Lecture Notes on Modular Arithmetic, CM3110

Corresponds to Section 1.4 in the main textbook ("Understanding Cryptography").

Contents

Modular reduction or "Bringing a number back into range" 2

What is 435 mod 13? 2

What if the original number is negative? For example, what is -11 mod 13? 2

Another way of writing mod 2

Modular addition, subtraction, multiplication 3

What is 12 + 7 mod 8? What about 7 – 12 mod 9? And 29*15 mod 13? 3

What if the numbers are large? Do we really have to multiply 29*15 and only then do modular reduction? 3

What is 3^100 mod 13? 3

Modular division and multiplicative inverses 4

What is 5/7 mod 13? Can we just do it as before, i.e. do a normal division and then do modular reduction? 4

What is 7^{-1}mod 11? We already computed 7^{-1}mod 13, isn't it the same? 5

Modular reduction or "Bringing a number back into range"

What is 435 mod 13?

When we do calculations "mod 13", all the end results that we find must be "in-range" for mod 13, i.e. the result must be one of the numbers 0, 1, 2, …, 10, 11, 12. For "mod 71" the range would be 0, 1, 2, …, 69, 70, i.e. from 0 up to one less than 71. In general, for "mod *m*" the range is 0, 1, 2, …, *m*-1, where *m* is called the **modulus** and it must be **a positive number**.

How do we bring a number back into range? This process is called **modular reduction**, or **reduction modulo m**.

There are two ways to do modular reduction; they both give the same result.
Example for 435 mod 13:

1. Long division. Divide 435 by 13 and keep the remainder.
2. Subtract multiples of 13 from 435 until the result is "in-range". For example, 30*13 = 390 is a multiple of 13, so we subtract it from 435, and we get 435 - 390 = 45. But 45 is not yet in range, so we keep going. Another multiple of 13 is 3 *13 = 39, so we subtract 45 – 39 = 6. Now we are done, because 6 is in range. So, we write **435 mod 13 = 6**.

What if the original number is negative? For example, what is -11 mod 13?

Long division and finding remainders with negative numbers is less intuitive, so we go with the second option, but we **add** multiples of 13 until the result is in range (instead of subtracting as we did before). For -11 mod 13, we just need to add 13 to -11 to bring it into range, because -11 + 13 = 2, and 2 is in range. So, we write **-11 mod 13 = 2**.

Another way of writing mod

An equivalent way of writing **435 mod 13 = 6** is **435 ≡ 6 mod 13**, or similarly for **-11 mod 13 = 2** we can write **-11 ≡ 2 mod 13**. We read it as "-11 is equivalent to 2 modulo 13".

Modular addition, subtraction, multiplication

What is 12 + 7 mod 8? What about 7 – 12 mod 9? And 29*15 mod 13?

To perform modular addition/subtraction/multiplication, we just add/subtract/multiply the numbers as usual and then we do modular reduction (bring the number back into range).
So:
12 + 7 mod 8 = 19 mod 8 = 3 (subtract 2*8=16 from 19)
7 – 21 mod 9 = -14 mod 9 = 4 (add 2*9 = 18 to -14)
29*15 mod 13 = 435 mod 13 = 6 (see earlier example).

What if the numbers are large? Do we really have to multiply 29*15 and only then do modular reduction?

We can apply the modular reduction to each term separately and only then add/subtract/multiply as usual.
So:
29*15 mod 13 =
(Apply mod 13 to each of 29 and 15 separately. 29 mod 13 = 3, 15 mod 13 = 2)
3 *2 mod 13 = 6 mod 13 = 6

What is 3^100 mod 13?

The previous trick is particularly useful when doing exponentiation (which is just repeated multiplication). To compute 3^100 mod 13, we don't really want to compute 3^100 first. So, we start multiplying 3*3*3… until we first exceed the modulus (13). In this case, 3*3=9, and 3*3*3=27, so we exceed the modulus after 3 multiplications. We then immediately do a modular reduction to keep the numbers small: 27 mod 13 = 1.

