Vertiefung Elementare Zahlentheorie

WS 2010/2011, Lösungen zur Klausur 2, 29.3.2011

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

Lösung 1. $\mathrm{ggT}(2947, 910) = 7 = 21 \cdot 2947 - 68 \cdot 910$

Folgende Probe bietet sich an: 910 hat die Primfaktor-Zerlegung $2 \cdot 5 \cdot 7 \cdot 13$; 2947 wird nicht von 2, 5, 13 geteilt, wohl aber von 7. Die lineare Darstellung überprüft man durch Ausrechnen.

Lösung 2. $x \equiv 18 \pmod{140}$

Hier sollte man unbedingt die Probe machen!

Lösung 3.

(a) $222^{333} \equiv 2^{333} \equiv 2^3 \equiv 8 \pmod{11}$, $200^{200} \equiv 4^{200} \equiv 4^2 \equiv 2 \pmod{7}$

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

(b) $987^{6543} \equiv 7^{6543} \equiv 7^3 \equiv 3 \pmod{10}$, also Endziffer 3.

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 7 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:

$7^{6543} \equiv 1 \pmod{2}$ und $7^{6543} \equiv 2^{6543} \equiv 2^3 \equiv 3 \pmod{5}$, also wieder $7^{6543} \equiv 3 \pmod{10}$

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

Lösung 5.

(a) $120 = 2^3 \cdot 3 \cdot 5$, $\phi(120) = 32$;

(b) $625 = 5^4$, $\phi(625) = 500$;

(c) $2222 = 2 \cdot 11 \cdot 101$, $\phi(2222) = 1000$;

(d) $10000 = 2^4 \cdot 5^4$, $\phi(10000) = 4000$.

Lösung 6.

(a)

i	0	1	2	3	4	5	6	7	8	9	10	11
2^i	1	2	4	8	3	6	12	11	9	5	10	7

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	0	1	4	2	9	5	11	3	8	10	7	6

(b) $x \equiv 7$ oder 8 oder 11 (mod 11)

Lösung 7.

(a) $(\frac{60}{233}) = (\frac{4}{233}) \cdot (\frac{3}{233}) \cdot (\frac{5}{233}) = 1 \cdot (-1) \cdot (-1) = 1$:
$(\frac{4}{233}) = 1$,
$(\frac{3}{233}) = (\frac{233}{3}) = (\frac{2}{3}) = -1$,
$(\frac{5}{233}) = (\frac{233}{5}) = (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3} = -1$.

(b) $(\frac{62}{263}) = (\frac{2}{263}) \cdot (\frac{31}{263}) = 1 \cdot 1 = 1$:
$(\frac{2}{263}) = 1$,
$(\frac{31}{263}) = -(\frac{263}{31}) = -(\frac{15}{31}) = -(\frac{3}{31}) \cdot (\frac{5}{31}) = (\frac{31}{3}) \cdot (\frac{31}{5}) = (\frac{1}{3}) \cdot (\frac{1}{5}) = 1 \cdot 1 = 1$.

(c) $(\frac{64}{293}) = 1$ (denn $64 = 8^2$).

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) Durch Probieren findet man genau eine Darstellung $z = 37 = 6^2 + 1^2$ mit den geforderten Eigenschaften. Mit $x = 2uv$ und $y = u^2 - v^2$ erhält man das primitive pythagoreische Tripel $(12, 35, 37)$, dem man noch $(35, 12, 37)$ hinzufügen muss.

(b) $z = 39$ ist überhaupt keine Summe von zwei Quadraten; man kann dies durch Probieren bestätigen oder sich auf den Zwei-Quadrate-Satz berufen: es ist ja $39 = 3 \cdot 13$, der Primfaktor 3 ($\equiv 3 (\mathrm{mod}\, 4)$) hat einen ungeraden Exponenten. Es gibt also kein primitives pythagoreisches Tripel der Form $(x, y, 39)$.

(c) Hier ist nur die Darstellung $z = 41 = 5^2 + 4^2$ zulässig; sie führt auf $(40, 9, 41)$ und $(9, 40, 41)$.

Lösung 9.

(a) $226 = 2 \cdot 113 = 2 \cdot (8^2 + 7^2) = (8+7)^2 + (8-7)^2 = 15^2 + 1^2$

(b) $4453 = 61{\cdot}73 = (6^2{+}5^2)(8^2{+}3^2) = (6{\cdot}8{+}5{\cdot}3)^2{+}(6{\cdot}3{-}5{\cdot}8)^2 = 63^2{+}22^2$ oder

$$4453 = 61{\cdot}73 = (6^2{+}5^2)(3^2{+}8^2) = (6{\cdot}3{+}5{\cdot}8)^2{+}(6{\cdot}8{-}5{\cdot}3)^2 = 58^2{+}33^2$$

(c) $101^5 \cdot 103^4 \cdot 107^3 \cdot 109^2$ ist nicht als Summe von zwei Quadraten darstellbar, da der Primfaktor $107\,(\equiv 3 (\mathrm{mod}\, 4))$ einen ungeraden Exponenten hat (Zwei-Quadrate-Satz!).

Lösung 10. Hätte die gegebene Gleichung eine Lösung, dann auch die Kongruenz

$$x^2 + y^2 + z^2 \equiv 7 \,(\mathrm{mod}\, 8).$$

Aber die einzigen Quadrate modulo 8 sind 0, 1, 4, und die Summen von drei Quadraten (bis au die Reihenfolge der Summanden) sind

$0+0+0$,
$0+0+1$,
$0+0+4$,
$0+1+1$,
$0+1+4$,
$0+4+4$,
$1+1+1$,
$1+1+4$,
$1+4+4$,
$4+4+4$;

sie sind sämtlich $\not\equiv 7 \,(\mathrm{mod}\, 8)$.