

Polynomialer deterministischer Algorithmus von Agrawal-Kayal-Saxena

1.1. Kongruenzen modulo $(h(x), n)$. Fixieren wir ein Polynom $h(x) \in \mathbb{Z}[x]$ und eine natürliche Zahl n . Sei $f(x)$ ein beliebiges Polynom aus $\mathbb{Z}[x]$. Ein *Rest von $f(x)$ modulo $(h(x), n)$* ist ein Polynom $r(x)$, das in den folgenden zwei Schritten berechnet wird:

1) Teilen wir $f(x)$ durch $h(x)$ und finden die Polynome $q(x)$ und $s(x)$, so daß

$$f(x) = h(x)q(x) + s(x)$$

gilt, wobei $\text{Grad}(s(x)) < \text{Grad}(h(x))$ ist;

2) In dem Polynom $s(x)$ ersetzen wir alle Koeffizienten nach ihre Reste modulo n . Das Resultat bezeichnen wir als $r(x)$.

Man sagt, daß zwei Polynome $f(x), g(x) \in \mathbb{Z}[x]$ modulo $(h(x), n)$ kongruent sind, wenn ihre Reste modulo $(h(x), n)$ gleich sind. In dem Fall schreibt man

$$f(x) \equiv g(x) \pmod{(h(x), n)}. \quad (1.1)$$

Zum Beispiel:

$$x^3 + 3x^2 + 4x + 1 \equiv x + 1 \pmod{(x^2 + x + 1, 2)}.$$

Aufgabe. Die Kongruenz (1.1) gilt nur dann, wenn ein Polynom $q(x) \in \mathbb{Z}[x]$ existiert, so daß alle Koeffizienten des Polynomes $f(x) - g(x) - h(x)q(x)$ durch n teilbar sind.

1.2. Der Ring $\mathbb{Z}_n[x]/\langle h(x) \rangle$. Sei F die Menge aller möglichen Reste modulo $(h(x), n)$, also die Menge aller Polynomen, dessen Grad kleiner als Grad $h(x)$ ist und dessen Koeffizienten in der Menge $\{0, 1, \dots, n-1\}$ liegen.

Diese Reste kann man natürlicherweise addieren und multiplizieren. Die Summe der Reste $r_1(x)$ und $r_2(x)$ ist den Rest von $r_1(x) + r_2(x)$ modulo $(h(x), n)$. Analog definiert man das Produkt der Reste $r_1(x)$ und $r_2(x)$.

Die Menge F mit einer so definierten Addition und Multiplikation bildet ein Ring. Bezeichnen wir diesen Ring als $\mathbb{Z}_n[x]/\langle h(x) \rangle$.

Zum Beispiel, der Ring $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ enthält die Reste $0, 1, x, x + 1$, die werden mit folgenden Regeln addiert und multipliziert:

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

·	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

1.3. Kinder binomialer Satz. Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$ und $\text{ggT}(n, a) = 1$. Die Zahl n ist eine Primzahl genau dann, wenn gilt

$$(x + a)^n \equiv x^n + a \pmod{n}. \quad (1.2)$$

Beweis. Nach binom Newton haben wir

$$(x + a)^n - (x^n + a) = \sum_{i=1}^{n-1} \binom{n}{i} x^i a^{n-i} + a^n - a. \quad (1.3)$$

Wenn n eine Primzahl ist, dann ist $\binom{n}{i}$ durch n teilbar für $1 \leq i \leq n-1$. Ausserdem ist $a^n - a$ durch n teilbar (nach dem kleinen Fermatischen Satz). Deshalb gilt die Kongruenz (1.2) für alle Primzahlen n .

Sei n eine zusammengesetzte Zahl und sei $n = p^e p_1^{e_1} \cdots p_s^{e_s}$ die Primzahlzerlegung von n . Dann ist $\binom{n}{p}$ durch p^{e-1} aber nicht durch p^e teilbar. Deshalb ist der Koeffizient bei x^p in (1.3) nicht durch n teilbar. Also gilt für zusammengesetzte n die Kongruenz (1.2) nicht. \square

Seien n und r teilerfremde natürliche Zahlen. Bezeichnen wir als $\text{ord}_r(n)$ die Ordnung des Elementes n modulo r . Mit anderen Worten $\text{ord}_r(n)$ ist die minimale natürliche Zahl $k \geq 1$, so daß $n^k \equiv 1 \pmod{r}$ gilt. Des weiteren bedeutet $\log n$ der Logarithmus von n zur Basis 2.

