Solutions to Exercise Sheet 3

Solution 3.1. *Examples of primitive roots.*

(1) Since the group $\mathbb{Z}_{29}^*$ has $\phi(29) = 28$ elements, we need to show that 2 has order 28 modulo 29. All positive divisors of 28 are $1, 2, 4, 7, 14$ and 28. Since the order of 2 must be a positive divisor of 28, it suffices to show that $2^k \not\equiv 1 \pmod{29}$ for $k = 1, 2, 4, 7, 14$. This can be done by direct computation. $2^1 \equiv 2 \pmod{29}$, $2^2 \equiv 4 \pmod{29}$, $2^4 \equiv 16 \pmod{29}$, $2^7 = 128 \equiv 12 \pmod{29}$, $2^{14} \equiv 12^2 = 144 \equiv 28 \equiv -1 \pmod{29}$. None of these remainders is $1 \pmod{29}$, hence the order of 2 must be 28. In other words, 2 is a primitive root modulo 29. The number of generators of $\mathbb{Z}_{29}^*$ is $\phi(28) = 28(1 - \frac{1}{2})(1 - \frac{1}{7}) = 12$.

(2) By Remark 3.9, it suffices to show that 2 is a primitive root modulo 11 and the condition $2^{10} \not\equiv 1 \pmod{11^2}$. To show 2 is a primitive root modulo 11, we need to show 2 has order 10 modulo 11. In other words, its order is not $1, 2$ or 5. Indeed, $2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^5 = 32 \equiv 10 \pmod{11}$. None of them is congruent to 1 modulo 29, hence 2 is a primitive root modulo 11. To show the second condition $2^{10} \not\equiv 1 \pmod{11^2}$, we simply compute $2^{10} = 1024 \equiv 56 \not\equiv 1 \pmod{121}$. Hence 2 is a primitive root modulo 11^3. The number of generators in $\mathbb{Z}_{11^3}^*$ is given by $\phi(\phi(11^3)) = \phi(10 \times 11^2) = 440$.

(3) We consider primitive roots modulo 10. We have $\phi(10) = 4$ and we can even write down $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$. We show 3 is a primitive root (in other words $\overline{3}$ is a generator of $\mathbb{Z}_{10}^*$). Indeed, $3 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, so the order of 3 modulo 10 is not 1 or 2, hence must be 4. By Remark 3.2 (3), the generators of $\mathbb{Z}_{10}^*$ are $\overline{3}$ and $\overline{3}^3 = \overline{27} = \overline{7}$. Hence $a \in \mathbb{Z}$ is a primitive root modulo 10 iff $a \equiv 3$ or $7 \pmod{10}$.

We consider primitive roots modulo 11. We have found in part (2) that 2 is a primitive root modulo 11. By Remark 3.2 (3), we need to compute the congruence classes of 2^k modulo 11, where $1 \leqslant k \leqslant 10$ and $\mathrm{hcf}(k, 10) = 1$; i.e., $k = 1, 3, 7, 9$. So we have $2^1 \equiv 2 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^7 = 128 \equiv 7 \pmod{11}$, $2^9 \equiv 7 \times 4 \equiv 6 \pmod{11}$. Therefore $a \in \mathbb{Z}$ is a primitive root modulo 11 iff $a \equiv 2, 6, 7$ or $8 \pmod{11}$.

We finally consider primitive roots modulo 12. We have the factorisation $12 = 2^2 \times 3$. We compare it with the list of forms in Theorem 3.10, but it does not match any of the given forms. Therefore there are no primitive roots modulo 12.

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

(1) Since g is a primitive root modulo p, we know that the order of g modulo p is $\phi(p) = p - 1$. In other words, $g^{p-1} \equiv 1 \pmod{p}$ and $g^l \not\equiv 1 \pmod{p}$ for any

$1 \leqslant l < p-1$. Let $a = g^{\frac{p-1}{d}}$. We want to show a has order d. In other words, $a^d \equiv 1 \pmod p$ and $a^k \not\equiv 1 \pmod p$ for any $1 \leqslant k < d-1$.

On one hand, $a^d = g^{p-1} \equiv 1 \pmod p$. On the other hand, for any k with $1 \leqslant k < d$, $a^k \equiv g^{k \cdot \frac{p-1}{d}} \pmod p$. Since $0 < k \cdot \frac{p-1}{d} < p-1$, $a^k \not\equiv 1 \pmod p$. Therefore we conclude a has order d modulo p.

