Der diskrete Logarithmus

04.07.18

Sei p eine Primzahl & sei $G = (\mathbb{Z}/p\mathbb{Z})^*$

Nach Kor. 4.43 existiert eine Primitivwurzel modulo p.

D.h. G ist zyklisch von r erzeugt.

↝ Die Elemente von G lassen sich schreiben als

$G = \{r, r^2, r^3, \dots, r^{p-1}\}$

Definition 5.4

Mit der Definition wie oben definieren wir die Exponential-funktion bzgl. der Primitivwurzel als die Abb.

$$\exp_r : \mathbb{Z}/(p-1)\mathbb{Z} \to G = (\mathbb{Z}/p\mathbb{Z})^* \quad (\neq G \text{ i.A.})$$
$$[i] \mapsto r^i \pmod p$$

Die Funktion $\exp_r$ heißt Exponentialfunktion, da

$\exp_r(i+j) = \exp_r(i) \cdot \exp_r(j)$

Da $G = \{r, r^2, \dots, r^{p-1}\}$ ist $\exp_r$ bijektiv.

Die Umkehrfunktion

$$\operatorname{dlog}_r : G \to \mathbb{Z}/(p-1)\mathbb{Z}, \quad a = r^i \mapsto [i]$$

heißt der diskrete Logarithmus (bzgl. der Primitivwurzel)

Genauso wie $\exp_r$ hängt auch dlog_r von der Wahl der Primitivwurzel ab.

Beispiel 5.5

$p = 7$, $G = (\mathbb{Z}/7\mathbb{Z})^*$, $r = 5$ ist eine Primitivwurzel

a	$1 \equiv 5^6 \bmod 7$	$2 \equiv 5^4 \bmod 7$	$3 \equiv 5^5 \bmod 7$	4	5	6
$\operatorname{dlog}_5(a)$	6	4	5	2	1	3

Mit dem diskreten Log. lassen sich Gleichungen der Form $x^e \equiv a \bmod p$ lösen.

Sei r eine Primitivwurzel mod p. Ist $i := \operatorname{dlog}_r(a)$ & $y := \operatorname{dlog}_r(x)$ so ist die obige Gleichung aquivalent zu $e \cdot y \equiv i \bmod p-1$.

Für lineare Kongruenzen dieser Form kennen wir bereits ein Lösungsschema

Beispiel 5.6

Wollen $x^5 \equiv 4 \mod 7$.

Wegen $5^2 \equiv 4 \mod 7$ ist $\text{dlog}_5(4) = 2$

Da $\text{ggT}(5,6) = 1$ hat diese lineare Kongruenz eine eindeutige Lösung $y \equiv 4 \mod 6$.

$\rightsquigarrow x \equiv \exp_r(y) = \exp_5(4) \equiv 5^4 \equiv 2 \mod 7$

In der Tat ist $2^5 \equiv 4 \mod 7$.

Allgemein ist die Berechnung von expr effizient möglich via schneller Exponentation (vgl. Blatt 11)

Für die Berechnung von dlog_r gibt es allerdings keine effiziente Methode.

Um $\text{dlog}_r(a)$ zu erhalten(?) müssen wir alle Potenzen r^i berechnen bis $r^i \equiv a \mod p$ gilt.

Für große Primzahlen p ist dies sehr AUFWÄNDIG. Dies nennt man auch das diskrete Logarithmus Problem

Sei $a \in (\mathbb{Z}/p\mathbb{Z})^*$ gegeben. Berechne $\text{dlog}_r(a)$

Da $\exp_r$ sehr gut & $\log_r$ sehr schwer zu berechnen ist. lassen sich damit kryptologische Verfahren bauen:

Setup: Alice & Bob wollen über einen unsicheren Kanal vertrauliche Nachrichten austauschen. Sie wollen dazu ein symmetrisches Verschlüsselungsverfahren verwenden.

Um einen gemeinsamen privaten Schlüssel auszutauschen, haben sie auch nur den unsicheren Kanal zur Verfügung?

