Staff Solutions to Problem Set 5

Reading:
- Chapter 8. Number Theory: Congruences through 8.11. RSA Cryptosystem.

STAFF NOTE: Lectures covered: Number Theory (Congruences) Ch. 8.6-8.9; \( \mathbb{Z}_n \), Euler’s Theorem, Ch. 8.10; RSA, Ch. 8.11-8.12.

Problem 1.
The sum of the digits of the base 10 representation of an integer is congruent modulo 9 to that integer. For example

\[ 763 \equiv 7 + 6 + 3 \pmod{9}. \]

This is not always true for the hexadecimal (base 16) representation, however. For example,

\[ (763)_{16} = 7 \cdot 16^2 + 6 \cdot 16 + 3 \equiv 7 \neq 7 + 6 + 3 \pmod{9}. \]

(a) For exactly what integers \( k > 1 \) is it true that the sum of the digits of the base 16 representation of an integer is congruent modulo \( k \) to that integer? Justify your answer.

Solution.

3, 5, 15.

Summing the digits mod \( k \) works iff \( 16 \equiv 1 \pmod{k} \). This is equivalent to \( k \mid 16 - 1 = 15 \). So the three factors of 15 are exactly the \( k \)'s that work.

To see why only these \( k \)'s work, just look at two-digit hex numbers \( 16c + d \) where \( c, d \in [0, 16) \). In this case the digit-sum requirement means that for all such \( c, d \),

\[ 16c + d \equiv c + d \pmod{k}, \]

so letting \( c = 1, d = 0 \) gives \( 16 \equiv 1 \pmod{k} \).

(b) Give a rule that generalizes this sum-of-digits rule from base \( b = 16 \) to an arbitrary number base \( b > 1 \), and explain why your rule is correct.

Solution. By the reasoning of part (a) with “16” replaced by “\( b \)” a necessary and sufficient condition for a number \( k > 1 \) to satisfy the sum-of-digits condition is that \( k \) be a divisor of \( b - 1 \).

Problem 2.
**Definition.** Define the order of \( k \) over \( \mathbb{Z}_n \) to be

\[
\text{ord}(k, n) := \min \{ m > 0 \mid k^m = 1 \ (\mathbb{Z}_n) \}.
\]

If no positive power of \( k \) equals 1 in \( \mathbb{Z}_n \), then \( \text{ord}(k, n) := \infty \).

(a) Show that \( k \in \mathbb{Z}_n^* \) iff \( k \) has finite order in \( \mathbb{Z}_n \).

**Solution.** If \( k \) has finite order in \( \mathbb{Z}_n \), then \( k \text{ord}(k, n) \) is an inverse of \( k \) in \( \mathbb{Z}_n \), so \( k^2 \in \mathbb{Z}_n \) by Theorem 8.9.5.

Conversely, since \( \mathbb{Z}_n \) has \( n \) elements, some number must occur twice in the list

\[
k^0, k^1, k^2, \ldots, k^n \quad (\mathbb{Z}_n).
\]

That is,

\[
k^i = k^{i+m} \quad (\mathbb{Z}_n)
\]

for some \( i, m \in [1, n] \). But if \( k \in \mathbb{Z}_n^* \), then \( k \) is cancellable over \( \mathbb{Z}_n \), so we can cancel the first \( i \) of the \( k \)'s on both sides of (1) to get

\[
1 = k^m \quad (\mathbb{Z}_n).
\]

It follows that \( k \) has order \( < n \) \( (\mathbb{Z}_n) \).

(b) Prove that for every \( k \in \mathbb{Z}_n^* \), the order of \( k \) over \( \mathbb{Z}_n \) divides \( \phi(n) \).

