Vertiefung Elementare Zahlentheorie

WS 2010/2011, Lösungen zur Klausur 1, 4.2.2011

Bei Rechenaufgaben ist meist nur das Resultat angegeben. Andererseits sind Kommentare angefügt, die natürlich nicht zur eigentlichen Lösung gehören.

Lösung 1. $\mathrm{ggT}(1099, 210) = 7 = 13 \cdot 1099 - 68 \cdot 210$

Folgende Probe bietet sich an: 210 hat die Primfaktor-Zerlegung $2 \cdot 3 \cdot 5 \cdot 7$; 1099 wird nicht von 2, 3, 5 geteilt, wohl aber von 7. Die lineare Darstellung überprüft man durch Ausrechnen.

Lösung 2. $x \equiv 59 \pmod{60}$

Hier sollte man unbedingt die Probe machen!

Lösung 3.

(a) $234^{234} \equiv 3^{234} \equiv 3^4 \equiv 4 \pmod{11}$, $100^{100} \equiv 2^{100} \equiv 2^4 \equiv 2 \pmod{7}$

Hier wird jeweils im zweiten Schritt der Satz von Fermat angewendet.

(b) $333^{999} \equiv 3^{999} \equiv 3^3 \equiv 7 \pmod{10}$, also Endziffer 7.

Hier darf man sich natürlich nicht auf den Satz von Fermat berufen, denn 10 ist ja keine Primzahl! Aber man kann im zweiten Schritt den Satz von Euler anwenden, da 3 teilerfremd zu 10 ist; dabei benötigt man $\phi(10) = 4$.
Andere Möglichkeit: Man verwendet den chinesischen Restsatz und für die Primzahl 5 dann doch den Satz von Fermat:

$3^{999} \equiv 1 \pmod{2}$ und $3^{999} \equiv 3^3 \equiv 2 \pmod{5}$, also wieder $3^{999} \equiv 7 \pmod{10}$

Lösung 4. Die Behauptung ist eine einfache Umformulierung des Satzes von Wilson; siehe Übungen!

Lösung 5.

(a) $60 = 2^2 \cdot 3 \cdot 5$, $\phi(60) = 16$;

(b) $81 = 3^4$, $\phi(81) = 54$;

(c) $1000 = 2^3 \cdot 5^3 4$, $\phi(1000) = 400$;

(d) $1111 = 11 \cdot 101$, $\phi(1111) = 1000$.

Lösung 6.

(a)

i	0	1	2	3	4	5	6	7	8	9
2^i	1	2	4	8	5	10	9	7	3	6

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(a)$	0	1	8	2	4	9	7	3	6	5

(b) $x \equiv 5$ oder $6 \pmod{11}$

Lösung 7.

(a) $(\frac{120}{179}) = (\frac{4}{179}) \cdot (\frac{2}{179}) \cdot (\frac{3}{179}) \cdot (\frac{5}{179}) = 1 \cdot (-1) \cdot 1 \cdot 1 = -1$:
$(\frac{4}{179}) = 1$,
$(\frac{2}{179}) = -1$,
$(\frac{3}{179}) = -(\frac{179}{3}) = -(\frac{2}{3}) = 1$,
$(\frac{5}{179}) = (\frac{179}{5}) = (\frac{4}{5}) = 1$.

(b) $(\frac{121}{181}) = 1$ (denn $121 = 11^2$).

(c) $(\frac{122}{191}) = (\frac{2}{191}) \cdot (\frac{61}{191}) = 1 \cdot (-1) = -1$:
$(\frac{2}{191}) = 1$,
$(\frac{61}{191}) = (\frac{191}{61}) = (\frac{8}{61}) = (\frac{4}{61}) \cdot (\frac{2}{61}) = 1 \cdot (-1) = -1$.

Lösung 8. Die dritte Komponente eines primitiven pythagoreischen Tripels (x, y, z) besitzt bekanntlich eine Darstellung $z = u^2 + v^2$ mit $u > v > 0$, u und v teilerfremd, u und v nicht beide ungerade.

(a) Etwa durch Probieren (eigentlich sollte man es wissen) findet man genau eine Darstellung $z = 25 = 4^2 + 3^2$ mit den geforderten Eigenschaften (die Darstellung $25 = 5^2 + 0^2$ ist natürlich nicht zulässig). Mit $x = 2uv$ und $y = u^2 - v^2$ erhält man das primitive pythagoreische Tripel $(12, 7, 25)$, dem man noch $(7, 12, 25)$ hinzufügen muss.

(b) $z = 27$ ist überhaupt keine Summe von zwei Quadraten; man kann dies durch Probieren bestätigen oder sich auf den Zwei-Quadrate-Satz berufen: es ist ja $27 = 3^3$, der Primfaktor $3\,(\equiv 3 (\mathrm{mod}\, 4))$ hat einen ungeraden Exponenten. Es gibt also kein primitives pythagoreisches Tripel der Form $(x, y, 27)$.

(c) Hier ist nur die Darstellung $z = 29 = 5^2 + 2^2$ zulässig; sie führt auf $(20, 21, 29)$ und $(21, 20, 29)$.

Lösung 9.

(a) $106 = 2 \cdot 53 = 2 \cdot (7^2 + 2^2) = (7+2)^2 + (7-2)^2 = 9^2 + 5^2$

(b) $1073 = 29{\cdot}37 = (5^2{+}2^2)(6^2{+}1^2) = (5{\cdot}6{+}2{\cdot}1)^2{+}(5{\cdot}1{-}2{\cdot}6)^2 = 32^2{+}7^2$ oder

$1073 = 29{\cdot}37 = (5^2{+}2^2)(1^2{+}6^2) = (5{\cdot}1{+}2{\cdot}6)^2{+}(5{\cdot}6{-}2{\cdot}1)^2 = 17^2{+}28^2$

(c) $11^4 \cdot 13^3 \cdot 17^2 \cdot 19$ ist nicht als Summe von zwei Quadraten darstellbar, da der Primfaktor $19\,(\equiv 3 (\mathrm{mod}\, 4))$ einen ungeraden Exponenten hat (Zwei-Quadrate-Satz!).

Lösung 10. Nach Vorausetzung gilt

$$a^2 + b^2 \equiv 0 \,(\mathrm{mod}\, p) \text{ und etwa } b \not\equiv 0 \,(\mathrm{mod}\, p)$$

(natürlich gilt dann auch $a \not\equiv 0 \,(\mathrm{mod}\, p)$). Sei b' ein Inverses von b modulo p, also $b'b \equiv 1 \,(\mathrm{mod}\, p)$; Multiplikation der ersten Kongruenz mit $(b')^2$ liefert

$$(b')^2a^2 + 1 \equiv 0 \,(\mathrm{mod}\, p) \text{ und } (b'a)^2 \equiv -1 \,(\mathrm{mod}\, p).$$

Also ist -1 ein quadratischer Rest modulo p (d.h. $(\frac{-1}{p}) = 1$) und somit $p \equiv 1 \,(\mathrm{mod}\, 4)$ nach dem ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz.