Computational Number Theory - Homework 5

Philip Warton

March 12, 2021

Problem 31

Let p be an odd prime.

a)

Prove that -1 is a quadractic residue mod p if and only if $p \equiv 1 \mod 4$

Proof. We know that the legendre symbol of -1 is $\left(\frac{-1}{p}\right)$. By Euler's criterion, we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \mod p$$

Suppose $p = 4k+3$, then

$$(-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1$$

Thus -1 cannot be a quadractic residue mod p. Then suppose $p = 4k+1$,

$$(-1)^{(4k+1-1)/2} = (-1)^{4k} = 1$$

So it must be the case that -1 is a quadratic residue mod p. These are the only options for p, as p is an odd prime. □

b)

Assuming $p \geqslant 5$, prove that -3 is a quadractic residue mod p if and only if $p \equiv 1 \mod 3$.

Proof. We begin by writing the legendre symbol for -3,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right)$$

Suppose that $p \equiv 1$ mod 4, then by quadratic reciprocity we have

$$(-1)^{(p-1)/2}\left(\frac{3}{p}\right) = (-1)^{(4k+1-1)/2}\left(\frac{3}{p}\right) = (-1)^{2k}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

Then suppose we have $p \equiv 3$ mod 4, it follows that we get

$$(-1)^{(4k+3-1)/2}\left(\frac{3}{p}\right) = (-1)^{2k+1}(-1)\left(\frac{p}{3}\right) = (-1)(-1)\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

In either scenario, we have the end result of $\left(\frac{p}{3}\right)$.

Then we know that $\left(\frac{p}{3}\right) = \left(\frac{p \bmod 3}{3}\right)$. So if $p \equiv 1$ mod 3, clearly the legendre symbol of -3 is $\left(\frac{1}{3}\right) = 1$ and we say that -3 is a quadratic residue mod p. Then if $p \not\equiv 1$ mod 3, we must have $p \equiv 2$ mod 3, and so the legendre symbol of -3 is $\left(\frac{2}{3}\right) = -1$ so -3 is a quadractic non-residue mod p. □

Problem 32

Code:

```
def QuadraticResidues(p):
    QR = []
    for a in range(0, p):
        if legendre_symbol(a, p) == 1:
            QR.append(a)
    return(QR)

print(QuadraticResidues(17))
print(QuadraticResidues(53))
```

Output:

```
[1, 2, 4, 8, 9, 13, 15, 16]
[1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46,
 47, 49, 52]
```

Problem 33

Code:

```
def DiscreteLog(a, n):
    for k in range(0, n):
        if 2^k % n == a % n:
            return k
    return 0

print(DiscreteLog(452, 1019))
```

Output:

```
632
```

Problem 34

Euclid's GCD Algorithm:

```
def GCD(a, b):
    if a > b:
        temp = b
        b = a
        a = temp
    r = b % a
    if r == 0:
        return a
    else:
        return GCD(a, r)

# Tests
print(GCD(87444, 238))
print(GCD(28464, 812))
```

Output:

```
14
4
```