Aufgabe 1.
Es seien die *Fermat-Zahlen* gegeben durch

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \ldots.$$

a) Zeigen Sie die Rekursionsformel

$$\prod_{k=0}^{n-1} F_k = F_n - 2, \quad n \geq 1.$$

b) Zeigen Sie, dass je zwei verschiedene Fermat-Zahlen relativ prim sind und folgern Sie, dass es unendlich viele Primzahlen gibt.

Lösung:
a) vollständige Induktion
b) Ein gemeinsamer Teiler von F_k und F_n muss nach a) auch 2 teilen. Die Fermatzahlen sind aber sämtlich ungerade.

Aufgabe 2.
Sei p eine *Fermatsche Primzahl*, d.h. p sei von der Gestalt

$$p = 2^{2^n} + 1, \quad n \geq 1.$$

Zeigen Sie:
a) Die quadratischen Nichtreste modulo p sind Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$.
b) Für $p \neq 5$ ist 5 ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$.

Lösung:
a) Sei a ein quadratischer Nichtrest modulo p. Wir setzen in die bekannte Formel

$$\overline{\left(\frac{a}{p}\right)} = \overline{a}^{\frac{p-1}{2}} \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

ein und erhalten

$$\overline{a}^{\frac{p-1}{2}} = \overline{-1} \neq \overline{1} \quad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

Nun ist aber $p - 1 = 2^{2^n - 1}$, und somit ist auch die Ordnung $ord(\overline{a})$ eine Potenz von 2. Aus $ord(\overline{a}) \nmid \frac{p-1}{2}$ folgt, dass a Primitivwurzel modulo p ist.
b) Ist $p \neq 5$, dann ist entweder $p = 3$ (und 5 ist Primitivwurzel modulo 3) oder $p = 2^{2^n} + 1$ mit $n \geq 2$. Dann ist aber $p \equiv 2$ (5) und nach dem quadratischen Reziprozitätsgesetz erhalten wir

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$$

und die Behauptung folgt aus a).

Aufgabe 3.
Um vom Bismarckplatz zum Hauptbahnhof zu gelangen, kann man die Buslinien 32 und 34 sowie die OEG nehmen. Alle drei Linien fahren um 8.00 Uhr ab und danach in regelmäßigen Abständen von 3, 5 und 16 Minuten:

Linie 32	8.00	8.03	8.06	...
Linie 34	8.00	8.05	8.10	...
OEG	8.00	8.16	8.32	...

Carl Friedrich kommt vor 12 Uhr am Bismarckplatz vorbei und sieht auf der Anzeige, dass der nächste Bus der Linie 32 in 2 Minuten, der nächste Bus der Linie 34 in 3 Minuten und die nächste OEG in 5 Minuten kommt. Wieviel Uhr ist es?

Lösung:
Bezeichne n die Anzahl der Minuten, die seit 8.00 Uhr vergangen sind. Dann gilt $n \equiv 1\ (3)$, $n \equiv 2\ (5)$ *und* $n \equiv 11\ (16)$. *Man rechnet mit dem Algorithmus aus dem Chinesischen Restsatz* $n \equiv 187\ (240)$ *nach und damit* $n = 187$, *da* $n < 240$ *nach Voraussetzung. Es ist also 11.07 Uhr.*

Aufgabe 4.
Geben Sie die Zerlegung des Polynoms

$$f(X) = X^5 - 1 \in \mathbb{Z}[X]$$

in irreduzible Faktoren an.
(Hinweis: Man spalte einen Linearfaktor ab und zeige, dass der entstehende zweite Faktor irreduzibel ist.)

Lösung:

$$X^5 - 1 = (X - 1)\ (1 + X + X^2 + X^3 + X^4).$$

Der zweite Faktor, nennen wir in $g(X)$, *ist irreduzibel, da* $g(X + 1)$ *ein Eisensteinpolynom bzgl.* 5 *ist.*