Über Polynome mit Arithmetik modulo m

Um den „Fingerprinting-Satz“ über die Fingerabdrücke verschiedener Texte aus dem

„37. Algorithmus der Woche“
(`http://www-i1.informatik.rwth-aachen.de/~algorithmus/algo37.php`)

besser zu verstehen, muss man sich „Polynome modulo m“ anschauen. Hierfür braucht man Geduld, und man sollte sich vor ein bisschen Rechnerei mit Variablen und Unbekannten nicht fürchten. Die Überlegungen führen zu einem vollständigen Beweis des Satzes.

Einen Fingerabdruck für einen Text $(a_1, \ldots, a_n)$ (mit Zahlen zwischen 0 und $m-1$) hatten wir folgendermaßen berechnet:

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

Dabei war r eine Zahl zwischen 1 und $m-1$. Aber auch $r = 0$ ist nicht verboten, es ergibt sich nur immer der Wert 0.

Wir sehen uns Ausdrücke wie in (1) genauer an. Da man zunächst nicht weiß, welches r eingesetzt wird, schreibt man an die Stelle dieses r ein Symbol x, die „Variable“. Auf diese Weise landet man bei „Polynomen“.

Polynome modulo m

mod-m-Polynome zum Beispiel für $m = 17$ sind Ausdrücke wie

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

Man hat also Potenzen

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

eines Symbols x (der „Variablen“). Darunter ist auch die Potenz x^0, die als „1“ zu verstehen ist, und als als Faktor weggelassen wird: $2 \cdot x^0 = 2$. Statt x^1 schreibt man x. Solche Potenzen kann man Zahlen zwischen 0 und $m-1$ multiplizieren, und die sich ergebenden Ausdrücke kann man addieren. Damit man nicht durcheinanderkommt, ordnet man die Summanden nach Möglichkeit nach (fallenden) x-Potenzen, aber man darf auch $5x + 3x^2 + 1$ oder $5x + 2x^2 + 1 + x^2$ schreiben und betrachtet dies als dasselbe wie $3x^2 + 5x + 1$. Wenn man einen Ausdruck wie

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

hat, der eigentlich kein Polynom modulo 17 ist, weil negative Faktoren und solche größer als 16 nicht erlaubt sind, kann man alle Zahlen modulo 17 nehmen, und erhält ein ordentliches mod-17-Polynom:

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

Folgendes ist die allgemeine Form eines mod-m-Polynoms:

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

Dabei sind $c_n, \ldots, c_0$ Zahlen zwischen 0 und $m - 1$.[1]

Interessanterweise braucht man sich bei der Speicherung eines Polynoms in einem Computer überhaupt nicht um das „x“ zu kümmern. Man speichert die Zahlen $c_0, c_1, \ldots, c_n$, zum Beispiel in einem Array `C[0..n]`, und hat die ganze Information.

Rechnen mit mod-m-Polynomen

Mit mod-m-Polynomen kann man die arithmetischen Operationen **Addition**, **Subtraktion** und **Multiplikation** durchführen. Diese Operationen ergeben sich, indem man die gewöhnlichen Rechenregeln wie Ausklammern und Ausmultiplizieren anwendet, und mit Zahlen immer modulo m rechnet.

Addition: Wir **addieren** zwei mod-m-Polynome, indem wir ganz normal rechnen, als ob x eine Unbekannte wäre, und Terme mit derselben Potenz von x zusammenfassen. Dabei werden die Faktoren bei derselben Potenz von x addiert – modulo m natürlich. Zum Beispiel ($m = 17$):

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

(Der Summand mit x^3 fällt weg, weil $(3 + 14) \bmod 17 = 0$ ist.)

