1 Classical Cryptosystems

(Continued from Lecture 2.)

1.1 Interlude: GCDs

Definition 1.1: Greatest Common Divisor

The **greatest common divisor** (or *GCD*) of two integers a and b that are not both zero is denoted $\gcd(a, b)$ and is defined to be the largest integer which is both a divisor of a and a divisor of b.

(Example.) Suppose we wanted to compute $\gcd(14, 21)$.

- The factors of 14 are 1, 2, 7, and 14.
- The factors of 21 are 1, 3, 7, and 21.

Therefore, as 7 is the *largest integer* which is both a divisor of 14 and 21, it follows that $\gcd(14, 21) = 7$.

Note that, while intuitive, this is actually not the best way of finding GCDs. Finding the factors of a number, especially a large one, is difficult. However, there exists algorithms that we can use to quickly calculate GCDs.

(Example.) Suppose a is a nonzero integer. What is $\gcd(a, 0)$?

The answer is $\gcd(a, 0) = |a|$. To see why this is the case, consider the following points.

1. If $a \neq 0$, the largest value that divides a is $|a|$.

   For example, the largest value that divides 100 is $|100| = 100$. Likewise, the largest value that divides -100 is still $|-100| = 100$.

2. If you think about it, all integers divide 0.

   Recall that, if a and b are integers, a divides b if there is an integer c such that

   $$ac = b.$$

   Here, we write that $a|b$ to mean that a divides b.

   With this in mind, we note that

   $$a \cdot 0 = 0$$

   and therefore

   $$a|0.$$

3. Therefore, it follows that $\gcd(a, 0) = |a|$.

   To see this, note that the factors of 10 and -10 are

   $$\{-10, -5, -2, -1, 1, 2, 5, 10\},$$

   and we know that all factors of 0 are effectively all integers. Therefore, it follows that 10 would be the answer here.

1.1.1 Euclidean Algorithm

The Euclidean Algorithm for computing GCDs relies on the following observation, defined as a lemma.

Lemma 1.1

Let n be a positive integer and $a \equiv b \pmod{n}$. Then, $\gcd(a, n) = \gcd(b, n)$.

Proof. Let $c = \gcd(a, n)$ and $d = \gcd(b, n)$. Let k be an integer such that

$$a - b = nk.$$

Since c is a factor of both a and n, it is also a factor of $a - nk = b$. Thus, c is a common factor of both b and n as well, so $c \leq d$ bby definition of d. On the other hand, the same logic shows that d is a common factor of both a and n, so $d \leq c$ and thus $d = c$. □

Corollary 1.1

Let n be a positive integer and let r be the remainder when an integer a is divided by n. Then, $\gcd(a, n) = \gcd(r, n)$.

This brings us to the Euclidean Algorithm:

Suppose a and b are two positive integers, and assume without loss of generality (WLOG) that $b \geq a$. To find $\gcd(a, b)$, we can do the following:

- Divide b by a and let r be the remainder. Then,
  - If $r = 0$, output a.
  - Otherwise, replace b with a and a with r. Then, repeat.

(Example.) Suppose we wanted to compute $\gcd(115, 35)$. We divide the bigger number by the smaller one and get

$$115 = 3 \cdot 35 + 10.$$

The remainder, $r = 10$, is nonzero, so we'll divide again, but this time, we'll divide the dividend (35) by the remainder (10) to get

$$35 = 3 \cdot 10 + 5.$$

The remainder is nonzero again, so we repeat to get

$$10 = 2 \cdot 5 + 0.$$

Since the remainder is 0, we output the dividend: $\boxed{5}$. Therefore,

$$\gcd(115, 35) = 5.$$

(Exercise.) Compute the following GCDs using the Euclidean Algorithm.

- $\gcd(180, 120)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
120	180	$180 = 120q + r$	1	60
60	120	$120 = 60q + r$	2	0

Therefore, the answer must be $\boxed{60}$.

- gcd(180, 81).

