Homework 5

Due: Wednesday, March 9, 2016

All homeworks are due at 12:55 PM in the CS22 bin on the CIT second floor, next to the Fishbowl.

Include our cover sheet or equivalent, write your Banner ID (but not your name or your CS login) on each page of your homework, label all work with the problem number, and staple the entire handin before submitting.

Be sure to fully explain your reasoning and show all work for full credit. Consult the style guide for more information.

Problem 1

Consider the following way to express a non-negative integer \( m \):

\[
m = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0
\]

where \( 0 \leq a_i < n \) for all \( i \), and \( n \in \mathbb{Z} \).

For any fixed \( m \) and \( n \), we will call the above equation the expansion of \( m \) in base \( n \). So, the expansion of 8073 in base 10 is \( 8 \cdot 10^3 + 7 \cdot 10 + 3 \). This is a bit long-winded, so it is often shortened to the string of \( a_i \)'s (digits), and the base is specified with a subscript, as in \( 8073_{10} \). As a further example, \( 8073_9 = 8 \cdot 9^3 + 0 \cdot 9^2 + 7 \cdot 9 + 3 = 5898_{10} \). Note that bases and single digits are always in base 10 (decimal).

a. Express each of the following decimal numbers in the given bases. Show both the expansion and the digit string within the given base. You do not need to show other work.
   
   a. \( m = 1024 \) for \( n = 2 \).
   
   b. \( m = 196 \) for \( n = 5 \).
   
   c. \( m = 614 \) for \( n = 9 \).
   
   d. \( m = 659.918 \) for \( n = 16 \). In the digit string, use the additional digits \( A = 10, B = 11, \ldots, F = 15 \).

a. Consider a binary number of the form \( m = 1010 \ldots 0_2 \), where the entire number is \( k \) digits long (i.e. there are \( k - 3 \) trailing zeroes). Express \( 6m \) as a binary string.

   Note: Think about how computers might use properties of binary to make binary multiplication simpler.
b. Prove that any positive integer \( m \) can be written as:

\[
a_k 3^k + a_{k-1} 3^{k-1} + \ldots + a_1 3^1 + a_0 \text{ where each } a_i \in \{-1, 0, 1\}
\]

**Solution**

a. \( 1024 = 2^{10} = 1000000000_2 \).

b. \( 196 = 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1 = 1241_5 \).

c. \( 614 = 7 \cdot 9^2 + 5 \cdot 9 + 2 = 752_9 \).

d. \( 659918 = 10 \cdot 16^4 + 16^3 + 12 \cdot 16 + 14 = A11CE_{16} \).

a. \( 6m = 11110 \ldots 0_2 \), where \( 6m \) has \( k+2 \) digits (or \( k-2 \) trailing zeroes). To see this, find \( 2m \) by adding a 0 to the end of \( m \). Then, find \( 4m \) by adding a 0 to the end of \( 2m \). Finally, add \( 2m + 4m \) to find \( 6m \).

b. We can prove this claim by induction.

Base Case (\( m = 1 \)): \( 1 \cdot 3^0 \)

Inductive Case: assume that all numbers up until (and including) \( m \) are representable in the form \( m = a_k \cdot 3^k + \ldots + a_0 \cdot 3^0, a_i \in \{-1, 0, 1\} \). We want to show that \( m + 1 \) is also representable in this form.

We can consider the three possible ways \( m + 1 \) can be represented using multiples of 3:

- \( (m+1) = 3j \) for some \( j \in \mathbb{Z}^+ \) s.t. \( j \leq m \). By the inductive hypothesis we know that \( j = a_k \cdot 3^k + \ldots + a_0 \cdot 3^0 \). Therefore, \( 3j = a_k \cdot 3^{k+1} + \ldots + a_0 \cdot 3^1 \). So, in this case, \( m + 1 \) is representable in this form.

- \( (m+1) = 3j + 1 \) for some \( j \in \mathbb{Z}^+ \) s.t. \( j \leq m \). Again, we know by the inductive hypothesis that \( j = a_k \cdot 3^k + \ldots + a_0 \cdot 3^0 \). We can then say that \( 3j + 1 = a_k \cdot 3^{k+1} + \ldots a_0 \cdot 3^1 + 1 \cdot 3^0 \), which is also in the correct form.

