Some facts about polynomials modulo m

(Full proof of the Fingerprinting Theorem)

In order to understand the details of the "Fingerprinting Theorem" on fingerprints of different texts from Chapter 19 of the book „Algorithms Unplugged“ [AU2011], you have to look at "polynomials modulo m". For this you need a little patience, and you should not be afraid of a fumbling around with variables, unknowns, integers, and prime numbers. The award in the end is a full proof of the theorem.

We have calculated a fingerprint for a text $(a_1, \ldots, a_n)$ (of numbers between 0 and $m-1$) as follows:

$$(a_1 \cdot r^n + a_2 \cdot r^{n-1} + \cdots + a_{n-1} \cdot r + a_n \cdot r) \bmod m. \tag{1}$$

Here r was a number between 1 and $m-1$. However, $r = 0$ is also allowed, it only always gives the result 0.

Let us look a little more closely at expressions as in (1). Since we don't know in advance which r is to be substituted, we write a symbol "x" in place of r, a "variable". In this way we enter the world of "polynomials".

Polynomials modulo m

Let us look at $m = 17$ as an example. Then mod-m-polynomials are expressions like

$$10x^4 + 14x + 2 \quad \text{or} \quad x^3 + 2x \quad \text{or} \quad x^{10} + 7.$$

This means there are powers

$$x^0 = 1, x^1 = x, x^2, x^3, x^4, \ldots,$$

of a symbol x (the *variable*). Among these powers there is the expression x^0, to be read as "1" and to be omitted when it appears as a factor: $2 \cdot x^0 = 2$. Instead of x^1 we write x. Such powers of x we can multiply with numbers c between 0 and $m-1$ to obtain *terms* cx^j. The factor c here is then called a *coefficient*. We get polynomials by adding arbitrary terms with different powers of x. In order not to get confused we normally order the terms according to falling powers of x, but we may also write $5x + 3x^2 + 1$ or $5x + 2x^2 + 1 + x^2$: these are just a different way of writing $3x^2 + 5x + 1$.

If we are given an expression like

$$2x^4 - 3x^3 + 30x^2 + 3$$

that is not really a polynomial modulo 17, because coefficients that are negative or larger than 16 are illegal, we may just take all numbers modulo 17 to obtain a proper mod-17-polynomial:

$$2x^4 + 14x^3 + 13x^2 + 3.$$

The *general* format for a mod-m-polynomial is the following:

$$c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \cdots + c_2 \cdot x^2 + c_1 \cdot x + c_0. \tag{2}$$

Here $c_n, \ldots, c_0$ are numbers between 0 and $m - 1$ (endpoints included).[1]

It is interesting to note that if one wants to calculate with polynomials there is no need to deal with the "x" and its powers at all. One just stores the numbers $c_0, c_1, \ldots, c_n$, e. g. in an array `C[0..`n`]`, and has the complete information.

Arithmetic for mod-m-polynomials

With mod-m-polynomials we can carry out the arithmetic operations **addition**, **subtraction**, and **multiplication**. This is very easy, if one just applies the standard rules for placing things outside brackets or multiplying out products of sums. With coefficients we always calculate modulo m.

Addition: We **add** two mod-m-polynomials by calculating as if x was just some unknown and collect terms that have the same power of x in them. The coefficients in these terms are added – of course modulo m. For example ($m = 17$):

$$(2x^4 + 3x^3 + 10x + 3) + (3x^5 + 14x^3 + 10x + 4) = 3x^5 + 2x^4 + 3x + 7.$$

(The summand with x^3 disappears, because $(3 + 14) \bmod 17 = 0$.)

Subtraction: We proceed in a way very similar to addition. For example:

$$(10x^3 + 3x + 2) - (x^3 + 2x + 13) = 9x^3 + x + 6.$$

[1] In comparison to (1) the numbering of the terms is reversed and a summand c_0 has been added.