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
81	180	$180 = 81q + r$	2	18
18	81	$81 = 18q + r$	4	9
9	18	$18 = 9q + r$	2	0

Therefore, the answer must be $\boxed{9}$.

- gcd(121, 77).

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
77	121	$121 = 77q + r$	1	44
44	77	$77 = 44q + r$	1	33
33	44	$44 = 33q + r$	1	11
11	33	$33 = 11q + r$	3	0

Therefore, the answer must be $\boxed{11}$.

1.1.2 Bezout's Theorem

Theorem 1.1: Bezout's Theorem

Suppose a and b are integers not both 0. Then, $\gcd(a, b)$ can be written as an *integer linear combination* of a and b, i.e., it can be written as $ax + by$ for some integers x and y. Integers x and y such that

$$\gcd(a, b) = ax + by$$

are called **Bezout's coefficients**.

We can use the Euclidean Algorithm to find the Bezout coefficients, as seen in the example below.

(Example.) Suppose we want to find the Bezout coefficients for $\gcd(115, 35)$. Recall the sequence of operations we had to do:

$$115 = 3 \cdot 35 + 10.$$

$$35 = 3 \cdot 10 + 5.$$

$$10 = 2 \cdot 5 + 0.$$

Suppose we rearrange the first and second equations, like so:

$$10 = 115 - 3 \cdot 35.$$

$$5 = 35 - 3 \cdot 10.$$

Plugging in the first equation into the second equation gives us

$$5 = 35 - 3 \cdot (115 - 3 \cdot 35).$$

Simplifying this gives us

$$\begin{aligned} 5 &= 35 - 3 \cdot (115 - 3 \cdot 35) \\ &= 35 - 3(115) + 9(35) \\ &= 10(35) - 3(115). \end{aligned}$$

Notice how we wrote $\gcd(115, 35)$ as an integer linear combination of those two numbers.

Essentially, the steps are as follows:

1. Find the GCD using the Euclidean Algorithm.
2. Rewrite the division for the *last nonzero remainder.*
3. Alternate between substitution for the remainder directly above, and then simplify. Alternatively, start from the last equation with a nonzero remainder and then keep using the equations before that equation (e.g., from equation n, the last equation with a nonzero remainder, substitute equation $n-1$ in the next step. Then, in the next step, substitute equation $n-2$. Keep doing this until you reach equation 1.)

(Example.) Suppose we want to find the Bezout coefficients for $\gcd(240, 46)$.

1. First, let's compute the GCD, keeping note of the sequence of operations we made.

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{b = aq + r}$	$\mathbf{q}$	$\mathbf{r}$
46	240	$240 = 46q + r$	5	10
10	46	$46 = 10q + r$	4	6
6	10	$10 = 6q + r$	1	4
4	6	$6 = 4q + r$	1	2
2	4	$4 = 2q + r$	2	0

This tells us that $\gcd(240, 46) = 2$. The operations we did were

- (Eq. 1) $240 = 46(5) + 10 \implies 10 = 240 - 46 \cdot 5$
- (Eq. 2) $46 = 10(4) + 6 \implies 6 = 46 - 10 \cdot 4$
- (Eq. 3) $10 = 6(1) + 4 \implies 4 = 10 - 6 \cdot 1$
- (Eq. 4) $6 = 4(1) + 2 \implies 2 = 6 - 4 \cdot 1$
- (Eq. 5) $4 = 2(2) + 0$

2. Rewriting the division for the last equation with the nonzero remainder (Eq. 4) gives us $2 = 6 - 4 \cdot 1$.
3. Starting from the division for the last nonzero remainder, let's rewrite it:

$$\begin{aligned}
2 &= 6 - 4 \cdot 1 && \text{From Eq. 4} \\
&= 6 - (\underbrace{10 - 6 \cdot 1}_{\text{Eq. 3}}) \cdot 1 && \text{Substitute Eq. 3} \\
&= 6 - 10 + 6 && \text{Expand} \\
&= 2 \cdot 6 - 1 \cdot 10 && \text{Rewrite to group like terms} \\
&= 2 \cdot (\underbrace{46 - 10 \cdot 4}_{\text{Eq. 2}}) - 1 \cdot 10 && \text{Substitute Eq. 2} \\
&= 2 \cdot 46 - 2 \cdot 10 \cdot 4 - 1 \cdot 10 && \text{Expand} \\
&= 2 \cdot 46 - 8 \cdot 10 - 1 \cdot 10 && \text{Simplify} \\
&= 2 \cdot 46 - 9 \cdot 10 && \text{Rewrite to group like terms} \\
&= 2 \cdot 46 - 9 \cdot (\underbrace{240 - 46 \cdot 5}_{\text{Eq. 1}}) && \text{Substitute Eq. 1} \\
&= 2 \cdot 46 - 9 \cdot 240 + 46 \cdot 5 \cdot 9 && \text{Expand} \\
&= 2 \cdot 46 - 9 \cdot 240 + 46 \cdot 45 && \text{Simplify} \\
&= 47 \cdot 46 - 9 \cdot 240 && \text{Rewrite to group like terms}
\end{aligned}$$

Notice how the Bezout coefficients are 47 and -9.

(Exercise.) Calculate Bezout's coefficients for the following GCDs using the extended Euclidean Algorithm.

- gcd(180, 120).

1. First, compute the GCD. We already did this in a previous exercise, but just to reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
120	180	$180 = 120q + r$	1	60
60	120	$120 = 60q + r$	2	0

Therefore, the GCD is 60. The operations that we did were

- (Eq. 1) $180 = 120(1) + 60 \implies 60 = 180 - 120(1)$
- (Eq. 2) $120 = 60(2) + 0$

2. Next, we just need to rewrite the last equation with a nonzero remainder.

$$180 = 120(1) + 60 \implies 60 = 180 - 120(1)$$

3. Finally, we need to work backwards, substituting the previous equations. Because we only have one operation which resulted in a non-zero remainder, it follows that we only need to do:

$$60 = 180 - 120(1).$$

Therefore, the Bezout coefficients are $\boxed{1}$ and $\boxed{-1}$.

- gcd(180, 81).

1. First, we need to compute the GCD. We already did this in a previous exercise, but to reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
81	180	$180 = 81q + r$	2	18
18	81	$81 = 18q + r$	4	9
9	18	$18 = 9q + r$	2	0

Therefore, the GCD is 9. The operations we did were

- (Eq. 1) $180 = 81(2) + 18 \implies 18 = 180 - 81(2)$
- (Eq. 2) $81 = 18(4) + 9 \implies 9 = 81 - 18(4)$
- (Eq. 3) $18 = 9(2) + 0$

2. Next, we need to rewrite the last equation with a nonzero remainder.

$$81 = 18(4) + 9 \implies 9 = 81 - 18(4).$$

3. Finally, we need to work backwards, substituting the previous equations as needed.

$$\begin{aligned} 9 &= 81 - 18(4) \\ &= 81 - \underbrace{(180 - 81(2))}_{\text{Eq. 1}} \cdot 4 \\ &= 81 - 180(4) + 81(8) \\ &= 81(9) - 180(4) \end{aligned}$$

Therefore, the Bezout coefficients are $\boxed{9}$ and $\boxed{-4}$.

- $\gcd(121, 77)$.

1. First, compute the GCD. To reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
77	121	$121 = 77q + r$	1	44
44	77	$77 = 44q + r$	1	33
33	44	$44 = 33q + r$	1	11
11	33	$33 = 11q + r$	3	0

Therefore, the GCD is 11. The operations that we did were
   - (Eq. 1) $121 = 77(1) + 44 \implies 44 = 121 - 77(1)$
   - (Eq. 2) $77 = 44(1) + 33 \implies 33 = 77 - 44(1)$
   - (Eq. 3) $44 = 33(1) + 11 \implies 11 = 44 - 33(1)$
   - (Eq. 4) $33 = 11(3) + 0$

2. Next, rewrite the last equation with a nonzero remainder.

$$44 = 33(1) + 11 \implies 11 = 44 - 33(1).$$

3. Finally, work backwards.

$$\begin{aligned} 11 &= 44 - 33(1) \\ &= 44 - \underbrace{(77 - 44(1))}_{\text{Eq. 2}} \cdot 1 \\ &= 44 - 77 + 44(1) \\ &= 44(2) - 77 \\ &= \underbrace{(121 - 77(1))}_{\text{Eq. 1}} \cdot 2 - 77 \\ &= 121(2) - 77(2) - 77 \\ &= 121(2) - 77(3). \end{aligned}$$

Thereforem the Bezout coefficients are $\boxed{2}$ and $\boxed{-3}$.

