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. \( m = 659918 \) for \( n = 16 \). In the digit string, use the additional digits \( A = 10, B = 11, \ldots, F = 15 \).

b. 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.

c. Prove that any positive integer \( m \) can be written as:

\[
a_k 3^k + a_{k-1} 3^{k-1} + \cdots + a_1 3^1 + a_0 \text{ where each } a_i \in \{-1, 0, 1\}
\]
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 \( n \).

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 \( m = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \) 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
\[
f(\{q_1, \ldots, q_k\}) = [q_1 \times q_2 \times \cdots \times q_k]_{R_m^n}
\]

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:
\[

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

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

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

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 \((q_1^*, q_2^*) \notin R_m^n\), concluding that \( g \) is injective. Why is that equivalent to injectivity?\(^1\)

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

---

\(^1\)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.
Note: You may assume the following result without proof. For $Q = \{q_1, \ldots, q_k\}$ and positive exponents $\lambda_1, \ldots, \lambda_k$,

\[
\left( q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k} \right) \in R_m^*.
\]

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.

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. $0 \lor 1 \Rightarrow 0 \land 0 \Rightarrow 1$

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. $(x \star (x \star y)) \star (y \star (y \star x))$