**Hint:** Let \( m = \text{ord}(k, n) \). Consider the quotient and remainder of \( \phi(n) \) divided by \( m \).

**Solution.** Proof. Let \( m = \text{ord}(k, n) \). Now we have

\[
1 = k^\phi(n) = k^m \cdot k^{\text{rem}(\phi(n), m)} \quad \text{(Euler)}
\]

\[
= (k^m)^{\text{qcnt}(\phi(n), m)} \cdot k^{\text{rem}(\phi(n), m)} \quad \text{(Division Theorem)}
\]

\[
= 1^{\text{qcnt}(\phi(n), m)} \cdot k^{\text{rem}(\phi(n), m)} \quad \text{(Def of m)}
\]

\[
= k^{\text{rem}(\phi(n), m)}. \quad (2)
\]

But \( \text{rem}(\phi(n), m) < m \) and \( m \) is the smallest positive power of \( k \) equal to 1 in \( \mathbb{Z}_n \), so (2) implies that \( \text{rem}(\phi(n), m) \) must equal 0, which means that \( m \mid \phi(n) \).

Problem 3.

In this problem we'll prove that for all integers \( a, m \) where \( m > 1 \),

\[
a^m \equiv a^{m-\phi(m)} \quad (\text{mod } m).
\]

(3)

Note that \( a \) and \( m \) need not be relatively prime.

Assume \( m = p_1^{k_1} \cdots p_n^{k_n} \) for distinct primes, \( p_1, \ldots, p_n \) and positive integers \( k_1, \ldots, k_n \).

(a) Show that if \( p_i \) does not divide \( a \), then

\[
a^{\phi(m)} \equiv 1 \quad (\text{mod } p_i^{k_i}).
\]
Solution.

\[ a^{\phi(m)} = a^{\phi(p_i^{k_i}) \cdot \phi(m/p_i^{k_i})} \]
\[ = \left( a^{\phi(p_i^{k_i})} \right)^{\phi(m/p_i^{k_i})} \]
\[ \equiv 1^{\phi(m/p_i^{k_i})} \pmod{p_i^{k_i}} \quad \text{(Euler’s Theorem, since } \gcd(a, p_i) = 1) \]
\[ = 1. \]

(b) Show that if \( p_i \mid a \) then

\[ a^{m - \phi(m)} \equiv 0 \pmod{p_i^{k_i}}. \quad (4) \]

Solution. Since \( p_i \mid a \), we have \( p_i^{k_i} \mid a^{k_i} \). That is

\[ a^{k_i} \equiv 0 \pmod{p_i^{k_i}}, \]

and hence

\[ a^n \equiv 0 \pmod{p_i^{k_i}} \]

for any \( n \geq k_i \). So we need only show that \( m - \phi(m) \geq k_i \). But \( m - \phi(m) \) is the number of integers in \( [0, m) \) that are not relatively prime to \( m \), and there are at least \( k_i \) of them, namely, \( 0, p_i, p_i^2, \ldots, p_i^{k_i - 1} \).

(c) Conclude (3) from the facts above.

*Hint:* \( a^m - a^{m - \phi(m)} = a^{m - \phi(m)}(a^{\phi(m)} - 1) \).

Solution. Let \( b := a^m - a^{m - \phi(m)} \). So (3) holds iff \( b \equiv 0 \pmod{m} \). But using the hint that \( b = cd \) where \( c := a^{m - \phi(m)} \) and \( d := a^{\phi(m)} - 1 \), we have from part (a) that

\[
\begin{align*}
  c &\equiv 0 \pmod{p_i^{k_i}}, & \text{if } p_i \text{ does not divide } a, \\
  d &\equiv 0 \pmod{p_i^{k_i}}, & \text{if } p_i \mid a.
\end{align*}
\]

so in any case,

\[ b = cd \equiv 0 \pmod{p_i^{k_i}} \quad \text{for } 1 \leq i \leq n. \]

This implies that \( b \equiv 0 \) modulo the product \( p_1^{k_1} \cdots p_n^{k_n} \), namely

\[ b \equiv 0 \pmod{m}. \]