**Math 55: Discrete Math**
G.S.I. Loren Looger
September 25, 1997
**Midterm #1 Solutions**

**(§1a ) Find the remainder when $2^{55}$ is divided by the prime number 53.**

**We see that we are working mod the prime number 53, and that the number we are exponentiating, 2, is relatively prime to 53. Also, the exponent of 2, that is, 55, is very close to $(53-1) = 52$. We should immediately suspect application of Fermat's Little Theorem. Thus, by Fermat:**

$$2^{53-1} = 2^{52} \equiv 1 (mod 53)$$

**But then,**

$$2^{55} = 2^{52} * 2^3 \equiv 1 * 2^3 \equiv 8 (mod 53).$$

**You will be given partial credit if you used fast modular exponentiation and got the correct answer.**

**(§1b ) Suppose that $f$ and $g$ are functions $S \to S$, where $S$ is the set of positive integers less than $10^3$. If the composition $f \circ g$ is 1-1 and onto, must $f$ and $g$ be 1-1 and onto? (Give a short proof or provide a counterexample.)**

**The actual size of $S$ is immaterial; we may think of $S$ as a two-element set. The important point is that $S$ is finite. Now, from two homework questions, we know that: (i) if $f \circ g$ is 1-1, then $g$ is 1-1. (ii) if $f \circ g$ is onto, then $f$ is onto. But now we know that a function mapping a finite set into itself is 1-1 if and only if it is onto. So $f$ and $g$ are both 1-1 and onto.**

**In the following problems, it will be extremely useful to know that:**

$$203 * 83 - 39 * 432 = 1.$$

**(§2a ) Find an integer $x$ such that $83x \equiv 1 (mod\ 432)$.**

**This problem is trivial once we know the given equality, for:**

$$83 * 203 = 1 + 39 * 432 \equiv 1 (mod\ 432).$$

**So take $x = 203$.**

**(§2b ) Find an integer $y$ such that $39y \equiv 4 (mod\ 203)$.**

**This problem is only slightly harder than the first part. We note that:**

$$39 * (-432) = 1 - 203 * 83 \equiv 1 (mod\ 203).$$

**Multiplying by 4, we have:**

$$39 * (-432) * 4 \equiv 1 * 4 \equiv 4 (mod\ 203).$$

**Thus a perfectly acceptable answer is $y = -4 * 432 = -1728$. Any number that is congruent to $-1728 (mod\ 203)$ is also a correct answer.**

**(§2c ) Find an integer $z$ such that $z \equiv 2$ mod 39 and $z \equiv 3$ mod 203.**

**This is a straightforward application of the Chinese Remainder Theorem. We have:**

$$a_1 = 2, m_1 = 39, a_2 = 3, m_2 = 203.$$

We quickly find $M_1$ and $M_2$:

$$M_1 = 39 * 203/39 = 203; M_2 = 39 * 203/203 = 39.$$

Now we find $y_1$ and $y_2$:

$$M_1 * y_1 = 203y_1 \equiv 8y_1 \equiv 1 mod\ 39.$$

By inspection, $y_1 = 5$ will work.

Also,

$$M_2 * y_2 = 39y_2 \equiv 1 mod\ 203.$$

But we have solved this congruence in part (b):

$$39 * (-432) \equiv 1 mod\ 203.$$

So take $y_2 = -432$. Thus our solution $z$ is:

$$z = a_1 y_1 M_1 + a_2 y_2 M_2 = 2 * 5 * 203 + 3 * (-432) * 39.$$

No simplification is required.

(§3 ) Can you conclude that $A = B$, if $A, B$ and $C$ are sets such that $A \cap C = B \cap C$, and $A \cup C = B \cup C$? (Explain why or why not.)

Yes, we may conclude this. We now give a short proof: Take $a \in A$. Now either $a \in C$ or $a \notin C$. If $a \in C$, then $a \in A \cap C$. As $A \cap C = B \cap C$, we must have $a \in B$. If $a \notin C$, then we use the second equality. Namely, $a \in A \cup C$, as $a \in A$, but $A \cup C = B \cup C$, so $a \in B \cup C$. But $a \notin C$, so $a \in B$. In either case, $a \in A$ implies $a \in B$. So $A \subseteq B$. A similar argument with $A$ and $B$ switched shows that $B \subseteq A$. So $A = B$.