1.4. Lemma. Für jede natürliche Zahl $n > 4$ existiert eine Primzahl $r \leq \log^5 n$ mit $r \nmid n$, so daß folgende Ungleichung gilt:

$$\text{ord}_r(n) > \log^2 n.$$

Beweis. Nehmen wir das Entgegengesetzte an: es existiert eine natürliche Zahl $n > 4$, so daß für alle Primzahlen r mit den Bedingungen $r \leq \lfloor \log^5 n \rfloor$ und $r \nmid n$ die Ungleichung

$$\text{ord}_r(n) \leq \log^2 n$$

gilt. Setzen wir $m = \lfloor \log^5 n \rfloor$. Dann ist jede solche Zahl r (und so ihr Produkt) ein Teiler von $\prod_{1 \leq i \leq \log^2 n} (n^i - 1)$. Von der anderen Seite ist das Produkt der Primzahlen r mit den Bedingungen $r \mid n$ und $r \leq m$ nicht größer als n . Daraus und aus der Folgerung 12.5 haben wir

$$2^{(\log e)m/2} = e^{m/2} \leq \prod_{\substack{r \leq m \\ r \text{ - eine Primzahl}}} r \leq n \cdot \prod_{1 \leq i \leq \log^2 n} (n^i - 1) < n^{1+1+2+\dots+\lfloor \log^2 n \rfloor} \leq 2^{(\log^5 n + \log^3 n + 2 \log n)/2}.$$

Daraus folgt

$$(\log e) \lfloor \log^5 n \rfloor < \log^5 n + \log^3 n + 2 \log n,$$

was unmöglich für $n > 4$ ist. Ein Widerspruch. \square

1.5. Satz (Agrawal, Kayal, Saxena, 2002). Sei $n > 1$ eine natürliche Zahl und sei r eine Primzahl, so daß folgende Bedingungen erfüllt sind:

- (1) n ist nicht durch die Primzahlen, die nicht größer als r sind, teilbar;
- (2) $\text{ord}_r(n) > \log^2 n$;
- (3) $(x + a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$ für alle $1 \leq a \leq A$, wobei $A = \sqrt{r} \log n$ ist.

Dann ist n eine Potenz einer Primzahl.

Beweis. Siehe Beilage A.

1.6. Deterministischer Primtest von Agrawal-Kayal-Saxena. Sei $n > 1$ eine natürliche Zahl. Bezeichnen wir $m = \lfloor \log^5 n \rfloor$. Für $n < 5690034$ prüfen wir nach, ob n eine Primzahl ist. Dafür benutzen wir eine Liste bekannter kleiner Primzahlen oder Eratosphenus sieb. Für $n > 5690034$ gilt $n > m$. In diesem Fall machen wir folgende Schritte.

(1) Prüfen wir nach, ob n durch eine natürliche Zahl aus dem Intervall $[2, m]$ teilbar ist. Wenn ja, dann ist n eine zusammengesetzte Zahl. Wenn nein, dann machen wir Schritt 2.

(2) Nach Lemma 13.4 existiert eine Primzahl $r \leq m$ mit $\text{ord}_r(n) > \log^2 n$. Finden wir eine solche Zahl mit Probemethode.

(3) Prüfen wir nach, ob die Kongruenz

$$(x + a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$$

für alle $1 \leq a \leq \sqrt{r} \log n$ gilt. Wenn nein, dann (nach dem Satz 13.3) ist n eine zusammengesetzte Zahl. Wenn ja, dann (nach dem Satz 13.5) ist n eine Potenz einer Primzahl. In dem Fall machen wir Schritt 4.

(4) Prüfen wir nach, ob existieren natürliche Zahlen q, l mit $n = q^l$, $l \geq 2$. Wenn ja, dann ist n eine zusammengesetzte Zahl. Wenn nein, dann ist n eine Primzahl.

