Kleiner Fermatscher Satz

Wenn p eine Primzahl ist und 0< a < p ist, dann gilt $a^{p-1} \underset{p}{\equiv} 1$.

1.) Wenn man bei **a^(p-1) mod p** eine 1 herausbekommt, ist p weiterhin ein K**andidat** für Primzahlen, ob p dann wirklich Primzahl ist, muss man anderweitig prüfen. Die Umkehrung dieses Sates gilt nicht. Zum Beispiel ist 8^8 mod 9 = 1

2.) Bei a=1 kommt immer 1 heraus. p ist Kandidat für Primzahl, aber das ist nun gar kein Erkenntnisgewinn. Also hat Janine Steinberg völlig recht, 1 einzusetzen, ist nicht verboten, aber es lohnt nicht.

3.) a darf genommen werden aus den Zahlen in **Z*(p**). Da ist 0 nicht drin. Wenn man **dann** bei a^(p-1) mod p **keine 1** herausbekommt, ist p sicher **keine** Primzahl. Und das gilt auch für p=2. In der Vorlesung haben wir nämlich an dieser Stelle nicht bedacht, dass Z*(2) ausschließlich die 1 enthält. Nun ist aber 1^(2-1) mod 2=1, also gilt der "kleine Fermat" auch für p=2.

4) Es zeigt sich hier für mich ein grundsätzliches Problem. Die **Einschränkung auf** habe ich nicht betont, um diese Stelle in der Vorlesung nicht mit weiteren Begriffen zu belasten. Es ist ja klar, dass ich als a weder p selbst noch Vielfache davon nehmen darf, dann erhalte ich immer 0 als Ergebnis. Daher durfte ich nämlich bei p=2 auch nicht a=2=p nehmen.

5) Man kann im kleinen Fermatschen Satz noch mehr Basen a zulassen. Für Primzahlen ist **Z*(p)** ={1,2,....,p-1}. Darum steht oben auch 0<a<p. Aber man kann auch alle a zulassen, die nicht Vielfache von p sind. Das sind die b mit b mod p ungleich 0. Man kann sie schreiben als b=a+np mit 0<a<p. Aus a^(p-1) mod p =1 folgt b^(p-1)=(a+np)^(p-1)=a^(p-1)+np A mod p = 1+ 0= 1. Dabei ist A Abkürzung für eine lange Summe. Uff!!!.

"Kleiner Fermat": Wenn p eine Primzahl, die nicht a teilt, dann gilt $a^{p-1} \underset{p}{\equiv} 1$.

Es ist eben immer eine Gratwanderung, wenn mann sich aufmacht, **Mathematik für alle** erklären zu wollen. Entweder droht der Absturz, weil man nicht so genau war, wie es die mathematische Theorie erfordert. Andererseits droht der Absturz, weil bei zuviel mathematischer Theorie keiner mehr zuhören mag.

Ich habe mich entschieden, in dieser Vorlesung die Exaktheit zurückzudrängen und die Hörer und ihre Möglichkeiten zum Maßstab zu machen. Für unerschrockene Interessenten liefere ich gern das Genaue nach.
Sie finden den exakten Aufbau der hier zuständigen Algebra und Zahlentheorie auf www.mathematik-verstehen.de unter Kryptografie .

Aber ich freue mich darüber, dass einige "es auf den Punkt bringen" wollen. Das zeigt ja nur, dass Mathematik spannend und vielschichtig ist.