

### Euclid's Algorithm and the RSA Encryption Scheme

1. For each pair of integers  $(a, b)$  below, find  $d = \gcd(a, b)$  **and** find a pair of numbers  $j$  and  $k$  such that  $d = j \cdot a + k \cdot b$ . (Use the Extended Euclidean algorithm.)
  - (a) 90 and 56
  - (b) 91 and 89
  - (c) 711 and 75
  - (d) 815 and 75
  - (e) 112 and 196
  - (f) 366 and 150
2. For each triple of integers  $p, q, e$  given below, find the (smallest positive) value of  $d$  that will work for the private key of the RSA algorithm (where, as usual,  $n = p \cdot q$  and  $\phi(n) = (p - 1)(q - 1)$ , and  $ed \equiv 1 \pmod{\phi(n)}$ ).  
Then suppose that the message (integer)  $M = 25$  is to be encoded using the public key  $n, e$  pair. Find the ciphertext that corresponds to that message  $M$ .
  - (a)  $p = 7, q = 13, e = 5$
  - (b)  $p = 5, q = 11, e = 3$
  - (c)  $p = 7, q = 17, e = 7$
3. Finally, suppose that  $p = 5, q = 17$ , and  $e = 13$ . First find the private key  $d$  for the RSA method with these parameters. Then decrypt the ciphertext messages, C, below to find the original (plaintext) messages.
  - (a) 12
  - (b) 9
  - (c) 27
  - (d) 84