

Math 400 Fall 2017
Cryptology HW 5 Solutions
Due Thursday, October 5

1. Is 2 a primitive root mod 31? Prove or disprove your answer.

Solution: $2^5 = 32 \equiv 1 \pmod{31}$ so 2 is not a primitive root mod 31.

2. Is 17 a primitive root mod 31? Prove or disprove your answer.

Solution: We compute

$$\begin{array}{llllll} 17 \equiv 17 \pmod{31} & 17^2 \equiv 10 \pmod{31} & 17^3 \equiv 15 \pmod{31} & 17^4 \equiv 7 \pmod{31} & & \\ 17^5 \equiv 26 \pmod{31} & 17^6 \equiv 8 \pmod{31} & 17^7 \equiv 12 \pmod{31} & 17^8 \equiv 18 \pmod{31} & & \\ 17^9 \equiv 27 \pmod{31} & 17^{10} \equiv 25 \pmod{31} & 17^{11} \equiv 22 \pmod{31} & 17^{12} \equiv 2 \pmod{31} & & \\ 17^{13} \equiv 3 \pmod{31} & 17^{14} \equiv 20 \pmod{31} & 17^{15} \equiv 30 \pmod{31} & 17^{16} \equiv 14 \pmod{31} & & \end{array}$$

Since it hasn't repeated already, it won't, so 17 is a primitive root.

We could in fact save ourselves some work by only checking the exponents 1, 2, 3, 5, 6, 10, 15.

3. Compute $\log_2(13) \pmod{23}$ and $\log_{10}(22) \pmod{47}$.

Solution: $\log_2(13) = 7 \pmod{23}$ and $\log_{10}(22) = 11 \pmod{47}$.

4. Suppose you are doing a Diffie-Hellman key exchange with Alice. You have agreed to use $p = 1373, g = 2$.

(a) You choose the secret value $b = 871$. What number should you send to Alice?

(b) Alice sends you $A = 974$. What is the secret shared key?

Solution:

(a) You send $g^b \equiv 2^{871} \equiv 805 \pmod{1373}$.

(b) The secret shared key is $B' = K \equiv A^b \equiv 974^{871} \equiv 397 \pmod{1373}$.

(I recommend using Wolfram Alpha or Mathematica or something similar for this one, to avoid long and tedious hand arithmetic).

5. From the definition of big-O notation, prove that $x^2 + \sqrt{x} = O(x^2)$.

Solution: When $x \geq 1$, we have $\sqrt{x} \leq x^2$ so $x^2 + \sqrt{x} \leq x^2 + x^2 = 2x^2$. Thus we can take $C = 1$ and $c = 2$.

6. Prove (using the definition or the limit property) that:

(a) $k^{300} = O(2^k)$

(b) $(\log_2(k))^{100} = O(k)$.

Solution:

(a) $\lim_{k \rightarrow \infty} \frac{k^{300}}{2^k} = 0$ so $k^{300} = O(2^k)$.

(b) $\lim_{k \rightarrow \infty} \frac{\log_2(k)^{100}}{k} = 0$ so $\log_2(k)^{100} = O(k)$.

7. Use the efficient modular exponentiation algorithm (showing your steps) to compute $3^{51} \pmod{71}$.

Solution: We compute

$$3^1 \equiv 3$$

$$3^2 \equiv 9$$

$$3^4 \equiv 81 \equiv 10$$

$$3^8 \equiv 100 \equiv 29$$

$$3^{16} \equiv 841 \equiv -11$$

$$3^{32} \equiv 121 \equiv 50$$

Then we have

$$3^{51} = 3^{32}3^{16}3^23^1 \equiv 50 \cdot -11 \cdot 9 \cdot 3 \equiv 50 \cdot -28 \cdot 3 \equiv 50 \cdot -13 \equiv 60 \pmod{71}.$$

8. Use Shanks's algorithm (showing your steps) to solve $11^x \equiv 21 \pmod{71}$.

Solution:

We take $n = 9$. Then we have

$$11^1 \equiv 11$$

$$11^2 \equiv 50$$

$$11^3 \equiv 53$$

$$11^4 \equiv 15$$

$$11^5 \equiv 23$$

$$11^6 \equiv 40$$

$$11^7 \equiv 14$$

$$11^8 \equiv 12$$

$$11^9 \equiv 61$$

and so $11^{-9} \equiv 7 \pmod{71}$. Now we compute

$$21 \cdot 7 \equiv 5$$

$$21 \cdot 7^2 \equiv 35$$

$$21 \cdot 7^3 \equiv 32$$

$$21 \cdot 7^4 \equiv 11$$

and we have a match. We have $i = 1$ and $j = 4$ so $x = i + jn = 1 + 4 \cdot 9 = 37$.