Math 240 – Assignment 4 Solutions

Assigned on 4 Nov, 2012. Due on 19 Nov, 2012, before 5PM.

1. (RSA Encryption). Recall that in RSA encryption I publicly reveal a prime $p$ and an integer $n$ that is the product of 2 primes. Together, the pair $(p, n)$ form my public key. For this question, my public key is $p = 23, n = 91$.

(a) Use RSA encryption to encrypt the message $M = 24$.

(b) Use RSA decryption to recover the message $M$ from the decrypted message $\hat{M}$ you calculated in part $(a)$.

In both parts, show your work.

2. (Bijections). Give a bijection between the set of all (positive and negative) integers and the set of positive integers that are perfect squares (i.e. the set $\{1, 4, 9, 16, \ldots \}$).

3. (The binomial theorem).

(a) What is the coefficient of $x^5y^8$ in $(2x + 3y)^{13}$?

(b) Prove that for all $n \geq 1$,

$$3^n = \sum_{0 \leq i \leq n} 2^i \cdot \binom{n}{i}.$$ 

(c) Explain the equality in (b) combinatorially, starting from the fact that $3^n$ is the way to assign one of the three colours red, yellow, or blue to each of the integers $\{1, \ldots, n\}$.

(d) Use the fact from (b) to show that

$$3^n = \sum_{0 \leq j \leq i \leq n} \binom{n}{i} \binom{i}{j}.$$ 

4. (Recurrence relations).

(a) Recall the definition of the Fibonacci numbers ($F_0 = 1, F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5$, then 8, 13, 21, ...). Show that for all $n \geq 1$,

$$F_n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}.$$ 

Recall that $\lfloor x \rfloor$ means the largest integer less than or equal to $x$, so $\lfloor n/2 \rfloor$ will equal $n/2$ if $n$ is even, and will equal $(n-1)/2$ if $n$ is odd. (Hint: one way to prove this is by induction, and you may have to do cases depending on whether $n$ is odd or even.)

(b) Solve the recurrence relation $A(n+1) = 3A(n) + 7$ with $A(0) = 2, A(1) = 13$. 

1
Solutions

1. (RSA Encryption).

(a) To encrypt the message $M = 24$ we must compute $M^p \pmod{n} = 24^{23} \pmod{91}$. For this note that $24^2 = 576 \equiv 30 \pmod{91}$, so

$$24^{23} = (24^2)^{11} \cdot 24 \equiv 30^{11} \cdot 24 \pmod{91}.$$

Next, $30^2 = 900 \equiv (-10) \pmod{91}$, so $30^4 \equiv 100 \pmod{91} \equiv 9 \pmod{91}$, so $30^8 \equiv 81 \pmod{91} \equiv -10 \pmod{91}$, so $30^{10} \equiv (-10)^2 \pmod{91} \equiv 9 \pmod{91}$. It follows that

$$30^{11} \equiv 9 \cdot 30 \equiv 270 \equiv -3 \pmod{91}.$$

Finally, we obtain that

$$24^{23} \equiv (-3) \cdot 24 \equiv 19 \equiv 19 \pmod{91},$$

so the encrypted message is 19.

(b) We have $91 = 7 \cdot 13$ so the decryption exponent is $x$ such that $23x \equiv 1 \pmod{72}$. Applying Euclid’s algorithm as you have learned in class, you will determine that $x = 47$. To decrypt we must therefore compute $19^{47} \pmod{91}$. For this first note $19^2 \equiv -3 \pmod{91}$ so $19^{12} \equiv (-3)^6 \pmod{91} = 729 \equiv 1 \pmod{91}$. It follows that $19^{48} = 19^{4 \cdot 12 + 1} \equiv 1 \pmod{91}$ so $19^{47} \equiv 19^{-1} \pmod{91}$. Using Euclid’s algorithm to compute $19^{-1} \pmod{91}$ we obtain that $19^{-1} \equiv 24 \pmod{91}$, so $19^{47} \pmod{91} = 24$, and we have indeed recovered the original message.

2. (Bijections). Many bijections are possible. Here is one. For $n \in \mathbb{Z}$ let

$$f(n) = \begin{cases} (2n + 1)^2 & \text{if } n \geq 0 \\ (2n)^2 & \text{if } n < 0. \end{cases}$$

This maps non-negative integers to squares of odd integers, and negative integers to squares of even integers.

3. (The binomial theorem).