- \( (m+1) = 3p + 2 = 3j - 1 \) for some \( j \in \mathbb{Z}^+ \) s.t. \( j \leq m \). Again, we know by the inductive hypothesis that \( j = a_k \cdot 3^k + \ldots a_0 \cdot 3^0 \). Thus, \( 3j - 1 = a_k \cdot 3^{k+1} + \ldots + a_0 \cdot 3^1 - 1 \cdot 3^0 \).

In all three cases, \( m + 1 \) is representable in this form, so by induction, any positive integer can be represented in this form.

**Problem 2**

Pam and Jim want to establish a secure communication channel to thwart Dwight’s persistent eavesdropping. Pam wants to use a cryptosystem that is both simple and
effective and has decided to use the RSA cryptosystem as a result. She then publishes the product of primes \( n = 1247 \), and the public key \( k = 13 \).

a. Dwight wants to send nonsense along the communication channel to disrupt Jim and Pam. Encrypt his favorite word, BEETS, by encrypting each letter separately by using the encoding of \( A = 1 \), \( B = 2 \), \( \ldots \), \( Z = 26 \). Your answer should be a sequence of numbers.

b. In a moment of weakness, Pam has revealed her decryption exponent, 181, to Dwight! Decrypt the most recent series of messages sent by Jim:

\[
(1070, 1108, 476, 476, 955)
\]

**Note:** Jim and Pam were using the same encoding as used in part a for encoding letters. As such, your answer should be a sequence of letters that Jim originally encoded.

c. Suppose Dwight has found two integers \( x \) and \( y \) such that \( x^2 \equiv y^2 \pmod{n} \), but \( x \not\equiv \pm y \pmod{n} \). Explain how Dwight can find \((p, q)\).

d. Pam has regained her senses and chosen the new encryption exponent 299. But Dwight has duped her once again and stolen the corresponding decryption exponent, 59. Use the two pairs of encryption and decryption exponents to factor \( n \).

---

**Solution**

a. An RSA ciphertext is the message raised to the encryption exponent \( (\text{mod } n) \). So to encrypt BEETS, Dwight would need to transfer all of the letters of BEETS to their encodings:

The encodings are:

\[
(2, 5, 5, 20, 19)
\]

Next, Dwight must encrypt them by raising them each to the 13\(^{th} \) \( (\text{mod } n) \). This yields

\[
(710, 1108, 1108, 277, 235)
\]

b. Decrypting an RSA ciphertext, raise the ciphertext to the decryption exponent.

To decrypt \((1070, 1108, 476, 476, 955)\), compute

\[
(1070^{181}, 1108^{181}, 476^{181}, 476^{181}, 955^{181}) \pmod{n}, \text{ which is } (10, 5, 12, 12, 15).
\]
c. We know that \(x^2 \equiv y^2 \pmod{n}\), which implies that \((x^2 - y^2) \equiv 0 \pmod{n}\) and \(n \mid (x^2 - y^2)\). However, we also know that \(n \nmid (x - y)\) AND \(n \nmid (x + y)\) because \(x \not\equiv \pm y \pmod{n}\). Recall that \(n \mid (x - y)(x + y)\). This means that \(pq \mid (x - y)(x + y)\). Therefore, we can conclude that either \(p\) or \(q\) divides \((x - y)\), but not both, otherwise \(n\) would actually divide \((x - y)\).

Now, we know WLOG that \(p \mid (x-y)\), so it must be true that \(\gcd(n, x-y) = p\). If we compute \(\gcd(n, x-y)\), we can find \(p\) and subsequently calculate \(q = \frac{n}{p}\).

d. Dwight has two encryption-decryption exponent pairs: \((13, 181)\) and \((299, 59)\).

Recall that for any encryption/decryption pair \(kd \equiv 1 \pmod{(p-1)(q-1)}\)
We therefore know that if we compute \(kd - 1\) for an encryption/decryption pair it will be a multiple of \((p-1)(q-1)\). We begin by using these two pairs to compute
\[
13 \times 181 - 1 = 2352
\]
\[
299 \times 59 - 1 = 17640
\]

Now that we have two pairs that are multiples of the \((p-1)(q-1)\), the \(\gcd\) of the two should be some small multiple of \((p-1)(q-1)\).

