Vertiefung Elementare Zahlentheorie

WS 2010/2011, Wiederholungsblatt 1

Die folgenden Aufgaben sollen nur zur Selbstkontrolle dienen; Lösungen müssen nicht abgegeben werden.

Aufgabe 1. Verwenden Sie den euklidischen Algorithmus zur Berechnung von $\mathrm{ggT}(a,b)$ und zur Bestimmung einer linearen Darstellung $\mathrm{ggT}(a,b) = xa + yb$ für

$$(a,b) = (7469, 2464), (2689, 4001), (2947, 3997).$$

Aufgabe 2. Bestimmen Sie alle ganzzahligen Lösungen (x, y) der folgenden linearen Gleichungen:

(a) $243x + 198y = 9$;

(b) $71x - 50y = 1$;

(c) $43x + 64y = 2$.

Aufgabe 3. Formulieren Sie den Fundamentalsatz der elementaren Zahlentheorie.

Aufgabe 4. Sei p eine Primzahl. Warum gilt $p \mid ab \implies p \mid a$ oder $p \mid b$?

Aufgabe 5. Bestimmen Sie die Primfaktorzerlegung von 594 und von 2550.

Aufgabe 6. (a) Zeigen Sie für $m \geq 1$ und $l \geq 1$:

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \ldots + x + 1),$$
$$y^{lm} - 1 = (y^l - 1)(y^{l(m-1)} + y^{l(m-2)} + \ldots + y^l + 1).$$

(b) Folgern Sie: Ist $2^n - 1$ $(n \geq 1)$ eine Primzahl, dann ist n eine Primzahl.

Aufgabe 7. (a) Zeigen Sie für m ungerade ≥ 1 und $l \geq 1$:

$$x^m + 1 = (x+1)(x^{m-1} - x^{m-2} + \ldots - x + 1),$$

$$y^{lm}+1=(y^l+1)(y^{l(m-1)}-y^{l(m-2)}+\ldots-y^l+1).$$

(b) Folgern Sie: Ist 2^N+1 ($N \geq 1$) eine Primzahl, dann ist N eine Zweierpotenz.

Aufgabe 8. Bestimmen Sie alle Lösungen der folgenden linearen Kongruenzen:

(a) $\quad 20x \equiv 4 \pmod{31}$;

(b) $\quad 20x \equiv 4 \pmod{32}$;

(c) $\quad 20x \equiv 5 \pmod{32}$.

Aufgabe 9. Bestimmen Sie alle Lösungen der folgenden Systeme linearer Kongruenzen:

(a) $\quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 5 \pmod{2}$;

(b) $\quad x \equiv 1 \pmod{4}, \quad x \equiv 0 \pmod{3}, \quad x \equiv 5 \pmod{7}$.

Aufgabe 10. Formulieren Sie den Satz von Fermat.

Aufgabe 11. (a) Bestimmen Sie die Reste von 1000^{1000}, 1001^{1001}, 1002^{1002} und 1003^{1003} bei Division durch 11.

(b) Bestimmen Sie die Endziffer in der Dezimaldarstellung von 987^{6543}, 876^{5432} und 765^{4321}.

Aufgabe 12. Formulieren Sie den Satz von Wilson.

Aufgabe 13. Zeigen Sie: Für jede Primzahl $p \neq 2$ gilt

$$(((p-1)/2)!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Aufgabe 14. Geben Sie die Definition der Eulerschen ϕ-Funktion.

Aufgabe 15. Bestimmen Sie die folgenden Werte der Eulerschen ϕ-Funktion:

(a) $\quad \phi(m)$, $1 \leq m \leq 30$;

(b) $\quad \phi(594)$, $\phi(2550)$.

Aufgabe 16. Bestimmen Sie alle $m \geq 1$ derart, dass $\phi(m) = 4$ bzw. $\phi(m) = 6$ bzw. $\phi(m) = 8$.

Aufgabe 17. Formulieren Sie den Satz von Euler.

Aufgabe 18. Geben Sie die Definition einer Primitivwurzel modulo einer Primzahl.

Aufgabe 19. (a) Finden Sie die kleinste Primitivwurzel > 0 modulo 17.
(b) Beschreiben Sie alle Primitivwurzeln modulo 17.

Aufgabe 20. (a) Erstellen Sie eine Index-Tabelle für die in Aufgabe 19 (a) gefundene Primitivwurzel.
(b) Verwenden Sie die Index-Tabelle aus (a), um alle Lösungen der folgenden Kongruenzen zu bestimmen:

$$x^3 \equiv 6 \pmod{17}; \quad x^4 \equiv 6 \pmod{17}; \quad x^5 \equiv 6 \pmod{17}.$$

Aufgabe 21. Bestimmen Sie alle Lösungen der folgenden quadratischen Kongruenz für $p = 3, 5, 7, 11$:

$$2x^2 + 3x + 1 \equiv 0 \pmod{p}.$$

Aufgabe 22. Bestimmen Sie für $p = 17$ und für $p = 19$ alle ganzen a mit $1 \leq a \leq p - 1$, die quadratische Reste modulo p sind.

Aufgabe 23. Zeigen Sie, dass es zu jeder ungeraden Primzahl p genau $(p-1)/2$ quadratische Nichtreste gibt.

Aufgabe 24. Geben Sie die Definition des Legendre-Symbols.

Aufgabe 25. Formulieren Sie das Euler-Kriterium.

Aufgabe 26. Formulieren Sie das quadratische Reziprozitätsgesetz.

Aufgabe 27. Formulieren Sie die beiden Ergänzungssätze zum quadratischen Reziprozitätsgesetz.

Aufgabe 28. Hat die Kongruenz $x^2 \equiv 150 \pmod{1009}$ eine Lösung?

Aufgabe 29. Berechnen Sie die folgenden Legendre-Symbole:
$(\frac{37}{73}), (\frac{38}{73}), (\frac{39}{73}), (\frac{40}{73})$.

Aufgabe 30. Bestimmen Sie alle Primzahlen $p \neq 3$ derart, dass -3 ein quadratischer Rest modulo p ist.

Schöne Ferien und alles Gute für 2011!