13.7. Warum der Primtest von Agrawal-Kayal-Saxena polynomiell ist.

Bemerken wir, daß $\log(n)$ ungefähr die Anzahl der Ziffern in binäre Darstellung von n ist. Man sagt, daß ein Test mit einem Input n polynomiell ist, wenn ein Polynom $P(x)$ existiert, so daß für jede Zahl n erfüllt den Test nicht mehr als $P(\log(n))$ Operationen, um eine Antwort auszugeben.

Der Primtest von Agrawal-Kayal-Saxena polynomiell ist. Die kurze Erklärung dafür ist, daß im Lemma 13.4 und im Satz 13.5 die Potenzen von $\log n$ auftauchen. Dazu muß man verstehen, daß die Reste von $x^n + a$ und $(x + a)^n$ modulo $(x^r - 1, n)$ schnell berechenbar sind. Der erste Rest gleich $x^s + a$ ist, wobei s ein Rest von n modulo r ist. Der zweite Rest wird mit folgender Bemerkung berechnet.

Seien $f(x)$ und $g(x)$ beliebige Reste modulo $(x^r - 1, n)$. Also $f(x)$ und $g(x)$ sind die Polynome von Grad kleiner als r mit Koeffizienten aus der Menge $\{0, 1, \dots, n - 1\}$. Dann kann der Rest von $f(x)g(x)$ modulo $(x^r - 1, n)$ mit Hilfe nicht mehr als r^2 Multiplikationen und r Additionen modulo n berechnet sein. Nennen wir die Menge dieser Operationen als Block-Schritt. Insbesondere, den Rest von $f(x)^2$ modulo $(x^r - 1, n)$ kann man in einem Block-Schritt berechnen.

Sei $n = 2^l$. Dann wird der Rest von $(x + a)^n$ modulo $(x^r - 1, n)$ in $l = \log n$ Block-Schritten berechnet.

Sei n eine beliebige natürliche Zahl. Stellen wir n in der Form $n = 2^{l_1} + 2^{l_2} + \dots + 2^{l_k}$ dar, wobei $l_1 > l_2 > \dots > l_k$ ist. Dann wird der Rest von $(x + a)^n$ modulo $(x^r - 1, n)$ in wenige als in $2\lfloor \log n \rfloor$ Block-Schritten berechnet (prüfen Sie das nach!).

13.8. Bemerkung. Seit Jahr 2002 sind etliche Modifikationen und Verbesserungen des Primetestes von Agrawal-Kayal-Saxena erschienen. Zu der Zeit ist bewiesen, daß die polynomiale Komplexität dieses Testes ist $O(\log^7 n)$ Bit-Operationen. In Praxis wird die Zahl r neben der Zahl $\log^2 n$ schnell zu finden sein. Die haupte Komplexität dieses Testes liegt im Schritt (3).

Beilage I
Irreduzible Polynome.
Wann ist der Ring $\mathbb{Z}_n[x]/\langle h(x) \rangle$ ein Körper

I.1. Definition. Sei K ein Ring und sei $h(x)$ ein Polynom aus $K[x] \setminus K$. Das Polynom $h(x)$ heißt *irreduzibel in $K[x]$* , wenn für jede Zerlegung $h(x) = h_1(x)h_2(x)$ gilt: $h_1(x) \in K$ oder $h_2(x) \in K$.

I.2. Aufgabe. 1) Prüfen Sie nach, daß das Polynom $x^2 + x + 1$ irreduzibel in $\mathbb{Z}_2[x]$, aber reduzibel in $\mathbb{Z}_3[x]$ ist.

2) Prüfen Sie nach, daß das Polynom $x^2 + x + 1$ irreduzibel in $\mathbb{Z}_p[x]$ für jede Primzahl p mit $p \equiv 2 \pmod{3}$ ist.

I.3. Lemma. Sei p eine Primzahl und sei $h(x)$ ein irreduzibles Polynom in $\mathbb{Z}_p[x]$. Dann ist der Ring $\mathbb{Z}_p[x]/\langle h(x) \rangle$ ein Körper.

