Drill and Skill number theory problems

None of the following problems require a calculator and although it might be easier to do one or two with one, try it without first.

- (a) Compute $\gcd(741, 221)$, the greatest common divisor of 741 and 221.

  (b) Find r and s such that $\gcd(741, 221) = 741r + 221s$.

- Factor 69689 given that $277^2 \equiv 17529^2 \equiv 7040 \pmod{69689}$.

- Calculate by operations of multiplication and squaring (hint: you might be able to reduce this before you start)

  $$54^{40} \pmod{79}$$

- (a) Compute $(\frac{15}{29})$, the Legendre symbol of 15 and 29.

  (b) Is there a value x such that $x^2 = 15 \bmod 29$? Explain.

- (a) Compute $J(30, 4891)$, the Jacobi symbol of 30 and 4891.

  (b) Compute $30^{2445} \bmod 4891$. (Hint: $30^{24} = 1 \bmod 4891$)

  (c) What do the answers to parts (a) and (b) tell you about the primality of 4891?

- Alice and Bob decided to communicate using a key arrived at from the Diffie-Hellman key exchange system. They first agree on a modulus of 53 and a primitive root of 22. Alice sends to Bob her public key of 19 and Bob sends to Alice his public key of 37. You intercept these exchanges. Use the table of powers of 2 below to help recover their secret keys S_A and S_B and their common key $22^{S_A S_B} (mod\ 53)$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13
$2^k(mod\ 53)$	2	4	8	16	32	11	22	44	35	17	34	15	30
k	14	15	16	17	18	19	20	21	22	23	24	25	26
$2^k(mod\ 53)$	7	14	28	3	6	12	24	48	43	33	13	26	52
k	27	28	29	30	31	32	33	34	35	36	37	38	39
$2^k(mod\ 53)$	51	49	45	37	21	42	31	9	18	36	19	38	23
k	40	41	42	43	44	45	46	47	48	49	50	51	52
$2^k(mod\ 53)$	46	39	25	50	47	41	29	5	10	20	40	27	1

- Assume that $n = 71107 = 337 \cdot 211$ and that $e = 11$. Find the value of d such that

  $$d \cdot e \equiv 1 \pmod{\phi(71107)}.$$

- Use the Euler-ϕ function from the last problem to calculate

  $$3^{70565} \pmod{71107}$$