Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 02
Lecture - 10

Mathematical Background for Cryptography

Hello, recall that cryptography can be used for encrypting information that is sent from a user Alice to a user Bob. So, this encryption helps in ensuring that intruders, say Trudy, are not able to read the messages sent from Alice to Bob. We now discuss some mathematical background for cryptography, and in the following classes, we'll discuss principles of cryptography. We start with modular arithmetic. Let d be an integer and n be a positive integer.

Suppose q is the quotient obtained from dividing d by n, and let r be the remainder obtained when d is divided by n. So, we can write the relationship between d, n, q, and r in the following way. $d = n * q + r, 0 \leq r < n.$ So, this is the dividend d and the divisor is n, q is the quotient and r is the remainder. We say that d is equal to r modulo n if the remainder obtained from dividing d by n is the same as the remainder obtained from dividing r by n. As an example in this equation, we can see that d and r are equal modulo n. So, if d is divided by n, then the remainder is r, and obviously if r is divided by n, then the remainder is r. So, d and r are equal modulo n. Another example is, consider the numbers 13 and 23.

These numbers are equal modulo 10. The remainder when 13 is divided by 10 is 3, and the remainder when 23 is divided by 10 is also 3. So, these numbers are equal modulo 10. So, this is expressed as $r \equiv d \ (mod\ n).$ Now, a claim is that for given values of n and r, there are infinite number of (d, q) pairs that satisfy equation 1). So, if you are given n and r, then we can find an infinite number of d and q which satisfy this equation.

That's because if a particular d satisfies this equation, then d + n also satisfies that equation. d + 2n also satisfies this equation, and so on and so forth. As an example, let n be 10 and r be 3. Then 13, 23, 33, and so on all satisfy this equation 1), with corresponding quotients being 1, 2, 3, and so on. In fact, each element of the following set satisfies equation 2).

So, consider this set consisting of elements which are listed here, -37 and elements before it, for example, -47, -57, and so on, and so forth, up to 23, 33, 43, and so on. So, all of these satisfy equation 2). Any two numbers in this set are said to be congruent modulo 10, and the set itself is referred to as a congruence class. Now, a simple fact is that if two integers are congruent modulo n, then they differ by an integral multiple of n. A proof of this fact is as follows. Suppose $a \ mod \ n = r$ and $b \ mod \ n = r$. So, a and b are two integers, which are congruent modulo n since they have the same remainder when divided by n.

Now, we have to show that the difference between a and b is an integral multiple of n. So, let us find out a - b. First, we write by definition of modular operation we can express a as, $a = n * q_1 + r$ and b as, $b = n * q_2 + r$, where q1 and q2 are some integers, which are the quotients. Now, let us take the difference between a and b. If we subtract these two equations, then we get: $a - b = n \ (q_1 - q_2)$ because r cancels off. So, from this we can see that the difference between a and b is an integer multiple of n, since q1 and q2 are integers. So, this proves the fact that if two integers are congruent modulo n, then they differ by an integral multiple of n. Here are some simple properties of modulo arithmetic, which are left as an exercise.

The claim is that, for arbitrary integers a, b, and $n > 0, (a + b) \ mod \ n = \big((a \ mod \ n) + (b \ mod \ n)\big) \ mod \ n.$

Similarly for subtraction, $(a - b) \ mod \ n = \big((a \ mod \ n) - \ (b \ mod \ n)\big) \ mod \ n.$ And for multiplication, $(a * b) \ mod \ n = \big((a \ mod \ n) * \ (b \ mod \ n)\big) \ mod \ n.$ These properties are easy to prove, and a simple exercise is to verify that these properties are true. Next, we review the concept of greatest common divisor (GCD). Given two non-negative integers a and b, we say that a divides b, and this is denoted by $a|b$, if there exists an integer $x \ \geq 1$ such that $a * x = b$. So, $a|b$ denotes that a divides b. In this case, a is said to be a divisor of b. Now, the definition of GCD is as follows. If a divides b and a divides c and there is no integer $a' > a$, such that $a'|b$ and $a'|c$, then a is referred to as the GCD of b and c. And this is denoted by $a = \gcd(b, c)$. So a is the greatest integer which divides b and c. So, it is the greatest common divisor.

An example is that the GCD of 24 and 78 can be found by inspection, and it is 6. Another definition is that if the $\gcd(b, c) = 1$, then we say that b and c are relatively prime, also known as co-prime numbers. A positive integer is prime if it is co-prime with all the positive integers less than it. Another way to say the same thing is that a positive integer is prime if it has only two distinct factors: the number itself and 1. So, this is an equivalent definition.