(a) Write $x' = 2x$, $y' = 3y$. By the binomial theorem, the coefficient of $(x')^5(y')^8$ in $(x' + y')^{13}$ is \( \binom{13}{5} \). Since $(x')^5(y')^8 = 2^5 \cdot 3^8 \cdot x^5 y^8$ it follows that the coefficient of $x^5 y^8$ in $(x + y)^{13}$ is

$$2^5 \cdot 3^8 \binom{13}{5} = 270207224.$$

(b) By the binomial theorem,

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Taking $x = 1$ and $y = 2$, we obtain that

$$3^n = \sum_{0 \leq i \leq n} \binom{n}{i} \cdot 2^i,$$

which is what we are asked to prove.
(c) First, part (c) states that $3^n$ is the way to assign one of the three colours red, yellow, or blue to each of the integers $\{1, \ldots, n\}$. This is obvious since we have three choices for each integer, and there are $n$ integers, so in total there are $3 \cdot 3 \cdot \ldots \cdot 3 = 3^n$ possibilities. We next describe a different way to count the number of possibilities. We will choose the set $B$ of “blue” integers in two steps, by first choosing its size $i$, and next choosing the precise set of integers to be coloured blue. Once we choose its size, there are $(\binom{n}{i})$ possibilities for the set $B$. Once we make this choice (so we have now chosen a set $B$ with $|B| = i$ to be coloured blue), we have to colour each of the remaining $n - i$ integers either yellow or red. In other words, we have to split the set $\{1, \ldots, n\} \setminus B$ into two parts: a red part, and a yellow part. Since $|\{1, \ldots, n\} \setminus B| = n - i$, we know there are $2^{n-i}$ ways to do this. Together these facts yield that the number of ways to colour each of $\{1, \ldots, n\}$ with one of red, yellow, or blue, is

$$\sum_{i=0}^{n} \binom{n}{i} 2^{n-i}.$$  

Since $(\binom{n}{i}) = (\binom{n}{n-i})$, the preceding sum is the same as

$$\sum_{i=0}^{n} \binom{n}{i} 2^i,$$

and this is the combinatorial explanation.

(d) We know that $2^i = \sum_{0 \leq j \leq i} \binom{n}{j}$, and so from (b) we have

$$3^n = \sum_{0 \leq i \leq n} \left[ \binom{n}{i} \cdot \sum_{0 \leq j \leq i} \binom{i}{j} \right].$$

Since $(\binom{n}{i})$ does not depend on $j$, we can move it inside the inner sum to get

$$3^n = \sum_{0 \leq i \leq n} \left( \binom{n}{i} \right) \sum_{0 \leq j \leq i} \binom{i}{j}.$$  

Finally, the last double sum counts all pairs of integers $i, j$ with $0 \leq j \leq i \leq n$, so we get

$$3^n = \sum_{0 \leq j \leq i \leq n} \binom{n}{i} \binom{i}{j}.$$  

4. *(Recurrence relations).*

(a) This is question 4.2.6 in the course book, and the answer is in the back of the book (a tiny amount of argument is left to the reader, but you should be able to fill in the remaining details from the answer given in the book).

(b) We saw that the general form of solutions to “quadratic” recurrence relations $x_{n+1} = ax^n + bx^{n-1}$ is given by solving a quadratic equation, and yields solutions of the form $x^n = A\phi^n + A'(\phi')^n$. Here we have a “linear” recurrence with a constant term; by analogy, we therefore expect our solution to have the form $A(n) = ax^n + b$ for some
constants $a, b, x$. If $A(n)$ is extremely large then $A(n + 1)$ is roughly $3A(n)$ and so we should have $x = 3$, so we should search for a solution of the form

$$A(n) = a \cdot 3^n + b.$$ 

In order for the recurrence to hold, the values $a$ and $b$ should satisfy that

$$3(a \cdot 3^n + b) + 7 = a \cdot 3^{n+1} + b,$$

or in other words when $3b + 7 = b$. This means $b = -7/2$, and so to have $A(0) = 2$ we must have $a + b = a - 7/2 = 2$, so we must have $a = 11/2$. We have derived that the solution should be

$$\frac{11}{2}3^n - 7/2.$$ 

This indeed equals 2 when $n = 0$ and 13 when $n = 1$, and satisfies the recurrence relation, so by induction we have $A(n) = (11/2)3^n - 7/2$ for all $n$. 

\[ \text{(4)} \]