Math 55—Fall 2012
Homework 8 Solutions

4.6 #30. First Alice and Bob agree on the prime $p = 101$ and primitive root $a = 2$. Alice sends Bob the number $2^7 \mod 101$, or 27, and Bob sends alice the number $2^9 \mod 101$, or 7. Now Alice calculates $7^7 \mod 101$, getting 90, and Bob calculates $27^9 \mod 101$, which is also equal to 90. Alice and Bob then communicate using some conventional cipher based on their shared secret key, 90.

Any eavesdropper will know $p = 101$, $a = 2$, and the numbers 27 and 7 transmitted by Alice and Bob, but can only find out their chosen exponents $k_1 = 7$ and $k_2 = 9$, and thereby learn their shared key 90, by solving a discrete logarithm problem modulo 101—not so hard in this case, but believed to be impractical if a large prime (of 100 digits, say) were used.

4.6 #32. Alice first encodes her message by converting blocks of letters to numbers, e.g. as 0120 2499 1314 2299, if she uses 0 to 25 for letters of the alphabet and 99 to indicate a space. Next she applies her own private key to each block, and then Bob's public key. For the first block, for example, she computes $120^{1183} \mod 2867 = 1665$, and then computes $1665^{21} \mod 3127 = 2806$.

When Bob receives this he first decrypts with his private key, recovering $2806^{1149} \mod 3127 = 1665$. Then he applies Alice's public key, recovering $1665^7 \mod 2867 = 0120$, the first block of the original message. Alice and Bob communicate the other message blocks in the same way.

Only Alice could have produced data which results in an intelligible message when her public key is applied, so Bob knows not only the contents of the message but also that it is genuinely from Alice.

5.1 #6. Basis step: for $n = 0$, both sides of the identity are equal to 0.

Induction step: for $n > 0$, assume by induction that the identity holds for $n - 1$, that is, we have

$$1 \cdot 1! + 2 \cdot 2! + \cdots + (n-1) \cdot (n-1)! = n! - 1.$$

Adding $n \cdot n!$ to both sides gives

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = n \cdot n! + n! - 1.$$

Now the right hand side is equal to $(n+1)n! - 1 = (n+1)! - 1$. The proof is complete.

5.1 #10. The formula is

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1},$$

valid for $n \geq 0$.

To prove this by induction, we observe as a basis step that it is correct for $n = 0$, where both sides are equal to 0. The left hand side is an empty sum in this case.

For the induction step, with $n > 1$, we may assume that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}.$$

Adding $1/(n(n+1))$ to both sides, we need to verify that

$$\frac{n-1}{n} + \frac{1}{n(n+1)} = \frac{n}{n+1},$$

which is a bit of easy algebra.

5.1 #22. The inequality $n^2 \leq n!$ holds for $n = 0$, $n = 1$ and $n \geq 4$. To prove it for $n \geq 4$, our basis step is $4^2 = 16 \leq 24 = 4!$. For $n > 4$ we assume by induction that $(n-1)^2 \leq (n-1)!$. Multiplying both sides by n gives $n(n-1)^2 \leq n!$. Now we need to show that $n^2 \leq n(n-1)^2$, and for this it is enough to show that $n \leq (n-1)^2$. Now $(n-1)^2 - n = n^2 - 3n + 1 = (n-1)(n-2) - 1$. Since $n > 4$, this is positive, so $n \leq (n-1)^2$.

5.1 #50. The basis step is false. For $n = 1$, the left hand side is 1, but the right hand side is $9/8$.

5.1 #52. Basis step: if $n = 1$, then $\{1, \ldots, n\} = \{1\}$, so the only function f from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ is the constant function $f(k) = 1$. For $m > 1$, this is not injective.

Induction step: for $n > 1$, consider two cases.

Case I: f maps at least two elements of $\{1, \ldots, m\}$ to n. Then f is not injective.

Case II: f maps at most one element of $\{1, \ldots, m\}$ to n. If there is such an element, call it k. Otherwise, let k be any element of $\{1, \ldots, m\}$, say $k = m$.

Now let g be a bijective function from $\{1, \ldots, m-1\}$ to $\{1, \ldots, m\} - \{k\}$, for example $g(i) = i$ for $i < k$, $g(i) = i + 1$ for $k \leq i < m$. Since f maps all elements other than k into $\{1, \ldots, n-1\}$, $f \circ g$ is a function from $\{1, \ldots, m-1\}$ to $\{1, \ldots, n-1\}$. Since $m > n$ implies $m - 1 > n - 1$, we can conclude by induction that $f \circ g$ is not injective. But since g is bijective, if f were injective, then $f \circ g$ would be injective. So f is not injective.

A remark: the theorem in this problem might seem to be obvious, since by definition the existence of an injective function from a set of cardinality m to a set of cardinality n implies that $m \leq n$. The point is that it is not *a priori* obvious that the definition of $m \leq n$ for cardinalities agrees (in the case of finite cardinalities) with the arithmetical definition of $m \leq n$ for natural numbers. Indeed, it is not even obvious that the sets $\{1, \ldots, m\}$ and $\{1, \ldots, n\}$ might not have the same cardinality, even though $m \neq n$.

That is what the theorem in this problem serves to show.

5.1 #64 The case $n = 1$ is tautological. Taking this as our basis step, we prove the result for $n > 1$ by induction. We apply Lemma 2 of Section 4.3 (proved there using Bezout's theorem, which follows from the Euclidean algorithm) with $a = p$, $b = a_n$ and $c = a_1 \cdots a_{n-1}$. Since p is prime, we either have $p | a_n$, in which case we are done, or else $\gcd(p, a_n) = 1$, which is the hypothesis of Lemma 2. In this second case it then follows that $p | a_1 \cdots a_{n-1}$, and we can conclude by induction that $p | a_i$ for some i between 1 and $n - 1$.

5.2 #6. With 3 and 10 cent stamps, we can form n cents postage for $n = 0, 3, 6, 9, 10, 12, 13, 15, 16$ and all $n \geq 18$. You can check the possible amounts for $n < 18$ exhaustively. We'll prove by (strong) induction that all amounts $n \geq 18$ can be formed.

We assume by induction that k cents of postage can be formed for all $18 \leq k < n$. If $n \geq 21$, then $18 \leq n - 3 < n$, so we can form $n - 3$ cents of postage and add one 3 cent

stamp. We are left to verify the cases $n = 18, 19, 20$ directly: $18 = 6 \times 3$, $19 = 10 + 3 \times 3$, $20 = 2 \times 10$.

5.2 #14. We assume by strong induction that the formula is correct for all piles of k stones with $1 \leq k < n$. If $n = 1$, there is no splitting to be done, and we get the empty sum 0, which is equal to $n(n-1)/2$ in this case. If $n > 1$, say we split the pile into piles of sizes r and s, both of which are less than n. By induction, the contributions to the total from further splitting of each of these two piles are $r(r-1)/2$ and $s(s-1)/2$, for a total of

$$rs + r(r-1)/2 + s(s-1)/2.$$

By a bit of algebra, this is equal to $(r+s)(r+s-1)/2$. Since $n = r + s$, the total is $n(n-1)/2$, as we were to prove.