Staff Solutions to Problem Set 5

Reading: Chapter 9.5, Congruences through 9.12. RSA & SAT, Chapter 10.5, DAGs & Scheduling

STAFF NOTE: Lectures covered: Number Theory: Congruences Ch. 9.5-9.9; \(\mathbb{Z}_n\), Euler’s Theorem, Ch. 9.10; RSA Cryptosystem, Ch 9.11-9.12, DAGs & Scheduling, Ch.10.5

Problem 1.
Find the last digit of \(7^{7^7}\).

Solution. 3.
The last digit of \(7^{7^7}\) is \(\text{rem}(7^{7^7}, 10)\). Because 7 and 10 are relatively prime,
\[
7^{7^7} \equiv 7^{\text{rem}(7^7, \phi(10))} = 7^{\text{rem}(7^7, 4)} \pmod{10}.
\]
So now we need to find \(\text{rem}(7^7, 4)\). Since 7 and 4 are relatively prime,
\[
7^7 \equiv 7^{\text{rem}(7, \phi(4))} = 7^{\text{rem}(7, 2)} \pmod{4}.
\]
But \(\text{rem}(7, 2)\) is clearly 1, so
\[
7^7 \equiv 7^1 \equiv 3 \pmod{4},
\]
and therefore
\[
\text{rem}(7^7, 4) = 3.
\]
Finally,
\[
7^{7^7} \equiv 7^{\text{rem}(7^7, 4)} = 7^3 \equiv 3 \pmod{10},
\]
so \(\text{rem}(7^{7^7}, 10) = 3\).

Problem 2.
Suppose \(a, b\) are relatively prime integers greater than 1. In this problem you will prove that Euler’s function is multiplicative, that is, that
\[
\varphi(ab) = \varphi(a)\varphi(b).
\]
The proof is an easy consequence of the Chinese Remainder Theorem.¹

¹The Chinese Remainder Theorem asserts that if \(a, b\) are relatively prime and greater than 1, then for all \(m, n\), there is a unique \(x \in [0, ab)\) such that
\[
\begin{align*}
x &\equiv m \pmod{a}, \\
x &\equiv n \pmod{b}.
\end{align*}
\]
A proof appears in Problem 9.58.
(a) Conclude from the Chinese Remainder Theorem that the function \( f : [0..ab) \to [0..a) \times [0..b) \) defined by
\[
\begin{align*}
   f(x) &:= (\text{rem}(x, a), \text{rem}(x, b))
\end{align*}
\]
is a bijection.

**Solution.** By definition, \( f \) has the \([= 1 \text{ out}], \text{total function} \) property.
The Chinese Remainder Theorem says that the congruences
\[
\begin{align*}
   x &\equiv m \pmod{a} ,
   x &\equiv n \pmod{b} ,
\end{align*}
\]
have a solution \( x \), which means that \( f \) has the \([= 1 \text{ in}], \text{surjective} \) property. Moreover, the solution is unique up to congruence modulo \( ab \), which means that all solutions have the same remainder modulo \( ab \). So in particular, there is a unique solution \( x \in [0..ab) \), which means that \( f \) has the \([= 1 \text{ in}], \text{injective} \) property, and hence \( f \) is a bijection, namely, \([= 1 \text{ out}] \) and \([= 1 \text{ in}] \).

(b) For any positive integer, \( k \), let \( \mathbb{Z}^*_k \) be the integers in \([0..k) \) that are relatively prime to \( k \). Prove that the function \( f \) from part (a) also defines a bijection from \( \mathbb{Z}^*_{ab} \) to \( \mathbb{Z}^*_a \times \mathbb{Z}^*_b \).

**Solution.** By Unique Factorization, \( x \) is relatively prime to \( ab \) iff \( x \) is relatively prime to \( a \) and \( x \) is relatively prime to \( b \). But since \( \gcd(x, a) = \gcd(a, \text{rem}(x, a)) \), it follows that \( x \) is relatively prime to \( a \) iff \( \text{rem}(x, a) \) is relatively prime to \( a \), and likewise for \( b \). That is,
\[
x \in \mathbb{Z}^*_a \times \mathbb{Z}^*_b \iff f(x) \in \mathbb{Z}^*_a \times \mathbb{Z}^*_b ,
\]
which means that \( f \) defines a total surjective function from \( \mathbb{Z}^*_{ab} \) to \( \mathbb{Z}^*_a \times \mathbb{Z}^*_b \). And since \( f : [0..ab) \to [0..a) \times [0..b) \) was injective, it remains injective when restricted to the domain \( \mathbb{Z}^*_{ab} \), which proves that \( f \) defines a bijection from \( \mathbb{Z}^*_{ab} \) to \( \mathbb{Z}^*_a \times \mathbb{Z}^*_b \).