(Exercise.) Observe that $\gcd(42, 12) = 6$. Show taht the pairs $(-1, 4)$ and $(1, -3)$ are both Bezout coefficients for 42 and 12.

- For the pair $(-1, 4)$, we have

$$42(-1) + 12(4) = -42 + 48 = 6.$$

- For the pair $(1, -3)$, we have

$$42(1) + 12(-3) = 42 - 36 = 6.$$

1.1.3 Modular Inversion

Suppose you are asked to solve the equation

$$5z = 7.$$

Intuitively, we can just divide both sides by 5. Stated differently, we can multiply both sides by $\frac{1}{5}$:

$$\left(\frac{1}{5}\right) \cdot 5z = \left(\frac{1}{5}\right) 7 \implies z = \frac{5}{7}.$$

In other words, we're able to "cancel out" the 5 that appears on the left-hand side, thus isolating z.

With modular inversion, we can recreate this process with *congruences*. For example, suppose we want to solve

$$5z \equiv 7 \pmod{11}.$$

We cannot "divide both sides by 5" because congruences only make sense when both sides of the congruence are *integers*. But, if we find an integer x with the property that

$$5x \equiv 1 \pmod{11},$$

then we can multiply both sides of our congruence by x to effectively eliminate the 5 on the left-hand side. In this example, there *is* an integer: $x = 9$. Using this integer, we have

$$5x = 9 \cdot 5 = 45 \equiv 1 \pmod{11}.$$

Therefore, multiplying both sides of our congruence by 9 gives us

$$z = 1 \cdot z \equiv (5 \cdot 9)z = 9 \cdot (5z) \equiv 9 \cdot 7 \pmod{11}.$$

Thus,

$$z \equiv 9 \cdot 7 = 63 \equiv 8 \pmod{11},$$

and we've solved our congruence: $z \equiv 8 \pmod{11}$. While we solved this congruence, note that we basically guessed what the solution is. However, there's a way to get such x.

Definition 1.2

Fix a positive integer n. An integer a is *invertible* mod n (or a *unit* mod n) if there exists another integer x such that $ax \equiv 1 \pmod{n}$. The number x is then called an *inverse of* a mod n and, in symbols, one writes $x \equiv a^{-1} \pmod{n}$.

So, in the above example, we found that $9 \equiv 5^{-1} \pmod{11}$ because $5 \cdot 9 \equiv 1 \pmod{11}$.

(Exercise.) Explain why 2 is not invertible mod 4.

Essentially, we need to show why there does not exist an integer x such that

$$2x \equiv 1 \pmod{4}.$$

However, notice that both 2 and 4 are even. Therefore, multiplying 2 by any integer gives us an even number. Because 4 is even as well, it follows that we'll never be able to find an x such that $2x \equiv 1 \pmod{4}$.

Theorem 1.2: Modular Inversion Theorem

Fix a positive integer n and another integer a. Then, a is invertible mod n if and only if $\gcd(a, n) = 1$. Moreover, if $\gcd(a, n) = 1$ and x and y are Bezout coefficients for a and n, then x is an inverse of a mod n.

(Example.) Suppose we want to find the inverse of 7 (mod 23). Using the Euclidean Algorithm to compute $\gcd(23, 7)$, we get

$$23 = 3 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

So, $\gcd(23, 7) = 1$ and thus 7 is in fact invertible mod 23. Working backwards, we find that

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (23 - 3 \cdot 7) \\ &= 10 \cdot 7 - 3 \cdot 23. \end{aligned}$$

Therefore, the Modular Inversion Theorem tells us that 10 is the inverse of 7 mod 23.

