

HW # 8

Solution

1. (10 points) Verify that Euler's theorem holds in Z_m , $m = 7, 10$ for all elements a for which $\gcd(a, m) = 1$. Also verify that the theorem does not hold for elements a for which $\gcd(a, m) \neq 1$.

$$\phi(7) = 6, \quad \phi(10) = 4$$

| Z_7 | | |
|-------|--------------|---------------|
| a | $\gcd(a, 7)$ | $a^6 \bmod 7$ |
| 0 | - | 0 |
| 1 | 1 | 1 |
| 2 | 1 | 1 |
| 3 | 1 | 1 |
| 4 | 1 | 1 |
| 5 | 1 | 1 |
| 6 | 1 | 1 |

| Z_{10} | | |
|----------|---------------|----------------|
| a | $\gcd(a, 10)$ | $a^4 \bmod 10$ |
| 0 | - | 0 |
| 1 | 1 | 1 |
| 2 | 2 | 6 |
| 3 | 1 | 1 |
| 4 | 2 | 6 |
| 5 | 5 | 5 |
| 6 | 2 | 6 |
| 7 | 1 | 1 |
| 8 | 2 | 6 |
| 9 | 1 | 1 |

2. (5 points) For the affine cipher the multiplicative inverse of an element modulo 26 can be found as

$$a^{-1} \equiv a^{11} \bmod 26$$

Derive this relationship by using Euler's theorem.

$$\begin{aligned} a^{\phi(m)} &= 1 \bmod m; & m &= 26 \\ a^{\phi(26)} &= 1 \bmod 26; & \phi(26) &= (13-1)(2-1) = 12 \\ a^{12} &= 1 \bmod 26 \\ a^{11} \cdot a^1 &= 1 \bmod 26 \\ a^{-1} &= a^{11} \bmod 26 \end{aligned}$$

3. (20 points) Write a C program which realizes the extended form of Euclid's algorithm. The following features must be supported:

- (a) The program should ask the user to enter r_0 and r_1 and write the return $s, t, \gcd(r_0, r_1)$ on the screen.

(b) In the beginning of the program, check whether $r_0 > r_1$. Otherwise, swap the two values.

Provide a print out of the C program as well as a sample run with one input pair r_0, r_1 of your choice.

No solution given.

4. (20 points) Modify the program from above, to compute $\phi(m)$ according to its definition, i.e., without using the prime factorization of m , for

Which of the numbers m are primes?

(a) $m = 13257$

```
> phi(13257);
```

8820

not prime

(b) $m = 13681$

```
> phi(13681);
```

13680

prime

(c) $m = 1000019$

```
> phi(1000019);
```

978696

not prime

(d) $m = 1000003$

```
> phi(1000003);
```

1000002

prime