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 $n = 2$.
   $2 * 10 + 0 * 9 ... + 0 * 0$
   10000000000

   b. $m = 196$ for $n = 5$.
   $(5^3) * 1 + (5^2) * 2 + (5^1) * 4 + (5^0) * 1$
   1241

   c. $m = 614$ for $n = 9$.
   $(9^2) * 7 + (9^1) * 5 + (9^0) * 2$
   752

d. $m = 659\,918$ for $n = 16$. In the digit string, use the additional digits $A = 10, B = 11, \ldots, F = 15$.
$(16^4) * 10 + (16^3) * 1 + (16^2) * 1 + (16^1) * 12 + (16^0) * 14$
A11CE

b. Consider a binary number of the form $m = 1010\ldots0_2$, 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.
6m = m + m + m + m + m + m
Adding $1010\ldots0_2$ to itself 6 times, we find $11110\ldots0_2$, or 1111 with k-4 trailing zeros.

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

$$a_k3^k + a_{k-1}3^{k-1} + \ldots + a_13^1 + a_0 \text{ where each } a_i \in \{-1, 0, 1\}$$

Proof. by contradiction
Assume $\exists x$ s.t. x can't be expressed by $a_k3^k + a_{k-1}3^{k-1} + \ldots + a_13^1 + a_0$
Case 1: x is not divisible by 3.
The nearest multiple of 3 is either $x + 1$ or $x - 1$.
Since every term excluding a_0 is divisible by 3, x can be expressed in terms of $a_k3^k + a_{k-1}3^{k-1} + \ldots + a_13^1 + a_0$, where a_0 is 1 or -1. Case 2: x is divisble by 3.
Since every term excluding a_0 is divisible by 3, x can be expressed in terms of $a_k3^k + a_{k-1}3^{k-1} + \ldots + a_13^1 + a_0$, where a_0 is 0.

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 seperately by using the encoding of $A = 1,\ B = 2,\ \ldots\ , Z = 26$. Your answer should be a sequence of numbers.

2 5 5 20 19

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.

J E L L O

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). $x^2 = nk + y^2$
$x^2 - y^2 = nk$
$(x - y)(x + y) = nk$
Either n divides (x-y) or n divides (x + y), and k divides (x - y) or k divides (x + y).
Thus, Dwight can simply check which of these is an integer to know which value is divisible by p and 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.

$kd \equiv 1 \pmod{\varphi n}$
$kd - 1 \equiv 0 \pmod{\varphi n}$
$kd - 1 = (p - 1)(q - 1)b$
gcd(13*181 -1, 299*59 -1) = (p-q)(q-1)b
$1176 = (p - 1)(q - 1)b$
$1176 = pq - p - q + 1$
$1176 = 1248 - p - q$
$p + q = 72$
$(x - p)(x - q) = 0$
$x^2 - x(p + q) + pq = 0$
$x = 29, x = 43$
Thus, n can be factored by 29 and 43.

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

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

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

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

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:

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

What kinds of patterns do you see in these equivalence classes? Make sure to pay special attention to $f(\varnothing)$ 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 $f(F) = \{0\}$?

   For $f(F)$ to contain elements other than 0, m must be at least 2 times larger than the product of the prime factors of m.
   For instance, in this case m must be at least 60, so that 2*3*5 = 30 would be in $f(F)$.

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?

Proof. by contradiction
Assume that there exists $q_1^{*a} \equiv q_2^{*b} \pmod{m}$
$q_1^{*a} = q_2^{*b} + mk$
Since q_1^* and q_2^* come from unique subsets, they must contain at least 1 unique value, or prime factor.
Thus, let r be a prime number that is a factor of q_2^{*b} and mk, but not of $q_1^* a$.
r does not divide $q_1^* a$, so $q_1^{*a} \not\equiv q_2^{*b} \pmod{m}$.
Thus, $(q_1^*, q_2^*) \notin R_m^*$.
Since, WLOG, Q_1 and Q_2 are unique subsets given $f(q)$, each subset of the powerset of F is yielded by exactly one input value q.
Thus, f is injective.

c. Consider some arbitrary element

$$x = c q_1^{b_1} q_2^{b_2} \dots q_k^{b_k},$$

where $Q = \{q_1, \dots, q_k\} \subseteq F$, $\gcd(c, m) = 1$, and all b_i are positive. Prove that $x \in f(Q)$, concluding that f is surjective. Why is that equivalent to surjectivity?
$x = c * q_1 * \cdots * q_k$
$x^a \equiv y^b \pmod{m}$
Find $x^a \equiv c(q_1 * \cdots * q_k) \pmod{m}$
gcd(c, m) = 1
$c^{\varphi(m)} \equiv 1 \pmod{m}$
Let b = $\varphi(m)$
$x^a \equiv (q_1^{b_1} + \cdots + q_k^{b_k})^b \pmod{m}$
$x^a \equiv (q_1^{b+1^{\varphi(m)}} + \cdots + q_k^{b+k^{\varphi(m)}}) \pmod{m}$
This satisfies our original form, $x = c * q_1 * \cdots * q_k$, where $x \in f(Q)$.
Since, WLOG, $x \in f(Q)$, every $f(Q)$ is mapped to. Thus, the function is surjective.
Note: You may assume the following result without proof. For $Q = \{q_1, \dots, q_k\}$ and positive exponents $b_1, \dots, b_k$,

$$\left(q_1 q_2 \dots q_k, q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}\right) \in R_m^*.$$

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

If m is prime, m has exactly two factors, m and 1. Since 1 is not prime, the function f cannot take it in as an input.
Thus, our two sets are $f(\emptyset)$ and $f(m)$.
$f(\emptyset)$ contains every number within M that is not divisible by m, AKA every number besides m.
In 4.5, we showed that every number in $M \times M$ is relatively prime with m because each number ¡ M.
Since $\not{x} \in M \times M$ s.t. $x \equiv 0 \pmod{m}$, $f(m) = \{0\}$.

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. $(0 \wedge 1) \vee 1 \Rightarrow (1 \wedge 1 \wedge 1) \vee 0$

b. $(1 \vee 0) \wedge 1 \wedge 1 \wedge 1 \wedge (1 \vee 0)$

c. $(1 \wedge 0) \vee 0 \Leftrightarrow (1 \Rightarrow 0)$

d. $(0 \vee 1) \Rightarrow (0 \wedge 0 \Rightarrow 1)$

Problem 5

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

$$x \star y \equiv \neg(x \wedge y)$$

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

a. $x \star x$

x	x$\star x$
T	F
F	T

This is equivalent to $\neg x$

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

x	y	x$\star y$	(x$\star y) \star (x \star y)$
T	T	F	T
T	F	T	F
F	T	T	F
F	F	T	F

This is equivalent to x AND y

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

x	y	x$\star x$	y $\star y$	x $\star x AND y \star y$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

This is equivalent to x OR y

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

x	y	x$\star y$	y $\star x$	x $\star (x \star y)$	y $\star (y \star x)$	(x $\star (x \star y)) \star (y \star (y \star x))$
T	T	F	F	T	T	F
T	F	F	T	T	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	F

This is equivalent to x XOR y.