Math 465 Number Theory, Spring 2025, Solutions 6

1. (i) Find the order of 2, 3 and 5 modulo 23. (ii) Find a primitive root modulo 23 and construct a table of indices. (iii) Solve the congruence $x^{39} \equiv 13 \pmod{23}$.

(i) 22 has proper divisors 1, 2, 11. $2^1 \not\equiv 1 \pmod{23}$, $2^2 = 4 \not\equiv 1 \pmod{23}$. $2^4 = 16$, $2^8 = 256 \equiv 3 \pmod{23}$, $2^{11} = 2^{1+2+8} \equiv 2.4.3 \equiv 24 \equiv 1 \pmod{23}$, $\mathrm{ord}_{23}(2) = 11$.

$3^1 \not\equiv 1 \pmod{23}$, $3^2 = 8 \not\equiv 1 \pmod{23}$, $3^4 = 81 \equiv 12 \pmod{23}$, $3^8 \equiv 144 \equiv 6 \pmod{23}$, $3^{11} = 3^{1+2+8} \equiv 3.9.6 \equiv 1 \pmod{23}$, $\mathrm{ord}_{23}(3) = 11$.

$5 = 5 \not\equiv 1 \pmod{23}$, $5^2 = 25 \equiv 2 \not\equiv 1 \pmod{23}$, $5^4 \equiv 4 \pmod{23}$, $5^8 \equiv 16 \pmod{23}$, $5^{11} = 51 + 2 + 8 \equiv 5.2.16 \equiv 5.9 \equiv -1 \not\equiv 1 \pmod{23}$, $\mathrm{ord}_{23}(5) = 22$.

(ii) From above, 5 is a primitive root (mod 23).

y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
5^y	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1
x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\mathrm{ord}_5 x$	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

(iii) The congruence becomes $39y \equiv 14 \pmod{22}$. Thus $17y \equiv 14 \pmod{22}$. By Euclid $y \equiv 6 \pmod{22}$ and so $x \equiv 8 \pmod{23}$.

2. First find a primitive root modulo 19 and then find all primitive roots modulo 19.

Checking $2^k \pmod{19}$ for $k = 2, 3, 6, 9$, the proper divisors of $\phi(19) = 18$ shows that 2 is a primitive root modulo 19. Then the numbers 2^m with $1 \le m \le 18$ and $(m, 18) = 1$ give all the primitive roots. $m = 1, 5, 7, 11, 13, 17$. Thus the primitive roots are 2, $3 \equiv 2^{13} \pmod{19}$, $10 \equiv 2^{17} \pmod{19}$, $13 \equiv 2^5 \pmod{19}$, $14 \equiv 2^7 \pmod{19}$, $15 \equiv 2^{11} \pmod{19}$.

3. Show that 3 is a primitive root modulo 17 and draw up a table of discrete logarithms to this base modulo 17. Hence, or otherwise, find all solutions to the following congruences. (i) $x^{12} \equiv 16 \pmod{17}$, (ii) $x^{48} \equiv 9 \pmod{17}$, (iii) $x^{20} \equiv 13 \pmod{17}$, (iv) $x^{11} \equiv 9 \pmod{17}$.

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^y	1	3	9	10	13	5	15	11	6	14	8	7	4	12	2	6
x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{dlog}_3 x$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(i) $12y \equiv 8 \pmod{16}$, $3y \equiv 2 \pmod{4}$, $y \equiv 2 \pmod{4}$, $y \equiv 2$, 6, 10 or 14 (mod 16). $x \equiv 9$, 15, 8 or 2 (mod 17). (ii) $48y \equiv 2 \pmod{16}$. $(48, 16) = 16 \nmid 2$ so no solutions. (iii) $20y \equiv 4 \pmod{16}$. $y \equiv 5y \equiv 1 \pmod{4}$ so $y \equiv 1$, 5, 9, 13 (mod 16) and $x \equiv 3$, 5, 14, 12 (mod 17). (iv) $11y \equiv 2 \pmod{16}$, $y \equiv 6 \pmod{16}$, $x \equiv 15 \pmod{17}$.

4. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that g is a quadratic non-residue modulo p.

We argue by contradiction. Suppose on the contrary that there is a primitive root g modulo p which is also a quadratic residue. Then there is an x so that $x^2 \equiv g \pmod{p}$. But by Euler's theorem $x^{p-1} \equiv 1 \pmod{p}$. Thus $g^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}$, contradicting the primitivity property of g.

5. Find a complete set of quadratic residues r modulo 29 in the range $1 \leq r \leq 28$.

$1, 4, 9, 16, 25, 36 \equiv 7, 49 \equiv 20, 64 \equiv 6, 81 \equiv 23, 100 \equiv 13, 121 \equiv 5, 144 \equiv 28, 169 \equiv 24, 196 \equiv 22.$

$1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28$