Aufgabe 1. Implementiere unter Verwendung der GMP ein Modul, welches die Punktegruppe einer elliptischen Kurve implementiert. Es sollten mindestens Funktionen zur Verfügung stehen, eine Kurve zu gegebenen Parametern a und b zu erzeugen und Punkte auf dieser Kurve zu addieren. Zum Testen empfehlen wir folgende Parameter:

$$E := \left\{ (x, y) \in \mathbb{F}_p^2 \,\middle|\, y^2 = x^3 + ax + b \right\} \cup \{ \mathcal{O} \}$$

mit den folgenden Parametern aus dem Brainpool Standard [1]:

```
Curve-ID: brainpoolP256r1
p = A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D526202820
    13481D1F6E5377
a = 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE9
    4A4B44F330B5D9
b = 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6B
    CCDC18FF8C07B6
x = 8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A
    4453BD9ACE3262
y = 547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C
    1D54C72F046997
q = A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F790
    1E0E82974856A7
h = 1
```

Die Parameter sind im Hexadezimalsystem angegeben. Hier ist außerdem $g = (x, y)$ ein Punkt auf der Kurve ist und $q = |\langle g \rangle|$ die Anzahl Punkte in der von g erzeugten Untergruppe.

Aufgabe 2. Implementiere Lenstras EC-Faktorisierungsalgorithmus (Pseudocode und Beispielzahl auf der Rückseite).

[1] http://www.ecc-brainpool.org/download/draft-lochter-pkix-brainpool-ecc-00.txt

```
0x2D42080FCFBC71D2EA9A7BE2CCB954C8749C90CAB5547E2D2C17
  23B5C9BBE302ED0405CCCBD4B7CDAF35F98B7094D420D77BDA9C
  966BC3394783502595C9C86BB0DA603826C159F23D73057E4865
  527B437418A0D83ABC5AE9DE0E30DB7A5FF6F420682E79E1CC01
  45A09C4CDDDF7F73AEBA1D013226835AA7CDEC03D3D4B4181212
  A5EAD2C1C6AC321B7DD93F93BF90B792FED921ACEF4304526218
  171CED29428D7627F20085D95EF8260F84BD2CF4F46DE29BB7C2
  19381F68F61A19CF3EE725C54E9531808912F635FD37EA50A5BD
  9C33215B03219AA78981EEE9B46360B555250FF5A80615A4FD97
  76A887BA17DE38E63005AC42EF8552334E36E909E5427
```

Algorithmus 1 Lenstras EC-Faktorisierungsalgorithmus

Input: Zahl $n \in \mathbb{Z}_+$.
Output: Ein Teiler d von n

Wähle zufällige $x_0, y_0, a \in \mathbb{Z}_n$
set $b := y_0^2 - x_0^3 - ax_0$
Sei E die Kurve zu den Parametern a und b.
set $p := (x_0, y_0) \in E$
for $m = 2, 3, 4, \ldots$ **do**
    set $p := m \cdot p \pmod{n}$
    if Berechnung schlägt fehl **then**
        Wir haben ein x gefunden, welches kein Inverses modulo n hat.
        set $d := \gcd(x, n)$
        if $d < n$ **then**
            return d
        else if $d = n$ **then**
            Starte Algorithmus neu
        end if
    end if
end for