Wolfgang K. Seiler
Tel. 2515

B6, B4.18

18. Mai 2020

10. Übungsblatt Elliptische Kurven

Aufgabe 1: *(4 Punkte)*
Faktorisieren Sie $N = 72\,263$ nach Pollards $(p-1)$-Methode mit Suchgrenze $B = 10$!

Lösung: Um zumindest am Anfang kleine Zahlen zu haben, versuchen wir es mit der Basis $a = 2$. Die kleinste Primzahl p ist zwei, und $2^3 = 8$ ist ihre größte Potenz unterhalb von $B = 10$. Also ersetzen wir a durch $2^8 \bmod N = 256$. Die nächste Primzahl ist drei, und $3^2 \le B$, als wird a ersetzt durch $256^9 \bmod N$. Da 256^9 für die meisten Taschenrechner bereits zu groß sein wird, potenzieren wir zweimal mit drei: $256^3 = 16\,777\,216$; modulo N ist das $12\,200$. Die dritte Potenz davon ist $1\,815\,848\,000\,000$; modulo N erhalten wir $67\,314$ als neues a.

Die nächste Primzahl ist fünf, und $5^2 > B$; also potenzieren wir mit fünf. Da die fünfte Potenz von $67\,314$ recht groß ist, verwenden wir dazu die binäre Methode. Das Quadrat von $67\,314$ ist $4\,531\,174\,596$ mit Rest $67\,707$ bei Division durch N. Das Quadrat davon ist $4\,584\,237\,849$, was modulo N zu $17\,655$ wird. Um die fünfte Potenz zu erhalten, müssen wir das noch mit $a = 67\,314$ multiplizieren; das Produkt ist $1\,188\,428\,670 \equiv 63\,635 \bmod N$. Also wird a ersetzt durch $a^5 \bmod N = 63\,635$.

Als letzte Potenz müssen wir noch die siebte Potenz davon berechnen: Das Quadrat ist $4\,049\,413\,225 \equiv 11\,494 \bmod N$, was wiederum das Quadrat $132\,112\,036 \equiv 15\,272 \bmod N$ hat. Die siebte Potenz ist das Produkt der drei berechneten Zahlen:

$$\begin{gathered} 63\,635 \cdot 11\,494 = 731\,420\,690 \equiv 46\,867 \bmod N \\ 46\,867 \cdot 15\,272 = 715\,752\,824 \equiv 60\,072 \bmod N\,. \end{gathered}$$

Falls der Ansatz erfolgreich war, ist dies kongruent eins modulo einem, aber nicht allen Teilern von N. Euklid gibt uns

$$\begin{gathered} 72\,263 : 60\,071 = 1 \text{ Rest } 12\,192 \\ 60\,071 : 12\,192 = 4 \text{ Rest } 11\,303 \\ 12\,192 : 11\,303 = 1 \text{ Rest } 889 \\ 11\,303 : 889 = 12 \text{ Rest } 635 \\ 889 : 635 = 1 \text{ Rest } 254 \\ 635 : 254 = 2 \text{ Rest } 127 \\ 254 : 127 = 2 \text{ Rest } 0 \end{gathered}$$

Damit haben wir den Teiler 127 von N gefunden. $72\,263 : 127 = 569$, also ist $N = 127 \cdot 569$, wobei beide Faktoren Primzahlen sind. Die Methode war erfolgreich, weil $126 = 2 \cdot 3^2 \cdot 7$ nur durch Primzahlpotenzen unterhalb der Suchgrenze teilbar ist, $568 = 2^3 \cdot 71$ aber mit 71 einen Teiler hat, der darüber liegt.

Aufgabe 2: *(3 Punkte)*
p sei eine Primzahl und g eine primitive Wurzel modulo p, d.h. alle Elemente von $\mathbb{F}_p^\times$ lassen sich als Potenzen von g darstellen. Zeigen Sie, daß dann $a_i = g$ für jeden Primteiler p_i von $p-1$ die Bedingungen des Primzahltests von POCKLINGTON erfüllt!

