline{1}$$

$\underline{13} = 3 * \underline{4} + 1$	($a = q * b + r$), where $r = a \bmod b$
$\underline{4} = 4 * \underline{1} + 0$	gcd(4, 1)
$\underline{1} = 1 * \underline{0} + 1$	gcd(1, 0) = 1

The final step is to use substitution $1 = 1*13 - 3 * 4$, which is obtained by from the first one on the gcd calculation

$$\underline{13} = 3 * \underline{4} + 1$$

$$1 = 1* \underline{13} - 3 * \underline{4}$$

to get $1 = -1 * \underline{4} + 5 * (1* \underline{13} - 3 * \underline{4})$

$$= \mathbf{5} * \underline{13} - 16 * \underline{4}$$

Using the pairs of blue colored numbers to complete i and j as in the table.

Now Example 0.43 is as follows:

If we can supply two numbers x and y such that d = i*x+ j*y, then we can be sure d = gcd(x, y). For instance, we know 1 is the gcd(13, 4), that is, gcd(13, 4) = 1. The reason is that 13 * 1 + 4 *(-3) = 1 (which is the least positive).

Using function extended-Euclid(13, 4), we have the following table:

x	**y**	$\lfloor$ **x/y** $\rfloor$	**gcd**	**i**	**j**	
13	4	3	1	5	-16	3^{rd} step
4	1	4	1	-1	5	2^{nd} step
1	0	-	1	1	-1	1^{st} step

1 = gcd(13, 4) = min {(13 * 5 + 4 *(-16)) | 13 * 5 + 4 *(-16) = 1 > 0} .
If apply the extended algorithm, i = 5, j = -16.
i.e., gcd(13, 4) = 1 = 13*5 + 4*(-16). (i, j) = {(5, -16), (1, -3), …} = min {1*(13i + 4j) | (13i + 4j) >0}. This implies that for any pair (i, j), 13i + 4j =1.

Example 0.46:

To compute gcd(25, 11), Euclid’s algorithm would proceed as follows:

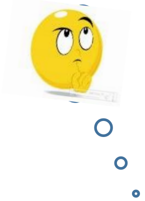
(x = q * y + r), where r = x mod y

$\gcd(25, 11)$	$\underline{25} = 2 * \underline{11} + 3$	$\rightarrow\ 3 = 1 * \underline{25} - 2 * \underline{11}$
$= \gcd(11, 3)$	$\underline{11} = 3 * \underline{3} + 2$	$\rightarrow\ 2 = 1 * \underline{11} - 3 * \underline{3}$
$= \gcd(3, 2)$	$\underline{3} = 1 * \underline{2} + 1$	$\rightarrow\ 1 = 1 * \underline{3} - 1 * \underline{2}.$
$= \gcd(2, 1)$	$\underline{2} = 2 * \underline{1} + 0$	$\rightarrow\ 0 = 1 * \underline{2} - 2 * \underline{1}$
$= \gcd(1, 0)$	$\underline{1} = 1 * \underline{0} + 1$	$\rightarrow\ 1 = 1 * \underline{1} - 1 * \underline{0}.$
$= 1$		

At each step, the gcd computation has been reduced to the underlined numbers.

$\underline{25} = 2 * \underline{11} + 3$	gcd(25, 11)
$\underline{11} = 3 * \underline{3} + 2$	gcd(11, 3)
$\underline{3} = 1 * \underline{2} + 1$	gcd(3, 2)
$\underline{2} = 2 * \underline{1} + 0$	gcd(2, 1)
$\underline{1} = 1 * \underline{0} + 1$	gcd(1, 0) = 1

To find x and y such that 25*i + 11*j = 1, we start by expressing 1 in terms of the last pair (1, 0). Then we work backwards and express it in terms of (2, 1), (3, 2), (11, 3) and finally (25, 11).



The first step is: use the last line $\underline{1} = 1 * \underline{0} + 1$ to get

$$1 = \underline{1} - 1 * \underline{0} = 1 * \underline{1} - 1 * \underline{0}. \quad \ldots.(1)$$

The second step is: use the 2nd last line $\underline{2} = 2 * \underline{1} + 0$, i.e., $0 = \underline{2} - 2 * \underline{1}$ to replace $\underline{0}$ in (1)

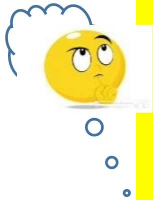
Then, $1 = 1 * \underline{1} - 1 * \underline{0}.$ from (1)

$$= 1 * \underline{1} - 1 * (\underline{2} - 2 * \underline{1}) = 1 * \underline{1} - 1 * \underline{2} + 2 * \underline{1}$$

$$= -1 * \underline{2} + 1 * \underline{1} + 2 * \underline{1} = -1 * \underline{2} + 3 * \underline{1}. \quad \ldots.(2)$$

The 3rd step is: Use the 3rd last line $\underline{3} = 1 * \underline{2} + 1$ which yields **1** $= \underline{3} - 1 * \underline{2}$.

