Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Exercise: **Introduction to Number Theory**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-19

1. Compute the result of $5^9 \, mod \, 7$ by hand. Don't use a calculator!

One Possible Solution

$(5^9) \, mod \, 7 = (5^2 \times 5^2 \times 5^2 \times 5^2 \times 5) \, mod \, 7$

$= (5^2 \times 5^2 \times 5^2 \times 5^2 \times 5) \, mod \, 7 = (((5^2) \, mod \, 7)^4 \times (5 \, mod \, 7)) \, mod \, 7$

$= ((25 \, mod \, 7)^4 \times (5)) \, mod \, 7$

$= (4^4 \times 5) \, mod \, 7$

$= (4^2 \times 4^2 \times 5) \, mod \, 7$

$= (2 \times 2 \times 5) \, mod \, 7$

$= (20) \, mod \, 7$

$= 6$

2. Which numbers are relative prime to 21?

Solution

$|\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}| = 12$

(Recall: $gcd(6, 21)$ is 3 and therefore 6 and 21 are not relatively prime!)

3. Compute the $gcd(1037, 768)$ using the Euclidean algorithm.

Solution

step	a	b	q	r
1	1037	768	1	269
2	768	269	2	230

3	269	230	1	39
4	230	39	5	35
5	39	35	1	4
6	35	4	8	3
7	4	3	1	1
8	3	1	3	0

4. Determine the result of Euler's Totient function ϕ for the value 37. Don't look it up; just think about it.

Solution

36 because 37 is a prime number. Hence all numbers below are necessarily relatively prime to 37!

5. Convince yourself that Fermat's (little) theorem holds. E.g., for the numbers: $a = 9, p = 7$.

Solution

$9^6 \, mod \, 7 = 531441 \, mod \, 7 = 1$

6. Convince yourself that Euler's theorem holds. E.g., for the following values: a=7 and n=9.

Solution

$\phi(9) = 6 = |\{1, 2, 4, 5, 7, 8\}|$

$7^6 \, mod \, 9 = 1$

7. Execute the Miller-Rabin Algorithm for n = 37.

Solution

```
primality test for 37:

k      s      a      x      y
round 0:
0      0     27     36      1
0      1     27      1      1
round 1:
```

```
1       0      19       6      36
1       1      19      36       1
round 2:
2       0      18      31      36
2       1      18      36       1
__________________________________
probably prime
```

Miller-Rabin Algorithm: