ulm university universität ulm

Übungen zur Angewandten Diskreten Mathematik

Dr. Hartmut Lanzinger, Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 14. Dezember 2012, vor den Übungen

1. Überpüfe, ob die gegebenen Systeme von Kongruenzen lösbar sind und bestimme im positiven Fall die kleinste positive Lösung.

   (a) $\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 3 \bmod 10 \\ x \equiv 13 \bmod 15 \end{cases}$

   (b) $\begin{cases} x \equiv 3 \bmod 4 \\ x \equiv 2 \bmod 7 \\ x \equiv 1 \bmod 8 \end{cases}$ (10 Punkte)

2. Es gilt $11^2 \equiv 14 \bmod 107$. Außerdem sind 53 und 107 Primzahlen.
   Bestimme $\operatorname{ord}_{107} 14$ mit Hilfe dieser Beobachtungen. (4 Punkte)

3. Wir wollen nun nachvollziehen, wie Leonhard Euler dazu kam, die Fermatzahl F_5 gerade auf den Primfaktor 641 zu untersuchen.
   Es sei $F_k = 2^{2^k} + 1$ die k- te Fermatzahl mit $k \geq 2$.
   Zeige:

   (a) Falls F_k eine Fermatsche Primzahl ist, gilt
   $$F_k = 2^{k+2} \cdot a + 1$$
   mit einem $a \in \mathbb{N}$.

   (b) Falls F_k zusammengesetzt ist, lässt sich jeder Primfaktor p von F_k in der Darstellung von Teilaufgabe a) schreiben.

   <u>*Hinweis:*</u>
   Bestimme zuerst $\operatorname{ord}_p 2$.
   Es darf ohne Beweis benützt werden, dass für $p \equiv 1 \bmod 8$ ein $x \in \mathbb{Z}$ existiert, so dass die Kongruenz $x^2 \equiv 2 \bmod p$ Lösungen besitzt.

   (c) Folgere daraus, dass 641 als Primfaktor von F_5 infrage kommt. (10 Punkte)