We compute the \(\gcd\):
\[
\gcd(2352, 17640) = 1176
\]

So 1176 is a small multiple of \((p-1)(q-1)\).

Let us continue supposing that 1176 is indeed \((p-1)(q-1)\). We can verify whether 1176 is actually \((p-1)(q-1)\) by trying to solve for \(p\) and \(q\).

Now, notice that:
\[
(p-1)(q-1) = pq - p - q + 1
\]
\[
(p-1)(q-1) = n - (p + q) + 1
\]
\[
(p + q) = n - (p-1)(q-1) + 1
\]

\[
1176 = 1247 - (p + q) + 1
\]
\[
(p + q) = 72
\]

Now that we have a value for \((p + q)\), we can use the quadratic equation:
\[
x^2 - (p + q)x + pq = 0
\]
The roots of this equation are \( x = p \) and \( x = q \). If we plug into the quadratic equation, we get:

\[
x^2 - 72x + 1247 = 0
\]

\[
(x - 43)(x - 29) = 0
\]

This equation has roots \( x = 43, x = 29 \). \( 29 \times 43 = 1247 \); success! If the product of the roots were not \( n \), however, this step should be repeated with 1176/2, 1176/3, and so on until the correct value of \((p - 1)(q - 1)\) is found.

Thus, \( n = 43 \times 29 \).

### Problem 3

**Note:** We recommend putting in a bit of extra effort to make sure you fully grasp this problem, because it will give you a deeper understanding of everything we have seen so far in this class. Come to clinic if you need guidance!

Recall the equivalence relation \( R_m \) on \( M = \{1, \ldots, m - 1\} \) from HW4. Consider the set \( M_0 = \{0, 1, \ldots, m - 1\} \), and the corresponding relation \( R_m^* \) on \( M_0 \) defined by

\[
\{ (x, y) \mid \exists a, b \in \mathbb{Z}^+, \text{ such that } x^a \equiv y^b \pmod{m} \}.
\]

Consider the prime factorization of \( m = p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n} \) for distinct primes \( p_1, \ldots, p_n \). Let us define the set \( F = \{p_1, p_2, \ldots, p_n\} \). Let \( E \subseteq \mathcal{P}(M_0) \) be the set of equivalence classes of \( R_m^* \). In this problem, you will be showing that \( R_m^* \) has \( |\mathcal{P}(F)| \) equivalence classes by proving that there is a bijection between them.

Define the function \( f : \mathcal{P}(F) \mapsto E \) by

\[
f(\{q_1, \ldots, q_k\}) = [q_1 \times q_2 \times \cdots \times q_k]_{R_m^*}
\]

In other words, \( f \) maps a subset of the prime factors of \( m \) to the equivalence class containing their product. As an example, we will look at \( m = 30 = 2 \times 3 \times 5 \). We then have that \( F = \{2, 3, 5\} \), and:

\[
\begin{align*}
f(\varnothing) &= \{1, 7, 11, 13, 17, 19, 23, 29\} \\
f(\{2\}) &= \{2, 4, 8, 14, 16, 22, 26, 28\} \\
f(\{3\}) &= \{3, 9, 21, 27\} \\
f(\{5\}) &= \{5, 25\} \\
f(\{2, 3\}) &= \{6, 12, 18, 24\}
\end{align*}
\]
\[ f(\{2, 5\}) = \{10, 20\} \]
\[ f(\{3, 5\}) = \{15\} \]
\[ f(\{2, 3, 5\}) = \{0\} \]

What kinds of patterns do you see in these equivalence classes? Make sure to pay special attention to \( f(\emptyset) \) and \( f(F) \).

a. Give an example of an \( m \) where \( f(F) \) is not just the set \( \{0\} \). What property must \( m \) have to make \( f(F) = \{0\} \)?

b. Consider two distinct subsets of \( F \), \( Q_1 \) and \( Q_2 \), and define
\[
q_1^* = \prod_{q \in Q_1} q
\]
\[
q_2^* = \prod_{q \in Q_2} q.
\]
Prove that \((q_1^*, q_2^*) \notin R_m^* \), concluding that \( f \) is injective. Why is that equivalent to injectivity?\(^1\)

c. Consider some arbitrary element
\[
x = c_{q_1}^{b_1} q_2^{b_2} \ldots q_k^{b_k},
\]
where \( Q = \{q_1, \ldots, q_k\} \subseteq F \), \( \gcd(c, m) = 1 \), and all \( b_i \) are positive. Prove that \( x \in f(Q) \), concluding that \( f \) is surjective. Why is that equivalent to surjectivity?