In principle, we have to continue multiplying until we multiply all 100 terms. But here we notice a pattern: If we multiply a triplet of 3s and do reduction mod 13, the result is 1. So, in a sense, this triplet "disappears" from the product. If we keep doing this with one triplet after the other, we will make 33 triplets disappear (because there are 33 triplets in 100 numbers) and there will be just one term left.
So: **3^100 mod 13 = 3**.

Modular division and multiplicative inverses

What is 5/7 mod 13? Can we just do it as before, i.e. do a normal division and then do modular reduction?

Modular division is done in two steps. Example for 5/7 mod 13:
Step 1:
Find the "multiplicative inverse" of 7 (of the denominator, i.e. the number we divide by) for the modulus 13. This is written **7^{-1} mod 13**, but 7^{-1} is just a symbol, there is no raising to the power -1 here. The inverse of a number exists only if the number (7 in our case) and the modulus (13 in our case) share no common factors. 7 and 13 indeed share no common factors, so we can look for the inverse of 7.
The inverse is one of the in-range elements, i.e. 0, 1, 2, …, 12 for modulus 13. We do modular multiplication of each of them by 7. If the result is 1, then we are done, and that number is the inverse. If the result is not 1, then we continue with the next number.
So:
7 * 0 mod 13 = 0 (not equal to 1, so we continue)
7 * 1 mod 13 = 7 (not equal to 1, so we continue)
7 * 2 mod 13 = 14 mod 13 = 1 (equal to 1, so we stop)

7^{-1} mod 13 = 2

Step 2:
Now that we have the inverse, we just need to do modular multiplication. We multiply the inverse by the numerator (5 in our case) and do modular reduction on the result.
So:
5/7 mod 13 =
5 * (7^{-1} mod 13) mod 13 =
5 * 2 mod 13 =
10 mod 13 =10

What is 6^{-1} mod 9? It does not exist!

We said that the multiplicative inverse only exists if the numbers (7 and 13 in our example) share no common factors. Here is what happens when they do share a common factor:

So, what is 6^{-1} mod 9? It does not exist, because 6 and 9 share 3 as a factor:
6*0 mod 9 = 0 (not equal to 1, so we continue)
6*1 mod 9 = 6 (…)
6*2 mod 9 = 12 mod 9 = 3
6*3 mod 9 = 18 mod 9 = 0
6*4 mod 9 = 24 mod 9 = 6
6*5 mod 9 = 30 mod 9 = 3
6*6 mod 9 = 36 mod 9 = 0
6*7 mod 9 = 42 mod 9 = 6
6*8 mod 9 = 48 mod 9 = 3

So we have run out of candidates (the candidates are 0, 1, …, 7, 8, because the modulus is 9), and the result was never 1. Therefore, there is no multiplicative inverse of 6 for modulus 9.

Greatest common divisor

The largest common factor shared by two numbers is their **greatest common divisor** (gcd). For example gcd(7,13)=1, because they share no common factors. But gcd(6,9) = 3. So, we can say that an integer *X* has a multiplicative inverse for modulus *m*, only if gcd(X, m) = 1.

For a particular modulus m, how many integers between 0 and m-1 have a multiplicative inverse?

There is a special notation for "the number of integers between 0 and *m*-1 whose gcd with *m* is 1", or equivalently "the number of integers between 0 and *m*-1 that have a multiplicative inverse for modulus *m*". This notation is **ϕ(m)**, pronounced "phi of m". For example, ϕ(5) = 4 because 1,2,3, and 4 (4 integers in total) have a gcd of 1 with 5. But ϕ(6) = 2, because only 1 and 5 have a gcd of 1 with 6.

What is 7^{-1}mod 11? We already computed 7^{-1}mod 13, isn't it the same?

We need to specify **both** the number **and** the modulus to compute the inverse.
7 * 0 mod 11 = 0
7 * 1 mod 11 = 7
7 * 2 mod 11 = 3
7 * 3 mod 11 = 10
7 * 4 mod 11 = 6
7 * 5 mod 11 = 2
7 * 6 mod 11 = 9
7 * 7 mod 11 = 5
7 * 8 mod 11 = 1
So:
7^{-1}mod 11 = 8, whereas 7^{-1}mod 13 = 2.