Subtraktion: Das Vorgehen bei der Subtraktion ist ähnlich wie bei der Addition. Beispiel:

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

Man subtrahiert die Faktoren bei denselben Potenzen von x und bildet dann die Reste modulo m. Wenn man das Rechnen mit negativen Zahlen vermeiden will, kann man auch im Subtrahenden den Faktor c durch $m - c$ ersetzen und das sich ergebende Polynom addieren statt subtrahieren, also im obigen Beispiel:

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

Eine besondere Situation entsteht, wenn man ein Polynom von sich selber subtrahiert:

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

Dieses Polynom, bei dem alle Faktoren bei allen Potenzen von x gleich 0 sind, heißt das **Nullpolynom**. Normalerweise wird man sich wohl nicht mit so einem komischen nichtssagenden Ding beschäftigen, aber wir müssen das Nullpolynom erkennen, wenn es auftaucht.

[1] Im Vergleich zu (1) haben wir die Nummerierung der Faktoren umgedreht und noch einen Summanden c_0 hinzugefügt.

Multiplikation: Bei der Multiplikation zweier Polynome (modulo m) multipliziert man aus und fasst dann Terme mit derselben x-Potenz zusammen. Beispiel:

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

Gibt es auch eine Division für Polynome? Ja, aber das ist etwas komplizierter.

Division: Nach dem Ergebnis der Multiplikation aus (3) wird man sicher schreiben (immer modulo m):

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

Manchmal jedoch (bzw. ziemlich häufig) „geht es nicht auf“. Wie bei der Division von Zahlen machen wir dann „Division mit Rest“. Damit wir nicht plötzlich Brüche bekommen, teilen wir nur durch Polynome, bei denen die höchste Potenz von x den Faktor 1 hat, zum Beispiel ist $x^{10} + 5$ als Divisor zugelassen, aber nicht $10x^2 + 3x + 1$.

Der „Rest“ bei der Polynomdivision ist wieder ein Polynom, dessen höchste x-Potenz kleiner ist als die höchste x-Potenz des Divisors.

Beispiel: Wir haben (modulo 17)

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

also schreiben wir

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

Es gibt auch einen Algorithmus zur Division von zwei Polynomen f und g, der immer den Quotienten und den Rest berechnet, aber uns reicht es hier festzustellen, dass man für jedes Polynom f und jedes Polynom g, das bei der höchsten x-Potenz den Faktor 1 hat, ein „Quotientenpolynom“ q und ein „Restpolynom“ re finden kann, so dass

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

ist. Dabei ist die höchste x-Potenz im Rest re niedriger als die höchste x-Potenz in g. Zum Beispiel ist in (4) die höchste x-Potenz im Rest $x = x^1$ niedriger als die höchste x-Potenz im Divisor (x^2).

Für unsere Fingerabdruck-Situation benötigen wir nur einen extrem einfachen Fall: Division durch Polynome $x + s$, wo s eine Zahl ist. Das sieht dann zum Beispiel so aus ($s = 3$):

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

wie man mit etwas Geduld nachrechnet; das heißt:

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

Allgemein ist es klar, dass bei der Division mit Rest durch ein Polynom $x + s$ der Rest einfach eine Zahl ist.[2]

[2]Wer Lust hat, kann versuchen, einen Algorithmus zu finden, mit dem man ein beliebiges Polynom $c_n x^n + \cdots + c_1 x + c_0$ durch ein Polynom $x + s$ teilt.

Einsetzen in Polynome, Nullstellen, Abspalten von Linearfaktoren

Bis jetzt haben wir mit Polynomen *gerechnet*. Eine weitere sehr wichtige Operation bei Polynomen ist das „Einsetzen“. Das heißt, dass man an der Stelle der Variablen x eine Zahl r zwischen 0 und $m-1$ setzt und ausrechnet, was herauskommt.

Wenn wir zum Beispiel im Polynom

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

für x die Zahl 2 einsetzen, bekommen wir

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

wenn wir für x die Zahl 14 einsetzen, bekommen wir

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

und so weiter.

