Math 255 - Spring 2017
Homework 9 Solutions

1. (a) We note that $\varphi(11) = 10$, so we are looking for an element of order 10. The strategy here is to go through each unit modulo 11 and compute its order. To speed things up, we note that since the order k of an integer modulo 11 must divide $\varphi(11) = 10$, to find the order of a it suffices to check a^2 and a^5 (we assume that $a \not\equiv 1 \pmod{11}$ since this obviously has order 1), since 2 and 5 are the only divisors of 10 that are strictly between 1 and 10.

   We first look at 2: $2^2 \equiv 4 \pmod{11}$ and $2^5 = 32 \equiv 10 \pmod{11}$. Therefore 2 is a primitive root.

   The other primitive roots are 6 (because $6^2 \equiv 3 \pmod{11}$ and $6^5 \equiv 10 \pmod{11}$), 7 (because $7^2 \equiv 5 \pmod{11}$ and $7^5 \equiv 10 \pmod{11}$) and 8 (because $8^2 \equiv 9 \pmod{11}$ and $8^5 \equiv 10 \pmod{10}$).

   For completeness we note that the elements of order 5 are $3, 4, 5$ and 9. 10 has order 2 (since $10 \equiv -1 \pmod{11}$, this isn't surprising) and 1 as always has order 1.

   (b) We use $r = 2$ from now on. Since it is the smallest primitive root, it is the one that makes the computations the easiest.

   We compute

$$2^2 \equiv 4 \pmod{11} \quad 2^3 \equiv 8 \pmod{11} \quad 2^4 \equiv 5 \pmod{11} \quad 2^5 \equiv 10 \pmod{11}$$
$$2^6 \equiv 9 \pmod{11} \quad 2^7 \equiv 7 \pmod{11} \quad 2^8 \equiv 3 \pmod{11} \quad 2^9 \equiv 6 \pmod{11}.$$

   This gives us the following table of discrete logarithms:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

   (c) i. Let $x \equiv 2^k \pmod{11}$, then $x^3 \equiv 2^{3k} \pmod{11}$. Since $7 \equiv 2^7 \pmod{11}$ and $3 \equiv 2^8 \pmod{11}$, we get the equation

$$2^7 2^{3k} \equiv 2^8 \pmod{11}$$

   or

$$2^{3k+7} \equiv 2^8 \pmod{11}.$$

   Taking $\log_2$ on both sides we get

$$3k + 7 \equiv 8 \pmod{10}.$$

   This is a linear equation which we now solve

$$3k + 7 \equiv 8 \pmod{10}$$
$$3k \equiv 1 \pmod{10}.$$

Since 3 is a unit modulo 10, with $3 \cdot 7 \equiv 1 \pmod{10}$, we can multiply both sides by 7 to get

$$k \equiv 7 \pmod{10}.$$

Therefore there is a unique solution, it is $x \equiv 2^7 \equiv 7 \pmod{11}$.

ii. This time if $x \equiv 2^k \pmod{11}$ then $x^4 \equiv 2^{4k} \pmod{11}$. Using that $3 \equiv 2^8 \pmod{11}$ and $5 \equiv 2^4 \pmod{11}$, the equation becomes

$$2^8 2^{4k} \equiv 2^4 \pmod{11}.$$

Combining the left hand side and taking $\log_2$ of both sides we get the linear equation

$$4k + 8 \equiv 4 \pmod{10},$$

or

$$4k \equiv -4 \pmod{10}.$$

This time 4 is not a unit modulo 10 so we cannot divide both sides by 4. Instead, because $\gcd(4, 10) = 2$, we divide everything by 2 and solve instead

$$2k \equiv -2 \pmod{5}.$$

Now 2 is a unit modulo 5 and we may divide both sides by 2 to get

$$k \equiv -1 \equiv 4 \pmod{5}.$$

Lifting back up to $\mathbb{Z}/10\mathbb{Z}$, we get two solutions,

$$k \equiv 4 \pmod{10} \quad \text{and} \quad k \equiv 9 \pmod{10}.$$

This gives two solutions to the equation,

$$x \equiv 5 \pmod{11} \quad \text{and} x \equiv 6 \pmod{11}.$$

iii. We apply the same technique: $x^8 \equiv 2^{8k} \pmod{11}$ and $10 \equiv 2^5 \pmod{11}$ so

$$2^{8k} \equiv 2^5 \pmod{11}.$$

Taking $\log_2$ on both sides, we get

$$8k \equiv 5 \pmod{10}.$$

Again, 8 is not a unit modulo 10, so we cannot divide both sides by 8. Instead, because $\gcd(8, 10) = 2$, we would like to divide everything by 2. However, 5 is not divisible by 2 and therefore this equation has no solution.

2. (a)
- We have that $2^7 = 128 \equiv 27 \pmod{101}$.
- Since $27 = 3^3$, this means that $2^7 \equiv 3^3 \pmod{101}$.

- Taking $\log_3$ of both sides and simplifying, we get

$$\log_3 2^7 \equiv \log_3 3^3 \pmod{100}$$
$$7 \log_3 2 \equiv 3 \log_3 3 \equiv 3 \pmod{100}$$

Since 7 is a unit modulo 100, we can find its inverse: We first do the Euclidean algorithm

$$100 = 14 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1.$$

Now we backsubstitute:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3(100 - 14 \cdot 7) \\ &= 7 - 3 \cdot 100 + 42 \cdot 7 \\ &= 43 \cdot 7 - 3 \cdot 100. \end{aligned}$$

Therefore $7^{-1} \equiv 43 \pmod{100}$. Multiplying both sides by 43 in the equation $7 \log_3 2 \equiv 3 \pmod{100}$, we get

$$\log_3 2 \equiv 129 \equiv 29 \pmod{100}.$$

This is the idea behind the index calculus attack: To find numbers that can be factored into small primes in two ways modulo 101 so that their logarithms give us equations to solve. Usually we would have many unknown $\log_3 a$s and many equations, this problem is a simplified version.

(b) We first do the Euclidean algorithm:

$$101 = 5 \cdot 17 + 16$$
$$17 = 16 + 1.$$

Backsubstituting we get:

$$\begin{aligned} 1 &= 17 - 16 \\ &= 17 - (101 - 5 \cdot 17) \\ &= 17 - 101 + 5 \cdot 17 \\ &= 6 \cdot 17 - 101. \end{aligned}$$

Therefore $17^{-1} \equiv 6 \pmod{101}$.

(c) Factoring 6, we write

$$2 \cdot 3 \cdot 17 \equiv 1 \pmod{101}.$$

Taking $\log_3$ on both sides and substituting the value we got from part (a) we get

$$\begin{aligned}
\log_3 2 + \log_3 3 + \log_3 17 &\equiv \log_3 1 \pmod{100} \\
29 + 1 + \log_3 17 &\equiv 0 \pmod{100} \\
30 + \log_3 17 &\equiv 0 \pmod{100} \\
\log_3 17 &\equiv -30 \equiv 70 \pmod{100}
\end{aligned}$$

And we have that $\log_3 17 \equiv 70 \pmod{100}$.