

10. Fermat and Euler's Theorems, RSA

1. Find prime factorizations for each of these numbers:

(a) 47.

(b) 99.

(c) 8.

(d) 72.

2. Find $\varphi(n)$ for each of these numbers:

(a) 47.

(b) 99.

(c) 8.

(d) 72.

3. Prove that if p is prime and n is a natural number, then

$$\varphi(p^n) = p^n - p^{n-1}.$$

4. Verify that $7^{120} = 1$ in \mathbb{Z}_{143} .
5. Alice wants to send the number 71 to Bob via an RSA code where $n = 143$ and $e = 17$. What is the encoded number?
Find d and check that you have encoded correctly.
6. Bob receives the number 53 from Alice which has been encrypted with an RSA code where $n = 143$ and $d = 59$. What is the unencrypted message.
7. An RSA code has $n = 2491$ and $e = 55$. Find p , q and d (ie. break the code).
8. A book has ISBN 0-534-35638-9. Is this a valid ISBN?