Note: You may assume the following result without proof. For \( Q = \{q_1, \ldots, q_k\} \) and positive exponents \( \lambda_1, \ldots, \lambda_k \),
\[
\left(q_1q_2 \ldots q_k, q_1^{\lambda_1}q_2^{\lambda_2} \ldots q_k^{\lambda_k}\right) \in R_m^*.
\]

d. Show that \( R_m^* \) has exactly two equivalence classes if \( m \) is prime, and show what they are.

Hint: Think back to HW4.5b.

Solution

a. \( f(F) = \{0\} \) iff \( m \) is square-free. The justification is that \( m \) is the product of its unique prime factors iff the powers of the primes in the decomposition of \( m \) are all 1 (square-free). If this is the case, then \( f(F) = [m] = [0] = \{0\} \).

A square free example is \( m = 30 = 2^1 \cdot 3^1 \cdot 5^1 \). A non-example is \( m = 60 = \)

\[^1\]If you have never seen this notation before, big Pi notation (\( \Pi \)) is used just like big Sigma notation (\( \Sigma \)), except it is used for products instead of for sums.
2^2 * 3^1 * 5^1, in which case \( f(F) = f(\{2, 3, 5\}) = \{0, 30\} \).

b. The sets \( Q_1 \) and \( Q_2 \) are distinct, so without loss of generality, we have a prime factor \( p \) of \( m \) such that \( p \in Q_2 \) and \( p \notin Q_2 \), thus \( p|q_2^* \) and \( p \nmid q_1^* \). We have:

\[
q_1^a \equiv q_2^b \pmod{m}
\]

\[
q_1^a = q_2^b + k_1 m
\]

For some \( k_1 \in \mathbb{Z} \). Since \( p \) divides both \( q_2^b \) and \( m \), we can rewrite the sum as:

\[
q_2^b + k_1 m = pk_2 + pk_3 = p(k_2 + k_3)
\]

\[
p(k_2 + k_3) = q_1^a
\]

for some \( k_2, k_3 \in \mathbb{Z} \). But then \( p|q_1^a \), a contradiction. Thus \( (q_1^a, q_2^a) \notin R_m^* \).

The definition of injectivity is that, given any \( Q_1, Q_2 \in P(F) \), we have:

\[
Q_1 \neq Q_2 \implies f(Q_1) \neq f(Q_2)
\]

We have just demonstrated above that if \( Q_1 \neq Q_2 \), then \( f \) maps \( Q_1 \) and \( Q_2 \) to different equivalence classes. But this means \( f(Q_1) \neq f(Q_2) \), so \( f \) is indeed injective.

c. Consider

\[
x^{\varphi(m)} = (cq_1^{b_1} q_2^{b_2} \cdots q_k^{b_k})^{\varphi(m)}
\]

\[
= c^{\varphi(m)} \cdot q_1^{\varphi(m)b_1} q_2^{\varphi(m)b_2} \cdots q_k^{\varphi(m)b_k}
\]

If we define \( \lambda_1 = \varphi(m)b_1 \), \( \lambda_2 = \varphi(m)b_2 \), \cdots, \( \lambda_k = \varphi(m)b_k \), then:

\[
x^{\varphi(m)} \equiv c^{\varphi(m)} \cdot q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k} \pmod{m}
\]

\[
\equiv 1 \cdot q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k} \pmod{m}
\]

\[
\equiv q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k} \pmod{m}
\]

Thus \( (x^{\varphi(m)}, q_1^{\lambda_1}, q_2^{\lambda_2}, \ldots, q_k^{\lambda_k}) \in R_m^* \). Using that \( (q_1 q_2 \cdots q_k, q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_k^{\lambda_k}) \in R_m^* \), along with transitivity, gives the desired result.

