Winter 2021 MTH 440/540 Homework 5
Wyatt Whiting

Instructions. Due via Gradescope on Friday March 12. Solutions must be typed.

31. Let p be an odd prime.

(a) Prove that -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 4$.

Assume -1 is a quadratic residue mod p. Then there exists some minimum positive integer $a < p$ such that $a^2 \equiv -1 \pmod p \implies a^4 \equiv 1 \pmod p$, so then a has order 4 mod p. Since a is not divisible by p by construction, then by Fermat's little theorem, we also have $a^{p-1} \equiv 1 \pmod p$, and therefore $1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}$. We can then see that since $1 \equiv (-1)^{(p-1)/2}$, then $(p-1)/2$ must be even, implying $(p-1)$ is a multiple of 4, and therefore $p \equiv 1 \pmod 4$

Now assume $p \equiv 1 \pmod 4$. Let's choose some $a < p$ such that a is a generator of p, so therefore a has order $p-1$. By Fermat's little theorem, we have $a^{p-1} \equiv 1 \pmod p \implies (a^{(p-1)/2})^2 \equiv 1 \pmod p$. We then know that $a^{(p-1)/2}$ is either -1 or 1. However, we chose a to have order $p-1$, so it must be the case that $a^{(p-1)/2} \equiv -1$. We now assert that -1 is a square mod p if and only if it is an even power of our generator a. We also know that all odd primes are either 1 (mod 4) or 3 (mod 4). For $\frac{p-1}{2}$ to be even, it can only be the case that $p \equiv 1 \pmod 4$.

We have shown both directions of implication, so we may conclude that -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod p$. ☠

(b) Assuming $p \geq 5$, prove that -3 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 3$.

Assume -3 is a quadratic residue mod p. Then,

$$\left(\frac{-3}{p}\right) = 1 = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \implies \left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right).$$

We now consider two cases: when $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

Case $p \equiv 1 \pmod 4$: by part (a) we know $\left(\frac{-1}{p}\right) = 1$ in this case, which gives us

$$\left(\frac{-1}{p}\right) = 1 = \left(\frac{3}{p}\right).$$

We can now apply quadratic reciprocity:

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

so we want $\left(\frac{p}{3}\right) = 1$. We can quickly enumerate all quadratic residues mod 3 to find that $0^2 \equiv 0 \pmod p, 1^2 \equiv 1 \pmod p$, and $2^2 \equiv 4 \equiv 1 \pmod p$, so in order for $\left(\frac{p}{3}\right) = 1$, it must be the case that $p \equiv 1 \pmod 3$.

Case $p \equiv 3 \pmod 4$: by part (a), we know $\left(\frac{-1}{p}\right) = -1$. So then

$$\left(\frac{-1}{p}\right) = -1 = \left(\frac{3}{p}\right).$$

Now applying quadratic reciprocity:

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

With the same reasoning as the first case, we must have $p \equiv 1 \pmod 3$ for this condition to hold.

In both cases, we have shown that $\left(\frac{-3}{p}\right) = 1 \implies p \equiv 1 \pmod 3$.

Now assume $p \equiv 1 \pmod 3$. To demonstrate that -3 is a quadratic residue mod p, we will show

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1.$$

As with the first part of this proof, we split this into two cases:

Case $p \equiv 1 \pmod 4$: we then have

$$\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot \left(\frac{3}{p}\right) \implies \left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right).$$

Now applying quadratic reciprocity,

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

We know $p \equiv 1 \pmod 3$ by assumption and have shown in the previous section that 1 is a quadratic residue mod p, giving us

$$\left(\frac{p}{3}\right) = 1 = \left(\frac{3}{p}\right) \implies \left(\frac{-3}{p}\right) = 1,$$

so -3 is a quadratic residue mod p.

Case $p \equiv 3 \pmod 4$: in this case, we have

$$\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = -1 \cdot \left(\frac{3}{p}\right) \implies \left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right).$$

Applying quadratic reciprocity,

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

We again know by the assumption $p \equiv 1 \pmod 3$ that $\left(\frac{p}{3}\right) = 1$, and it then follows that

$$\left(\frac{3}{p}\right) = -(1) \implies \left(\frac{-3}{p}\right) = -(-1) = 1,$$

and therefore -3 is a quadratic residue mod p.

With both these cases, we have now proven that if $p \equiv 1 \pmod 3$, then -3 is a quadratic residue mod p. Together with the previous proven implication, we have proven that -3 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 3$. ☠

32. Write a program in Sage that inputs an odd prime p, and outputs a list

$$v = (v[0], v[1], \ldots, v[n-1])$$

of length $n = (p-1)/2$ whose entries are all of the quadratic residues a modulo p with $1 \leq a < p$, in increasing order. So for example, for an input of $p = 7$, your program should output the list $v = (1, 2, 4)$. You can use Sage's built in `legendre_symbol( , )` command. Use your program to find the quadratic residues modulo 17 and also modulo 53.

```
def ResiduesModP(p):
    v = []
    for n in range(1, p):
        v.append(mod(n,p)^2)
    return list(set(v))

print(ResiduesModP(17))
print(ResiduesModP(53))
> [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]
```

The quadratic residues of 17 and 53 are given in the above lists, respectively.

33. Write your own Sage function called `DiscreteLog( , )`, which inputs an integer a and a positive integer n, and returns the smallest positive integer k such that $2^k \equiv a \pmod n$, if such k exists. If no such k exists, return 0. Use your function to find k such that $2^k \equiv 452 \pmod{1019}$.

```
def DiscreteLog(a, n):
    k = 1
    # loop until one of these conditions is met
    while 1:
        # if we have 2^n == a mod n, then k is the discrete log of a mod n
        if mod(2,n)^k == mod(a, n): return k
        # if it loops back, no log exists
        if mod(2,n)^k == mod(a, n): return 0
        k += 1
DiscreteLog(452, 1019)
> 632
```

We then have $2^{632} \equiv 452 \pmod{1019}$.

34. Choose **one** of the following algorithms to implement in Sage. (I encourage you to do them all! But choose only one to turn in for credit.) Write a general program and/or function and test it with at least two different choices of input data.

(a) Euclid's algorithm to find the gcd. Input: integers $a, b \in \mathbb{Z}$. Output: $d = \gcd(a, b)$.

I chose Euclid's GCD algorithm. This is made very simple with a recursive function:

```
def euclid_gcd(a, b):
    if b == 0: return a
    return euclid_gcd(b, mod(a, b))

for a in range(1,11):
    for b in range(1,11):
        print(euclid_gcd(a,b),end="\t")
    print("")
```

And the output:

```
1 1 1 1 1 1 1 1 1 1
1 2 1 2 1 2 1 2 1 2
1 1 3 1 1 3 1 1 3 1
1 2 1 4 1 2 1 4 1 2
1 1 1 1 5 1 1 1 1 5
1 2 3 2 1 6 1 2 3 2
1 1 1 1 1 1 7 1 1 1
1 2 1 4 1 2 1 8 1 2
1 1 3 1 1 3 1 1 9 1
1 2 1 2 5 2 1 2 1 10
```