Advanced Discrete Structure Homework 5 Tutorial

Simon Chang

Question 1

For each m greater than 1, how many primes are there in the closed interval $[m! + 2, m! + m]$?

Explain your answer.

Question 2

Let $S(m)$ be the smallest positive integer n for which there exists an increasing sequence of integers

$$m = a_1 < a_2 < \cdots < a_t = n$$

such that $a_1 a_2 \ldots a_t$ is a perfect square.

(If m is a perfect square,

we can let $t = 1$ and $n = m$.)

Question 2

For example, S(2) = 6 because the best such sequence is $a_1 = 2;\ a_2 = 3;\ a_3 = 6$.

m	1	2	3	4	5	6
S(m)	1	6	8	4	10	12

m	7	8	9	10	11	12
S(m)	14	15	9	18	22	20

Question 2 (a)

Show that S(m) exists for each $m \geq 1$.

Hint: Show that there is at least one such sequences $a_1, a_2, \ldots, a_t$ for each m.

a_t doesn't have to be the smallest possible one.

Question 2 (b)

Prove that $S(m) \neq S(m')$ whenever $0 < m < m'$.

Hint:

Prove by contradiction.

Question 3

Assume that a and b are integers not divisible by the prime p, establish the following:

(a) If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.

(b) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

[**Hint**: by (a), $a = b + pk$ for some k;

show that p^2 divides $a^p - b^p$.]

Question 3 (a)

If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.

Question 3 (b)

If $a^p \equiv b^p$ (mod p), then $a^p \equiv b^p$ (mod p^2).

[**Hint**: by (a), $a = b + pk$ for some k;

show that p^2 divides $a^p - b^p$.]

Question 4

Prove that if $n^j \equiv 1 \text{ (mod m)}$ and $n^k \equiv 1 \text{ (mod m)}$, then

$$n^{\mathrm{gcd}(j,k)} \equiv 1 \text{ (mod m)}$$

Hint: Properties of GCD.

Question 5

Decrypt the ciphertext

1485 2063 1244 2259 457 1503

that was encrypted using the RSA algorithm with key (n, k) = (2419, 211).

(You can write a program to save some time.)

Question 6 (Challenge)

Show that for all $n > 1$, $2^n \not\equiv 1 \pmod{n}$.