Math 25: Solutions to Homework #7

(8.4 # 6) What is the cipher text that is produced when RSA encryption with key $(e, n) = (7, 2627)$ is used to encrypt the message LIFE IS A DREAM?

The numerical equivalent of the plaintext is 1108 0504 0818 0003 1704 0012. Raising each of these blocks to the power 7 mod 2627 we get the ciphertext 1019 0014 1066 2187 1349 2155.

(8.4 # 8) If the ciphertext message produced by RSA encryption with the key $(e, n) = (5, 2881)$ is 0504 1874 0347 0515 2088 2356 0736 0468, what is the plaintext message?

We must first find the decryption key by solving $5d \equiv 1 \pmod{\phi(2881)}$. First, since $2881 = 43 \cdot 67$, $\phi(2881) = 42 \cdot 66 = 2772$. Then $d \equiv 5^{\phi(2772)-1} \pmod{2772}$. Since $2772 = 2^2 \cdot 3^2 \cdot 7 \cdot 11$, $\phi(2772) = \phi(2^2)\phi(3^2)\phi(7)\phi(11) = 2 \cdot 6 \cdot 6 \cdot 10 = 720$. Hence $d \equiv 5^{719} \equiv 1109 \pmod{2772}$. To decrypt, we raise each block of four digits to the power 719 mod 2881. We get the plaintext 0400 1902 0714 0214 1100 1904 0200 1004 which says EAT CHOCOLATE CAKE. Good words of advice.

(8.5 # 2) Show that if $a_1, a_2, \ldots, a_n$ is a super-increasing sequence, then $a_j \geq 2^{j-1}$ for $j = 1, 2, \ldots, n$.

We induct on $1 \leq j \leq n$. For the base case, since this must be a sequence of positive integers, $a_1 \geq 1 = 2^0 = 2^{1-1}$. Now let $1 \leq j < n$ and assume that $a_k \geq 2^{k-1}$ for all k with $1 \leq k \leq j$. Then

$$a_{j+1} > \sum_{k=1}^{j} a_k \geq \sum_{k=1}^{j} 2^{k-1} = 2^j - 1,$$

so $a_{j+1} \geq 2^j$. Therefore, by induction, $a_j \geq 2^{j-1}$ for $j = 1, 2, \ldots, n$.

(8.5 # 6) Encrypt the message BUY NOW using the knapsack cipher based on the sequence obtained from (17, 19, 37, 81, 160) by performing modular multiplication with multiplier $w = 29$ and modulus $m = 331$.

Multiplying by 29 mod 331, we get the sequence (162, 220, 80, 32, 6). The binary equivalent of BUY NOW is 00001 10100 11000 01101 01110 10110. For each string $x_1x_2x_3x_4x_5$, we compute $162x_1 + 220x_2 + 80x_3 + 32x_4 + 6x_5$. We get the ciphertext 6 242 382 306 332 274.

(11.1 # 6) Let a and b be integers not divisible by the prime p. Show that either one or all three of the integers a, b, and ab are quadratic residues of p.

We have $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Therefore if $\left(\frac{ab}{p}\right) = 1$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ so either both a and b are quadratic residues mod p, or both are quadratic nonresidues. If $\left(\frac{ab}{p}\right) = -1$, then

$\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$, so exactly one of $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ is a quadratic residue. In each case, there are either 1 or 3 quadratic residues from among a, b and ab.

(11.1 # 10) Show that if b is a positive integer not divisible by the prime p, then

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) = 0.$$

We have

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) =$$
$$\left(\frac{b}{p}\right)\left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{(p-1)}{p}\right)\right) = \left(\frac{b}{p}\right)(0) = 0$$

since there are the same number of quadratic residues as quadratic nonresidues mod p.

(11.1 # 12) Consider the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$, where p is prime and a, b, and c are integers with $p \nmid a$. Determine which quadratic congruences mod p have solutions.

(a) Let $p = 2$. Then there are four possible quadratic congruences:
 (i) $x^2 \equiv 0 \pmod{2}$,
 (ii) $x^2 + 1 \equiv 0 \pmod{2}$,
 (iii) $x^2 + x \equiv 0 \pmod{2}$, and
 (iv) $x^2 + x + 1 \equiv 0 \pmod{2}$.

 Since the only solutions mod 2 can be 0 or 1, they are easy to check. Of these, (i) has solution $x \equiv 0 \pmod{2}$, (ii) has solutions $x \equiv 0$ or $1 \pmod{2}$, and (iii) has solution $x \equiv 1 \pmod{2}$. Congruence (iv) has no solutions.

(b) Let p be an odd prime. If $ax^2 + bx + c \equiv 0 \pmod{p}$, then $ax^2 + bx + c = kp$ for some integer k. Using the quadratic formula,

$$x = \frac{-b \pm \sqrt{b^2 - 4a(c-kp)}}{2a}.$$

 Rearranging, we have

$$2ax + b = \pm\sqrt{b^2 - 4a(c-kp)}$$

 so, squaring,

$$(2ax+b)^2 = b^2 - 4a(c-kp).$$

 Then if we set $y = 2ax + b$ and $d = b^2 - 4ac$, we have $y^2 \equiv d \pmod{p}$. Starting with this congruence and performing the same steps in reverse, we recover the original congruence, so the two are equivalent. Then if $d \equiv 0 \pmod{p}$ then $y \equiv 2ax + b \equiv 0 \pmod{p}$, so $x \equiv -\overline{(2a)}b \pmod{p}$ is the only solution. If d is a quadratic residue mod p then there are exactly two solutions for $y^2 \equiv d \pmod{p}$, so exactly two solutions for the quadratic congruence, since $(2a, p) = 1$. If d is a quadratic nonresidue then there are no solutions for $y^2 \equiv d \pmod{p}$ and hence no solutions for the corresponding quadratic congruence mod p.

(11.1 # 14) Show that if p is primes and $p \geq 7$, then there are always two consecutive quadratic residues of p.

First suppose that $p = 7$. Then 1 and 2 are consecutive quadratic residues mod p. Now suppose that $p \geq 11$. Then 1, 4 and 9 are all quadratic residues mod p, and by problem # 6, at least one of 2, 5 or 10 is a quadratic residue mod p. Therefore at least one of the pairs $(1, 2)$, $(4, 5)$, or $(9, 10)$ is a pair of quadratic residues mod p.