Public Page 1

1. Fast computation with modular arithmetic.

   Find a number $a < 11$ whose powers cover every remainder mod 11. Make a table of these powers, and use this table to calculate the following:

Log rules! I for one welcome our new logarithmic overlords.

$$\log(a \cdot b) = \log(a) + \log(b) \qquad \log(\tfrac{a}{b}) = \log(a) - \log(b)$$
$$\log(a^b) = b \cdot \log(a) \qquad a = b^{\log_b(a)}$$

If we try using 3 as a base we'll find that we don't get all possible remainders 1 through 10:

k	1	2	3	4	5	6	7	8	9	10
$3^k \pmod{11}$	3	9	5	4	1	3	9	5	4	1

However, other numbers will work. Here's the same table with 2 as the base:

k	1	2	3	4	5	6	7	8	9	10
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

9 * 4 = 2^log2(9*4) (mod 11)
= 2^(log2(9) + log2(4))
= 2^(6 + 2)
= 2^8
= 3 (mod 11)

3^9 = 2^(log2(3^9)) (mod 11)
= 2^(9* log2(3))
= 2^(9* 8)
= 2^72
= 2^70 * 2^2
= (2^10)^7 * 2^2
= 1^7 * 2^2
= 2^2
= 4