COMP 2711H Discrete Mathematical Tools for Computer Science
Solutions to Tutorial 5

QB2-5. Prove that $n^{13} - n$ is divisible by 2730.

Solution Note that $2730 = 2{\cdot}3{\cdot}5{\cdot}7{\cdot}13$. We can prove that $2730|n^{13}-n$ by proving $n^{13}-n$ is divisible by each prime number. This is because if $a|n$, $b|n$ and $gcd(a, b) = 1$, then $a \cdot b|n$.

For any integer n and a prime number $p \in \{2, 3, 5, 7, 13\}$, either $p|n$ or $p \nmid n$.

- If $p|n$, it is obvious that $p|n^{13} - n$ as it is a linear combination of powers of n.
- If $p \nmid n$, we can express $n^{13} - n$ as $n^{k(p-1)+1} - n$ for some integer k for each $p \in \{2, 3, 5, 7, 13\}$. Then, by utilising $n^{p-1} \equiv 1 \pmod p$, the expression is also congruent to $n - n \equiv 0 \pmod p$, i.e. divisible by p.

EP2-14. Let n be a nonnegative integer. Prove that n and n^5 have the same last digit. For example:

$$\underline{2}^5 = 3\underline{2}$$
$$7\underline{9}^5 = 307705639\underline{9}$$

Solution It wants us to prove

$$x^5 \equiv x \pmod{10}$$

This is very similar to QB2-5. By factorising $10 = 2 \cdot 5$, we can use the same method to prove that $x^5 - x$ is divisible by both 2 and 5.

Euler Totient Theorem does not work, think about why?

QB2-6. Show that any prime $p > 5$ divides infinitely many integers in the sequence 9, 99, 999, 9999, ...

Solution For any prime $p > 5$, 10 is not a multiple of p. By Fermat's little theorem, we have that

$$10^{p-1} \equiv 1 \pmod p.$$

Hence, for any positive integer k, we have that

$$(10^{p-1})^k \equiv 1 \pmod p.$$

So, $p|(10^{k(p-1)} - 1)$ for any integer $k > 0$.

QB2-7. Consider the system of congruences $x \equiv 4 \pmod 6$ and $x \equiv 13 \pmod{15}$. Find all solutions to this system of congruences using two different methods: (a) the method of back substitution and (b) the method suggested by the construction used in the proof of the Chinese remainder theorem. (Hint: It may be convenient to first transform the congruences to equivalent congruences modulo suitable prime numbers.)

Solution The given system of congruences is equivalent to the following system.

$$
\begin{aligned}
x &\equiv 0 \pmod 2 \\
x &\equiv 1 \pmod 3 \\
x &\equiv 3 \pmod 5
\end{aligned}
$$

(a) Use the construction in the proof of Chinese remainder theorem.

- $a_1 = 0$, $a_2 = 1$, $a_3 = 3$
- $m_1 = 2$, $m_2 = 3$, and $m_3 = 5$
- $M = m_1 m_2 m_3 = 30$
- $M_1 = M/m_1 = 15$, $M_2 = M/m_2 = 10$, $M_3 = M/m_3 = 6$
- $M_1^{-1} \equiv 1 \pmod{m_1}$, $M_2^{-1} \equiv 1 \pmod{m_2}$, $M_3^{-1} \equiv 1 \pmod{m_3}$
- solution $x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} = 28$

(b) Use back substitution. From the first congruence, we know that $x = 2u$ for some integer u. Substitute this into the second congruence, we get

$$2u \equiv 1 \pmod 3.$$

Solving this congruence, we get $u \equiv 2 \pmod 3$. So, $u = 3s+2$ for some integer s, and $x = 2u = 6s + 4$. Then substituting this into the third congruence, we get

$$6s + 4 \equiv 3 \pmod 5.$$

Solving this congruence yields $s \equiv 4 \pmod 5$. So, $s = 5t + 4$ for some integer t, and the following is a solution to the system.

$$x = 6(5t + 4) + 4 = 30t + 28.$$

So, $x \equiv 28 \pmod{30}$ is the solution to the system of congruence.

QB2-8. Prove that an integer $n > 1$ is prime if and only if the following holds: $(n-1)! \equiv -1 \pmod n$. (This is known as Wilson's theorem.)

Solution

- If part: Since $(n-1)! \equiv -1 \pmod n$ and $(n-1) \equiv -1 \pmod n$, we have that

$$(n-1)! \cdot (n-1) \equiv 1 \pmod n.$$

Note that for any number $a \in \{1, \ldots, n-1\}$,

$$a \cdot \frac{(n-1)!}{a} \cdot (n-1) \equiv 1 \pmod n.$$

a has an inverse modulo n, so a is relatively prime to n. Therefore n is a prime.

- Only-if part: When $n = 2$, the congruence obviously holds. Without loss of generality, we assume that n is a prime greater than or equal to 3. Now consider the set $\{1, 2, \ldots, (n-1)\}$. We claim that 1 and $n-1$ are the only numbers in this set, which have their inverse to be themselves. To see this, consider the following equation.

$$a^2 \equiv 1 \pmod{n}$$

or, equivalently,

$$(a-1)(a+1) \equiv 0 \pmod{n}.$$

The roots of the equation are $a \equiv 1$ and $a \equiv -1$.
Since, for any number $a \in \{2, 3, \ldots, (n-2)\}$, a has a unique inverse a^{-1} and $a^{-1} \neq a$, we can pair a with its inverse. We get $(n-3)/2$ such pairs. So,

$$2 \cdot 3 \cdots (n-3) \cdot (n-2) \equiv 1^{(n-3)/2} \equiv 1 \pmod{n},$$

and

$$(n-1)! \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}.$$