Worksheet 12: Order, Primitive Roots, Review

Problem 1. Suppose $\gcd(a, n) = 1$ and that a has order k modulo n.

(a) Show that $a^m \equiv 1 \bmod n$ if and only if $k \mid m$.

(b) Show that, if $a^x \equiv a^y \bmod n$ for some integers x and y, then $x \equiv y \bmod k$.

Solution. For part (a), if $k \mid m$, there exists an integer x such that $m = kx$, and then $a^m = (a^k)^x \equiv 1^x = 1 \bmod n$. Conversely, suppose $a^m \equiv 1 \bmod n$. Using the division algorithm, we may write $m = kq + r$ for some $0 \leqslant r < k$. Then

$$1 \equiv a^m = a^{kq+r} = (a^k)^q a^r \equiv 1^q a^r = a^r.$$

Since k is the order of a and $0 \leqslant r < k$, the above implies that we must have $r = 0$, ie, that $k \mid m$.

For part (b), suppose $a^x \equiv a^y \bmod n$. Then $a^{x-y} \equiv 1 \bmod n$, so $k \mid x - y$, which means that $x \equiv y \bmod k$.

Problem 2. Suppose $\gcd(a, n) = 1$ and the order of a mod n is k. Let h be a positive integer. Show that the order of a^h mod n is $k/\gcd(h, k)$.

Solution. Let $d = \gcd(h, k)$ and let r be the order of a^h. We can write $k = yd$ for some integer y, and we want to show that $r = y$. Note that we can write $h = xd$ for some integer x, and the equation

$$d = \gcd(h, k) = \gcd(xd, yd) = \gcd(x, y) \cdot d$$

from Ste17, lemma 1.1.17 implies that $\gcd(x, y) = 1$. Now we have

$$(a^h)^y = (a^{xd})^y = (a^{yd})^x = (a^k)^x \equiv 1^x = 1 \bmod n.$$

This implies that $r \mid y$, so $r \leqslant y$.

On the other hand, we have

$$1 \equiv (a^h)^r = a^{hr} \bmod n$$

which means that $k \mid hr$, ie, $yd \mid xdr$, which means that $y \mid xr$. Since $\gcd(y, x) = 1$, this means that $y \mid r$, which means that $y \leqslant r$. This concludes the proof that $r = y$.

Problem 3. (a) Verify that 2 is a primitive root modulo 11. *Note.* Do this efficiently using Euler's theorem and problem 1(a).

(b) Find all of the other primitive roots modulo 11. *Note.* Do this efficiently using problem 2.

Solution. For (a), we know by Euler's theorem that $2^{10} \equiv 1 \bmod 11$. Thus, if r is the order of 2, we must have $r \mid 10$ by . In order to check that $r = 10$, it is sufficient to check that r cannot be 1, 2, or 5. Since $2 \not\equiv 1 \bmod 11$, clearly $r \neq 1$. Also $2^2 = 4 \not\equiv 1 \bmod 11$, so $r \neq 2$. Finally, $2^5 = 32 \equiv 10 \not\equiv 1 \bmod 11$, so $r \neq 5$. This shows that $r = 10$.

For (b), since 2 is a primitive root, we know that $2^0, 2^1, \cdots, 2^9$ is a complete set of residues mod 11. Moreover, we know that 2^h has order 10 if and only if $10/\gcd(h, 10) = 10$, if and only if $\gcd(h, 10) = 1$. Thus $2^1, 2^3, 2^7, 2^9$ are the primitive roots. We can calculate these using binary exponentiation and we find that 2, 8, 7, 6 are the primitive roots of 11.

Problem 4. Let p be a prime. How many (congruence classes of) primitive roots are there modulo p?

Solution. Let a be a primitive root mod p. Then a^h is a primitive root if and only if $(p-1)/\gcd(h, p-1) = p - 1$, if and only if $\gcd(h, p-1) = 1$. Thus there are $\phi(p-1)$ primitive roots mod p.

Problem 5. Suppose a is a primitive root modulo p for an odd prime p. Show that $a^{(p-1)/2} \equiv -1 \bmod p$. *Hint.* Use problem 2.

Problem 6. Find a number a such that $a^{19} \equiv 50 \bmod 137$. *Note.* Use Sage? Problem 1(b) might also be helpful.

Solution. We check with `is_prime(137)` that 137 is prime. Then we use `primitive_root(137)` to find that 3 is a primitive root of 137. We use `log(Mod(50, 137), Mod(3, 137))` to find that $3^{24} \equiv 50$.

Moreover, there exists some integer x such that $a \equiv 3^x \bmod 137$. Then

$$3^{24} \equiv 50 \equiv a^{19} \equiv (3^x)^{19} \equiv 3^{19x} \bmod 137$$

which means that $19x \equiv 24 \bmod 136$ by problem 1(b). We then find x using `Mod(24, 136) / Mod(19, 136)` and find $x \equiv 80 \bmod 136$. Thus $a \equiv 3^{80} \equiv 119 \bmod 137$.

We can check with `Mod(119, 137)^19` that $119^{19} \equiv 50 \bmod 137$.

Problem 7. Find a solution to the following system of congruences.

$$\begin{aligned} 2x &\equiv 1 \bmod 5 \\ 5x &\equiv 9 \bmod 11 \end{aligned}$$

Problem 8. Find the last two digits of $7^{4,000,000,000,000}$.

Solution. By Euler's theorem, $7^{40} \equiv 1 \bmod 100$, which implies 7 raised to any multiple of 40 will have last two digits 01. The exponent in the problem is clearly a multiple of 4.

Problem 9. Suppose $\gcd(a, 30) = 1$. Show that 60 divides $a^4 - 1$.

Solution. Observe also that $60 = 2^2 \cdot 3 \cdot 5$, so it is sufficient to show that $a^4 - 1$ is divisible by 4, 3, and 5, ie, that $a^4 \equiv 1 \bmod 4, 3,$ and 5. Since $30 = 2 \cdot 3 \cdot 5$ and $\gcd(a, 30) = 1$, we see that we must have $\gcd(a, 4) = \gcd(a, 3) = \gcd(a, 5) = 1$. Thus we can apply Euler's theorem for all of these moduli. Applying it for the modulus 4, we find $a^2 \equiv 1 \bmod 4$ since $\varphi(4) = 2$, so $a^4 \equiv 1 \bmod 4$ as well. Similarly, we have $a^2 \equiv 1 \bmod 3$, which means that $a^4 \equiv 1 \bmod 3$. Finally, we also have $a^4 \equiv 1 \bmod 5$.

Problem 10. Show that $13 \mid 11^{12n+6} + 1$ for all non-negative integers n.

Solution. Since $\gcd(11, 13) = 1$, we have $11^{12} \equiv 1 \bmod 13$ by Euler's theorem. Thus

$$11^{12n+6} = (11^{12})^n 11^6 \equiv 1^n 11^6 = 11^6 \bmod 13.$$

Now $11^2 = 121 \equiv -9 \equiv 4 \bmod 13$, and $11^4 \equiv (11^2)^2 \equiv 16 \equiv 3 \bmod 13$, so $11^6 \equiv 4 \cdot 3 \equiv 12 \equiv -1 \bmod 13$. Thus

$$11^{12n+6} + 1 \equiv -1 + 1 \equiv 0 \bmod 13.$$