Wenn $f(r) = 0$ ist, dann nennen wir r eine **Nullstelle** von f. Also ist zum Beispiel $r = 14$ eine Nullstelle von $f = 3x^4 + 13x^3 + 5x^2 + 2x + 1$. Wir teilen nun f durch $x - 14 = x + 3$ (modulo 17 gesehen!) und bemerken:

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

Die Division geht auf! Wir stellen fest, dass dieser Effekt immer eintritt. Weil diese Erkenntnis so wichtig ist, geben wir auch einen Beweis an.

Satz 1
Wir betrachten Polynome modulo m, für eine **Zahl** $m \geq 2$. Es gilt:
Wenn r eine Nullstelle des Polynoms f ist, dann ergibt die Division von f durch $x - r$ $(= x + (m - r))$ den Rest 0.
Das heißt: Man kann $f = (x - r) \cdot q$ schreiben, für ein (Quotienten-)Polynom q.

Beweis:
Wir können auf jeden Fall f mit Rest durch $x - r$ dividieren, also schreiben:

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

Dabei ist re eine Zahl zwischen 0 und $m-1$ und q ein Polynom. Jetzt setzen wir für x auf beiden Seiten r ein. Das liefert (weil r Nullstelle von f ist):

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

Weil der Rest re gleich 0 ist, ist $f = q \cdot (x - r)$, und Satz 1 ist bewiesen. $\square$

Man kann Satz 1 auch so beschreiben: Wenn r eine Nullstelle von f ist, dann kann man von f den Faktor $(x - r)$ „abspalten“. Der nächste Satz sagt, dass man dies nacheinander für mehrere verschiedene Nullstellen eines Polynoms machen kann. Der Beweis dieses Satzes ist ein bisschen knifflig; hier spielt die Voraussetzung, dass m eine Primzahl ist, die entscheidende Rolle.

Satz 2
Wir betrachten Polynome modulo m, für eine **Primzahl** $m \geq 2$.
Wenn $k \geq 1$ ist und die verschiedenen Zahlen $r_1, \ldots, r_k$ zwischen 0 und $m-1$ liegen und alles Nullstellen von f sind, dann kann man schreiben:

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

wobei h ein passendes Polynom ist.

Beweis: Wir sehen uns zuerst den Fall an, wo f zwei Nullstellen r und t hat. Nach Satz 1 schreiben wir

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

Weil t eine *andere* Nullstelle von f ist, haben wir (modulo m):

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

Das heißt: Die Zahl $q(t) \cdot (t - r)$, mit Rechenoperationen in den ganzen Zahlen (ohne Restbildung modulo m berechnet), ist durch m teilbar. Weil t und r verschiedene Zahlen zwischen 0 und $m-1$ sind, ist $t - r$ *nicht* durch m teilbar. Es ist nun eine bekannte Grundeigenschaft von Primzahlen m, dass aus

$$m \text{ teilt das Produkt } a \cdot b \text{ ohne Rest}$$

folgt, dass m Teiler von a oder von b (oder auch von beiden) ist[3]. Hier folgern wir: m teilt $q(t)$ (in den ganzen Zahlen berechnet). Das heißt: modulo m gesehen ist $q(t) = 0$. Damit ist t Nullstelle des Quotientenpolynoms q. Wir wenden Satz 1 noch einmal an und schreiben $q = p \cdot (x - t)$ für ein passendes Polynom p. Damit ist $f = p \cdot (x - t) \cdot (x - r)$, wie gewünscht.

Beispiel: Für $m = 17$ und

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

gilt, dass $f(2) = f(16) = 0$ ist, und dass

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

Wenn man mehr als zwei Nullstellen hat, kann man nach dem gleichen Muster weiter die entsprechenden Faktoren herausziehen, und bekommt schließlich die gewünschte Darstellung $f = (x - r_1) \cdot (x - r_2) \cdot \cdots \cdot (x - r_k) \cdot h$. $\square$

Nun können wir die für unser Ziel zentrale Aussage formulieren und beweisen.

