

# CS344: Design and Analysis of Computer Algorithms

## Homework 2

Group Members: Stephen Kuo, Derek Mui

1.11) Is  $4^{1536} - 9^{4824}$  divisible by 35?

**Answer:**

$$4^{1536} = (4^3)^{512} = 64^{512} = (35 + 29)^{512}$$

Since 35 is divisible by 35, we can continue with  $29^{512}$

$$29^{512} = (29^2)^{256} = 841^{256} = (840 + 1)^{256}$$

Since 840 is divisible by 35, we are left with  $1^{256} \bmod 35$

$$9^{4824} = (9^2)^{2412} = 81^{2412} = (70 + 11)^{2412}$$

Since 70 is divisible by 35, we can continue with  $11^{2412}$

$$(11^3)^{804} = 1331^{804} = (1330 + 1)^{804}$$

Since 1330 is divisible by 35, we are left with  $1^{804} \bmod 35$

$$(1^{256} \bmod 35) - (1^{804} \bmod 35) = 0 \text{ Thus, yes it is divisible by 35}$$

1.12) What is  $2^{2^{2006}} \bmod 3$

**Answer:**

$$2^{2^{2006}} = 4^{2^{2006}} = 4^{2^{1003}} = 16^{1003} = (15 + 1)^{1003}$$

We know 15 is divisible by 3, so that leaves us with  $1^{1003}$ .

Thus, the answer is 1

1.13) Is the difference of  $5^{30,000}$  and  $6^{123,456}$  a multiple of 31?

**Answer:**

$$5^{30000} = 5^{3^P 10000} = 125^{10000} = (124 + 1)^{10000}$$

Since 124 is divisible by 31, we are left with  $1^{10000} \bmod 31$

$$6^{123456} = 6^{2^6 1728} = 36^{61728} = (31 + 5)^{61728}$$

Since 31 is divisible by 31, we are left with  $5^{61728}$

$$5^{61728} = 5^{3^{20576}} = 125^{20576} = (124 + 1)^{20576}$$

Since 124 is divisible by 31, that leaves us with  $1^{20576}$

$$(1^{10000} \bmod 31) - (1^{20576} \bmod 31) = 0$$

Thus, yes, the difference is a multiple of 31

1.25) calculate  $2^{125} \bmod 127$  using any method you choose

**Answer:**

temp

1.33) Give an efficient algorithm to compute the least common multiple of two  $n$ -bit numbers  $x$  and  $y$ , that is, the smallest number divisible by both  $x$  and  $y$ . What is the running time of your algorithm as a function of  $n$ ?

**Answer:**

temp

1.39) Give a polynomial-time algorithm for computing  $a^{b^c} \bmod p$ , given  $a$ ,  $b$ ,  $c$ , and prime  $p$ .

**Answer:**

temp

Problem)

**Answer:**

temp