Beweis. Es ist genügend zu beweisen: für jedes nichtnullische Element $g(x)$ in dem Ring $\mathbb{Z}_p[x]/\langle h(x) \rangle$ existiert ein Inverses. Da $\text{Grad}(g(x)) < \text{Grad}(h(x))$ ist und $h(x)$ irreduzibel in $\mathbb{Z}_p[x]$ ist, haben wir $\mathbf{ggT}(g(x), h(x)) = 1$ in $\mathbb{Z}_p[x]$. Dann können wir mit Hilfe des Euklidischen Algorithmus einige Polynome $u(x), v(x) \in \mathbb{Z}_p[x]$ finden, so daß

$$g(x)u(x) + h(x)v(x) = 1$$

gilt. Dann gilt $g(x)u(x) \equiv 1 \pmod{(h(x), p)}$. Sei $\bar{u}(x)$ ein Rest von $u(x)$ modulo $(h(x), p)$. Dann gilt $g(x)\bar{u}(x) \equiv 1 \pmod{(h(x), p)}$. Also ist $\bar{u}(x)$ ein Inverses zu $g(x)$ in dem Ring $\mathbb{Z}_p[x]/\langle h(x) \rangle$. \square

Beilage A

Beweis des Agrawal-Kayal-Saxena Satzes über Primzahlen

A.1. Satz (Agrawal, Kayal, Saxena, 2002). Sei $n > 1$ eine natürliche Zahl und sei r eine Primzahl, so daß folgende Bedingungen erfüllt sind:

- (1) n ist nicht durch die Primzahlen, die nicht größer als r sind, teilbar;
- (2) $\text{ord}_r(n) > \log^2 n$;
- (3) $(x + a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$ für alle $1 \leq a \leq A$, wobei $A = \sqrt{r} \log n$ ist.

Dann ist n eine Potenz einer Primzahl.

Beweis. Sei p ein beliebiger Primteiler von n . Sei $h(x)$ ein irreduzibler Faktor von $x^r - 1$ in dem Ring $\mathbb{Z}_p[x]$, so daß $h(x) \neq x - 1$ ist. Ein solcher Faktor $h(x)$ existiert, sonst hätten wir $x^r - 1 = (x - 1)^r = x^r - rx^{r-1} + \dots$ in dem Ring $\mathbb{Z}_p[x]$. Dann wäre r durch p teilbar, was der Bedingung (1) widerspricht.

Nach Lemma I.3 ist der Ring $\mathbb{F} = \mathbb{Z}_p[x]/\langle h(x) \rangle$ ein Körper. Die Ordnung des Elementes $x \in \mathbb{F}^*$ ist r , weil $x^r = 1$ und $x \neq 1$ in \mathbb{F}^* gelten, wobei r eine Primzahl ist.

Beweisen wir, daß alle Elemente $x, x+1, x+2, \dots, x + \lfloor A \rfloor$ in \mathbb{F} ungleich null sind, und deshalb liegen sie in \mathbb{F}^* . Nehmen wir an, daß $x + a = 0$ in \mathbb{F} ist. Aus der Bedingung (3) folgt $x^n + a = (x + a)^n = 0$ in \mathbb{F} , und so gilt $x^n = -a = x$ in \mathbb{F} . Da $\text{ord}(x) = r$ ist, erhalten wir $n \equiv 1 \pmod{r}$, also $\text{ord}_r(n) = 1$ – ein Widerspruch mit der Bedingung (2).

Sei G eine Untergruppe von \mathbb{F}^* , die nur Elemente $x, x+1, x+2, \dots, x + \lfloor A \rfloor$ und alle ihre Produkte enthält. Nach dem Satz K.5 ist \mathbb{F}^* eine zyklische Gruppe. Deshalb ist G auch zyklisch.