(2) Let $b = g^{\frac{p-1}{2}}$. By part (1) we know b has order 2 modulo p. In other words, $b^2 \equiv 1 \pmod p$ and $b \not\equiv 1 \pmod p$. The first condition implies $p \mid (b^2-1) = (b+1)(b-1)$, hence either $p \mid b+1$ or $p \mid b-1$, or equivalently, $b \equiv -1 \pmod p$ or $b \equiv 1 \pmod p$. The second condition rules out the second possibility. Hence $g^{\frac{p-1}{2}} = b \equiv -1 \pmod p$ is the only possibility.

(3) Let $g = 2$ be the primitive root modulo 29 found in Exercise 3.1 (1), then $g^{28} \equiv 1 \pmod{29}$. Therefore for any $k \in \mathbb{Z}$, $x \equiv g^{4k} \pmod{29}$ is a solution to the equation $x^7 \equiv 1 \pmod{29}$ because $(g^{4k})^7 = g^{28k} \equiv 1^k = 1 \pmod{29}$. In particular, the congruence classes of g^{4k} for $0 \leqslant k \leqslant 6$ are distinct solutions because g has order 28 modulo 29 (indeed, the congruence classes of g^l for $0 \leqslant l < 28$ modulo 29 are all distinct). On the other hand, since $\mathbb{Z}_{29}$ is a field by Proposition 2.9, the equation $x^7 = 1$ has at most 7 distinct solutions in $\mathbb{Z}_{29}$; in other words, at most 7 distinct congruence classes. Therefore $x \equiv g^{4k} \pmod{29}$ for $0 \leqslant k \leqslant 6$ are all solutions. We do explicit computation: $2^0 \equiv 1 \pmod{29}$, $2^4 \equiv 16 \pmod{29}$, $2^8 \equiv 16^2 \equiv 24 \equiv -5 \pmod{29}$, $2^{12} = 2^4 2^8 \equiv 16 \times (-5) \equiv 7 \pmod{29}$, $2^{16} = (2^8)^2 \equiv (-5)^2 = 25 \equiv -4 \pmod{29}$, $2^{20} \equiv 2^4 2^{16} \equiv 16 \times (-4) \equiv 23 \equiv -6 \pmod{29}$, $2^{24} \equiv (2^{12})^2 \equiv 7^2 \equiv 20 \pmod{29}$. Therefore all solutions to the equation $x^7 \equiv 1 \pmod{29}$ are $x \equiv 1, 16, 24, 7, 25, 23$ or $20 \pmod{29}$.

Solution 3.3. *Applications in higher order residues.*

(1) For the "if" part, we assume $a \equiv g^{dk} \pmod p$. Then $x \equiv g^k \pmod p$ is clearly a solution to $x^d \equiv a \pmod p$. For the "only if" part, assume $x^d \equiv a \pmod p$ has a solution $x \equiv x_0 \pmod p$. Then $p \nmid x_0$ because $x_0^d \equiv a \pmod p$ and $p \nmid a$. Therefore $\overline{x}_0$ is an element in $\mathbb{Z}_p^*$ hence $x_0 \equiv g^k \pmod p$ for some $k \in \mathbb{Z}$ (because $\overline{g}$ is a generator of $\mathbb{Z}_p^*$). Therefore $a \equiv x_0^d \equiv g^{dk} \pmod p$.

(2) By part (1), it suffices to show that $a \equiv g^{dk} \pmod p$ is equivalent to $a^{\frac{p-1}{d}} \equiv 1 \pmod p$. We first assume $a \equiv g^{dk} \pmod p$. Then $a^{\frac{p-1}{d}} \equiv (g^{dk})^{\frac{p-1}{d}} = g^{k(p-1)} \equiv 1 \pmod p$ since $g^{p-1} \equiv 1 \pmod p$. For the other direction, since $p \nmid a$, $\overline{a} \in \mathbb{Z}_p^*$. Hence $a \equiv g^l \pmod p$ for some $l \in \mathbb{Z}$. Then $a^{\frac{p-1}{d}} \equiv g^{l \cdot \frac{p-1}{d}} \equiv 1 \pmod p$. Since g has order $p-1$ modulo p, we conclude that $l \cdot \frac{p-1}{d}$ must be a multiple of $p-1$. (This uses a fact in group theory: assume an element g in a group G has order q, then $g^r = e$ is the identity of the group iff $q \mid r$.) In other words, there exists

some $k \in \mathbb{Z}$, such that $l \cdot \frac{p-1}{d} = k(p-1)$. This simplifies to $l = dk$, hence $a \equiv g^{dk} \pmod p$ for some $k \in \mathbb{Z}$.

