Kryptologie: Übungsblatt 9, Besprechung ab dem 25.6.2018, 10:15, H20

83.) Du musst den diskreten Logarithmus berechnen. Also, gegeben ist n (Primzahl) und a (eine Primitivwurzel modulo n) sowie $y < n$. Gesucht ist x, so dass $y = a^x \bmod n$. Die Zahlen bestehen aus Hunderten von Dezimalziffern; eine "Brute Force"-Suche nach x ist also völlig ausgeschlossen.

Jemand behauptet, er hätte einen effizienten Algorithmus zur Verfügung, der für 1 Prozent aller z tatsächlich den diskreten Logarithmus von z berechnen könne. (Leider ist das fragliche y, für das du den diskreten Logarithmus berechnet möchtest, bei diesem 1 Prozent-Anteil nicht dabei.)

Gib einen effizienten (probabilistischen, Las Vegas-) Algorithmus an, der mit Hilfe dieses "1 Prozent-Algorithmus" den diskreten Algorithmus immer korrekt berechnen kann, insbesondere auch für dein y.

84.) Im Rahmen dieser Aufgabe soll unter einer "Einwegfunktion" eine bijektive Funktion $f : A \to A$ mit $f \in P$ und $f^{-1} \notin P$ verstanden werden. In diesem Sinne seien f und g Einwegfunktionen auf derselben Grundmenge A.

Zeige, dass die Hintereinanderausführung, erst f, dann g, ebenfalls eine Einwegfunktion ist. Dies sei die Funktion h. (Meine Notation hierfür ist $h = f \circ g$, nicht in Übereinstimmung mit manchen Mathe-Lehrbüchern.)

85.) Die Zahlen $n_1 = 4$ und $n_2 = 9$ sind teilerfremd. Der Chinesische Restsatz gibt eine bijektive Abbildung zwischen $\mathbb{Z}_4 \times \mathbb{Z}_9$ und $\mathbb{Z}_{36}$ an. Tatsächlich besteht auch eine bijektive Abbildung in Bezug auf die betreffenden reduzierten Restklassen, also zwischen $\mathbb{Z}_4^* \times \mathbb{Z}_9^*$ und $\mathbb{Z}_{36}^*$. Es ist $\mathbb{Z}_4^* = \{1, 3\}$, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ sowie $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$. Tragen Sie diese Bijektion in folgende Tabelle ein:

	1	2	4	5	7	8
1						
3						

86.) Sei $n = 113$. Berechne das Profil von $a = 2$ modulo n. Ist dieses regulär oder irregulär?

87.) Sei $n = 103$. Dies ist eine Primzahl. Man überprüfe mit dem Euler-Kriterium, dass $8 \in QR_{103}$ und berechne die Quadratwurzeln von 8 modulo 103.

88.) Sei $n = 437 = p \cdot q$, wobei $p = 19$ und $q = 23$. Bestimme alle Quadratwurzeln von $x = 100$ modulo 437.

89.) Sei n eine ungerade Primzahl und a teilerfremd zu n.

a) Was lässt sich folgern, wenn $a^{(n-1)/2} \equiv -1 \pmod{n}$?

mögliche Folgerungen:	**wahr**	**falsch**	**keine Aussage möglich**
a ist quadratischer Rest modulo n			
a ist Primitivwurzel modulo n			

b) Was lässt sich folgern, wenn $a^{(n-1)/2} \equiv +1 \pmod{n}$?

mögliche Folgerungen:	**wahr**	**falsch**	**keine Aussage möglich**
a ist quadratischer Rest modulo n			
a ist Primitivwurzel modulo n			

90.) [RP versus NP]
Bei der Definition von RP ist mit einer gewissen Wahrscheinlichkeit, die nach oben durch $\varepsilon \in (0, 1)$ beschränkt ist, bei Eingabe von $x \in A$ erlaubt, dass der probabilistische Algorithmus (fälschlicherweise) 0 ausgibt. Dementsprechend ist die Wahrscheinlichkeit, korrekt 1 auszugeben, mindestens $1 - \varepsilon$.

a) Man zeige, dass man die Wahrscheinlichkeit $1-\varepsilon$ hierbei ersetzen kann durch $1/p(|x|)$, wobei p ein Polynom ist. Die Klasse RP ändert sich bei dieser alternativen Definition nicht.

b) Man zeige, dass ein Entscheidungsproblem A in NP liegt, genau dann wenn es einen probabilistischen Algorithmus gibt, analog wie bei RP, nur dass die Wahrscheinlichkeit bei Eingabe $x \in A$ (korrekt) 1 auszugeben, nur noch $2^{-p(|x|)}$ beträgt (wobei p ein Polynom ist).

91.) Berechnen Sie das Jacobi-Symbol $\left(\frac{3}{105875}\right)$ unter Zuhilfenahme der Primfaktorzerlegung $105875 = 5^3 \cdot 7 \cdot 11^2$.

Berechnen Sie dieses Jacobi-Symbol nochmals mittels der Methode der Prozedur *Jacobi*.