Betrachten wir alle Polynome $g(x) \in \mathbb{Z}[x]$, die die Form $g(x) = \prod_{0 \leq a \leq A} (x + a)^{e_a}$ mit $e_a \geq 0$ haben. Wegen des kanonischen Homomorphismus $\mathbb{Z}[x] \rightarrow \mathbb{F}$ repräsentiert $g(x)$ ein Element $\bar{g}(x)$ von G . Deshalb nennen wir $g(x)$ ein *G-Polynom*. Für jedes G -Polynom $g(x)$ haben wir

$$g(x)^n = \prod_a ((x + a)^n)^{e_a} \equiv \prod_a (x^n + a)^{e_a} = g(x^n) \pmod{(x^r - 1, p)}.$$

Bezeichnen wir

$$I_{g(x)} = \{m > 0 \mid g(x)^m \equiv g(x^m) \pmod{(x^r - 1, p)}\}.$$

Dann gilt $n, p \in I_{g(x)}$.

A.2. Lemma. Die Menge $I_{g(x)}$ ist bezüglich der Multiplikation geschlossen.

Beweis. Sei $m, k \in I_{g(x)}$. Dann haben wir

$$g(x)^{mk} \equiv (g(x)^m)^k \pmod{(x^r - 1, p)}.$$

Außerdem (wenn wir x^m als y bezeichnen) haben wir

$$(g(x^m))^k \equiv g(x^{mk}) \pmod{(x^{mr} - 1, p)}.$$

Daraus folgt

$$(g(x^m))^k \equiv g(x^{mk}) \pmod{(x^r - 1, p)}.$$

Aus dieser und der ersten Kongruenz entspringt $mk \in I_{g(x)}$. \square

A.3. Lemma. Sei $g(x)$ ein G -Polynom, das ein Erzeugendes $\bar{g}(x)$ der Gruppe G repräsentiert. Seien m_1, m_2 zwei Elemente von $I_{g(x)}$. Wenn

$$m_1 \equiv m_2 \pmod{r}$$

gilt, dann gilt auch

$$m_1 \equiv m_2 \pmod{|G|}.$$

Beweis. Sei $m_2 = m_1 + kr$. In der folgenden Kette von Gleichungen in \mathbb{F} benutzen wir die Definition von $I_{g(x)}$ und die Gleichung $x^r = 1$ in \mathbb{F} .

$$\bar{g}(x)^{m_1} \bar{g}(x)^{kr} = \bar{g}(x)^{m_2} = \bar{g}(x^{m_2}) = \bar{g}(x^{m_1+kr}) = \bar{g}(x^{m_1}) = \bar{g}(x)^{m_1}.$$

Da $\bar{g}(x) \neq 0$ in \mathbb{F} ist, können wir $\bar{g}(x)^{kr} = 1$ ableiten. Daraus folgt, daß kr durch die Ordnung von $\bar{g}(x)$, also durch $|G|$, teilbar ist. \square

Sei R eine maximale (bezüglich einer Einbettung) Untermenge der Menge $\{n^i p^j \mid i, j \geq 0\}$, so daß die Zahlen aus R paarweise inkongruent modulo r sind. Es ist klar, daß $|R| \leq r$ ist. Außerdem haben wir nach Lemma A.2 $R \subset I_{f(x)}$ für jedes G -Polynom $f(x)$.

Am Anfang wurde p als beliebiger Primteiler von n gewählt. Ab hier werden wir annehmen, daß p ein minimaler Primteiler von n ist.

Nehmen wir an, daß n keine Potenz von p ist.

Dann sind die Zahlen $n^i p^j$ für $i, j \geq 0$ paarweise unterschiedlich. Für $0 \leq i \leq \sqrt{|R|/2}$ und $0 \leq j \leq \sqrt{2|R|}$ gibt es mehr als $|R|$ solche Zahlen. Deshalb müssen irgendwelche zwei der Zahlen kongruent modulo r sein:

$$n^i p^j \equiv n^I p^J \pmod{r}.$$

Nach Lemma A.2 liegen die Zahlen $n^i p^j$ und $n^I p^J$ in $I_{g(x)}$, und nach Lemma A.3 ist ihre Differenz durch $|G|$ teilbar. Daraus folgt

$$|G| \leq |n^i p^j - n^I p^J| < n^{\sqrt{|R|/2}} p^{\sqrt{2|R|}} < n^{\sqrt{2|R|}}.$$

Weiter werden wir nachprüfen, daß $|G| > n^{\sqrt{2|R|}}$ gilt, so erhalten wir einen Widerspruch. Daraus wird folgen, daß n eine Potenz von p ist.