Lösung: Wir müssen zeigen, daß $g^{p-1} \equiv 1 \bmod p$ ist, was aus dem kleinen Satz von FERMAT folgt, und daß für jeden Primteiler p_i von $p-1$ gilt $\operatorname{ggT}(g^{(p-1)/p_i} - 1, p) = 1$. Da g eine primitive Wurzel ist, hat g die Ordnung $p-1$, so daß $g^{(p-1)/p_i} \bmod p$ ungleich eins sein muß. Damit ist $g^{(p-1)/p_i} - 1$ nicht durch p teilbar, und da p eine Primzahl ist, muß der größte gemeinsame Teiler der beiden Zahlen eins sein.

Aufgabe 3: *(6 Punkte)*
E sei modulo 35 gegeben durch die Gleichung $y^2 = x^3 + x + 3$. Faktorisieren Sie 35, indem Sie das Vierfache des Punktes $(1,4)$ berechnen!

Lösung: Zur Anwendung der Verdoppelungsformel berechnen wir zunächst in $\mathbb{Z}/35$ die Steigung

$$m = \frac{3 \cdot x_1^2 + a}{2y_1} = \frac{4}{8} = \frac{1}{2} = 18$$

im Punkt P. (Das Doppelte von 18 ist $36 = 35 + 1$.) Die Koordinaten von $2P$ sind somit

$$x_3 = m^2 - 2x_1 = 18^2 - 2 = 322 = 7 \quad \text{und} \quad y_3 = m(x_1 - x_3) - y_1 = 18 \cdot (-6) - 4 = -112 = 28\,,$$

d.h. $2P = (7, 28)$. Anwendung der Verdoppelungsformel darauf liefert die neue Steigung

$$m = \frac{3 \cdot 7^2 + 1}{2 \cdot 28} = \frac{148}{56} = \frac{8}{21}\,.$$

Zur Inversion von 21 müssen wir den erweiterten EUKLIDischen Algorithmus anwenden auf 35 und 21:

$$\begin{aligned} 35 : 21 &= 1 \text{ Rest } 14 \Longrightarrow 14 = 35 - 21 \\ 21 : 14 &= 1 \text{ Rest } 7 \Longrightarrow 7 = 2 \cdot 21 - 35 \\ 14 : 7 &= 2 \text{ Rest } 0 \end{aligned}$$

Damit ist der ggT 7 ein echter Teiler von 35, und wir haben die Faktorisierung $35 = 5 \cdot 7$ gefunden.

Aufgabe 4: *(7 Punkte)*

E sei in der affinen Ebene über $\mathbb{Z}/29\mathbb{Z}$ gegeben durch die Gleichung $y^2 = x^3 + x + 5$.

a) Zeigen Sie, daß der Punkt $(3, 8)$ der zugehörigen projektiven Kurve die Ordnung 15 hat.

Lösung: Die Verdoppelungsformel liefert für $P = (3, 8)$ nacheinander die Punkte

$$2P = (17, 11), \qquad 4P = (1, 6) \quad \text{und} \quad 8P = (11, 10)\,.$$

Daraus können wir schrittweise nach der Additionsformel $15P$ berechnen:

$$3P = 2P + P = (17, 11) + (3, 8) = (16, 12), \quad 7P = 4P + 3P = (1, 6) + (16, 12) = (11, 19)$$

und $15P = 8P+7P = (11, 10)+(11, 19) = \mathcal{O}$, da wir gleiche x-Koordinate, aber verschiedene y-Koordinaten haben. Die Ordnung ist also ein Teiler von 15 und nicht drei, da $3P \neq \mathcal{O}$. Sie könnte noch fünf sein, aber $5P = 4P + P = (26, 27) \neq \mathcal{O}$. Somit muß die Ordnung gleich 15 sein.

b) Folgern Sie daraus, daß 29 eine Primzahl ist.

Lösung: Der Punkt $P_1 = 3P$ erfüllt die Gleichung $5P_1 = 15P = \mathcal{O}$, und $P_2 = 5P$ erfüllt die Gleichung $3P_2 = 15P = \mathcal{O}$. Das Produkt der beiden Primzahlen drei und fünf ist fünfzehn und damit größer als $(\sqrt[4]{29}+1)^2 \approx 11{,}026$. Damit sind die Bedingungen des Primzahltests mit elliptischen Kurven erfüllt, d.h. 29 ist eine Primzahl.