

Übungen zu Theoretische Informatik 3

*A very special case of this theorem^a was stated by the Chinese mathematician Sun-Tsu, who gave a rule called *tái-yen* (“great generalization”); the date of his writing is very uncertain, it may have been as early 200 B.C. or as late as 200 A.D. Curiously, the Greek mathematician Nichomachus gave exactly the same special case of the theorem about the same time (100 A.D.). The Theorem was apparently first stated and proved in its proper generality by L. Euler in 1734, although a description of most of the necessary principles was given in China by Chhin Chiu-Shao in his *Shu Shu Chiu Chang* (1247).*

D.E. Knuth in Kap. 4.3.2 von TAOCP

^aChinesischer Restesatz

• Aufgabe 26: Modulare Arithmetik

1. Berechnen Sie das Produkt $x = 23 \times 41$, indem Sie die Information verwenden, daß $0 \leq x < 990 = 9 \cdot 10 \cdot 11$ ist.
2. Berechnen Sie mittels *modularer Arithmetik* die Determinante der Matrix

$$M = \begin{bmatrix} -3 & 12 & -13 \\ 12 & -64 & 72 \\ -13 & 72 & -83 \end{bmatrix}$$

wobei Sie folgende Informationen verwenden:

$$0 \leq |\det M| < 84 \quad \text{und} \quad 3 \cdot 7 \cdot 8 = 168.$$

3. Bestimmen Sie die modulare Darstellung (Partialbruchzerlegung) des Bruches $2333/900$, bei der Sie die Primfaktorisierung des Nenners benutzen.

• Aufgabe 27: Chinesischer Restesatz für beliebige Moduln

1. Welche ganzen Zahlen x erfüllen das Kongruenzsystem

$$x \equiv 3 \pmod{8}$$

$$x \equiv 7 \pmod{12}$$

Beachten Sie, daß die Moduln 8 und 12 nicht teilerfremd sind! Zeigen Sie, daß das System mit teilerfremden Moduln

$$x \equiv 3 \pmod{8}$$

$$x \equiv 1 \pmod{3}$$

äquivalent zu dem zuerst gegebenen System ist, d.h. die gleiche Lösungsmenge hat. Lösen sie dieses zweite System.

2. Ist folgendes Kongruenzsystem ganzzahlig lösbar?

$$x \equiv 5 \pmod{8}$$

$$x \equiv 7 \pmod{12}$$

3. Ersetzen sie das System von Kongruenzen

$$x \equiv 5 \pmod{8}$$

$$x \equiv 7 \pmod{14}$$

$$x \equiv 21 \pmod{35}$$

durch ein äquivalentes System mit teilerfremden Moduln und lösen sie dieses.

• **Aufgabe 28: Eine Aufgabe aus einem chinesischen Rechenbuch**

In dem Rechenbuch *Shu-Shu Chiu-Chang* des bedeutenden chinesischen Mathematikers CH'IN CHIU-SHAO (1202–1261) findet sich folgende Aufgabe:

Drei Bauern teilen ihre gemeinsame Reisernte gleichmässig unter sich auf und jeder bringt seinen Anteil zu einem Markt. Auf dem ersten Markt wird ein Gewicht von 83 Pfund zum Abmessen benutzt, auf dem zweiten Markt ein Gewicht von 110 Pfund, auf dem dritten Markt ein Gewicht von 135 Pfund. Jeder von den drei Bauern verkauft so viele volle Maße wie möglich. Als sie wieder nach Hause kommen, hat der erste 32 Pfund Reis übrig, der zweite bringt 70 Pfund zurück und der dritte 30 Pfund. Wieviel Reis habe sie insgesamt auf den Markt gebracht?

1. Formulieren sie diese Aufgabe als System von Kongruenzen, also im Kontext des chinesischen Restesatzes.
2. Sie werden feststellen, daß die Moduln nicht teilerfremd sind. Ersetzen sie das Kongruenzsystem durch ein gleichwertiges, aber mit paarweise teilerfremden Moduln.
3. Lösen sie dieses System. (Unterstützung durch Taschenrechner kann hilfreich sein — aber bedenken sie, dass CH'IN CHIU-SHAO und seine Schüler solche Hilfsmittel nicht hatten).

• **Aufgabe 29: Zeugen für Primtests**

1. Bestimmen Sie für die zusammengesetzte Zahl $N = 21$ die Mengen der Teilbarkeits-, Euklid-, Fermat und Miller-Rabin-Zeugen.
2. Bestimmen Sie für die zusammengesetzte Zahl $N = 105$
 - einen Teilbarkeits-Zeugen;
 - einen Euklid-Zeugen, der kein Teilbarkeitszeuge ist;
 - einen Fermat-Zeugen, der kein Euklid-Zeuge ist;
 - einen Miller-Rabin-Zeugen, der kein Fermat-Zeuge ist.

