Karlsruher Institut für Technologie

Institut für Algebra und Geometrie
PD Dr. Fabian Januszewski
Tobias Columbus

Faktorisierung natürlicher Zahlen

Übungsblatt 1

Aufgabe 1 (2 Punkte)

(a) Berechnen Sie ein multiplikatives Inverses von 37 in $\mathbf{Z}/(40)$.

(b) Es seien $f = x^4 + 3x^3 - 4x^2 - 5x - 7$ und $g = x^3 - 1$ Polynome aus $\mathbf{Q}[x]$. Berechnen Sie mit dem erweiterten euklidischen Algorithmus den größten gemeinsamen Teiler d von f und g sowie eine Darstellung $d = af + bg$ mit $a, b \in \mathbf{Q}[x]$.

Aufgabe 2 (2 Punkte)
Faktorisieren Sie die Zahlen

(a) $176653 = 78^2 + 413^2 = 138^2 + 397^2$ und
(b) $20386777 = 236^2 + 4509^2 = 3156^2 + 3229^2$

mit der Methode von Leonhard Euler.

Aufgabe 3 (4 Punkte)
Faktorisieren Sie die Zahlen

(a) $N = 5456887$ mit $\lceil N^{1/2} \rceil = 2336$,
(b) $N = 7676063$ mit $\lceil N^{1/2} \rceil = 2771$ und
(c) $N = 68084509$ mit $\lceil N^{1/2} \rceil = 8252$

mit der Methode von Pierre Fermat.

Aufgabe 4 (4 Punkte)

(a) Installieren Sie die Bibliothek `GMP` für Langzahlarithmetik sowie das Python-Interface `gmpy` auf Ihrem Computer oder nutzen Sie die Computer des Rechenzentrums.

(b) Schreiben Sie eine Funktion mit der Signatur

```
factor(N, B),
```

die einen Primteiler p von N mit $2 \leq p \leq \min(B, \lfloor \sqrt{N} \rfloor)$ sucht. Findet die Funktion einen solchen Primteiler p, so gibt sie das Tupel `(True, p)` zurück — andernfalls `(False, None)`. Verwenden Sie zur Auflistung der Primzahlen p mit $2 \leq p \leq \min(B, \lfloor \sqrt{N} \rfloor)$ die Funktion `gmpy.next_prime`.

(c) Können Sie mit Ihrem Programm die natürlichen Zahlen
(i) 10002200057,
(ii) 1434066926429,
(iii) 248659641376093 und
(iv) 23718387370018463
faktorisieren?

Aufgabe 5 (4 Punkte)
Implementieren Sie mit `gmpy` den Algorithmus von Fermat und faktorisieren Sie mit Ihrem Programm die natürlichen Zahlen aus Aufgabe 4 sowie die Zahlen

(a) 12330057232561 und
(b) 105186267544111029958651.

Abgabe am Donnerstag, den 5. 11. 2015, in der Übung.