Algorithmus 5.7 (Diffie - Hellman Schlusselaustauschverfahren)

Schritt 1: Alice & Bob wählen eine Primzahl p, sowie eine Primitivwurzel r modulo p

$(p, r) \hat{=}$ öffentlicher Schlüssel.

Schritt 2: Bob wählt (zufällig) ein $i \in \{1, \dots, p-1\}$ & berechnet $b = r^i$ & schickt "b" an Alice.

Schritt 3: Alice wählt (zufällig) ein $j \in \{1, \dots, p-1\}$ & berechnet $a = r^j$ & schickt "a" an Bob

Schritt 4: Alice & Bob können nun beide das Element $k = a^i = r^{i \cdot j} = b^j \in (\mathbb{Z}/p\mathbb{Z})^*$ berechnen.

Dies ist der private Schlüssel.

Eve hat den unsicheren Kanal abgehört und kennt p, r, a, b.

Um den privaten Schlüssel zu berechnen müsste Eve i oder j berechnen. Hierzu müsste sie das diskrete Logarithmus Problem $j = d\log_r(a)$ bzw. $i = d\log_r(b)$ lösen.

Für $p \gg 0$ ist das unmöglich.

Eine Weiterentwicklung dieses Verfahrens ist das sg. El Gamal - Kryptoverfahren. (1984 Taher El Gamal)

Primzahltest & Pseudoprimzahlen

In diesem Abschnitt möchten wir ein Verfahren beschreiben, welches uns mit beliebig hoher Wahrscheinlichkeit sagt, ob eine gegebene Zahl eine Primzahl ist.

Ist p eine Primzahl, so ist nach dem kleinen Satz von Fermat $b^p \equiv b \mod p \quad \forall b \in \mathbb{Z}$.

Wenn also ein $b \in \mathbb{Z}$ existiert mit $b^p \not\equiv b \mod p$, so kann p keine Primzahl sein.

Dies gibt uns einen ersten Primzahltest:

1) Gegeben sei $n \in \mathbb{N}$
2) Wähle eine Basis $b \in \mathbb{Z}$
3) Teste, ob $b^n \equiv b \mod n$
4) Falls "ja" könnte n eine Primzahl sein.

! Carmichaelzahlen

Definition 5.8

Eine natürliche Zahl $n \in \mathbb{N}$ heißt (Fermatsche) Pseudoprimzahl zur Basis b, falls n zusammengesetzt ist & $b^n \equiv b \mod n$ gilt.

Beispiel 5.9

Wollen testen ob $n = 1234567893$ & $m = 1234567891$ Primzahlen sind. Würden wir dies mittels Probedivision versuchen zu testen, so müssen wir $\sim \sqrt{n} > 10.000$ Divisionen mit Rest durchführen. Mittels schneller Exponentation berechnen wir

$$2^{1234567893} \equiv 942902069 \mod n$$

$$2^{1234567891} \equiv 2 \mod m$$

$\Rightarrow$ n ist keine Primzahl

m könnte Primzahl sein (ist es auch)

Beispiel 5.10

Die kleinste Pseudoprimzahl zu Basis 6 ist 2

Es ist $341 = 11 \cdot 31$ aber $2^{341} \equiv 2 \mod 341$.

Wir fragen uns wieviele Pseudoprimzahlen es zu einer festen Basis gibt. Für $b = 2$ erhalten wir

# ungerade Pseudoprimzahlen	$<$	10^3	3
# Primzahlen	$<$	10^3	168
# ungerade Pseudoprimzahlen	$<$	10^6	245
# Primzahlen	$<$	10^6	78498

Gilt also $2^n \equiv 2 \mod n$ ist die Wahrscheinlichkeit sehr hoch, dass n eine Primzahl ist. Demnach gilt:

Satz 5.11

Es gibt unendlich viele Pseudoprimzahlen zur Basis $b=2$.

Beweis: Übung!