(Exercise.) For each of the following, determine whether a is invertible mod n. If it is, find an inverse of a mod n.

- $a = 14, n = 21$.

First, let's calculate $\gcd(14, 21)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
14	21	$21 = 14q + r$	1	7
7	14	$14 = 7q + r$	2	0

Therefore, $\gcd(14, 21) = 7$. By Theorem (1.2), it follows that 14 is not invertible mod 21.

- $a = 3, n = 7$.

First, we calculate $\gcd(3, 7)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
3	7	$7 = 3q + r$	2	1
1	3	$3 = 1q + r$	3	0

Therefore, $\gcd(3, 7) = 1$. By Theorem (1.2), it follows that 3 is invertible mod 7.

With this in mind, let's find the Bezout coefficients. We note that the equations we used to find the GCD were

- (Eq. 1) $7 = 3(2) + 1 \implies 1 = 7 - 3(2)$
- (Eq. 2) $3 = 1(3) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$7 = 3(2) + 1 \implies 1 = 7 - 3(2).$$

Because we are able to write an equation in terms of 3 and 7, we find that

$$\gcd(3, 7) = 1 = 3(-2) + 7(1).$$

From this, it follows that $x = -2$ and $y = 1$. So, by Theorem (1.2), it follows that -2 is an inverse of 3 (mod 7).

We should note that Bezout coefficients are not unique. If we wanted a positive answer, we note that

$$-2 \equiv 5 \pmod{7}$$

so that another possible answer is $\boxed{5}$.

- $a = 41, n = 50$.

First, we calculate $\gcd(41, 50)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
41	50	$50 = 41q + r$	1	9
9	41	$41 = 9q + r$	4	5
5	9	$9 = 5q + r$	1	4
4	5	$5 = 4q + r$	1	1
1	4	$4 = 1q + r$	4	0

Therefore, $\gcd(41, 50) = 1$. By Theorem (1.2), it follows that 41 is invertible mod 50.

Next, we need to find the Bezout coefficients. We note that the equations we used to find the GCD were

- (Eq. 1) $50 = 41(1) + 9 \implies 9 = 50 - 41(1)$
- (Eq. 2) $41 = 9(4) + 5 \implies 5 = 41 - 9(4)$
- (Eq. 3) $9 = 5(1) + 4 \implies 4 = 9 - 5(1)$
- (Eq. 4) $5 = 4(1) + 1 \implies 1 = 5 - 4(1)$
- (Eq. 5) $4 = 1(4) + 0$

Now, working backwards from the last equation with a nonzero remainder (i.e., Eq. 4):

$$\begin{aligned}
1 &= 5 - 4(1) \\
&= 5 - (\underbrace{9 - 5(1)}_{\text{Eq. 3}})(1) \\
&= 5 - 9 + 5 \\
&= 5(2) - 9 \\
&= (\underbrace{41 - 9(4)}_{\text{Eq. 2}})(2) - 9 \\
&= 41(2) - 9(4)(2) - 9 \\
&= 41(2) - 9(8) - 9 \\
&= 41(2) - 9(9) \\
&= 41(2) - (\underbrace{50 - 41(1)}_{\text{Eq. 1}})(9) \\
&= 41(2) - 50(9) + 41(9) \\
&= 41(11) - 50(9)
\end{aligned}$$

Therefore, we have

$$\gcd(41, 50) = 1 = 41(11) + 50(-9)$$

and so $x = 11$ and $y = -9$. From this, by Theorem (1.2) it follows that $\boxed{11}$ is an inverse of 41 (mod 50).

(Exercise.) Solve the following congruences for z.

