Elementary Number Theory (TN410)

Exercises: Sheet #2

March 21, 2015

1. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of real or complex numbers and $\phi(x)$ a function of class $\mathcal{C}^1$. Prove that

$$\sum_{1\leq n\leq x} a_n\phi(n) = A(x)\phi(x) - \int_1^x A(u)\phi'(u)\,\mathrm{d}u \qquad \text{where} \qquad A(x) := \sum_{1\leq n\leq x} a_n$$

and that, more generally, we have $\displaystyle\sum_{x<n\leq y} a_n\phi(n) = A(y)\phi(y) - A(x)\phi(x) - \int_x^y A(u)\phi'(u)\,\mathrm{d}u\,.$

2. Find all integer solutions of in the interval $[-500, 500]$ of the following linear congruences:

$$5X \equiv 10(\mathrm{mod}35), \qquad 12X \equiv 14(\mathrm{mod}106), \qquad 12X \equiv 12(\mathrm{mod}42), \qquad 36X \equiv 18(\mathrm{mod}60).$$

3. Find all integer solutions in the interval $[-500, 500]$ of

$$\begin{cases} x\equiv 2 \pmod 3\\ x\equiv 3 \pmod 4\\ x\equiv 4 \pmod 5\end{cases} \qquad \begin{cases} x\equiv 3 \pmod 6\\ x\equiv 4 \pmod 7\\ x\equiv 7 \pmod{11}\end{cases} \qquad \begin{cases} x\equiv 1 \pmod{11}\\ x\equiv 2 \pmod{21}\\ x\equiv 3 \pmod{10}\end{cases} \qquad \begin{cases} x\equiv 5 \pmod{31}\\ x\equiv 3 \pmod{27}\\ x\equiv 4 \pmod 8.\end{cases}$$

4. (*Extended Chinese remainder Theorem.*)Let $m_1, \ldots, m_s$ be positive integers and let $a_1, \ldots, a_s \in \mathbb{Z}$. Prove that

$$\begin{cases} X \equiv a_1 \bmod m_1\\ \vdots\\ X\equiv a_s \bmod m_s\end{cases}$$

has a solution exists if and only if $a_i \equiv a_j \mod \gcd(m_i, m_j)$ for all i, j. Moreover, in the case when has a solution exists, any two solutions differ by some common multiple of $m_1, \ldots, m_n$.

5. Compute all primitive roots modulo 50, 54, 81, 162 and 250.

6. Let $\alpha\in\mathbb{N}$, $\alpha\geq 3$. Prove that for any $a\in\mathbb{Z}$ odd, there exists $\nu\in\{0,1\}$ and $\mu\in\{0,\ldots,2^{\alpha-2}-1\}$ such that

$$a \equiv (-1)^\nu \cdot 5^\mu \bmod 2^\alpha.$$

Deduce that $\qquad U(\mathbb{Z}/2^\alpha\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{\alpha-2}\mathbb{Z}.$

7. (*The Lifting Solutions Lemma*) Let $f(X)$ be a polynomial with integer coefficients and with degree n, let p be a prime and let $a\in\mathbb{N}$. Prove the following:

   (a) Suppose that $\zeta\in\mathbb{Z}$ is a solution of $f(X)\equiv 0 \bmod p^{a+1}$ then $\zeta = \xi + sp^a$ where ξ is a solution of $f(X)\equiv 0 \bmod p^a$ and $s\in\{0,\ldots,p-1\}$.

(b) If $\xi \in \mathbb{Z}$ is a solution of $f(X) \equiv 0 \bmod p^a$ such that the derivative $f'(\xi) \not\equiv 0 \bmod p$, then there exists a unique integer $s \in \{0, \ldots, p-1\}$ such that $\xi + sp^a$ is a solution of $f(X) \equiv 0 \bmod p^{a+1}$.

(c) If $\xi \in \mathbb{Z}$ is a solution of $f(X) \equiv 0 \bmod p^a$ such that the derivative $f'(\xi) \equiv 0 \bmod p$, then for all $s \in \{0, \ldots, p-1\}$ either

i. $\xi + sp^a$ is always a solution of $f(X) \equiv 0 \bmod p^{a+1}$ or

ii. $\xi + sp^a$ is never a solution of $f(X) \equiv 0 \bmod p^{a+1}$.

(***hint:*** *Use the Taylor expansion of* f)

8. For any polynomial with integer coefficients f and any $m \in \mathbb{N}$, we set $N_f(m)$ to be the number of solutions in any complete set of residues modulo m of the congruence $f(X) \equiv 0 \bmod m$. Prove that $N_f(m) = \prod_{p|m} N_f(p^{v_p(m)})$.

9. Let m be an odd integer and $a \in \mathbb{Z}$. Prove that if $X^2 \equiv a \bmod m$ is solvable then $\left(\frac{a}{m}\right)_J = 1$. Give an example of a and m where the opposite does not hold.

10. Compute a formula for the number of square roots of an integer a modulo m in terms of the Legendre symbols $\left(\frac{a}{p}\right)_L$ where $p \mid m$.

11. Prove that, for $p \geq 3$,

$$\left(\frac{-3}{p}\right)_L = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 3 \\ 0 & \text{if } p = 3 \\ -1 & \text{if } p \equiv 2 \bmod 3. \end{cases} \quad \text{and that} \quad \left(\frac{3}{p}\right)_L = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \\ 0 & \text{if } p = 3 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12. \end{cases}$$

12. Compute the following Jacobi symbols without ever factoring the odd integers involved:

$$\left(\frac{2725}{9473}\right)_J, \quad \left(\frac{5811}{1013}\right)_J, \quad \left(\frac{7269}{573}\right)_L, \quad \left(\frac{7307}{5809}\right)_J, \quad \left(\frac{1269}{7231}\right)_J \quad \left(\frac{89439}{20259}\right)_J \quad \left(\frac{57599}{5557}\right)_J.$$