(3) We use the result from part (1). $x^4 \equiv a \mod 29$ has solutions iff $a \equiv g^{4k} \pmod{29}$. We know from Exercise 3.1 (1) that $g = 2$ is a primitive root modulo 29. Therefore $a \equiv 2^{4k} \pmod{29}$ for $k \in \mathbb{Z}$. For $0 \leqslant k \leqslant 6$ the formula gives distinct congruence classes. Therefore $x^4 \equiv a \pmod{29}$ has solutions iff $a \equiv 2^{4k}$ for $0 \leqslant k \leqslant 6$. To find the corresponding values of a within the range $0 < a < 29$, we need to find the remainder of each 2^{4k} modulo 29. This calculation has been done in Exercise 3.3 (3); i.e. $a = 1, 16, 24, 7, 25, 23$ or 20.

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

(1) Since $a \equiv b \pmod{p^l}$, we can write $a = b + c \cdot p^l$ for some $c \in \mathbb{Z}$. We then take p-th power on both sides and expand the right-hand side. We get

$$a^p = (b + c \cdot p^l)^p = b^p + p \cdot b^{p-1}cp^l + \sum_{i=2}^{p} \binom{p}{i} b^{p-i}c^i p^{il}.$$

We claim that every term on the right-hand side except b^p is divisible by p^{l+1}. Indeed, the second term $p \cdot b^{p-1}cp^l$ is clearly divisible by p^{l+1}. For every term in the summation, the exponent in the power p^{il} is at least $il \geqslant 2l = l + l \geqslant l + 1$, hence p^{l+1} divides the term $\binom{p}{i} b^{p-i}c^i p^{il}$ for each $i \geqslant 2$. Therefore, modulo p^{l+1}, the above equation can be written as $a^p \equiv b^p \pmod{p^{l+1}}$.

(2) We assume the order of g modulo p^m is d. We need to show $d = \phi(p^m)$. It suffices to prove that $d \mid \phi(p^m)$ and $\phi(p^m) \mid d$. For the first division, notice that $\mathbb{Z}_{p^m}^*$ has order $\phi(p^m)$, hence the order d of any element $\overline{g}$ is a positive divisor of $\phi(p^m)$; that is $d \mid \phi(p^m)$. For the second division, we apply the statement in part (1) on the congruence $g^d \equiv 1 \pmod{p^m}$ for $n - m$ times. Step by step we will get $g^{dp} \equiv 1 \pmod{p^{m+1}}, g^{dp^2} \equiv 1 \pmod{p^{m+2}}, \cdots, g^{dp^{n-m}} \equiv 1 \pmod{p^n}$. Since g has order $\phi(p^n)$ modulo p^n, the last congruence implies $\phi(p^n) \mid dp^{n-m}$. (This uses again the fact in group theory: assume an element g in a group G has order q, then $g^r = e$ is the identity of the group iff $q \mid r$.) Hence $dp^{n-m} = c\phi(p^n) = c(p-1)p^{n-1}$ for some $c \in \mathbb{Z}$. It follows that $d = c(p-1)p^{m-1} = c\phi(p^m)$, hence $\phi(p^m) \mid d$ which is the second division. The two divisions guarantee $d = \phi(p^m)$.

(3) The sufficiency is stated in Remark 3.9 and proved in Proposition 3.8. We still need to prove the necessity of the two given conditions. Since g is a primitive root modulo p^l, using the statement in part (2), we know g is a primitive root modulo p and p^2 because $l \geqslant 2$, which prove the two conditions respectively. Indeed, the first condition is clear. For the second condition, since g has order $\phi(p^2)$ modulo p^2, we know that for any integer d, $1 \leqslant d < \phi(p^2)$, $g^d \neq 1 \pmod{p^2}$. In particular, it holds for $d = p - 1$.