A.4. Lemma. Seien $f_1(x), f_2(x)$ zwei G -Polynomen aus $\mathbb{Z}[x]$ des Grades kleiner als $|R|$. Nehmen wir an, daß ihre Abbildungen in \mathbb{F} gleich sind: $f_1(x) \equiv f_2(x) \pmod{(h(x), p)}$. Dann gilt $f_1(x) = f_2(x)$ in $\mathbb{Z}_p[x]$.

Beweis. Da $R \subset I_{f_i(x)}$ für $i = 1, 2$ ist, gilt für jeweils $k \in R$

$$f_i(x^k) \equiv f_i(x)^k \pmod{(h(x), p)}.$$

Daraus und aus der Bedingung des Lemmas folgt

$$f_1(x^k) \equiv f_2(x^k) \pmod{(h(x), p)}.$$

Merken wir an, daß die Elemente $x^k \in \mathbb{F}$ unterschiedlich für verschiedene $k \in R$ sind. (Das entspringt dem Fakt, daß die Zahlen aus R paarweise inkongruent modulo r sind und $\text{ord}(x) = r$ in \mathbb{F}^* ist.) Deshalb haben die Polynome f_1 und f_2 die gleichen Werte auf $|R|$ Elemente des Körpers \mathbb{F} . Da die Grade von f_1 und f_2 kleiner sind als $|R|$, haben sie gleiche Koeffizienten bei gleichen Potenzen von x . Da diese Koeffizienten in dem Körper \mathbb{F} liegen und frei von x sind, geben sie gleiche Reste modulo p . \square

• Beweisen wir, daß $|G| > n\sqrt{2|R|}$ gilt. Man kann annehmen, daß die Zahlen $1, n, \dots, n^{\text{ord}_r(n)-1}$ in R liegen. Deshalb ist $|R| \geq \text{ord}_r(n) > \log^2 n$ und so $|R| > B$, wobei $B = \lfloor \sqrt{|R|} \log n \rfloor$ ist. Außerdem gilt $A \geq B$, wobei A in der Bedingung (3) definiert wurde.

Betrachten wir die G -Polynome $\prod_{0 \leq a \leq B} (x+a)^{e_a}$ mit der Bedingung $\sum_{0 \leq a \leq B} e_a = B$. Die Anzahl der Polynomen ist gleich der Anzahl der Verteilungen der Zahl B in $(B+1)$ nicht negative Summanden, also gleich $\binom{2B}{B}$. Für jedes solcher Polynome sind die Nullstellen

$$\left(\underbrace{0, \dots, 0}_{e_0}, \dots, \underbrace{-B, \dots, -B}_{e_B} \right).$$

Diese Zahlen sind nicht positiv und nicht kleiner als $-p$, weil

$$B < |R| < r < p$$

ist. Deshalb haben die Polynome verschiedene Tupels der Nullstellen modulo p für verschiedene Tupels der Potenzen (e_0, \dots, e_B) . Das bedeutet, daß die Polynomen in dem Ring $\mathbb{Z}_p[x]$ unterschiedlich sind. Nach Lemma A.4 sind ihre Abbildungen in \mathbb{F} unterschiedlich. Da diese Abbildungen in G liegen, erhalten wir mit Hilfe des Lemmas 12.2

$$|G| \geq \binom{2B}{B} \geq \frac{4^B}{2B^{1/2}} > \frac{4\sqrt{|R|} \log n - 1}{2p^{1/2}} > \frac{n^2 \sqrt{|R|}}{8n^{1/4}}.$$

Es bleibt zu beweisen, daß der letzte Ausdruck größer ist als $n\sqrt{2|R|}$. Äquivalent ist:

$$n^{(2-\sqrt{2})\sqrt{|R|}-1/4} > 8.$$

Da $|R| > \log^2 n$ gilt, genügt es, die folgende Ungleichung zu beweisen:

$$n^{(2-\sqrt{2}) \log n - 1/4} > 8.$$

Diese Ungleichung gilt für alle $n \geq 6$. Und das ist genau unser Fall, weil wir angenommen haben, daß n keine Potenz einer Primzahl ist. Der Satz ist bewiesen. \square