Examples of Modular Exponentiation

Problem 1:

Calculate the value of: $\mathbf{23^{20}}$ ***mod*** **29.**

exponent	$(23^{(exp-1)}mod29)\bullet 23$	$(23^{(exp-1)}mod29\bullet 23)mod29$	Comment
2	23•23 = 529	529 *mod* 29 = 7	
3	7•23 = 161	161 *mod* 29 = 16	
4	16•23 = 368	368 *mod* 29 = 20	
5	20•23 = 460	460 *mod* 29 = 25	
6	25•23 = 575	575 *mod* 29 = 24	
7	24•23 = 552	552 *mod* 29 = 1	
8	1•23 = 23	23 *mod* 29 = 23	
9	23•23 = 529	529 *mod* 29 = 7	Value is identical to $23\bullet 23 = 23^2$.
10	7•23 = 161	16	
11	16•23 = 368	20	
12	20•23 = 460	25	
13	25•23 = 575	24	
14	24•23 = 552	1	
15	1•23 = 23	23	
16	23•23 = 529	7	
17	7•23 = 161	16	
18	16•23 = 368	20	
19	20•23 = 460	25	
20		***ANSWER*:** **24**	

Please note that 23^{20} = 171,615,583,134,458,634,923,895,201 (a 27-digit decimal integer), and that (23^{20}) *mod* 29 = **24**.

Note also that we could have obtained the answer much faster:

Once we had determined that 23^2 *mod* 29 = 7, we could have squared that result to obtain $23^4 = (23^2\bullet 23^2) = 7\bullet 7$ *mod* 29 = 49 *mod* 29 = 20, **bypassing** the calculation of 23^3.

Next, we could have jumped ahead from 23^4 to 23^8 by squaring 23^4:

$23^8 = (23^4\bullet 23^4) = 20\bullet 20$ *mod* 29 = 400 *mod* 29 = 23, **bypassing** the calculation of 23^5, 23^6, and 23^7.

Next, we could have jumped ahead from 23^8 to 23^{16} by squaring 23^8:

$23^{16} = (23^8\bullet 23^8) = 23\bullet 23$ *mod* 29 = 529 *mod* 29 = 7, **bypassing** the determination of the values of 23^9, 23^{10}, 23^{11}, 23^{12}, 23^{13}, 23^{14}, and 23^{15}.

Finally, we could have made use of the values 23^4 and 23^{16}, multiplying one of these values by the other to obtain 2^{20}.

$23^{20} = (23^4\bullet 23^{16}) = 20\bullet 7$ *mod* 29 = 140 *mod* 29 = **24**, **bypassing** the determination of the values of 23^{17}, 23^{18}, and 23^{19}.

Problem 2:

Calculate the value of: $\mathbf{23^{391}}$ ***mod*** **55.**

exponent	$(23^{(exp/2)}\bullet 23^{(exp/2)})$	$(23^{(exp-1)}\bullet 23^{(exp/2)})$ *mod* 55	Comment
1	[special] $23^1 = 23$	23 *mod* 55 = 23	
2	23•23 = 529	529 *mod* 55 = 34	
4	34•34 = 1156	1156 *mod* 55 = 1	Continuing to square *ad infinitum* will not change the result.
8	1•1 = 1	1 *mod* 55 = 1	
16	1•1 = 1	1 *mod* 55 = 1	
32	1•1 = 1	1 *mod* 55 = 1	
64	1•1 = 1	1 *mod* 55 = 1	
128	1•1 = 1	1 *mod* 55 = 1	
256	1•1 = 1	1 *mod* 55 = 1	
512	1•1 = 1	1 *mod* 55 = 1	
			Note that 391 = 256 + 128 + 4 + 2 + 1
391	$23^{256}\bullet 23^{128}\bullet 23^{4}\bullet 23^{2}\bullet 23^{1}$ = 1•1•1•34•23 = 782	782 *mod* 55 = **12**	
Note that 23^{391} = 2.7263642784296496195425150858433e+532 (390 multiplications resulting in the generation of a 533-digit decimal integer), and that (23^{391}) *mod* 55 = **12**			

Problem 3:

Calculate the value of: $\mathbf{31^{397}}$ ***mod*** **55.**

exponent	$(31^{(exp/2)}\bullet 31^{(exp/2)})$	$(31^{(exp/2)}\bullet 31^{(exp/2)})$ *mod* 55 = 31^{exp} *mod* 55	Comment
1	[special] $31^1 = 31$	31 *mod* 55	
2	31•31 = 961	961 *mod* 55 = 26	
4	26•26 = 676	676 *mod* 55 = 16	
8	16•16 = 256	256 *mod* 55 = 36	
16	36•36 = 1,296	1,296 *mod* 55 = 31	
32	31•31 = 961	961 *mod* 55 = 26	
64	26•26 = 676	16	Note that (31^{64} *mod* 55) ≡ (31^4 *mod* 55)
128	16•16 = 256	36	
256	36•36 = 1,296	31	
512	31•31 = 961	26	
			Note that 397 = 256 + 128 + 8 + 4 + 1
391	31•36•36•16•31 = (1116 *mod* 55)•36•16•31 = 16•36•16•31 = (576 *mod* 55) •16•31 = 26•16•31 = (416 *mod* 55)•31 = 31•31 = 961 *mod* 55 = **26.** Note that 31^{397} = 1.1765014105569728144308343503655e+592 (396 multiplications resulting in a 593-digit decimal integer), and that (31^{395}) *mod* 55 = **26.**		