Man könnte den Fermatschen Primzahltest verbessern, indem man unterschiedliche Basen wählt.

Ein Problem stellen die folgenden Zahlen dar:

Definition 5.12 (vgl. B10 A4)

Eine zusammengesetzte Zahl n heißt Carmichael-Zahl falls $b^n \equiv b \mod n \ \forall b \in \mathbb{Z}$.

Der folgende Satz liefert eine Charakterisierung solcher Zahlen

Satz 5.13 (Korselt)

Sei $n = p_1 \cdot \ldots \cdot p_n$ mit paarw. verschiedenen Primzahlen, dann gilt: $(p_i - 1) \mid (n-1) \ \forall i \iff n$ ist Carmichael-Zahl.

Bemerkung: Es gibt unendlich viele Carmichael Zahlen (1994, Alford, Granville & Pomerance)

Dennoch sind diese Zahlen sehr selten.

Das folgende Lemma wird uns helfen einen besseren Primzahltest zu bauen.

Lemma 5.14

Sei $p > 2$ eine Primzahl und sei $b \in \mathbb{N}^*$ mit $ggT(b,p) = 1$.

Wir schreiben $p-1 = 2^s \cdot t$ mit $t \in \mathbb{N}$ ungerade.

Es gilt dann

(1) $b^t \equiv 1 \mod p$ oder

(2) Für ein $i \in \{0,\dots,s\}$ ist $b^{2^i} \equiv -1 \mod p$

Beweis:

Wegen dem kleinen Satz von Fermat gilt: $b^{p-1} \equiv 1 \mod p$.

Da $p-1 = 2^s \cdot t$ ist eine der Zahlen $b^t, b^{2t}, \dots, b^{2^s \cdot t}$ kongruent zu $1 \mod p$.

Ist $b^t \equiv 1 \mod p$ so gilt (1). Andernfalls existiert ein $i \in \{1,\dots,s\}$ mit $b^{2^i \cdot t} \equiv 1 \mod p$ & $b^{2^{i-1} \cdot t} \not\equiv 1 \mod p$

$\Rightarrow p \mid (b^{2^i \cdot t} - 1) = (b^{2^{i-1} \cdot t} - 1) \cdot (b^{2^{i-1} \cdot t} + 1)$

Da $p \nmid (b^{2^{i-1} \cdot t} - 1) \overset{p \text{ prim}}{\Rightarrow} p \mid (b^{2^{i-1} \cdot t} + 1)$

$\Rightarrow b^{2^{i-1} \cdot t} \equiv -1 \mod p$. Also gilt (2)

Definition 5.15

Eine ungerade zusammengesetzte Zahl n heißt starke Pseudoprimzahl zur Basis b, falls $ggT(b,n) = 1$ und n die Aussage aus Lemma 5.14 erfüllt.

Falls n keine starke Pseudoprimzahl zur Basis b ist, so heißt b ein Zeuge für n.

Beispiel 5.16

(a) $n = 561 = 3 \cdot 11 \cdot 17$ ist eine Carmichael Zahl.

Sei $b = 2$. Es ist $560 = 2^4 \cdot \underbrace{5 \cdot 7}_{t}$

$$\left.\begin{aligned} 2^t &\equiv 263 \mod n \\ 2^{2t} &\equiv 166 \mod n \\ 2^{4t} &\equiv 67 \mod n \\ 2^{8t} &\equiv 1 \mod n \\ 2^{16 \cdot t} &\equiv 1 \mod n \end{aligned}\right\}$$

561 ist keine starke Pseudoprimzahl zur Basis $b = 2$.

(demnach ist 561 eine starke Pseudoprimzahl zur Basis $b = 50$)

(b) Sei $n = 91 = 7 \cdot 13$ & $b = 10$.

Es ist $n - 1 = 90 = 2 \cdot \underbrace{45}_{t}$

Wegen $b^t \equiv -1 \mod 91$ ist 91 eine starke Pseudoprimzahl zur Basis $b = 10$.