Substituting this in



$$1 = -1 * \underline{2} + 3 * \underline{1} \qquad \text{….(2)}$$

$$= -1 * \underline{2} + 3 * (\underline{3} - 1 * \underline{2})$$

$$= 3 * \underline{3} - 4 * \underline{2} \qquad \text{…..(3)}$$

Continuing in this same way with substitutions $2 = 11 - 3 * 3$ and then $3 = 25 - 2 * 11$ into (3) and (4) gives

$$1 = 3 * \underline{3} - 4 * \underline{2} \qquad \text{from (3)}$$

$$= 3 * \underline{3} - 4 * (\underline{11} - 3 * \underline{3})$$

$$= -4 * \underline{11} + 15 * \underline{3} \qquad \text{…..(4)}$$

$$= -4 * \underline{11} + 15 * (\underline{25} - 2 * \underline{11})$$

$$= 15 * \underline{25} - 34 * \underline{11} \qquad \text{…..(5)}$$

$\underline{25} = 2 * \underline{11} + 3$ gcd(25, 11)

$\underline{11} = 3 * \underline{3} + 2$ gcd(11, 3)

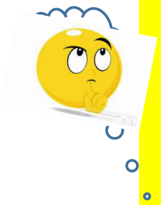
$\underline{3} = 1 * \underline{2} + 1$ gcd(3, 2)

$\underline{2} = 2 * \underline{1} + 0$ gcd(2, 1)

$\underline{1} = 1 * \underline{0} + 1$ gcd(1, 0) = 1

We are done: 15 * 25 – 34 * 11 = 1, so i = 15 and j = -34.

That means, gcd(25, 11) = 25 *15 + 11*(-34) = 1



Using function extended-Euclid(25, 11) we obtained the following table:

x	**y**	**$\lfloor x/y \rfloor$**	**d = gcd**	**i**	**j**	
25	11	2	1	15	-34	5th step
11	3	3	1	-4	15	4th step
3	2	1	1	3	-4	3rd step
2	1	1	1	-1	3	2nd step
1	0	-	1	1	-1	1st step

Thus, the gcd(25, 11) = 1 = min { 1*(15 * $\underline{25}$ – 34 * $\underline{11}$) | 15 * $\underline{25}$ – 34 * $\underline{11}$ > 0}.

Note that the values for (i, j) are not unique for the same (x, y)

Modular Division

ax and 1 are equivalent mod n.
ax and 1 are congruent mod n.
ax is congruent to 1 mod n.
n | ax – 1 or n| 1 – ax.

Modular Division

- Every number $a \neq 0$ has a multiplicative inverse, $\frac{1}{a}$.
- Any number x divides by a is x multiplying by this inverse $\frac{1}{a}$;
  - i.e., $\frac{x}{a} = x * (\frac{1}{a}) = x * a^{-1}$.

- x is the multiplicative inverse of ***a*** modulo n if $\boldsymbol{a}x \equiv 1 \pmod{n}$.
  - $\boldsymbol{a}x \equiv 1 \pmod{n}$ iff $x \equiv \frac{1}{a} \pmod{n}$ iff $x \equiv \boldsymbol{a}^{-1} \pmod{n}$.

Corollary 0.4.7 Existence of Inverse Modulo n

For all integers a and n, if $\gcd(a, n) = 1$,

then there exists an integer x such that $ax \equiv 1 \pmod{n}$. i.e., $n \mid ax - 1$ or $n \mid 1 - ax$.

The integer x is called the (multiplicative) inverse of a mod n.

Example 0.4.7 (Find an Inverse Modulo n):

Find an inverse for 43 modulo 660 (i.e., Compute 43^{-1} mod 660.).
i.e., find an integer x such that $43x \equiv 1 \pmod{660}$.
Solution: using $x = q * y + r$, which yields $r = x - q*y$, we write:

$\underline{660} = \underline{43} * 15 + 15$, which yields $15 = \underline{660} - 15 * \underline{43}$. gcd(660, 43)
$\underline{43} = \underline{15} * 2 + 13$, which yields $13 = \underline{43} - 2 * \underline{15}$. = gcd(43, 15)
$\underline{15} = \underline{13} * 1 + 2$, which yields $2 = \underline{15} - 1 * \underline{3}$. = gcd(15, 13)
$\underline{13} = \underline{2} * 6 + 1$, which yields $1 = \underline{13} - 6 * \underline{2}$. = gcd(13, 2)
$\underline{2} = \underline{1} * 2 + 0$, which yields $0 = \underline{2} - 2 * \underline{1}$. = gcd(2, 1)
$\underline{1} = \underline{0} * 0 + 1$, which yields $1 = \underline{1} - 0 * \underline{0}$. = gcd(1, 0) = 1

To express 1 as a linear combination of 660 and 43, substitute back:

$1 = 1 * \underline{1} - 0 * \underline{0} = 1 * \underline{1} - 0 * (1*\underline{2} - 2*\underline{1}) = 1 * \underline{1}$
$= 1 * (1*\underline{13} - \underline{2}*6) = 1*\underline{13} - 6 * \underline{2} = 1*\underline{13} - 6 * (1*\underline{15} - 1*\underline{13})$
$= -6*\underline{15} + 7*\underline{13} = -6*\underline{15} + 7 * (1 * \underline{43} - 2*\underline{15}) = 7*\underline{43} - 20*\underline{15}$
$= 7*\underline{43} - 20*(1*\underline{660} - 15*43) = -20*\underline{660} + 307*\underline{43}$

We find $307 * 43 - 20 * 660 = 1$.

$$307 * 43 = 1 + 20 * 660.$$

Thus by definition of congruence modulus 660, and Theorem 0.1.4.1

$$307 * 43 \pmod{660} = (1 + 20 * 660) \pmod{660}$$

$$307 * 43 \pmod{660} = (1 \pmod{660} + 20 * 660 \pmod{660})) \pmod{660}\ .$$

$$307 * 43 \pmod{660} = (1 \pmod{660} + 0)\pmod{660}$$

$$307 * 43 \pmod{660} = (1 \bmod 660) \bmod 660$$

$$307 * 43 \pmod{660} = 1 \bmod 660$$

$$307 * 43 \equiv 1 \pmod{660}.$$

$$307 \equiv 43^{-1} \pmod{660}.$$

So 307 is the inverse (i.e., the multiplicative inverse) of 43 modulo 660.

Note that 307*43 (= 13201) is an element of the equivalence class modulo 660 containing an integer 1, $[1]_{660}$ where $[a]_n = \{a + i * n \mid i \,\varepsilon\, Z\}$. For this case i =20

Example: 0.4.7.1

Find a positive inverse for 3 modulo 40.

That is, find a positive integer x such that 3x ≡ 1(mod 40).

Solution:

Find a linear combination of 3 and 40 that equals 1.

40 = 13 * 3 + 1 which yields 1 = 1 * 40 – 13 * 3. gcd(40, 3)

3 = 3 * 1 + 0 which yields 0 = 1 * 3 – 3 * 1 = gcd(3, 1)

1 = 0 * 0 + 1 which yields 1 = 1 * 1 – 0 * 0 = gcd(1, 0) = 1.

Since 1 = 1 * 40 – 13 * 3, then

1 = 1 * 1 - 0 * 0 yields 1 = 1 * (40 – 13 * 3). Linear combination of 40 and 3.

This yields (-13)* 3 = 1 + (-1)*40 .

By definition of congruence modulo n,

(-13)* 3 (mod 40) = (1 mod 40 + (-1)*40 mod 40) mod 40.

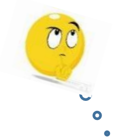
(-13)* 3 ≡ 1(mod 40).

This result implies that -13 is an inverse for 3 mod 40. In symbol, (-13)* 3 ≡ 1(mod 40).

To find a positive inverse, compute 40 -13 which yields 27, and 27 ≡ (−13)(mod 40) because 27 – (-13) = 40. So, by Theorem 0.1.4.3(3. ab ≡ cd (mod n),

27 * 3 ≡ (-13) *3 ≡ (1 mod 40),

and thus by the transitive property of congruence modulo n, 27 is a positive integer that is an inverse for 3 modulo 40.



Example: 0.4.7.1 [another crazy way]

Find a positive inverse for 3 modulo 40.
That is, find a positive integer x such that $3x \equiv 1 \pmod{40}$.
Solution:
Find a linear combination of 3 and 40 that equals 1.

40 = 13 * 3 + 1. This yields 1 = 1 * 40 – 13 * 3. gcd(40, 3)
3 = 3 * 1 + 0. This yields 0 = 1 * 3 – 3 * 1. = gcd(3, 1)
1 = 1 * 0 + 1. This yields 1 = 1 * 1 – 0 * 0. = gcd(1, 0) = 1. (What if?)