We subtract the coefficients that come with the same powers of x, always thinking modulo m. One can avoid subtraction or the use of negative numbers by first replacing coefficient c by $m - c$ in the polynomial to be subtracted, and add the resulting polynomial. In the example from above the calculation then runs as follows:

$$(10x^3 + 3x + 2) + (16x^3 + 15x + 4) = 9x^3 + x + 6.$$

A special situation occurs if one subtracts a polynomial from itself:

$$(10x^3 + 3x + 2) - (10x^3 + 3x + 2) = (10x^3 + 3x + 2) + (7x^3 + 14x + 15) = 0.$$

The result is a polynomial in which all powers of x have a coefficient that is 0. This polynomial is called the *zero polynomial.* Although normally one would not really like to deal with such a strange thing that tells us “nothing”, we will see that the zero polynomial is very special and it is very important for our purpose that we recognize it when it shows up.

Multiplication: In order to multiply two polynomials (modulo m) we multiply out and then collect terms with the same power of x. For example:

$$\begin{aligned} &(10x^4 + 3x + 2) \cdot (x^3 + 2x + 13) \\ (3) \qquad = \;& (10x^7 + 3x^5 + 11x^4) + (3x^4 + 6x^2 + 5x) + (2x^3 + 4x + 9) \\ = \;& 10x^7 + 3x^5 + 14x^4 + 2x^3 + 6x^2 + 9x + 9. \end{aligned}$$

Is there also a division for polynomials? Yes, but that is a little more complicated.

Division: After the result of the multiplication from (3) we will certainly write (always modulo m):

$$(10x^7 + 3x^5 + 14x^4 + 2x^3 + 6x^2 + 9x + 9) : (x^3 + 2x + 13) = 10x^4 + 3x + 2.$$

Somtimes however (well, actually more often than not) it “doesn’t add up”. Just as with ordinary numbers we then do “division with remainder”. We don’t want to run into problems with dividing numbers modulo m, so as divisors we admit only polynomials in which the highest power of x appears with a coefficient of 1. For example, $x^{10} + 5$ is admissible as divisor, but $10x^2 + 3x + 1$ is not.

The remainder in polynomial division is again a polynomial whose highest power of x is smaller than the highest power of x that occurs in the divisor.

Exampe: We have (modulo 17)

$$(2x+5)\cdot(x^2+4)+(2x+4)=2x^3+5x^2+10x+7,$$

and so we write

$$(2x^3+5x^2+10x+7):(x^2+4)=(x^2+4) \text{ with remainder } 2x+4. \tag{4}$$

There is even an algorithm for dividing a polynomial f by a polynomial g, which always calculates the quotient polynomial and the remainder polynomial. We don't need such an algorithm here. All we have to know is that for every polynomial f and every polynomial g that has coefficient 1 with its highest power of x (which of course is at least x^0) there is a "quotient polynomial" q and a "remainder polynomial" re so that the following equation holds:

$$f=g\cdot q+re\ ; \tag{5}$$

here the highest power of x appearing in re is smaller than the highest power of x in g. For example, in (4) the highest power of x in the remainder $x=x^1$ is smaller than the highest power of x in the divisor (x^2).

For our fingerprint application we only need an extremely simple case: Division by polynomials $x+s$, for s a number. With a little patience you can check that (here: $s=3$):

$$3x^4+13x^3+5x^2+2x+6=(3x^3+4x^2+10x+6)\cdot(x+3)+5.$$

That is,

$$(3x^4+13x^3+5x^2+2x+6):(x+3)=3x^3+4x^2+10x+6 \text{ with remainder } 5.$$

In general it is clear that when dividing by a polynomial $x+s$ the remainder is simply a number.[2]

[2] The interested reader may want to try and find an algorithm to divide a polynomial $c_nx^n+\cdots+c_1x+c_0$ by a polynomial $x+s$.

Substituting into polynomials, roots, factoring out linear factors $x - r$

Up to here we only *calculated* with polynomials as formal expressions, never touching the "variable" x. Another very important operation with polynomials is „substitution“. That means, at least in our simple situation, that we replace the x by some number between 0 and $m-1$ and evaluate to see what the resulting number is.

