HOMEWORK 4: SOLUTIONS - MATH 110
INSTRUCTOR: George Voutsadakis

Problem 1

Using results discussed in Section 2.3 estimate the number of prime numbers that are less than 10^{10}.

Solution:

The number of primes that are less than n is approximated by $\frac{n}{\ln n}$ for large n. Hence, the number of primes that are less than 10^{10} is approximated by

$$\frac{10^{10}}{\ln 10^{10}} = \frac{10^{10}}{10 \ln 10} = 434294482.$$

■

Problem 2 *Does there exist a number n so that both n and $n+1$ are prime numbers? If so, find such an n. If not, show why not.*

Solution:

Since one of the two numbers $n, n+1$ must be even and the only even number is 2, the only possibility is $n = 2$, which gives the two prime numbers 2 and 3. ■

Problem 3 *Which of the following is the correct UPC for Canada Dry tonic water? Show why the other numbers are not valid UPCs.*

$$0 \quad 1\,6\,9\,0\,0 \quad 0\,0\,3\,0\,3 \quad 4,$$

$$0 \quad 2\,4\,0\,0\,1 \quad 1\,0\,6\,9\,1 \quad 3,$$

$$0 \quad 1\,0\,0\,1\,0 \quad 2\,0\,1\,1\,0 \quad 5$$

Solution:

To check these we have to perform arithmetic mod 10 as follows:

													Sums
Multiplying Numbers	3	1	3	1	3	1	3	1	3	1	3	1	
First Code	0	1	6	9	0	0	0	0	3	0	3	4	
Profucts	0	1	18	9	0	0	0	0	9	0	9	4	50
Second Code	0	2	4	0	0	1	1	0	6	9	1	3	
Products	0	2	12	0	0	1	3	0	18	9	3	3	51
Third Code	0	1	0	0	1	0	2	0	1	1	0	5	
Products	0	1	0	0	3	0	6	0	3	1	0	5	19

Thus, only the first sum is equivalent to 0 mod 10. Hence the only valid bar code is the first code. ■

Problem 4 *In our discussion the two public numbers 7 and 143 were given. How would you encode the word "2"? The secret decoding number is 103. Without performing the calculation, how would you decode the encrypted message you just made if you are the receiver?*

Solution:

First, you raise 2 to the 7th power and then you obtain the remainder of the division of the result by 143. This is you encoded message.

$$2^7 \pmod{143}.$$

Second, you take you encoded message, and raise it to the 103rd power and compute the remainder of the division of the result by 143. Thus, the decoded message will be

$$(2^7)^{103} \pmod{143}.$$

This is equivalent to 2 mod 143!! ■

Problem 5 *Recall how exponents work, for example,* $7^{15} = 7^{(12+3)} = 7^{12} \times 7^3$. *Now, using exponent antics, compute* $5^{668} (\text{mod } 7)$.

Solution:

We have mod 7

$$\begin{aligned}
5^{668} &= 5^{666}5^2 \\
&= (5^6)^{111}5^2 \\
&\equiv 1^{111} \cdot 25 \quad \text{(by Fermat's Little Theorem)} \\
&\equiv 25 \\
&\equiv 4.
\end{aligned}$$

■

Problem 6 *Show that* $\sqrt{5}$ *is irrational.*

Solution:

Suppose that $\sqrt{5}$ is rational. Then there exist natural numbers m, n, such that $\sqrt{5} = \frac{m}{n}$. Without loss of generality we may assume that m, n do not have any prime factors in common; otherwise we would have simplified the fraction and obtained a reduced fraction which we would consider as our rational expression for $\sqrt{5}$. Now, we have $\sqrt{5} = \frac{m}{n}$ implies $5 = \frac{m^2}{n^2}$, i.e., $m^2 = 5n^2$. This shows that 5 divides m^2, whence, since 5 is a prime, it must divide m. Hence m can be written in the form $m = 5k$, for some natural number k. But then $m^2 = (5k)^2 = 5n^2$, whence $25k^2 = 5n^2$, which gives $5k^2 = n^2$. Thus 5 divides n^2, whence, since 5 is prime, 5 must divide n. Therefore $n = 5l$, for some natural number l.

Our reasoning gave us numbers k, l, such that $m = 5k$ and $n = 5l$. Thus m, n share the common factor 5, which contradicts our hypothesis. This shows that $\sqrt{5}$ cannot be written in the form $\frac{m}{n}$, for any natural numbers m, n. Therefore $\sqrt{5}$ is irrational. ■