For example, the integers 14 and 9 are co-prime because their GCD is 1, but neither is a prime number. So, for example, 14 has factors 7 and 2, and 9 has a factor 3. So, they have factors other than the number itself and 1. So, they are not prime, but these integers have a GCD of 1, so they are co-prime. We now discuss Euclid's algorithm.

Euclid's algorithm can be used to find the GCD of two integers b and c. Without loss of generality, let $b > c$. The first step is to divide b by c, explicitly showing the quotient q and the remainder r. So, we write the following: $b = c * q + r$. Then, in every following step, we write a similar equation that is illustrated by this example here. In this example, we compute the GCD of 161 and 112. So, 161 is the number b in this example, and 112 is the number c in this example. In the first step, as we said, we write $b = c * q + r$. The quotient q is 1, and the remainder r is 49. Then, in the next step, the new dividend, which is the leftmost number, that is, 112.

And the new divisor, which is this number 49 to the right of the equal sign, these are respectively, the divisor and the remainder from the previous step. So, the divisor from the previous step that is 112 becomes the dividend now, and the remainder from the previous step, 49, now becomes the divisor. So, we write an equation similar to that in step 1. 112 equals 49 into 2 plus 14. 2 is the quotient, and 14 is the remainder.

Then again, the divisor 49 now becomes the dividend in step 3, and the remainder 14 becomes the divisor in step 3, and we write a similar equation, and so on and so forth. Then again, 14, which is the divisor in step 3 that becomes the dividend in the next step, and 7, which is the remainder, becomes the divisor in the next step. So, we will continue this process. So, it's easy to verify that the sequence of remainders keeps decreasing. So, the remainder in the first step is 49, then in the next step it's 14, then 7, and then 0.

Since the remainder is a non-negative integer, the sequence is finite. So, after a finite number of steps, the sequence ends, and we get a remainder of 0. But the question is; does the sequence always end with a remainder of 0? So, the claim is yes, the last remainder is always 0 because if not, then we can do another division and continue this until we get a remainder of 0. Eventually the remainder will become 0, or the remainder will be 0, in which case, we'll do another division and then the remainder will become 0.

So, the last remainder is always 0. So, the sequence of divisions continues until the remainder of 0 is encountered. Now, the following are two key observations about the above procedure. So, we have to show that this procedure indeed provides the gcd(b,c). So, we'll show that using the following two observations. The first observation is the following.

gcd(b,c) divides every non-zero remainder. So, in this example, we'll see that the gcd(161,112) is 7. We can see that 7 divides 49, 7 divides 14, and 7 divides 7. So, the GCD divides every non-zero remainder. Now, let us prove this property.

Consider dividing each term of the equation in step 1 by the gcd(b,c). So, consider the gcd(b,c), whatever it is. This is b; this is c. If we divide this equation throughout by gcd(b,c), then we will get a positive integer here. We will get a positive integer here. So, this is an integer, and this is an integer. So, if we divide this remainder by gcd(b, c), then we must get another integer.

Otherwise, if we don't get an integer by dividing this by gcd(b, c), then it would mean that a fraction equals some integer, which is not possible. So, hence, it follows that this 49 is divisible by gcd(b,c). So, gcd(b,c) divides this remainder. Now, consider step 2. Here we have shown that 49 is divisible by gcd(b,c) and 112 is divisible by gcd(b,c), since this is c itself. So, again, we can divide throughout by gcd(b,c), and that leads us to infer that 14 is divisible by gcd(b,c). And we can repeat this procedure, and that proves this claim that gcd(b,c) divides every non-zero remainder in this sequence. So, this proves the statement in 1), that is, gcd(b,c) divides each non-zero remainder.

Now, another observation is the following. The remainder just above the zero in this procedure is gcd(b,c). So, in this example, 7 is the gcd(161,112). We now prove this property. Let $g = \text{gcd}(b, c)$. So, we have shown that every remainder in this sequence is divisible by gcd(b, c).

So, hence, this remainder just above the 0 is divisible by gcd(b,c). So, hence, there are only two possibilities: either the remainder equals g itself, or it is a multiple of g, say $k_1 * g$, where k_1 is some positive integer which is greater than 1. Now, we'll show that k_1 is actually 1. The divisor in the penultimate step is a multiple of g, say $k_2 * g$, where $k_2 > k_1$. The last step can then be expressed as follows.

