Theory of Computation

Homework 4

Due: 2015/12/08

Problem 1. Find all the primitive roots of 5 and all the primitive roots of 7.

Solution.

The primitive roots of 5 are 2 and 3, because $\phi(5) = 4$ and

$$2^1 \equiv 2 \pmod{5} \;\; ; \;\; 2^2 \equiv 4 \pmod{5},$$
$$2^3 \equiv 3 \pmod{5} \;\; ; \;\; 2^4 \equiv 1 \pmod{5},$$

and

$$3^1 \equiv 3 \pmod{5} \;\; ; \;\; 3^2 \equiv 4 \pmod{5},$$
$$3^3 \equiv 2 \pmod{5} \;\; ; \;\; 3^4 \equiv 1 \pmod{5}.$$

Similarly, the primitive roots of 7 are 3 and 5 because $\phi(7) = 6$ and

$$3^1 \equiv 3 \pmod{7} \;\; ; \;\; 3^2 \equiv 2 \pmod{7},$$
$$3^3 \equiv 6 \pmod{7} \;\; ; \;\; 3^4 \equiv 4 \pmod{7},$$
$$3^5 \equiv 5 \pmod{7} \;\; ; \;\; 3^6 \equiv 1 \pmod{7},$$

and

$$5^1 \equiv 5 \pmod{7} \;\; ; \;\; 5^2 \equiv 4 \pmod{7},$$
$$5^3 \equiv 6 \pmod{7} \;\; ; \;\; 5^4 \equiv 2 \pmod{7},$$
$$5^5 \equiv 3 \pmod{7} \;\; ; \;\; 5^6 \equiv 1 \pmod{7}.$$

□

Problem 2. We know that 3-SAT is NP-complete. Show that for $n > 3$, n-SAT is also NP-complete. (You don't need to show that is in NP.)

Solution.
We reduce 3-SAT to n-SAT as follows. Let ϕ be a 3-SAT boolean expression. For any clause $(a \vee b \vee c)$, we replace it with $(a \vee b \vee \underbrace{c \vee \cdots \vee c}_{n-2 \text{ times}})$. By repeating this process in all the clauses of ϕ, we get an n-SAT boolean expression ϕ'. Now, we proceed to show that this is a reduction from 3-SAT to n-SAT as follows:

($\Rightarrow$) From the construction, we see that if a truth assignment satisfies ϕ, then it must satisfy ϕ'.

($\Leftarrow$) Let's note that if a truth assignment satisfy ϕ', then it must also satisfy ϕ.

From this, we then deduce that ϕ is satisfiable if and only if ϕ' is satisfiable; hence 3-SAT is reducible to n-SAT, proving that n-SAT is NP-complete. $\square$