- $2z \equiv 3 \pmod{11}$

Trivially, $\gcd(2, 11) = 1$. However, let's find the GCD using the Euclidean Algorithm regardless.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
2	11	$11 = 2q + r$	5	1
1	2	$2 = 1q + r$	2	0

Therefore, the GCD is 1. We can now find the Bezout coefficients. Note that the equations used to find the GCD were

- (Eq. 1) $11 = 2(5) + 1$
- (Eq. 2) $2 = 1(2) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$1 = 11 - 2(5).$$

Immediately, it follows that

$$\gcd(2, 11) = 1 = 11(1) + 2(-5).$$

Hence, by Theorem (1.2), $x = -5 \equiv 6 \pmod{11}$ is the inverse of $2 \pmod{11}$.

With this in mind, we now know that

$$\begin{aligned} & 2z \equiv 3 \pmod{11} \\ & \quad \implies 6(2z) \equiv 6(3) \pmod{11} \\ & \quad \implies 12z \equiv 18 \pmod{11} \\ & \quad \implies z \equiv 7 \pmod{11}. \end{aligned}$$

Therefore, the answer is $z \equiv \boxed{7} \pmod{11}$.

- $3z \equiv 2 \pmod 7$

Using the strategy of trial-and-error, we find that $z \equiv 3 \pmod 7$.

- $5z \equiv 3 \pmod{15}$

We note that $\gcd(5, 15) = 5$. Therefore, by Theorem (1.2), there is no solution that satisfies this congruence.

- $5z \equiv 17 \pmod{101}$

First, we want to find $\gcd(5, 101)$. Using the Euclidean Algorithm gives us:

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{b = aq + r}$	$\mathbf{q}$	$\mathbf{r}$
5	101	$101 = 5q + r$	20	1
1	5	$5 = 1q + r$	5	0

Therefore, the GCD is 1. We can now find the Bezout coefficients. Note that the equations used to find the GCD were

- (Eq. 1) $101 = 5(20) + 1 \implies 1 = 101 - 5(20)$
- (Eq. 2) $5 = 1(5) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$1 = 101 - 5(20).$$

Immediately, it follows that

$$\gcd(5, 101) = 1 = 101(1) + 5(-20).$$

Hence, by Theorem (1.2), $x = -20 \equiv 81 \pmod{11}$ is the inverse of $5 \pmod{101}$.

With this in mind, we now know that

$$\begin{aligned} 5z &\equiv 17 \pmod{101} \\ &\implies 81(5z) \equiv 81(17) \pmod{101} \\ &\implies 405z \equiv 1377 \pmod{101} \\ &\implies z \equiv 64 \pmod{101}. \end{aligned}$$

Therefore, the answer is $z \equiv \boxed{64} \pmod{101}$.

If we use $x = -20$ instead, we have

$$\begin{aligned} 5z &\equiv 17 \pmod{101} \\ &\implies -20(5z) \equiv -20(17) \pmod{101} \\ &\implies -100z \equiv -340 \pmod{101} \\ &\implies z \equiv -340 \pmod{101} \\ &\implies z \equiv 64 \pmod{101}. \end{aligned}$$

So, in summary, given the congruence $az \equiv b \pmod{n}$, the steps for solving for z are as follows:

1. Find $\gcd(a, n)$. If $\gcd(a, n) \neq 1$, then there are no possible solutions.
2. Find the Bezout coefficients for $\gcd(a, n)$. Specifically, for

   $$\gcd(a, n) = ax + ny,$$

   find x (the Bezout coefficients for a). This represents your inverse of $a \pmod{n}$.
3. Multiply both sides of the congruence by x; that is,

   $$x(az) \equiv x(b) \pmod{n},$$

   and then simplify.

As you can tell, Bezout coefficients are not unique, and inverses aren't strictly unique either. Notice, for example, that $3(2) \equiv 1 \pmod{5}$ and $8(2) \equiv 1 \pmod{5}$ so that 8 and 3 are both inverses of $2 \pmod{5}$. However, notice that $8 \equiv 3 \pmod{5}$. In other words, inverses are *kind of* unique when they exist: they are unique mod n.

Lemma 1.2

Fix a positive integer n and suppose a is invertible mod n. If x and x' are both inverses of a mod n, then

$$x \equiv x' \pmod{n}.$$