$k_2 * g = k_1 * g * q'$, where q' is the quotient in the last step. So, g cancels off in this equation, and we get $k_2 = k_1 * q'$. Now, the claim is thatgcd$(k_1, k_2) = 1$. So, to see this, if thegcd$(k_1, k_2) \neq 1$, if it is greater than 1, then gcd$(k_1, k_2) * g$ divides both the remainder and divisor in the penultimate step. So, in this example, $\gcd(k_1, k_2) * g$ gcd(k1, k2), divides 14 as well as 7.

And hence, dividing this equation throughout by$\gcd(k_1, k_2) * g$, we get that$\gcd(k_1, k_2) * g$ divides 49 as well. And again, then, in this equation, $\gcd(k_1, k_2) * g$ divides 49 as well as 14, so it divides 112 as well. And then, in this equation, it divides 112 by 49, and hence, it divides 161. So, hence, since $\gcd(k_1, k_2) * g$ divides 161 as well as 112, it follows that the $\gcd(b, c) > g$. It is equal to $\gcd(k_1, k_2) * g$. So, that is the contradiction. So, hence, $\gcd(k_1, k_2)$ must be equal to 1.

Now, since $k_2 = k_1 * q'$, the $\gcd(k_1, k_2) = k_1$. That's because $q' \geq 1$. So, from this equation, it follows that $\gcd(k_1, k_2) = k_1$.

Now, since $\gcd(k_1, k_2) = k_1$ and $\gcd(k_1, k_2) = 1$, it follows that $k_1 = 1$. So, hence, this claim is true that the remainder just above the 0 is gcd(b, c).

So, hence, we have proved that Euclid's algorithm indeed finds the GCD of numbers b and c. So, this sequence of steps to compute the GCD of two integers is called Euclid's algorithm. We now discuss another useful result, that is, the GCD theorem. So, again, recall this procedure: Euclid's Algorithm. Given two integers b and c, there exist two integers x and y such that $b * x + c * y = \gcd(b, c)$. So, we demonstrate this theorem by an example.

Suppose, again, that b is 161 and c is 112. Then, from step 3, we can write the following. So, $7 = 49 - 14 * 3$; that follows from step 3. We want to eliminate 14 from this equation. So, we can substitute 14 for it in this equation.

That is Step 2. We substitute 14 from step 2 into this equation to get the following. $7 = 19 - (112 - 49 * 2) * 3$. So, we can multiply out this 3 to get the following. $7 = 49 * 7 + 112 * (-3)$.

Now, we want to eliminate 49 from this equation. So, we substitute 49 from step 1 to get the following. $7 = (161 - 112 * 1) * 7 + 112 * (= 3)$. So, substituting for 49 from step 1, we get this equation. Now, this can be rewritten in the following way: $161 * 7 + 112 * (-10) = 7$.

Notice that this equation is of the form $b * x + c * y = \gcd(b, c)$, where x is 7 and y is minus 10 and the$\gcd(b, c) = 7$. In this way, we have found out these integers x and y, such that $b * x + c * y = \gcd(b, c)$. So, this is a useful corollary of the GCD theorem. If b and c are relatively prime, then there exists integers x and y, such that $b * x + c * y = 1$. So, this corollary follows because if b and c are relatively prime, then their GCD is 1. So, in this equation, the GCD just becomes 1.

So, hence, there exists integers x and y, such that $b * x + c * y = 1$. So, in cryptography, we often need to compute the multiplicative inverses modulo a prime number. In particular, suppose n is a prime number. The multiplicative inverse of a number ‘a’, modulo prime number n is defined to be a number b, such that $a * b \; mod \; n = 1$. So, the multiplicative inverse of a modulo n is a number b, such that $a * b \; mod \; n = 1$.

Now, corollary 1 can be used to obtain the inverse of c modulo a prime number b. So, this can be done as follows. Since $c * x$ differs from 1 by an integer multiple of b, $c * y \equiv 1 (mod \; b)$. So, we can take modulo b throughout this equation. So, $b * x \; mod \; b = 0$ since $b * x$ is a multiple of b. So, taking modulo b throughout this equation, we get that $c * y \; mod \; b = 1$. Hence, y mod b is the inverse of c, so from this equation we can find out the multiplicative inverse of c mod b, so the multiplicative inverse is y mod b. So, hence, this is a useful corollary given numbers b and c, where b is prime; we can find the multiplicative inverse of a number c modulo b.

