

## MTH 309

### Additional Problems for Section 4.4

1. For each of the following, determine whether  $a$  has a multiplicative inverse mod  $m$ . If so, find the multiplicative inverse of  $a$  in  $\mathbb{Z}_m$ . Do this by using the Euclidian algorithm to obtain gcd's and Bézout coefficients.
  - (a)  $a = 2, m = 17$
  - (b)  $a = 34, m = 89$
  - (c)  $a = 200, m = 1001$
2. Encrypt the message ATTACK using the RSA system with public key  $(n, e) = (2537, 13)$ , translating each letter into integers and grouping together pairs of integers. To compute the modular exponential  $[a^e]_n$  you can type  $(a) \wedge e \text{ mod } n$  into google.
3. Consider the RSA system with public key  $(n, e)$ . Find the decryption exponent  $d$  for
  - (a)  $(n, e) = (77, 17)$
  - (b)  $(n, e) = (43 \cdot 59, 13)$ .