We have just demonstrated that given any element \([x] \in E\) of the codomain, there exists a element of the domain \( Q \in P(F) \) such that \( f(Q) = [x] \). But this is precisely the definition of surjectivity, thus \( f \) is surjective.
d. Recall that if \( m \) is prime, by \( F\ell T \) we have \( \forall x, y \in \{1, \ldots, m-1\} = M: \)

\[
x^{m-1} \equiv y^{m-1} \equiv 1 \pmod{m}
\]

Thus all such \( \forall x, y \in M, (x, y) \in R_m^* \). Now for any \( x \in M \), \( x \) is not divisible by the prime \( m \), thus \( x^k \) is not divisible to the prime factor \( m \) for any \( k \). Thus \( x \) cannot be related to 0 via \( R_m^* \), which demonstrates that 0 is in its own equivalence class. So the classes are:

\[ [0] = \{0\} \]
\[ [1] = \{1, 2, \ldots, m - 1\} \]

### Problem 4

Kevin Malone, Dunder-Mifflin Accountant Extraordinaire, has again messed up his accounting records (which are not really accounting records, but boolean expressions; we’re not really sure why he was hired as an accountant.) It’s your job to help fix them: add parentheses to the following expressions to make them true. Note 1 represents true, and 0 represents false.

a. \( 0 \land 1 \lor 1 \Rightarrow 1 \land 1 \land 1 \lor 0 \)

b. \( 1 \lor 0 \land 1 \land 1 \land 1 \lor 0 \)

c. \( 1 \land 0 \lor 0 \leftrightarrow 1 \Rightarrow 0 \)

d. \( 0 \lor 1 \Rightarrow 0 \land 0 \Rightarrow 1 \)

### Solution

There are many possible solutions for each problem.

**Note:** Since this question asked you to add parentheses, we subtracted points if any sub-expression of operations was left ambiguous, even if the expression evaluated to true under all possible placements of parentheses, with two exceptions: if the sub-expression contained only one type of operator and that operator is transitive (i.e. \( a_1 \lor a_2 \lor \ldots \lor a_n \) or \( a_1 \land a_2 \land \ldots \land a_n \)), or if you explicitly stated that the expression evaluated to true under all possible placements of parentheses.

a. Example: \( ((0 \land 1) \lor 1) \Rightarrow ((1 \land 1) \land (1 \lor 0)) \)

All syntactically correct expressions evaluated to true if “\( \Rightarrow \)” was the highest-
order term (i.e. “⇒” separated the expression into two sub-expressions),
regardless of the other parentheses. There are other possible true answers.
b. Example: \(((1 \lor 0) \land (1 \land 1)) \land (1 \land (1 \lor 0))\)
   All syntactically correct expressions evaluated to true, regardless of parenthe-
   ses.
c. Example: \((1 \land (0 \lor 0)) \iff (1 \Rightarrow 0)\)
   All syntactically correct expressions evaluated to true, regardless of parenthe-
   ses.
d. Example: \(((0 \lor 1) \Rightarrow (0 \land 0)) \Rightarrow 1\)
   All syntactically correct expressions evaluated to true if and only if there
   were not parentheses around the last two terms; that is, if and only if the
   expression did not include \((0 \Rightarrow 1)\).

Problem 5

Suppose we define a new operation \(\star\) on logical propositions such that

\[ x \star y \equiv \neg(x \land y) \]

Create a truth table for each of the following expressions, and state which logical
operator the expression is equivalent to.

a. \(x \star x\)
b. \((x \star y) \star (x \star y)\)
c. \((x \star x) \star (y \star y)\)
d. \((x \star (x \star y)) \star (y \star (y \star x))\)

Solution

<table>
<thead>
<tr>
<th>(x)</th>
<th>(x \star x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

\(x \star x\) is equivalent to \(\neg x\).
b. 

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>(x ⋆ y) ⋆ (x ⋆ y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

(x ⋆ y) ⋆ (x ⋆ y) is equivalent to x \land y.

c. 

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>(x ⋆ x) ⋆ (y ⋆ y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

(x ⋆ x) ⋆ (y ⋆ y) is equivalent to x \lor y.

d. 

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>(x ⋆ (x ⋆ y)) ⋆ (y ⋆ (y ⋆ x))</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

(x ⋆ (x ⋆ y)) ⋆ (y ⋆ (y ⋆ x)) is equivalent to x \oplus y.