And that can be done by first finding integers x and y such that $b * x + c * y = 1$. And then, noting that y mod b is the multiplicative inverse of c. The formal procedure to obtain the inverse of c modulo b is called the extended Euclidean algorithm. And this is an automated version of this example. We won't discuss the details, but it is evident from here that we can easily extend this procedure to find the multiplicative inverse of any number. We'll use this fact later on when we discuss the RSS scheme for cryptography, which is a cryptographic scheme.

So, we'll use this fact later on in that context. Next, we discuss the Chinese Remainder Theorem. It is used to prove several results in cryptography. Suppose we want to solve the following set of equations: $x \; mod \; 5 = 2$, and $x \; mod \; 7 = 3$.

This is an example where the Chinese Remainder Theorem is applicable. First we note that, if x is a solution to this set of equations, then x + 35k is also a solution for every integer k. That's because we note that $(x + 35k) \; mod \; 5 = x \; mod \; 5$. That is because $35k \; mod \; 5 = 0$ and similarly, $(x + 35k) \; mod \; 7 = x \; mod \; 7$, so x + 35k is also a solution for every integer k. So, hence, this is an infinite number of solutions. But is there a unique solution modulo 35?

So, in the range of integers from 0 to 34, is there a unique solution? It follows from the Chinese Remainder Theorem that the answer is yes. Now, by inspection, we can see that the solution to the above set of equations is 17 because $17\ mod\ 5 = 2$ and $17\ mod\ 7 = 3$. The Chinese Remainder Theorem implies that this is a unique solution modulo 35. Now, this is the formal statement of the Chinese Remainder Theorem.

Suppose $n_1, n_2, \dots, n_k$ are relatively prime numbers where k is a positive integer, and let $N = n_1 * n_2 * \dots * n_k$. Consider the following set of equations: $x\ mod\ n_1 = x_1, x\ mod\ n_2 = x_2$, and so on and so forth, up to $x\ mod\ n_k = x_k$. The claim is that this set of equations has a unique solution for x modulo N. An example of the Chinese Remainder Theorem is this set of equations, which we discussed earlier. In this case, n_1 was 5 and n_2 was 7, and N was 35. So, this system of equations has a unique solution for $x\ mod\ n$.

To gain more insight into the Chinese Remainder Theorem, we'll demonstrate the existence of such a number x, which satisfies all these equations. We won't prove the uniqueness of x. So, to see a proof of the uniqueness of x, you can refer to a textbook on number theory. But we'll show that we can construct a number x which satisfies all these equations. Consider the factorization of an integer N. N can be written as: $N = n_1 * n_2 * \dots * n_k$, where $n_1, n_2, \dots, n_k$ are pairwise relatively prime.

That is the $\gcd(n_i, n_j) = 1, 1 \leq i, j \leq k, i \neq j$. Now, let Z_n denote the set of integers $\{0, 1, \dots, n - 1\}$. Consider the mapping $f: Z_N \rightarrow Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$.

This mapping is defined by $f(x) = (x\ mod\ n_1, x\ mod\ n_2, \dots, x\ mod\ n_k)$. Here, $0 \leq x < N$ and f(x) is the set of remainders that are obtained by dividing x by $n_1, n_2, \dots, n_k$. Here is an example: let N be 30, and suppose n_1 is 6 and n_2 is 5.

The function $f(i), 0 \leq i > 30$ is shown below. So, offline, you can take a look at these values of f and verify that they are indeed true. As an example, if $f(0) = (0,0)$ that's because $0\ mod\ 6 = 0$ and $0\ mod\ 6 = 0$.

As another example, $f(19) = (1,4)$ because $19\ mod\ 6 = 1$ and $19\ mod\ 5 = 4$; hence, $f(19) = (1,4)$. So, this shows the function f for different values of i.

It refers to compute f(x) given an x that is, given x; we can find $x\ mod\ n_1, x\ mod\ n_2, \dots, x\ mod\ n_k$. So, this list is the function f(x). But consider the reverse: suppose we are given a tuple in $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$.

So, this tuple is the set of remainders when some number x is divided by $n_1, n_2,$ and so on. So, how do we get the number x whose remainders these are? More fundamentally, if we are given a tuple $(x_1, x_2, \dots, x_k)$, which are the remainders when a certain number is divided by $n_1, n_2, \dots, n_k$, then does there exist an $x \in Z_n$ such that $f(x) = (x_1, x_2, \dots, x_k)$? That is, does there exist an x such that $x \ mod \ n_1 = x_1, x \ mod \ n_2 = x_2, \dots, x \ mod \ n_k = x_k$?

