Math 110 HW 2 solutions

1. Two possible definitions of ISBN numbers are:

$$a_1a_2 \dots a_10 \text{ such that } a_1 + 2a_2 + \dots + 10a_{10} \equiv 0 \mod 11.$$
$$a_1a_2 \dots a_10 \text{ such that } 10a_1 + 9a_2 + \dots + a_{10} \equiv 0 \mod 11.$$

   Prove that these definitions are equivalent. (i.e., a string is an ISBN number under the first definition if and only if it is an ISBN number under the second definition.)

   Solution:

$$\text{If } a_1 + 2a_2 + \dots + 10a_{10} \equiv b \mod 11$$
$$\text{and } 10a_1 + 9a_2 + \dots + a_{10} \equiv c \mod 11$$

   then, adding the two equations, we obtain

$$11a_1 + 11a_2 + \dots + 11a_{10} \equiv b + c \mod 11$$

   Since $11 \equiv 0 \mod 11$, we get $b + c \equiv 0 \mod 11$. Therefore $b \equiv 0 \mod 11$ if and only if $c \equiv 0 \mod 11$, so the two equations given in the problem each imply the other, as was to be shown.

   Another way of writing the same proof is to note that $10 \equiv -1 \mod 11$, $9 \equiv -2 \mod 11$ and so on, so that the two equations are negatives of each other mod 11, and therefore $b \equiv -c$.

2. Show that 0-13-116093-8 is not a valid ISBN number, and find two different valid ISBN numbers that each differ from 0-13-116093-8 in exactly one digit. (This shows that although the ISBN scheme can detect a single error, it cannot correct a single error.)

   Let's use the second equation given in the previous problem, so the larger digits are multiplied by bigger numbers. Also let's list the numbers as $0, 1, 3, 1, 1, -5, 0, -2, 3, -3 \mod 11$. Then we obtain $10 * 0 + 9 * 1 + 8 * 3 + 7 * 1 + 6 * 1 - 5 * 5 + 4 * 0 - 3 * 2 + 2 * 3 - 1 * 3$, or

$$0 + 9 + 24 + 7 + 6 - 25 + 0 - 6 + 6 - 3 = 18 \equiv 7 \mod 11,$$

   which is not 0 so this is not a valid ISBN number.

   So, if we change the fourth digit from 1 to 0, we will have the equation $0 + 9 + 24 + 0 + 6 - 25 + 0 - 6 + 6 - 3 = 11 \equiv 0 \mod 11$. Thus 0-13-016093-8 is a valid ISBN number.

   But we can also change the seventh digit from 0 to 1, and then we will get $0 + 9 + 24 + 7 + 6 - 25 + 4 - 6 + 6 - 3 = 22 \equiv 0 \mod 11$. Thus 0-13-116193-8 is a valid ISBN number.

3. The ciphertext 75 was obtained using the RSA algorithm with $n = 437$ and $e = 3$. You know that the plaintext is a positive integer less than 10. Determine which integer this is without factoring n.

   If the plaintext is a positive integer less than 10, we just need to know which of those has a cube that is $75 \mod 437$. Since 75 is not a cube in the integers (specifically $4^3 = 64 < 75$ and $5^3 = 125 > 75$), the number must have a cube greater than 437. As $7^3 = 343 < 437$ but $8^3 = 512 > 437$, the candidates are 8 and 9. As a matter of fact $512 \equiv 75 \mod 437$ so we hypothesize that the plaintext is 8. Just to check, however, note that $9^3 = 729$ and $437 * 2 = 874$ so $9^3 \equiv 55 \mod 437$. Thus the plaintext must be 8.

4. Three RSA users have public keys with modulus N_1, N_2, N_3 (you may assume if you want that these moduli are pairwise coprime) and each use the encryption exponent $e = 3$. Suppose that the same message $m(0 \leq m \leq N_i)$ is sent to each RSA user, and you intercept the three ciphertexts $c_i \equiv m^3 \pmod{N_i}$ for $i = 1, 2, 3$.

   Show that $0 \leq m^3 \leq N_1 N_2 N_3$, and hence that using the Chinese remainder theorem, you can not only calculate the value of $m^3 \pmod{N_1 N_2 N_3}$, but that you actually obtain the exact value of m^3 and hence can read the message m.

