Exercise Sheet 3

This sheet is due in the lecture on Tuesday 21st October, and will be discussed in the exercise class on Friday 24th October.

Exercise 3.1. *Examples of primitive roots.*

(1) Show that 2 is a primitive root modulo 29. How many generators does $\mathbb{Z}_{29}^*$ have?

(2) Show that 2 is a primitive root modulo $1331 = 11^3$. How many generators does $\mathbb{Z}_{1331}^*$ have? (Hint: Remark 3.9.)

(3) Find all primitive roots modulo 10, 11 and 12 respectively, if there is any.

Exercise 3.2. *Applications in solving non-linear equations.*

Let p be an odd prime and g a primitive root modulo p.

(1) For any $d \mid (p-1)$, show that $g^{\frac{p-1}{d}}$ has order d modulo p.

(2) Show that $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

(3) Use the primitive root in Exercise 3.1 (1) to find all solutions to $x^7 \equiv 1 \pmod{29}$.

Exercise 3.3. *Applications in higher order residues.*

Let p be an odd prime and g a primitive root modulo p. Assume $d \mid (p-1)$ and $p \nmid a$.

(1) Show that $x^d \equiv a \pmod{p}$ has solutions iff $a \equiv g^{dk} \pmod{p}$ for some $k \in \mathbb{Z}$.

(2) Show that $x^d \equiv a \pmod{p}$ has solutions iff $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$.

(3) Find all values of a with $0 < a < 29$ such that $x^4 \equiv a \pmod{29}$ has solutions. (Hint: you can use Exercise 3.1 (1) or Exercise 3.2 (3).)

Exercise 3.4. *Characterisation of primitive roots modulo higher powers of odd primes.*

Let p be an odd prime.

(1) For any positive integer l, if $a \equiv b \pmod{p^l}$, show that $a^p \equiv b^p \pmod{p^{l+1}}$. (Hint: write $a = b + c \cdot p^l$ for some $c \in \mathbb{Z}$ and compute a^p.)

(2) For any positive integers $m < n$, if g is a primitive root modulo p^n, show that g is a primitive root modulo p^m. (Hint: prove by contradiction and use part (1).)

(3) For any integer $l \geqslant 2$, conclude that a necessary and sufficient condition for g being a primitive root modulo g^l is that g is a primitive root modulo p and $g^{p-1} \not\equiv 1 \pmod{p^2}$. (Hint: use part (2) to prove necessity. Sufficiency has been proved in Proposition 3.8; see Remark 3.9.)