So, we now show that such a reverse mapping does indeed exist. We'll demonstrate the existence of an x, which has remainders $x_1, x_2, \dots, x_k$, when divided by the numbers $n_1, n_2, \dots, n_k$. Let $a_i = N/n_i$. Note that n_i is a factor of N; hence, a_i is an integer for every $1 \leq i \leq k$. Let α_i be the inverse of a_i in the modulo n_i sense; that is, $\alpha_i \times a_i = 1 \ (mod \ n_i)$. Now, we are given a tuple $(x_1, x_2, \dots, x_k)$.

Consider the following number. $x = (x_1 \times a_1 \times \alpha_1 + \cdots + x_k \times a_k \times \alpha_k) \ mod \ N$. So, x is defined to be this. We claim that $f(x) = (x_1, x_2, \dots, x_k)$. So, to verify this claim, first, note that this quantity, $(x_1 \times a_1 \times \alpha_1 + \cdots + x_k \times a_k \times \alpha_k) \ mod \ n_i = x_i$. So, it is easy to verify that this $x \ mod \ n_i$ is the same as this quantity, $(x_1 \times a_1 \times \alpha_1 + \cdots + x_k \times a_k \times \alpha_k) \ mod \ n_i$ because n is a multiple of n_i.

Now, the claim is that this $(x_1 \times a_1 \times \alpha_1 + \cdots + x_k \times a_k \times \alpha_k) \ mod \ n_i = x_i$. So, to show that this is indeed true, for a given value of n_i , this term $(x_i \times a_i \times \alpha_i) \ mod \ n_i = x_i$ because$(a_i \times \alpha_i) \ mod \ n_i = 1$ because a_i and α_i are inverses modulo n_i. So, one of the terms, the i^{th} term in this parenthesis, that the i^{th} term $mod \ n_i = x_i$. And the other terms have this form: $(x_j \times a_j \times \alpha_j) \ mod \ n_i, i \neq j$. So, they are each 0 because by construction each a_j has n_i as a factor. Recall that $a_j = N/n_j$.

So, $a_j = \frac{N}{n_j}$. And recall that $N = n_1 \times n_2 \times \cdots \times n_k$.

So, hence, it follows that a_j has n_i as a factor, so, in summary, this x, which is defined in this way, this has remainders $x_1, x_2, \dots, x_k$ when divided by the integers $n_1, n_2, \dots, n_k$. So, because of this result, we have proved a part of the Chinese remainder theorem, that is, there exists an x, which has remainders $x_1, x_2, \dots, x_k$ corresponding to the $n_1, n_2, \dots, n_k$. So, we have not shown the uniqueness of this x. That part we have omitted. Here is an example.

Let $N = 210$, and $n_1 = 5, n_2 = 6,$ and $n_3 = 7$. So, we see that $n_1, n_2,$ and n_3 are relatively prime. We want to compute $f^{-1}(3,5,2)$. That is, we are given that $x_1 = 3, x_2 = 5,$ and $x_3 = 2$. So, we want an x such that $x \ mod \ 5 = 3, x \ mod \ 6 = 5,$ and $x \ mod \ 7 = 2$.

So, we use the above procedure. First, we find $a_1 = \frac{N}{n_1} = 42, a_2 = \frac{N}{n_2} = 35, a_3 = \frac{N}{n_3} = 30.$

Now, the inverses are as follows: $\alpha_1 = 42^{-1}(mod\ 5) = 3$; you can check that this inverse is 3. Notice that $(42\ \times 3) mod\ 5 = 126\ mod\ 5 = 1$, so hence, 3 is the multiplicative inverse of 42. Similarly, $35^{-1}(mod\ 6) = 5$, and $30^{-1}(mod\ 7) = 4$. Now, let x be this expression, which we discussed earlier.

Now, let us substitute all the quantities that appear in this expression. So, substituting and then simplifying, we get 1493 mod 210, and that turns out to be 23. We can verify that $23\ mod\ 5 = 3, 23\ mod\ 6 = 5,$ and $23\ mod\ 7 = 2$. So, the remainders are 3, 5, and 2, as required. So, this is an illustration of the Chinese Remainder Theorem.

This concludes our review of mathematical background for cryptography. In the next few lectures, we will discuss the principles of cryptography. Thank you.