(c) Conclude from the preceding parts of this problem that
\[
\phi(ab) = \phi(a)\phi(b). \tag{1}
\]

**Solution.** The mapping \( f \) defines a bijection between \( \mathbb{Z}^*_{ab} \) and \( \mathbb{Z}^*_a \times \mathbb{Z}^*_b \). So
\[
\phi(ab) := |\mathbb{Z}^*_{ab}| = |\mathbb{Z}^*_a \times \mathbb{Z}^*_b| = |\mathbb{Z}^*_a| \cdot |\mathbb{Z}^*_b| = \phi(a) \cdot \phi(b).
\]

(d) Prove Corollary 9.10.11: for any number \( n > 1 \), if \( p_1, p_2, \ldots, p_j \) are the (distinct) prime factors of \( n \), then
\[
\phi(n) = n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_j} \right).
\]

**Solution.** We know from Theorem 9.10.10 that for all primes, \( p \), and \( k > 0 \),
\[
\phi(p^k) = p^k - p^{k-1} = p^k \left( 1 - \frac{1}{p} \right).
\]
**Problem 3.** Suppose Alice and Bob are using the RSA cryptosystem to send secure messages. Each of them has a public key visible to everyone and a private key known only to themselves, and using RSA in the usual way, they are able to send secret messages to each other over public channels.

But a concern for Bob is how he knows that a message he gets is actually from Alice—as opposed to some imposter claiming to be Alice. This concern can be met by using RSA to add unforgeable “signatures” to messages. To send a message $m$ to Bob with an unforgeable signature, Alice uses RSA encryption on her message $m$, but instead using Bob’s public key to encrypt $m$, she uses her own private key to obtain a message $m_1$. She then sends $m_1$ as her “signed” message to Bob.

(a) Explain how Bob can read the original message $m$ from Alice’s signed message $m_1$. (Let $(n_A, e_A)$ be Alice’s public key and $d_A$ her private key. Assume $m \in [0..n_A]$.)

**Solution.** By definition of RSA, the message $m_1$ will be

$$m_1 := \text{rem}(m^{d_A}, n_A),$$

where $d_A$ is Alice’s private key.

RSA encryption is based on the choice of a private key $d$ and a public key $(e, n)$ which satisfy the condition that $d \cdot e \equiv 1 \pmod{\phi(n)}$. But this condition is symmetric in $d$ and $e$, so reversing their roles allows Alice’s private key $d_A$ to be used to “encrypt” $m$ as the message $m_1$. Now Bob can apply RSA to $m_1$ using Alice’s public key $e_A$ in place of his private key to reconstruct $m$ from $m_1$:

$$m = \text{rem}(m_1^{e_A}, n)$$

(b) Briefly explain why Bob can be confident, assuming RSA is secure, that $m_1$ came from Alice rather than some imposter.
Solution. The message $m$ that Bob reconstructs from $m_1$ can only have been “encrypted” using Alice’s private key, $d_A$. Assuming RSA is secure, only Alice knows her private key $d_A$, so Bob can conclude the message came from Alice.

(c) Notice that not only Bob, but anyone can use Alice’s public key to reconstruct her message $m$ from its signed version $m_1$. So how can Alice send a secret signed message to Bob over public channels?

Solution. After signing her message with her private key to obtain $m_1$, Alice can use RSA in the usual way to encrypt $m_1$ using Bob’s public key and send it to Bob. Now only Bob can read the signed message.

Problem 4.
The following operations can be applied to any digraph, $G$:

1. Delete an edge that is in a cycle.
2. Delete edge $(u \rightarrow v)$ if there is a path from vertex $u$ to vertex $v$ that does not include $(u \rightarrow v)$.
3. Add edge $(u \rightarrow v)$ if there is no path in either direction between vertex $u$ and vertex $v$.

The procedure of repeating these operations until none of them are applicable can be modeled as a state machine. The start state is $G$, and the states are all possible digraphs with the same vertices as $G$.

(a) Let $G$ be the graph with vertices $\{1, 2, 3, 4\}$ and edges

\[
\{(1 \rightarrow 2), (2 \rightarrow 3), (3 \rightarrow 4), (3 \rightarrow 2), (1 \rightarrow 4)\}
\]

What are the possible final states reachable from $G$?

Solution. There are six:

\[
\begin{align*}
\{ & (1 \rightarrow 2), (2 \rightarrow 3), (3 \rightarrow 4) \} \\
\{ & (1 \rightarrow 3), (3 \rightarrow 2), (2 \rightarrow 4) \} \\
\{ & (3 \rightarrow 1), (1 \rightarrow 2), (2 \rightarrow 4) \} \\
\{ & (1 \rightarrow 3), (3 \rightarrow 4), (4 \rightarrow 2) \} \\
\{ & (3 \rightarrow 1), (1 \rightarrow 4), (4 \rightarrow 2) \} \\
\{ & (3 \rightarrow 4), (4 \rightarrow 1), (1 \rightarrow 2) \}
\end{align*}
\]

The last five can all be reached by deleting first $(1 \rightarrow 4)$ and then $(2 \rightarrow 3)$.

A line graph is a graph whose edges are all on one path. All the final graphs in part (a) are line graphs.

