COMP 2711H Discrete Mathematical Tools for Computer Science
Solutions to Tutorial 6

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

EP3-1. In how many different ways can five persons be seated on a bench?

Solution There are five seats for five persons. There are 5 choices for the first man to take, and $5 - 1 = 4$ choices for the second man ... And only 1 choices for the last man. So the total solution is,
$$5 \times 4 \times 3 \times 2 \times 1 = 5! = 120$$

EP3-2. How many three-digit odd numbers can be formed with the digits $1, 2, ..., 9$ if no digit is repeated in any number?

Solution For the units digit, there are 5 choices $(1, 3, 5, 7, 9)$;

For the tens digit, there are 8 choices (all digits without the units digit);

For the hundreds digit, there are 7 choices. So the total answer is,

$$5 \times 8 \times 7 = 280$$

EP3-3. In how many ways can three boys and three girls be seated in a row if boys and girls alternate?

Solution There are 2 cases if boys and girls alternate, BGBGBG and GBGBGB. For the boys seats, there are 3! methods for boys. (The same as EP3-1) And for girls, there are also 3!. So the total answer is,

$$2 \times 3! \times 3! = 72$$

EP3-6. In how many ways can the offices of chairman, vice-chairman, secretary, and treasurer be filled from a committee of seven?

Solution For the chairman office, there are 7 committee to pick;

For the vice-chairman office, there are 6 committee to pick, except the person already in chairman office;

And the remaining two offices, there are 5 and 4 committee to pick respectively.

So the answer is,

$$7 \times 6 \times 5 \times 4 = 840$$

EP3-7. How many three-digit numbers greater than 300 can be formed with the digits $1, 2, ..., 6$ if no digit is repeated in any number?

Solution For the hundreds digit, there are 4 choices (3,4,5,6);

For the tens digit, there are 5 choices (all digits without the hundreds digit);

For the units digit, there are 4 choices (all digits without the tens and hundreds digits).

So the total answer is,

$$4 \times 5 \times 4 = 80$$