

Blatt 9

Aufgabe 1

Schreiben Sie ein Pari- oder Sage-Programm für das Pollard $(p-1)$ Faktorisierungsverfahren.

Benutzen Sie dieses, um die Zahl $n=$

50134924947513420874783890696108129678824480209797429859714017803551642090975977
87933106312314003034663815996880416684771534026078407209732467237556499994589447
49822387987555325498343910256847070191201979642721409922958169280013698169183021
zu faktorisieren. (Kein anderes Verfahren sollte dazu in der Lage sein.)

Um zu sehen, wie die Zahl n konstruiert wurde und wieso das Verfahren funktioniert, nehmen Sie den gefundenen Primfaktor p von n und geben z.B. in pari den Befehl `factor((n-1)/2)`.

Aufgabe 2

Auch wenn einigen von Ihnen diese Aufgabe schon bekannt ist:

Der österreichische Briefbombenattentäter Franz Fuchs hatte dummerweise angenommen, es würde mehrere Wochen dauern, eine auf der Basis des RSA-Moduls $n=$

630548215070129547156718332495889632234434145411971275888376987603
260225252787926135276738944105689100036295535868141424386536403649
578707699128189491432138631900590774729214990015369102760964884776
344849717811484309528915040117952098061886881

verschlüsselte Nachricht zu entschlüsseln.

Dabei findet man einen Faktor von n schon mit der einfachsten Version der Fermat-Faktorisierung!

a) Wie also lautet die Primfaktorzerlegung von n ?

b) Franz Fuchs hatte als öffentlichen Exponenten die Zahl $e=$

508075310835159009812633969174411123496728859672737076695139826186
257647581337481521676692825102982808222076238747753504407

gewählt, und die erste Zeile seiner verschlüsselten Botschaft sah so aus $c=$

463316335616613937318842101415083702006628892795168389554894402706
884035322375721126316678871052346087047872057770161604068825594947
480777575090664841774749749032122958886916388656231305149413112661
671360620310298582755616480043108904735117491

Finden Sie die Zahl $t \in \mathbb{Z}_n$, für die gilt $t^e = c$.

Wenn sie t als Dezimalzahl nehmen, interpretieren Sie jede 3-Zifferngruppe als Ascii-Code.

Wie lautete demnach die erste Zeile von Fuchsens Botschaft?

Aufgabe 3 Fermat-Faktorisierung mit Faktorbasis:

Auch dies eine Aufgabe aus dem letzten Jahr: Betrachten Sie die zusammengesetzte Zahl $n=48202631$.

Nehmen Sie als Faktorbasis $B=\{p_1, p_2, p_3, p_4, p_5\}=\{2,3,5,7,11\}$.

Wählen Sie solange zufällige Elemente $x \in \mathbb{Z}_n$, bis Sie 8 gefunden haben, für die x , als natürliche Zahl interpretiert, größer als \sqrt{n} ist und für die $z=x^2$, interpretiert als natürliche Zahl, in der Faktorbasis aufgeht.

Wir haben dann also $z_i=2^{\alpha_{1,i}} \cdot 3^{\alpha_{2,i}} \cdot 5^{\alpha_{3,i}} \cdot 7^{\alpha_{4,i}} \cdot 11^{\alpha_{5,i}}$ für $i=1, \dots, 8$.

Man bilde jetzt eine Matrix $A=(a_{j,i})$ mit 5 Zeilen und 8 Spalten und Koeffizienten in \mathbb{Z}_2 . Dabei sei $a_{j,i}=0$, falls $\alpha_{j,i}$ gerade und $a_{j,i}=1$, falls $\alpha_{j,i}$ ungerade. Man finde jetzt mehrere Vektoren $\lambda \in \mathbb{Z}_2^8$

mit $A\lambda=0$. Für ein solches λ berechne man $\prod_{i=1}^8 z_i^{\lambda_i} = \prod_{j=1}^5 p_j^{\sum_{i=1}^8 \alpha_{j,i} \lambda_i}$. Nun ist $\beta_j = \sum_{i=1}^8 \alpha_{j,i} \lambda_i$ gerade.

Setzt man $y = \prod_{j=1}^5 p_j^{\beta_j/2}$ und $x = \prod_{i=1}^8 x_i^{\lambda_i}$, so folgt $x^2 = y^2$ als Gleichung in \mathbb{Z}_n .

Man benutze diese Gleichung zur Faktorisierung von n , ggf. durch Zuhilfenahme weiterer Lösungen λ der Gleichung $A\lambda=0$.