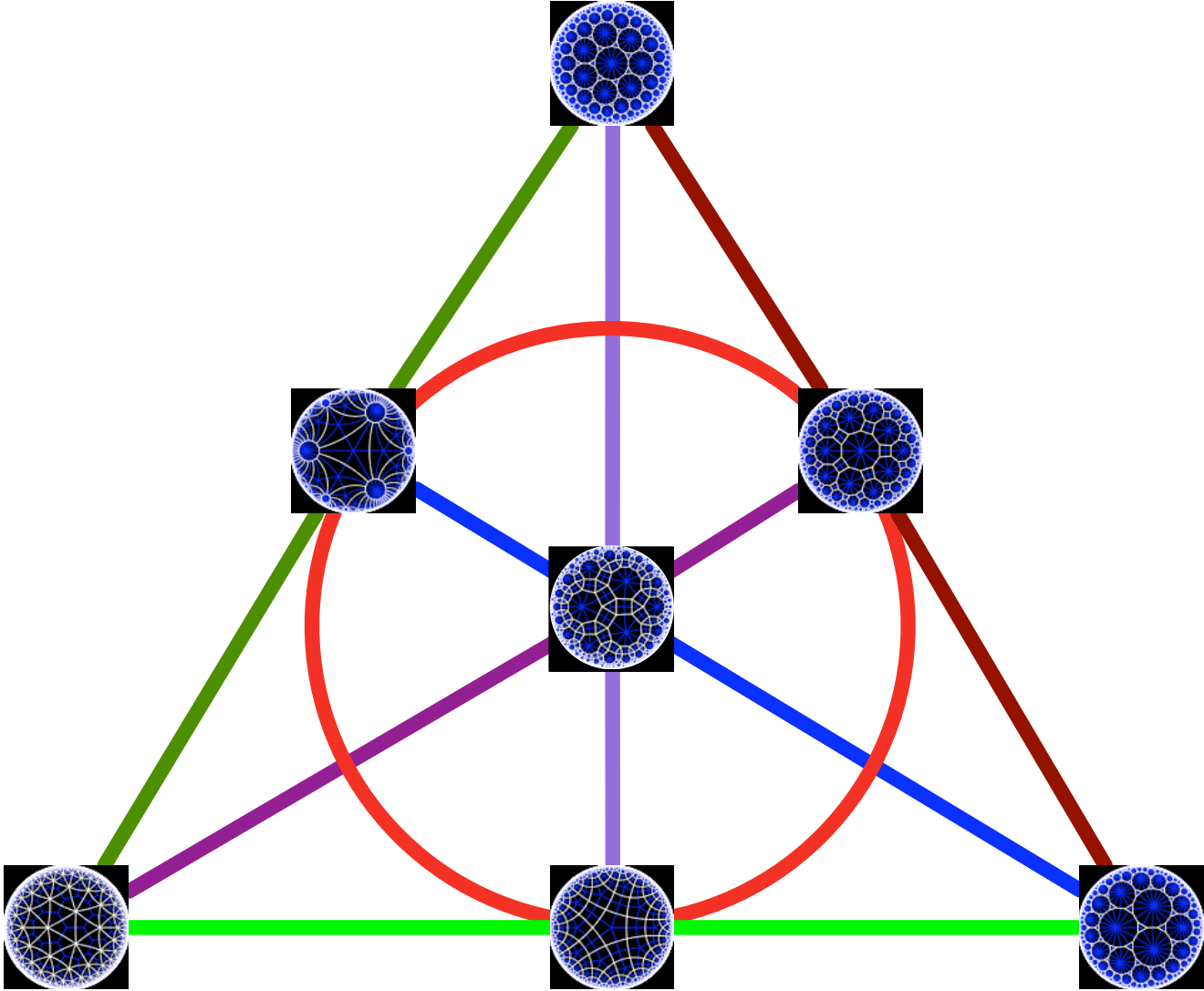
• **Aufgabe 30: Eine Pseudoprimzahl**

Die Zahl $N = 3828001$ ist keine Primzahl ist, obwohl sie die Bedingung der FERMAT-Kongruenz

$$(F) \quad \forall a \in \mathbb{Z} : \text{ggT}(a, N) = 1 \Rightarrow a^{N-1} \equiv 1 \pmod{N}$$

erfüllt.

1. Beschaffen Sie sich die Primfaktorisierung von N (woher auch immer, alles ist erlaubt) und weisen Sie nach, dass (F) gilt.
NB: Wie im Fall $N = 561$ (Vorlesung) gilt: wenn Sie glauben, hierfür viel rechnen zu müssen, haben Sie möglicherweise etwas noch nicht verstanden.
2. Bestimmen Sie einen Miller-Rabin-Zeugen für die Nicht-Primheit von N .



Erholsame Feiertage und einen guten Start ins neue Jahr!