   We are given that $0 \leq m \leq N_i$ for each i. Without loss of generality, suppose that $N_1 \leq N_2 \leq N_3$. Therefore, $m^3 \leq N_1^3 \leq N_1 N_2 N_3$. Since $m \geq 0$, we also have $0 \leq m^3$ as requested. If we assume that N_1, N_2 and N_3 are pairwise coprime, then by the Chinese Remainder Theorem, there is a unique solution to $m^3 \equiv c_1 \pmod{N_1}, m^3 \equiv c_2 \pmod{N_2}$.

5. Find the remainder when 5^{1056} is divided by 7.

   Since 7 is prime we know $5^6 \equiv 1 \mod 7$. Also, 1056 is divisible by 2 and by 3, so it's a multiple of 6; therefore $5^{1056} \equiv 1 \mod 7$. Thus, the remainder when 5^{1056} is divided by 7 is 1.

6. Find all four solutions to $x^2 \equiv 1 \mod 187$.

   Two solutions we know already are $\pm 1 \mod 187$, or 1 and 186. Also, $187 = 11 \times 17$, the factors are two distinct primes, so they are coprime. Furthermore, $x^2 \equiv 1 \mod 11$ has only the solutions ± 1, and $x^2 \equiv 1 \mod 17$ has only the solutions ± 1. (To check this for 11 we can use the book section 3.9, to check it for 17 we do it explicitly since $17 \equiv 1 \mod 4$.)

   So a number that is $1 \mod 17$ and $-1 \mod 11$ is needed, as well as a number that is 1 mod 11 and $-1 \mod 17$. 67 is a number that is $1 \mod 11$ and $-1 \mod 17$, so $67^2 = 4489 = 1$ mod 187. Then -67 is the other equivalence class mod 187 desired, which is to say 120 mod 187.

   So the four solutions are $\pm 1, \pm 67 \mod 187$, or $1, 67, 120, 186 \mod 187$.

7. Let p and q be distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

   Let us find all the numbers $a : 1 \leq a \leq pq$ such that $\gcd(a, pq) \neq 1$. The gcd must be either p, q, or pq itself. So first let's count multiples of p. There are q multiples of p from 1 to pq, and among them, only pq is divisible by q; so there are $q - 1$ values of a such that $gcd(pq, a) = p$. Similarly there are $p - 1$ values of a such that $gcd(pq, a) = q$. And then there is one number $a = pq$ such that $gcd(pq, a) = pq$.

   So $\phi(pq)$, the number of integers from 1 to pq that are coprime to pq, is $pq - (q-1) - (p-1) - 1$, or $pq - p - q + 1$. That factors into $(p-1)(q-1)$ as was to be shown.

8. Using the inequality from the previous problem set

$$\prod_p p^{\lfloor \log_p(2n) \rfloor} \geq \binom{2n}{n},$$

   prove that there are innitely many primes. For this you will need a handle on how large the right hand side is. There is an estimate $\binom{2n}{n} \geq 4^n/(2n+1)$ which is obtained as follows:

Expand $4^n = (1+1)^{2n}$ using the binomial expansion. There are a total of 2n + 1 terms and the largest is $\binom{2n}{n}$.

Solution:

Suppose there are only finitely many primes. Let q be the largest prime, and from now on let us consider only values of n such that $2n \geq q$. Then for any prime p, $\log_p(2n) \leq \log_2(2n)$. Also, $p \leq q$. So if there are k distinct primes, then we have

$$\prod_p p^{\lfloor \log_p(2n) \rfloor} \leq q^{k \log_2(2n)}.$$

Now $\log_2(2n) = \log_q(2n)/\log_q(2)$, so the right hand side may be written $(2n)^{k/\log_q(2)}$. Let K be the constant $k/\log_q(2)$. Then $(2n)^K \geq \binom{2n}{n} \geq 4^n/2n+1$ for all $n \geq q/2$. But in that case, $(2N)^K(2n+1) \geq 4^n$, which is not true for sufficiently large n. This contradicts the assumption that there are finitely many primes. Therefore there are infinitely many primes.