For example, if in the polynomial

$$f = 3x^4 + 13x^3 + 5x^2 + 2x + 1$$

we substitute the number 2 for x, we get

$$f(2) = (3 \cdot 2^4 + 13 \cdot 2^3 + 5 \cdot 2^2 + 2 \cdot 2 + 1) \bmod 17 = 7,$$

if we substitute the number 14 for x, we get

$$f(14) = (3 \cdot 14^4 + 13 \cdot 14^3 + 5 \cdot 14^2 + 2 \cdot 14 + 1) \bmod 17 = 0,$$

and so on.

If $f(r) = 0$ we call r a *root* of f. Thus, $r = 14$ is a root of $f = 3x^4 + 13x^3 + 5x^2 + 2x + 1$. Now we divide f by $x - 14 = x + 3$ (viewed modulo 17) and note:

$$(3x^4 + 13x^3 + 5x^2 + 2x + 1) : (x + 3) = 3x^3 + 4x^2 + 10x + 6.$$

There is no remainder in the division! We can try more examples with dividing polynomials by $x - r$, where r is a root, and will always find that there is no remainder. Here's the general fact, and because it is very important for us, we prove it.

Theorem 1
For polynomials modulo m, for a number $m \geq 2$, we have:
if r is a root of the polynomial f, then division of f by $x - r$ $(= x + (m - r))$ yields remainder 0.
This means: It is possible to write $f = (x - r) \cdot q$, for some (quotient) polynomial q.

Proof:
We can certainly divide f by $x - r$, with remainder, that is, we can write:

$$f = q \cdot (x - r) + re.$$

Here re is a number between 0 and $m - 1$, and q is a polynomial. Now we substitute r for x on both sides. Because r is a root of f, we get:

$$0 = f(r) = q(r) \cdot (r - r) + re = re.$$

Since the remainder re is 0, we get $f = q \cdot (x - r)$, and Theorem 1 is proved. □

One can put Theorem 1 as follows: If r is a root of f, one can "factor out" the factor $x - r$ from f. The next theorem says that if m is a prime number this can be done with several roots of a polynomial one after the other. The proof is a little more tricky.

Theorem 2
Consider polynomials modulo m, for a **prime number** $m \geq 2$.
If $k \geq 1$ and $r_1, \ldots, r_k$ are different roots of f between 0 and $m - 1$, then it is possible to write

$$f = (x - r_1) \cdot (x - r_2) \cdot \cdots \cdot (x - r_k) \cdot h,$$

for some polynomial h.

Proof: Let us first consider the case where f has two different roots r und t. By Theorem 1 we can write

$$f = q \cdot (x - r).$$

Since t is a root of f, we have (modulo m):

$$0 = f(t) = q(t) \cdot (t - r).$$

This means: The number $q(t) \cdot (t - r)$, calculated with integer arithmetic (without taking remainders modulo m), is divisible by m. Because t and r are different numbers between 0 and $m - 1$, the number $t - r$ is *not* divisible by m. Now it is a well known basic fact about prime numbers m that from

$$m \text{ is a divisor of } a \cdot b$$

it follows that m must divide a or b (or both)[3]. This gets us that m divides $q(t)$ (in the integers). Viewed modulo m this means that $q(t) = 0$. Thus t is a root of the quotient polynomial q. We apply Theorem 1 once again and write $q = p\cdot(x-t)$ for a suitable polynomial p. Thus we get that $f = p\cdot(x-t)\cdot(x-r)$, as desired.

Example: For $m = 17$ and

$$f = x^4 + 16x^3 + x^2 + 14x + 11 \tag{6}$$

we have that $f(2) = f(16) = 0$ and that

$$f = (x-2)\cdot(x-16)\cdot(x^2+3) = (x+15)\cdot(x+1)\cdot(x^2+3).$$

If f happens to have more than two roots, one can proceed along the same pattern and keep factoring out linear factors, until the desired representation $f = (x-r_1)\cdot(x-r_2)\cdot\cdots\cdot(x-r_k)\cdot h$ is obtained. (Formally, one uses induction on k.) □

Now we can formulate and prove the statement we need for our purposes.