(b) Prove that if the procedure terminates with a digraph, $H$, then $H$ is a line graph with the same vertices as $G$.

Hint: Show that if $H$ is not a line graph, then some operation must be applicable.

Solution. Since vertices are not changed in any transition, $H$ will have the same vertices as $G$. So we need only show that if $H$ is not a line graph, then an operation is applicable.
Now if \( H \) has a directed cycle, then operation 1. applies. So \( H \) must be a DAG. Further, if there are two incomparable elements, \( u \neq v \) in the partial order defined by this DAG, then operation 3. would be applicable to add either \( \langle u \to v \rangle \) or \( \langle u \to v \rangle \). So the DAG must define a linear order.

All that remains is to prove that no vertex has in-degree or out-degree greater than one. The proof for in-degree and out-degree is virtually the same, and we’ll just prove that out-degree is at most one.

So suppose to the contrary that in \( H \), a vertex \( u \) has out-degree of 2 or more. So there are vertices \( v \neq w \) and edges \( \langle u \to v \rangle \) and \( \langle u \to w \rangle \) in \( H \). Now since \( H \) defines a linear order, there must be a directed path, \( \pi \), in one direction or the other between \( v \) and \( w \); moreover \( \pi \) does not go through \( u \) (if it did, there would be a cycle). Hence, the path \( u, \pi \) goes from \( u \) to \( w \) without including \( \langle u \to w \rangle \), which means that \( \langle u \to w \rangle \) could be deleted by applying operation 2.

(c) Prove that being a DAG is a preserved invariant of the procedure.

Solution. Deleting an edge cannot create a cycle, and neither can adding an edge between unconnected vertices. So if there was no cycle in a graph, there wouldn’t be any after one state transition.

(d) Prove that if \( G \) is a DAG and the procedure terminates, then the walk relation of the final line graph is a topological sort of \( G \).

Hint: Verify that the predicate

\[
P(u, v) ::= \text{there is a directed path from } u \text{ to } v
\]

is a preserved invariant of the procedure, for any two vertices \( u, v \) of a DAG.

Solution. Proof. To prove \( P(u, v) \) is an invariant, suppose \( P(u, v) \) holds in some DAG \( H \). Then operation 1. won’t be applicable since there are no cycles. Also, since adding an edge preserves all existing paths, operation 3. will preserve \( P(u, v) \). This leaves only operation 2, to consider.

So suppose operation 2. is applied to delete an edge \( \langle x \to y \rangle \) of \( H \). By definition of the operation, this would only be possible if there remains a directed path, \( \pi \), from \( x \) to \( y \). Hence for any directed path that includes \( \langle x \to y \rangle \), there remains a directed path between the same endpoints obtained by replacing edge \( \langle x \to y \rangle \) by \( \pi \). So \( P(u, v) \) will still hold.

Since \( G \) is a DAG, its walk relation is a partial order, \( \leq_G \). By part (b), the procedure terminates with a DAG, \( H \), that defines a linear order, \( \leq_H \). So to show that \( \leq_H \) is a topological sort of \( \leq_G \), we need only check that

\[
u \leq_G v \text{ IMPLIES } u \leq_H v.
\]

But \( u \leq_G v \) is equivalent to \( P(u, v) \) holding in \( G \), and since \( P \) is preserved, \( P(u, v) \) still holds in \( H \), and this is equivalent to \( u \leq_H v \).

(e) Prove that if \( G \) is finite, then the procedure terminates.

Hint: Let \( s \) be the number of cycles, \( e \) be the number of edges, and \( p \) be the number of pairs of vertices with a directed path (in either direction) between them. Note that \( p \leq n^2 \) where \( n \) is the number of vertices of \( G \). Find coefficients \( a, b, c \) such that \( as + bp + e + c \) is nonnegative integer valued and decreases at each transition.
Solution. Since \( s, e \in \mathbb{N} \) and \( 0 \leq p \leq n^2 \), where \( n \) is the number of vertices of \( G \), the value

\[
2n^2 s - 2p + e + 2n^2
\]

is always nonnegative. We claim it is strictly decreasing. To prove this, we consider the effect of the three kinds of operations.

Adding edge \( \langle u \rightarrow v \rangle \) by operation 3. adds one to \( e \) and leaves \( s \) unchanged. Also, pairs of vertices connected by a directed path remain connected after adding an edge, and adding \( \langle u \rightarrow v \rangle \) creates the new connected pair, \( (u, v) \), so \( p \) increases by at least one. Therefore \( 2n^2 s - 2p + e \) decreases by at least one.

Deleting an edge by operation 1. decreases \( e \) and \( s \) by at least one. It could also decrease \( p \), but not by more than the total number, \( n^2 \), of pairs of vertices, so \( 2n^2 s - 2p + e \) decreases by at least one.

Finally, deleting an edge decreases \( e \) by one and never increases \( s \). Further, deleting an edge by operation 2. does not change the walk relation, as explained in the solution to part (c), so \( p \) does not change. so \( 2n^2 s - 2p + e \) decreases by at least one.

\[\square\]