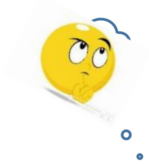
Since 4 * 40 = 53 * 3 + 1, then 1 = 4 * 40 + (-53) * 3 .
by definition of congruence modulo n, and Theorem 0.1.4.1 (modular equivalence)

$$(-53) * 3 \equiv 1 \pmod{40}.$$

This result implies that -53 is an inverse for 3 mod 40. In symbol, $-53 \equiv 3^{-1} \pmod{40}$.
To find a positive inverse, compute -53 + 40 = -13, and then -13 + 40 = 27.

$$27 * 3 \equiv (-13) * 3 \equiv (-53) * 3 \equiv (1 \bmod 40),$$

Then -53, -13 and 27 are the inverse of 3 modulo 40. Therefore, 27 is a positive integer, that is an inverse for 3 modulo 40.



Example 0.52: Compute 11^{-1} mod 25.

What is the multiplicative inverse of 11 modulo 25?
i.e., find x such that $11x \equiv 1 \bmod 25$. equivalently, $25 \mid (11x - 1)$.

$$\begin{aligned}
\gcd(25, 11) &= \gcd(11, 25 \bmod 11) = \gcd(11, 3) \\
&= \gcd(3, 11 \bmod 3) = \gcd(3, 2) \\
&= \gcd(2, 3 \bmod 2) = \gcd(2, 1) \\
&= \gcd(1, 2 \bmod 1) = \gcd(1, 0) = 1.
\end{aligned}$$

Thus, $\gcd(25, 11) = 1$.

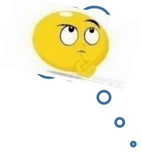
Using extended Euclid's Algorithm, we have

$$\gcd(25, 11) = 15 * \underline{25} + (-34) * \underline{11} = 1,$$

where $a = 25$ and $b = 11$, and $x = 15$ and $y = -34$.

(see example 0.46)

Example 0.52: Compute 11^{-1} mod 25.



…

Reduce both sides of $25 * 15 + 11 * (-34) = 1$ by mod 25.

We have $(25 * 15 + 11 * (-34)) \bmod 25 \equiv 1 \bmod 25$.

$((25 * 15) \bmod 25 + (11 * (-34)) \bmod 25) \bmod 25 \equiv 1 \bmod 25$,

where $25 *15 \bmod 25 = 0$.

$(11 * (-34)) \bmod 25) \bmod 25 \equiv 1 \bmod 25$,

$11 * (-34) \bmod 25 = 1$,

Therefore, 1 is generated by $11*(-34)$ mod 25. [i.e., 25 divides $(-34 * 11 – 1)$].

And we write $-34 * \mathbf{11} \equiv 1 \bmod 25$.

$$-34 \equiv \frac{1}{11} \bmod 25.$$

$$-34 \equiv 11^{-1} \bmod 25.$$

By definition, -34 is the multiplicative inverse of **11** mod 25.

This concludes that -34 is 11^{-1}modulo 25.

Or $-34 + 25 + 25 = 16$ is 11^{-1}modulo 25. QED

Modular division theorem:

GCD(8, 7) = 1 = -6*8 + 7*7 >0

What is 7^{-1} mod 8? Let a = 7 and N = 8. They are relative prime. Then 7 has a multiplicative inverse mod 8. That is, 7 is the multiplicative inverse of 7 mod 8. That is $7 \equiv \frac{1}{7}$ mod 8 and therefore $7 * 7 \equiv 1$ mod 8. We say 7 is the 7^{-1} mod 8.

For any *a* mod N, *a* has a multiplicative inverse modulo N iff it (*a*) is relatively prime to N.

- When this inverse exists, it can be found in time $O(n^3)$ (where n denotes the number of bits of N) by running the extended Euclid algorithm.
- Example: let a = 11 and N = 25. They are relatively prime.
  - Then 11 has a multiplicative inverse mod N.
  - That is, -34 is the multiplicative inverse of 11 mod 25.
    - This means, $-34 \equiv 11^{-1}$ mod 25, which is $-34 \equiv \frac{1}{11}$ mod 25.
    - Therefore -34 * **11** $\equiv$ 1 mod 25.

Primality testing

Cryptography – The RSA Public Key Cryptosystem

The Rivest-Shamir-Adleman (RSA) cryptosystem uses all the ideas we have introduced in this lecture note. It derives very strong guarantees of security by ingeniously exploiting the wide gulf between the polynomial-time computability of certain number-theoretic tasks: (

- modular exponentiation,
- greatest common divisor,
- primality testing) and
- the intractability of others (factoring).