Lab Report (Lab 5 - jpy19)

Question One

Questions

a. $x \equiv 5 \mod 7 \, and \, x \equiv 7 \mod 10$
b. $x \equiv 3 \mod 7 \, and \, x \equiv 7 \mod 14$
c. $x \equiv 2 \mod 6 \, and \, x \equiv 3 \mod 11$

Solutions

a. $x \equiv 5 \mod 7 \, and \, x \equiv 7 \mod 10$

b_i	N_i	x_i	$b_i N_i x_i$
5	10	5	250
7	7	3	147

$pq = 70$

$x = 397 \mod 70$

$x = 47 \mod 70$

1b)

b. $x \equiv 3 \mod 7 \, and \, x \equiv 7 \mod 14$

> NOTE: gcd(7, 14) = 7 not co-prime

1c)

c. $x \equiv 2 \mod 6 \, and \, x \equiv 3 \mod 11$

b_i	N_i	x_i	$b_i N_i x_i$
2	11	5	$2 \cdot 11 \cdot 5$
3	6	2	$3 \cdot 6 \cdot 2$

$pq = 66$

$x = 146 \mod 66$

$x = 14 \mod 66$

Question Two

Find $\phi(20)\ \phi(21)\ \phi(22)\ \phi(23)\ \phi(24)\ \phi(25)$

- $\phi(20) = (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 8$
- $\phi(21) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$
- $\phi(22) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$
- $\phi(23) = 23 - 1 = 22$
- $\phi(24) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$
- $\phi(25) = 25 \cdot \frac{4}{5} = 20$

Question Three

Questions

Find the discrete logarithm of the number 3 with regard to base 2 for:

a. modulus p = 5
b. modulus p = 11
c. modulus p = 29

Solutions

- $2^3 \equiv 3 \mod 5$
- $2^8 \equiv 3 \mod 11$
- $2^5 \equiv 3 \mod 29$

Question Four

Use the Fermat test to check whether the following numbers are prime or not:

- 979
- 983

```python
def fermats_prime(a, primes):
    for prime in primes:
        for ab in a:
            print("Number:", prime, "Value: ", ab**(prime-1) % prime)
```

- 979 is not prime
- 983 is prime

Question Five

We first recall the Miller-Rabin algorithm. Let n and u be odd, and v s.t. $n - 1 = 2^v u$:

a. using the above algorithm, check $n = 17$ if n is prime
b. using the above algorithm, check $n = 15$ if n is prime

```
def miller(n,a,u,v):
    b = a**u % n
    if b == 1:
        return True
    else:
        for _ in range(0, v-1):
            if b == -1:
                return True
            b = b**2 % n
        return False
```

With values $n = 17, a = 11, u = 1, v = 3$

Miller-Rabin algorithm returns:

- $n = 17$ is prime
- $n = 15$ is composite