[3]Für Nicht-Primzahlen m muss das nicht so sein: Die Zahl 6 teilt das Produkt $4 \cdot 9 = 36$, aber 6 teilt weder 4 noch 9.

Satz 3
Wir betrachten Polynome modulo m, für eine Primzahl $m \geq 2$.
Wenn f ein Polynom ist, das nicht das Nullpolynom ist, bei dem x^n die höchste in f (mit Faktor $\neq 0$) vorkommende Potenz von x ist, dann hat f höchstens n verschiedene Nullstellen.

Beispiele: (Immer modulo 17.) Das Polynom $2x + 11$ hat eine Nullstelle (nämlich 3), das Polynom $2x^2 + 7x + 12$ hat zwei Nullstellen (nämlich 2 und 3), das Polynom $x^4 + 16x^3 + x^2 + 14x + 11$ aus (6) hat keinesfalls mehr als vier Nullstellen (tatsächlich sind es nur zwei, nämlich 2 und 16).

Beweis von Satz 3: Wir nehmen irgendwelche k verschiedenen Nullstellen von f, und nennen sie $r_1, \ldots, r_k$. Nach Satz 2 kann man schreiben:

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

Dabei kann h nicht das Nullpolynom sein, sonst wäre f selber das Nullpolynom und x^n könnte keinen Faktor haben, der nicht 0 ist. Daher kommt in h eine höchste Potenz von x mit einem Faktor vor, der nicht 0 ist, zum Beispiel dx^ℓ, $d \neq 0$, $\ell \geq 0$. Dann sieht man, dass beim Ausmultiplizieren in (7) die Potenz $x^{k+\ell}$ entsteht, ebenfalls mit dem Faktor d, und dass dies die höchste Potenz von x ist, die es in dem Produkt gibt. Also ist die höchste Potenz von x, die in f vorkommt, $x^{k+\ell}$. Weil x^n die höchste solche Potenz ist, ist $n = k + \ell \geq k$. Also hat f keinesfalls mehr als n Nullstellen. $\square$

Polynome und Fingerabdrücke

Nach diesen länglichen Vorbereitungen können wir den „Fingerprinting-Satz“ von der Webseite beweisen.

Fingerprinting-Satz: Wenn T_A und T_B verschiedene Texte (Zahlenfolgen) der Länge n sind, und wenn m eine Primzahl ist, die größer ist als die größte Zahl in T_A und T_B, dann können von den m Zahlenpaaren

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

höchstens n viele aus gleichen Zahlen bestehen.

Beweis: Sehen wir uns zwei gleich lange „Texte“ (also Zahlenfolgen)

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

an. Dabei sollen die Zahlen $a_1, \ldots, a_n, b_1, \ldots, b_n$ zwischen 0 und $m - 1$ liegen. Zu diesen Texten bilden wir zwei Polynome:

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

und dann noch das Polynom g, das wir durch Subtrahieren modulo m bekommen:

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

Wenn nun T_A und T_B *verschiedene* Text sind, dann ist (auch modulo m gesehen) mindestens einer der Faktoren $(a_i - b_i)$ in g nicht 0, also ist g ein Polynom, das nicht das Nullpolynom ist, und bei dem keine höhere x-Potenz als x^n vorkommt. (Aber natürlich muss nicht x^n vorkommen, weil ja $a_1 = b_1$ sein könnte.)

Nun ist offenbar

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

Wenn also die Fingerabdrücke $\mathrm{FP}(T_A, r)$und $\mathrm{FP}(T_B, r)$ gleich sind, dann ist $f_A(r) = f_B(r)$, also $g(r) = 0$ – das heißt, dass r eine Nullstelle von g ist.

Nach Satz 3 hat g keinesfalls mehr als n Nullstellen. Also gibt es nicht mehr als n Zahlen r mit $\mathrm{FP}(T_A, r) = \mathrm{FP}(T_B, r)$, und der Fingerprinting-Satz ist bewiesen. $\square$

Martin Dietzfelbinger, 14.01.2008