Computational Number Theory - Homework 4

Philip Warton

February 26, 2021

Problem 24

Problem 25

a)

$$x^2 \equiv 17 \mod 67$$

$$\begin{aligned}\left(\frac{17}{67}\right) &= \left(\frac{67}{17}\right) && (1)\\ &= \left(\frac{16}{17}\right) && (2)\\ &= \left(\frac{2}{17}\right)^4 && (3)\\ &= 1 && (4)\end{aligned}$$

b)

$$x^2 \equiv 3 \mod 67$$

$$\begin{aligned}\left(\frac{3}{67}\right) &= (-1)\left(\frac{67}{3}\right) && (5)\\ &= (-1)\left(\frac{1}{3}\right) && (6)\\ &= -1 && (7)\end{aligned}$$

c)

$$2x^2 + 5x + 1 \equiv 0$$

d)

$$x^2 \equiv 65 \mod 101$$

$$\begin{aligned}\left(\frac{65}{101}\right) &= (-1)\left(\frac{101}{65}\right) && (8)\\ &= (-1)\left(\frac{31}{65}\right) && (9)\\ &= (-1)\left(\frac{65}{31}\right) && (10)\\ &= (-1)\left(\frac{3}{31}\right) && (11)\\ &= \left(\frac{31}{3}\right) && (12)\\ &= \left(\frac{1}{3}\right) = 1 && (13)\end{aligned}$$

e)

$$x^2 \equiv 5 \mod 2 \cdots 1$$

$$\begin{aligned}
\left(\frac{5}{2\cdots 1}\right) &= (-1)\left(\frac{2\cdots 1}{5}\right) && (14)\\
&= (-1)\left(\frac{1}{5}\right) && (15)\\
&= -1 && (16)
\end{aligned}$$

Problem 26

Code:

```
def solve_quadratic(b, n):
    for a in range(1, n):
        if a^2 % n == b:
            return a
        else:
            a = a + 1
    return 0

print(solve_quadratic(17, 67))
print(solve_quadratic(65, 101))
```

Output:

```
33
41
```

The answer to $\boxed{\text{a.}}$ is 33, and the answer to $\boxed{\text{d.}}$ is 41.

Problem 27

Code:

```
def discrete_log(n, a, b):
    k = 1
    while(a^k % n != b):
        k = k + 1
    return k

def diffie_hellman(p, g, g_a, g_b):
    a = discrete_log(p, g, g_a)
    b = discrete_log(p, g, g_b)
    s = g^(a*b) % p
    return s

print(diffie_hellman(49253, 2, 558, 32288))
```

Output:

```
43739
```

Problem 28

Code:

```
def fermat_factorization(n):

    #--STEP 1--
    t_0 = ceil(sqrt(n))

    #--STEP 2--
    l = 0
    while (not is_square((t_0 + l)^2 - n)):
        l = l + 1
    t = t_0 + l
    s = sqrt(t^2 - n)

    #--STEP 3--
    return (t - s, t + s)

print(fermat_factorization(41156989185107))
```

Output:

```
(6409511, 6421237)
```

Problem 29

$$x^7 \equiv 17792272918826 \mod 41156989185107$$
$$6409511 \cdot 6421237 = 41156989185107$$

$$x^7 \equiv 17792272918826 \mod 6421237 \tag{17}$$
$$x^7 \equiv 17792272918826 \mod 6409511 \tag{18}$$

We get the solution 9546903516023, but this cannot be right since there is no 95th or 54th character.