

1. Using Mersenne prime for my attempted guess,  $2^{500}$  operations will be taken for the task. So the answer is:

**d.  $2^{500}$**

2. True. Let  $f_1(x) = (2x^2 + 3x + 1)$  and  $f_2(x) = (x^2 - 7x - 4)$  where  $g(x) = O(x^2)$ . Then  $f_1(x) + f_2(x) = [(2x^2 + 3x + 1) + (x^2 - 7x - 4)] = (3x^2 - 4x - 3)$ , which is still  $O(x^2)$ .
3.  $n$  is the exponent = 1048576,  $y = 1$  and  $x \equiv 3 \pmod{7} = 3$

$n = 1048576$  is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \pmod{p}$

$$x^2 \pmod{p} = 3^2 \pmod{7}$$

$$x^2 \pmod{p} = 9 \pmod{7}$$

$$9 \pmod{7} = 2, \text{ reset } x \text{ to } 2$$

Then, cut  $n$  in half and take the integer value:

$$1048576 \div 2 = 524288$$

$n = 524288$  is even

$524288$  is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \pmod{p}$

$$x^2 \pmod{p} = 2^2 \pmod{7}$$

$$x^2 \pmod{p} = 4 \pmod{7}$$

$$4 \pmod{7} = 4, \text{ reset } x \text{ to this value}$$

Then, cut  $n$  in half and take the integer value:

$$524288 \div 2 = 262144$$

$n = 262144$  is even

$262144$  is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \pmod{p}$

$$x^2 \pmod{p} = 4^2 \pmod{7}$$

$$x^2 \pmod{p} = 16 \pmod{7}$$

$$16 \pmod{7} = 2, \text{ reset } x \text{ to this value}$$

Then, cut  $n$  in half and take the integer value:

$$262144 \div 2 = 131072$$

$n = 131072$  is even

131072 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 2^2 \bmod 7$$

$$x^2 \bmod p = 4 \bmod 7$$

$4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:

$$131072 \div 2 = 65536$$

$n = 65536$  is even

65536 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 4^2 \bmod 7$$

$$x^2 \bmod p = 16 \bmod 7$$

$16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value :  $65536 \div 2 = 32768$

$n = 32768$  is even

32768 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 2^2 \bmod 7$$

$$x^2 \bmod p = 4 \bmod 7$$

$4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $32768 \div 2 = 16384$

$n = 16384$  is even

16384 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 4^2 \bmod 7$$

$x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $16384 \div 2 = 8192$

$n = 8192$  is even  
 $8192$  is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 2^2 \bmod 7$   
 $x^2 \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $8192 \div 2 = 4096$

$n = 4096$  is even  
 $4096$  is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 4^2 \bmod 7$   
 $x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $4096 \div 2 = 2048$

$n = 2048$  is even  
 $2048$  is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 2^2 \bmod 7$   
 $x^2 \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $2048 \div 2 = 1024$

$n = 1024$  is even  
 $1024$  is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 4^2 \bmod 7$   
 $x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $1024 \div 2 = 512$

$n = 512$  is even

512 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 2^2 \bmod 7$$

$$x^2 \bmod p = 4 \bmod 7$$

$4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $512 \div 2 = 256$

$n = 256$  is even

256 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 4^2 \bmod 7$$

$$x^2 \bmod p = 16 \bmod 7$$

$16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $256 \div 2 = 128$

$n = 128$  is even

128 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 2^2 \bmod 7$$

$$x^2 \bmod p = 4 \bmod 7$$

$4 \bmod 7 = 4$ , so we reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $128 \div 2 = 64$

$n = 64$  is even

64 is even, keep  $y = 1$  as is

next sub step, determine  $x^2 \bmod p$

$$x^2 \bmod p = 4^2 \bmod 7$$

$$x^2 \bmod p = 16 \bmod 7$$

$16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $64 \div 2 = 32$

$n = 32$  is even  
32 is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 2^2 \bmod 7$   
 $x^2 \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $32 \div 2 = 16$

$n = 16$  is even  
16 is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 4^2 \bmod 7$   
 $x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $16 \div 2 = 8$

$n = 8$  is even  
8 is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 2^2 \bmod 7$   
 $x^2 \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $8 \div 2 = 4$

$n = 4$  is even  
4 is even, keep  $y = 1$  as is  
next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 4^2 \bmod 7$   
 $x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $4 \div 2 = 2$

$n = 2$  is even  
 $2$  is even, keep  $y = 1$  as is  
 next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 2^2 \bmod 7$   
 $x^2 \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $2 \div 2 = 1$

$n = 1$  is odd  
 $1$  is odd, calculate  $(yx) \bmod p$   
 $yx \bmod p = (1)(4) \bmod 7$   
 $yx \bmod p = 4 \bmod 7$   
 $4 \bmod 7 = 4$ , now reset  $y$  to this value  
 next sub step, determine  $x^2 \bmod p$   
 $x^2 \bmod p = 4^2 \bmod 7$   
 $x^2 \bmod p = 16 \bmod 7$   
 $16 \bmod 7 = 2$ , reset  $x$  to this value

Then, cut  $n$  in half and take the integer value:  $1 \div 2 = 0$

$n = 0$ ,  $y = 4$ , so  $3^{1048576} \bmod 7 \equiv 4$  (Dreadful).

4. Prime factorization of  $(2^{16} - 1) = 3 \times 5 \times 17 \times 257$
5. If  $n$  is a natural number, then  $(2^{2n} - 1)$  must be divisible by 3.  
 Definition:  $a$  is divisible by  $b$  if  $(a / b)$  is a whole number. So, divisible by 3 means divisible by  $\{0, 3, 6, 9, 12, 15, \dots, 3(n-1), 3n\}$ .  
 Let  $n$  be an arbitrary natural number, say 6, then  $(2^{2n} - 1) / 3 = (2^{12} - 1) / 3 = 1365$ . Hence, the statement is true.
6. Ran out of time.
7. Ran out of time. Must turn HW in now.