(§4 ) The Numbers $A_n$ are defined recursively as follows:

$$A_0 = 0; A_1 = 1; A_n = 5A_{n-1} - 6A_{n-2},\ \ n \geq 2.$$

Prove that $A_n = 3^n - 2^n$ for all $n \geq 0$.

This is obviously an application of mathematical induction. We first prove our two base cases:

$$A_0 = 0 = 1 - 1 = 3^0 - 2^0$$

$$A_1 = 1 = 3 - 2 = 3^1 - 2^1.$$

So our base cases both satisfy the statement. We must only prove the inductive step. So assume that the statement is true for all nonnegative integers up to a certain $n$, where $n \geq 2$. So in particular, the statement is true for $n$ and $n-1$. We must verify that the statement is true for $n+1$. To show this, we merely substitute into the definition of $A_{n+1}$ given our assumptions:

$$A_{n+1} = 5A_n - 6A_{n-1} = 5(3^n - 2^n) - 6(3^{n-1} - 2^{n-1}).$$

But this is

$$5 * 3 * 3^{n-1} - 5 * 2 * 2^{n-1} - 6 * 3^{n-1} + 6 * 2^{n-1}.$$

Gathering terms, we have

$$A_{n+1} = (15 - 6) * 3^{n-1} - (10 - 6) * 2^{n-1} = 3^2 * 3^{n-1} - 2^2 * 2^{n-1} = 3^{n+1} - 2^{n+1}.$$

So we have verified the statement for $n+1$. So by induction, the statement holds for all integers $n \geq 0$.

**(§5 ) Suppose that $f(x) = 5^x$ and $g(x) = 10^x$. Decide whether each of the following statements is true. Explain your reasoning.**

(a) $f(x) = O(g(x))$: This is true. In fact, $5^x \leq 1 * 10^x, x \geq 0$. So taking $C = 1$, and $K = 0$, we see that $5^x = O(10^x)$.

(b) $g(x) = O(f(x))$: This statement is false. If it were true, we would have:

$$\lim_{x \to \infty} \frac{g(x)}{f(x)} \leq C < \infty.$$

But:

$$\frac{g(x)}{f(x)} = \frac{10^x}{5^x} = 2^x.$$

So:

$$\lim_{x \to \infty} \frac{g(x)}{f(x)} = \lim_{x \to \infty} 2^x = \infty.$$

This contradiction shows that $g(x) \neq O(f(x))$.

(c) log $g(x) = O($ log $f(x))$: This statement is true. For: $log\ g(x) = x * log5$. Also, $log f(x) = x * log10$.

Thus, $log\ g(x) = \frac{log5}{log10} * log f(x)$. Thus $log\ g(x) = O(log f(x))$.

(d) $f(x) = O(log\ g(x))$. This is false. For if it were true, we would have:

$$\lim_{x \to \infty} \frac{f(x)}{log\ g(x)} \leq C < \infty.$$

But by L'Hôpital's Rule, we have that:

$$\lim_{x \to \infty} \frac{f(x)}{log\ g(x)} = \lim_{x \to \infty} \frac{5^x}{x * log10} = \lim_{x \to \infty} \frac{(5^x)'}{(x * log10)'} = \lim_{x \to \infty} \frac{5^x * log5}{log10} = \infty.$$

This contradiction shows that $f(x) \neq O(log\ g(x))$.

**(§6a ) Find an integer $d$ such that $(M^{11})^d \equiv M$ mod 55 for all integers $M$ such that gcd($M$,55) = 1.**

This is a very small RSA Decryption problem for the case $p = 5, q = 11$. We calculate $(p-1)(q-1) = 4 * 10 = 40$, and see that gcd(11,40) = 1, so the required decrypting exponent $d$ is the inverse of 11 mod 40, that is:

$$11d \equiv 1\ mod\ 40$$

We may solve this any way we like; we quickly find that $11 * 11 = 121 \equiv 1$ mod 40. So take $d = 11$.

**(§6b ) Determine whether $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is a tautology.**

This is indeed a tautology. Perhaps the most clear demonstration is a truth table:

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \rightarrow q$ | $(\neg q \wedge (p \rightarrow q))$ | $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg q$ |
|---|---|---|---|---|---|---|
| **T** | **T** | **F** | **F** | **T** | **F** | **T** |
| **T** | **F** | **F** | **T** | **F** | **F** | **T** |
| **F** | **T** | **T** | **F** | **T** | **F** | **T** |
| **F** | **F** | **T** | **T** | **T** | **T** | **T** |

So the statement is indeed a tautology.