Theorem 3
Consider polynomials modulo m, for a prime number $m \geq 2$.
If f is a polynomial that is not the zero polynomial, and x^n is the highest power of x that occurs in f (with a coefficient $c_n \neq 0$), then f has no more than n distinct roots between 0 and $m-1$.

Examples: (Always modulo 17.) The polynomial $2x+11$ has one root, which is 3; the polynomial $2x^2 + 7x + 12$ has two roots, which are 2 and 3; the polynomial $x^4 + 16x^3 + x^2 + 14x + 11$ from (6) cannot have more than four roots (actually, there are only two roots: 2 and 16).

Proof of Theorem 3: We take any k distinct roots of f and call them $r_1, \ldots, r_k$. The aim is to show that k cannot be larger than n. By Theorem 2 we can write:

$$f = (x-r_1)\cdot(x-r_2)\cdot\cdots\cdot(x-r_k)\cdot h. \tag{7}$$

[3] For numbers m that are not prime this is not necessarily so: the number 6 divides $4\cdot 9 = 36$, but 6 divides neither 4 nor 9.

Here h cannot be the zero polynomial, since otherwise f would be the zero polynomial. In h there is a highest power of x, dx^ℓ, say, with $d \neq 0$, $\ell \geq 0$. Now if we multiply out the right hand side of (7) we obtain the power $x^{k+\ell}$, with factor d as well, and there is no other term in the product with a larger power of x. Since x^n is the highest power of x in f with a nonzero coefficient, we must have $n = k + \ell \geq k$, as desired. □

Polynomials and fingerprints

After these preparations we can finally prove the fingerprinting theorem from [AU2011].

Fingerprinting Theorem
If T_A and T_B are different texts of length n, and if m is a prime number that is larger than the largest number occurring in T_A and T_B, then at most n out of the m pairs of numbers

$$\mathrm{FP}(T_A, r), \mathrm{FP}(T_B, r), \quad 0 \leq r < m,$$

can consist of two equal numbers.

Proof: We look at two "texts" (that is to say: sequences of numbers)

$$T_A = (a_1, \ldots, a_n) \text{ and } T_B = (b_1, \ldots, b_n) .$$

The numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$ are between 0 and $m-1$. From these texts we form two polynomials:

$$\begin{aligned} f_A &= a_1 \cdot x^n + \cdots + a_n \cdot x \text{ and} \\ f_B &= b_1 \cdot x^n + \cdots + b_n \cdot x, \end{aligned}$$

and the polynomial g obtained from f_A and f_B by subtraction modulo m:

$$g = f_A - f_B = (a_1 - b_1) \cdot x^n + \cdots + (a_n - b_n) \cdot x.$$

Now if T_A and T_B are *different* texts, then (also if we look at the numbers modulo m) at least one of the coefficients $(a_i - b_i)$ in g is not zero, hence g is not the zero polynomial. Obviously, in g no power of x with an exponent larger than n can occur. (Note that x^n need not occur, since we could have

$a_n = b_n$. It very much depends on the texts what g looks like. Maybe it has only one nonzero term.)

Now, obviously,

$$\mathrm{FP}(T_A, r) = f_A(r) \quad \text{and} \quad \mathrm{FP}(T_B, r) = f_B(r).$$

So if the fingerprints $\mathrm{FP}(T_A, r)$ and $\mathrm{FP}(T_B, r)$ are equal, then $f_A(r) = f_B(r)$, hence $g(r) = 0$ — and this means that r is a root of g.

By Theorem 3 the polynomial g cannot have more than n roots. Hence there are no more than n numbers r with $\mathrm{FP}(T_A, r) = \mathrm{FP}(T_B, r)$, and hence the Fingerprinting Theorem is proved. □

Literatur

[AU2011] Vöcking, B., Alt, H., Dietzfelbinger, M., Reischuk, R., Scheideler, C., Vollmer, H., Wagner, D. (Eds.), *Algorithms Unplugged*, Springer-Verlag, 2011, ISBN: 978-3-642-15327-3.