Vertiefung Elementare Zahlentheorie

WS 2010/2011, Wiederholungsblatt 1

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

Aufgabe 1. Use the Euclidean Algorithm to calculate $\gcd(a, b)$ and to determine a linear representation $\gcd(a, b) = xa + yb$ for

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

Aufgabe 2. Determine all integer solutions (x, y) of the following linear equations:

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

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

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

Aufgabe 3. State the Fundamental Theorem of Elementary Number Theory.

Aufgabe 4. Let p be a prime. Why does $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$ hold?

Aufgabe 5. Determine the prime factor decomposition of 594 and of 2550.

Aufgabe 6. (a) Show for $m \geq 1$ and $l \geq 1$:

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

(b) Conclude: If $2^n - 1$ $(n \geq 1)$ is prime, then n is prime.

Aufgabe 7. (a) Show for m odd ≥ 1 and $l \geq 1$:

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

(b) Conclude: If $2^N + 1$ ($N \geq 1$) is prime, then N is a power of 2.

Aufgabe 8. Determine all solutions of the following linear congruences:
(a) $\quad 20x \equiv 4 \pmod{31}$;
(b) $\quad 20x \equiv 4 \pmod{32}$;
(c) $\quad 20x \equiv 5 \pmod{32}$.

Aufgabe 9. Determine all solutions of the following systems of linear congruences:
(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. State Fermat's theorem.

Aufgabe 11. (a) Determine the remainders of 1000^{1000}, 1001^{1001}, 1002^{1002} and 1003^{1003} when divided by 11.
(b) Determine the last digit in the decimal representation of 987^{6543}, 876^{5432} and 765^{4321}.

Aufgabe 12. State Wilson's theorem.

Aufgabe 13. Show for every prime $p \neq 2$:

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

Aufgabe 14. Give the definition of Euler's ϕ-function.

Aufgabe 15. Calculate the following values of Euler's ϕ-function:
(a) $\quad \phi(m)$, $1 \leq m \leq 30$;
(b) $\quad \phi(594)$, $\phi(2550)$.

Aufgabe 16. Determine all $m \geq 1$ such that $\phi(m) = 4$, resp. $\phi(m) = 6$ resp. $\phi(m) = 8$.

Aufgabe 17. State Euler's theorem.

Aufgabe 18. Give the definition a primitive root modulo a prime.

Aufgabe 19. (a) Find the smallest primitive root > 0 modulo 17.
(b) Describe all primitive roots modulo 17.

Aufgabe 20. (a) Construct an index table for the primitive root found in exercise 19(a).
(b) Use the index table from (a) to determine all solutions of the following congruences:

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

Aufgabe 21. Determine all solutions of the following quadratic congruence for $p = 3, 5, 7, 11$:

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

Aufgabe 22. Determine for $p = 17$ and for $p = 19$ all integers a with $1 \leq a \leq p - 1$ that are quadratic residues modulo p.

Aufgabe 23. Show that for any odd prime p there are exactly $(p - 1)/2$ quadratic nonresidues.

Aufgabe 24. Give the definition of the Legendre symbol.

Aufgabe 25. State the Euler criterion.

Aufgabe 26. State the quadratic reciprocity law.

Aufgabe 27. State the two supplementary theorems of the quadratic reciprocity law.

Aufgabe 28. Does the congruence $x^2 \equiv 150 \pmod{1009}$ have a solution?

Aufgabe 29. Calculate the following Legendre symbols:
$(\frac{37}{73}), (\frac{38}{73}), (\frac{39}{73}), (\frac{40}{73})$.

Aufgabe 30. Determine all primes $p \neq 3$ such that -3 is a quadratic residue modulo p.

Schöne Ferien und alles Gute für 2011!