

Mathematics of Coding and Cryptography
Worksheet 5

1. Let φ be Euler's φ -function.

(a) Prove that

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right);$$

(b) Prove that, for $m > 0$, $\varphi(n^m) = n^{m-1}\phi(n)$.

2. Find the last 4 digits of $7^{7^{7^7}}$.

3. Suppose $n = pq$ where p and q are distinct primes congruent to 3 (mod 4). Suppose further, that a and b are solutions to $x^2 \equiv y \pmod{n}$ such that $a \not\equiv \pm b$.

(a) Show that $-a$ and $-b$ are also solutions to $x^2 \equiv y \pmod{n}$.

(b) Show that either

$$\begin{array}{l} a \equiv b \pmod{p} \\ a \equiv -b \pmod{q} \end{array}, \quad \text{or} \quad \begin{array}{l} a \equiv b \pmod{q} \\ a \equiv -b \pmod{p} \end{array}.$$

(c) Show that, in the first case $\gcd(a - b, n) = p$. What happens in the second case?

4. Consider the simplified DES algorithm given in class (using the same expander function E and S -boxes S_1 and S_2) with key $K = 010011001$. We will encode letters into 5-bits by setting $A = 00001$, $B = 00010$, $C = 00011$, etc. (That is, the n th letter is represented by the 5-bit representation for n), and we will represent spaces by 00000.

(a) Translate the plaintext "PURPLE MONKEY DISHWASHER" into 120-bits using this alphabet encoding.

(b) What is the ciphertext (as 120-bits) after encrypting with DES using one iteration? two iterations?

(c) Decipher (into English) the following message using two iterations of the DES algorithm:

010010101000101000111011101010100011001100111101010111000111