KRY: Wahlfach Kryptologie
Serie 12: Modulare Wurzeln, Addition auf elliptischen Kurven

Aufgabe 1 (P)
Erstellen Sie für die Klasse `BigInteger` der Package `mybiginteger` eine Methode

`BigInteger myModSqrt(BigInteger p)`,

welche entscheidet, ob Quadratwurzeln von `this` in $\mathbb{Z}_p^*$ existieren, und falls ja nach dem Algorithmus von Tonelli eine davon berechnet und zurückgibt. Falls keine Lösung existiert, soll die Methode den Wert `-1` (vom Typ `BigInteger`) zurückgeben. Überprüfen Sie den Algorithmus in der Testumgebung "Prakt. 12.1".

Tests

(1) **Eingabe:** $n = 10$, $p = 31$. **Ausgabe:** 14 oder 17.

(2) **Eingabe:** $n = 37$, $p = 41$. **Ausgabe:** 23 oder 18.

Aufgabe 2 (P)
Schreiben Sie für die Klasse `BigInteger` der Package `mybiginteger` eine Methode

`BigInteger[] elliptAdd (BigInteger P_y, BigInteger Q_x, BigInteger Q_y, BigInteger p, BigInteger a, BigInteger b)`,

die falls möglich über dem Körper $K = GF(p)$ für die elliptische Kurve E: $y^2 = x^3 + ax + b$ den Punkt $R = P + Q$ berechnet und zurückgibt. Falls P = (`this`, `P_y`) oder Q = (`Q_x`, `Q_y`) nicht zu E gehören, so soll eine `NumberFormatException` mit der Nachricht `Punkt liegt nicht auf der Kurve!` ausgegeben werden. Der unendlich ferne Punkt O soll in der Form $(p, *)$ entgegengenommen bzw. zurückgegeben werden, wobei $*$ ein beliebiger Wert sein darf (weil er nirgends weiter beachtet wird). Überprüfen Sie den Algorithmus in der Testumgebung "Prakt. 12.2".

Tests

(1) **Eingabe:** $p = 13$, $a = 2$, $b = 7$, $P = (3, 12)$, $Q = (6, 1)$. **Ausgabe:** $(3, 1)$

(2) **Eingabe:** $p = 13$, $a = 2$, $b = 7$, $P = (3, 12)$, $Q = (3, 1)$. **Ausgabe:** O

(3) **Eingabe:** $p = 13$, $a = 2$, $b = 7$, $P = (13, 4)$, $Q = (6, 12)$. **Ausgabe:** $(6, 12)$